

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner

v.

CARDWARE INC.,
Patent Owner

Inter Partes Review Case No. IPR2025-01151
U.S. Patent No. 11,328,286

**PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 11,328,286**

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	THE '286 PATENT	1
A.	DESCRIPTION OF THE '286 PATENT	1
B.	FIELD OF ENDEAVOR AND PROBLEM SOLVED BY THE INVENTORS	2
C.	PRIORITY AND PROSECUTION HISTORY	2
D.	LEVEL OF SKILL OF A POSITA	3
III.	REQUIREMENTS UNDER 37 C.F.R. § 42.104	3
A.	STANDING UNDER 37 C.F.R. § 42.104(A)	3
B.	IDENTIFICATION OF CHALLENGE UNDER 37 C.F.R. § 42.104(B)	4
C.	CLAIM CONSTRUCTION UNDER 37 C.F.R § 42.104(B)(3).....	5
	1. <i>Claim limitations directed to printed matter are not entitled to patentable weight</i>	6
IV.	SHOWING OF ANALOGOUS PRIOR ART	7
A.	COLLINGE	7
	1. <i>Collinge Incorporated all Provisionals for All Purposes</i>	9
	2. <i>Obvious to Combine Provisional Features</i>	10
B.	BONA	12
C.	SMITH	13
D.	LIN.....	14
E.	PATTERSON.....	15
F.	KRANZLEY	16
G.	ENG.....	16
H.	CHIN	17
I.	FISHER	18
J.	HAMMAD	18
K.	ANALOGOUS ART.....	18
V.	GROUND 1: <i>COLLINGE</i> IN VIEW OF <i>BONA</i>	19

A.	CLAIM 15	19
	(a) Bona’s Teachings	21
	(b) Collinge’s Teachings.....	23
	(c) Motivation to Combine	23
B.	CLAIM 17	42
C.	CLAIM 18	44
VI.	GROUND 2: <i>COLLINGE</i> IN VIEW OF <i>BONA</i>, AND <i>SMITH</i>.....	46
A.	CLAIM 1	46
	1. <i>Claim 1(Pre):</i>	46
	2. <i>Claim 1(a):</i>	46
	3. <i>Claim 1(b):</i>	46
	4. <i>Claim 1(b)(1):</i>	47
	5. <i>Claim 1(b)(2):</i>	47
	6. <i>Claim 1(b)(3):</i>	47
	7. <i>Claim 1(c):</i>	47
	8. <i>Claim 1(d):</i>	49
	(a) Collinge’s Teachings.....	50
	(b) Smith’s Teachings	50
	(c) Motivation to Combine	53
	10. <i>Claim 1(d)(2):</i>	58
	11. <i>Claim 1(e):</i>	60
	(a) Bona’s Teachings	60
	(b) Collinge’s Teachings.....	61
	(c) Motivation to Combine	62
	13. <i>Claim 1(g):</i>	63
	14. <i>Claim 1(h):</i>	63
	15. <i>Claim 1(i):</i>	63
	16. <i>Claim 1(j):</i>	63
B.	CLAIM 5	63

C.	CLAIM 8:	65
D.	CLAIM 11	66
	(a) Collinge’s Teachings	66
E.	CLAIM 14	68
	(a) Bona’s Teachings	69
	(b) Collinge’s Teachings	69
	(c) Motivation to Combine	69
F.	CLAIM 20	70
	(a) Motivation to Combine	73
G.	CLAIM 21	73
H.	CLAIM 22	73
I.	CLAIM 23	73
J.	CLAIM 24	74
K.	CLAIM 25	74
L.	CLAIM 26	74
M.	CLAIM 27	74
VII.	GROUND 3: <i>COLLINGS</i> IN VIEW OF <i>BONA, SMITH, AND PATTERSON</i>	74
A.	CLAIM 2	74
	(a) Bona’s Teachings	75
	(b) Patterson’s Teachings	75
	(c) Motivation to Combine	77
B.	CLAIM 3	78
C.	CLAIM 4	78
VIII.	GROUND 4: <i>COLLINGS</i> IN VIEW OF <i>BONA, SMITH AND LIN</i>	79
A.	CLAIM 9	79
	(a) Lin’s Teachings	79
	(b) Motivation to Combine	80
IX.	GROUND 5: <i>COLLINGS</i> IN VIEW OF <i>BONA, SMITH, AND KRANZLEY</i>	81

A.	CLAIM 10	81
(a)	Collinge	81
(b)	Kranzley	82
(c)	Motivation to Combine	83
X.	GROUND 6: <i>COLLINGE</i> IN VIEW OF <i>BONA AND KRANZLEY</i>.....	84
A.	CLAIM 16	84
XI.	GROUND 7: <i>COLLINGE</i> IN VIEW OF <i>BONA AND ENG</i>	84
A.	CLAIM 19	84
(a)	Bona’s Teachings	84
(b)	Eng’s Teachings	85
(c)	Motivation to Combine	86
XII.	GROUND 8: <i>COLLINGE</i> IN VIEW OF <i>BONA, SMITH, AND CHIN</i>.....	87
A.	CLAIM 12	87
(a)	Collinge’s Teachings.....	88
(b)	Chin’s Teachings.....	88
(c)	Motivation to Combine	89
B.	CLAIM 13	90
XIII.	GROUND 9: <i>COLLINGE, BONA, SMITH, AND FISHER</i>	91
A.	CLAIM 7	91
(a)	Collinge’s Teachings.....	91
(b)	Fisher’s Teachings.....	91
(c)	Motivation to Combine	92
XIV.	GROUND 10: <i>COLLINGE, SMITH, BONA, AND HAMMAD</i>	93
A.	CLAIM 6	93
(a)	Hammad’s Teachings.....	93
(b)	Collinge’s Teachings.....	94
(c)	Motivation To Combine	95
XV.	DISCRETIONARY DENIAL	97

XVI. CONCLUSION.....	97
XVII.MANDATORY NOTICES UNDER 37 C.F.R. § 42.8	98
A. REAL PARTY-IN-INTEREST UNDER 37 C.F.R. § 42.8(B)(1).....	98
B. RELATED MATTERS UNDER 37 C.F.R. § 42.8(B)(2)	98
C. LEAD AND BACK-UP COUNSEL UNDER 37 C.F.R. § 42.8(B)(3).....	98
D. 37 C.F.R. 42.8(B)(4) – SERVICE INFORMATION.....	99

I. INTRODUCTION

Apple Inc., (“Petitioner”) respectfully requests *inter partes* review (“IPR”) of claims 1-27 (“Challenged Claims”) of U.S. Patent No. 11,328,286 (“’286 Patent”).

II. THE ’286 PATENT

A. Description of the ’286 Patent

The ’286 Patent describes an electronic payment card capable of “generating a limited-duration credit card number...which is limited in scope of use to a predetermined number of authorized transactions.” ’286 *Patent* (Ex.1001) at 2:33-39, 2:57-3:5, 10:63-12:4, Fig. 7.

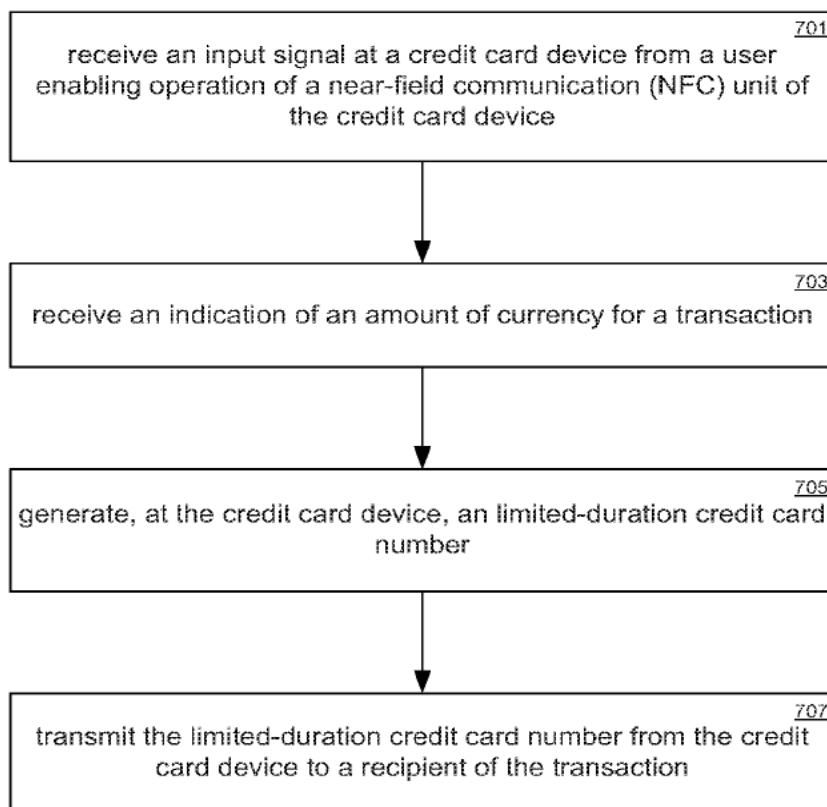


FIG. 7

’286 *Patent*, Fig. 7.

B. Field of Endeavor and Problem Solved by the Inventors

The '286 Patent defines the “Field of the Invention” as relating to “electronic or smart multi-function electronic devices and, more specifically, to more secure, smart multi-function electronic payment card and device systems and transaction processing thereof.” Ex.1001, 1:31-35, 2:4-12 (criticizing existing systems as “susceptible to theft and/or compromise”). A POSITA would have understood the field of endeavor of the '286 Patent includes more secure payment cards, devices, and systems, and the '286 Patent aims to solve the problem of providing payment solutions that limit opportunities for theft or compromise of payment credentials. *Dec.*, ¶¶32-36.

C. Priority and Prosecution History

The '286 Patent claims priority to Provisional Application No. 61/794,891, filed March 15, 2013. Because the '286 Patent claims the benefit of a filing date before March 16, 2013, Petitioner applies the pre-AIA versions of §§ 102, 103. For this proceeding, Petitioner applies March 15, 2013, as the priority date for the Challenged Claims.¹ Unless noted, the below analysis would not change under the AIA.

¹ Petitioner does not concede that any of the Challenged Claims are entitled to claim priority to March 15, 2013. Multiple claims of the '286 Patent recite features not

The '286 Patent did not face any prior art rejections during prosecution. '286
File History (Ex.1002).

D. Level of Skill of a POSITA

A POSITA at the time of the '286 Patent would have had a bachelor's degree in computer science, computer engineering, electrical engineering or the equivalent, and one or two years of experience working with payment processing and/or digital authentication systems, including familiarity with short-range wireless technology. *Dec.*, ¶¶28-30.² Additional industry experience or technical training may offset less formal education, while advanced degrees or additional formal education may offset lesser levels of industry experience. *Id.*

III. REQUIREMENTS UNDER 37 C.F.R. § 42.104

A. Standing Under 37 C.F.R. § 42.104(a)

Petitioner certifies the '286 Patent is eligible for IPR.

described in CardWare's provisional application. *See e.g.*, PGR2023-00013 (Paper 14 at 9-12); PGR2023-00012 (Paper 14 at 10-13) (preliminarily finding insufficient support for at least claim 5 in CardWare's March 15, 2013 provisional application).

² All references to "*Dec.*" are to Ex.1003, Declaration of Dr. Neuman.

B. Identification of Challenge Under 37 C.F.R. § 42.104(b)

The Challenged Claims are unpatentable on the following grounds under 35 U.S.C. § 103:

Ground	Claim(s)	References
1	15, 17-18	Collinge (Ex.1004) and Bona (Ex.1009)
2	1, 5, 8, 11, 14, 20-27	Collinge, Bona, and Smith (Ex.1010)
3	2-4	Collinge, Bona, Smith, and Patterson (Ex.1011)
4	9	Collinge, Bona, Smith, and Lin (Ex.1012)
5	10	Collinge, Bona, Smith, and Kranzley (Ex.1013)
6	16	Collinge, Bona, and Kranzley
7	19	Collinge, Bona, and Eng (Ex.1014)
8	12, 13	Collinge, Bona, Smith, and Chin (Ex.1015)
9	7	Collinge, Bona, Smith, and Fisher (Ex.1016)
10	6	Collinge, Bona, Smith, and Hammad (Ex.1017)

The earliest claimed priority date of the '286 Patent is March 15, 2013 (the “Critical Date”).³ Each of the prior art references applied in this Petition qualifies as prior art to the '286 Patent:

Reference	Filed	Published	Prior Art Basis
Collinge	03/14/2013	10/3/2013	§102(e) ⁴

³ Unless specifically noted, the analysis presented in this petition remains the same regardless of whether March 15, 2013 or some later date is used as the Critical Date.

⁴ Collinge is prior art of its filing date. Should CardWare attempt to establish an earlier date of reduction to practice, Apple will show that Collinge is entitled to a

Bona	8/19/2009 (PCT)	6/16/2011	§102(b)
Smith	11/17/2009	5/20/2010	§102(b)
Lin	8/11/2009	4/8/2010	§102(b)
Kranzley	6/1/2009	5/20/2010	§102(b)
Eng	11/5/2012	3/21/2013	§102(e)
Chin	7/25/2011	11/17/2011	§102(b)
Fisher	12/7/2012	4/18/2013	§102(e)
Hammad	06/18/2007	06/22/2010	§102(b)

None of these references were cited or discussed during prosecution of the '286 Patent.

C. Claim Construction Under 37 C.F.R § 42.104(b)(3)

In this proceeding, claims are interpreted under the same standard applied by Article III courts (i.e., the *Phillips* standard). 37 C.F.R. § 42.100(b); *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (*en banc*). For purposes of this

priority date of at least April 18, 2012 under 35 U.S.C. § 102(e) based on Collinge's provisional applications, which provide written description support for the subject matter relied upon in this Petition and at least one claim of the Collinge Publication. *In re Giacomini*, 612 F.3d 1380, 1383 (Fed. Cir. 2010); *Dec.*, ¶¶77-87. *See also Dynamic Drinkware, LLC v. Nat'l Graphics, Inc.*, 800 F.3d 1375, 1381 (Fed. Cir. 2015) (holding Petitioner did not have the burden of producing evidence relating to earlier effective filing date based on provisional application until Patent Owner argued for an earlier date of reduction to practice).

proceeding, Petitioner applies the plain and ordinary meaning of all claim terms as understood by a POSITA.⁵

Petitioner reserves the right to respond to any constructions offered by Patent Owner or adopted by the Board.

1. Claim limitations directed to printed matter are not entitled to patentable weight.

The Challenged Claims include several limitations that are directed to printed matter that has no structural or functional relationship to the claimed substrate on which the information is disposed or printed. The Federal Circuit has repeatedly found that such claim limitations are entitled to no patentable weight, and thus “will not distinguish the invention from the prior art in terms of patentability.” *In re Gulack*, 703 F.2d 1381, 1385 (Fed. Cir. 1983); *In re DiStefano*, 808 F.3d 845, 848-851 (Fed. Cir. 2015).

The following table identifies limitations from the Challenged Claims that are directed to printed matter and thus are entitled to no patentable weight.⁶ For the

⁵ Petitioner’s application of prior art to the Challenged Claims is not a waiver of any argument in litigation that any claim is indefinite, invalid, or requires claim construction.

⁶ The Board preliminarily agreed that these limitations are directed to printed subject matter and entitled to no patentable weight in PGR2023-00012, Paper 14 at 24-26.

reasons discussed below at §V, each limitation is nevertheless rendered obvious by the cited art.

Claim	Printed Matter
1	“free of any fixed payment numbers visible thereon” / “a card payment information not visible on the payment card device”
5	“wherein the payment card device is absent a payment number information necessary for completing an online transaction”
15	“free of any fixed payment numbers disposed thereon”
19	“wherein the payment card device comprises fixed payment information disposed thereon, and wherein the fixed payment information comprises only: a card-holder name; a payment issuing logo; a card payment network logo, and a card reader interface icon, and wherein the payment card device is free of any account numbers, expiration dates, card security codes, or other fixed payment numbers, disposed thereon.”
20	“free of any depictions of fixed payment numbers thereon”
20	“issuer-provided payment information, associated with, but not depicted on, the payment card device”

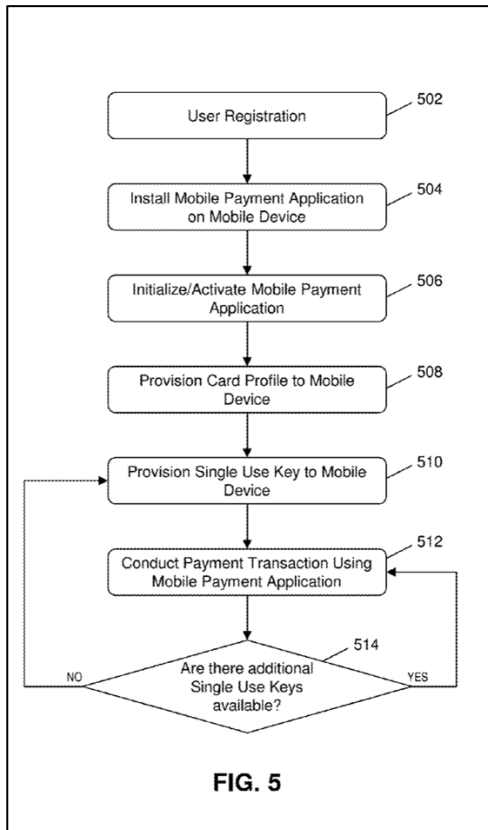
IV. SHOWING OF ANALOGOUS PRIOR ART

A. Collinge

Collinge teaches “[a] method for generating and provisioning payment credentials to a mobile device lacking a secure element” which payment credentials may be used “in conducting a near field financial transaction[.]” *Collinge*, Abstract; [0002].

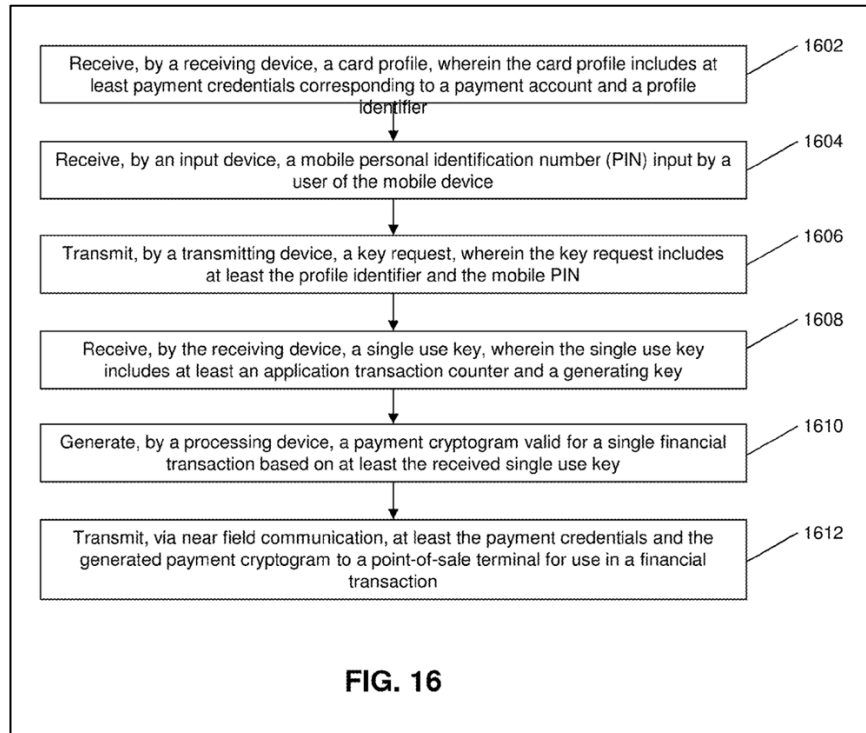
Collinge teaches that a user may register their mobile device for use in contactless payments and install a mobile payment application on the mobile device. *Collinge*, [0065]-[0066]. Collinge teaches that after registration, the mobile payment

application of the mobile device is provisioned with a card profile and single use key from a remote secure element. *Collinge*, [0068]-[0069]; Fig. 5.



Using the provisioned single use key, the mobile payment application within Collinge’s mobile device generates a payment cryptogram valid for a single financial transaction. *Collinge*, [0069]. The single-use “payment cryptogram may be, for example, an application cryptogram or a dynamic card validation code (CVC3).” *Collinge*, [0077].

Collinge’s mobile device “may conduct a contactless/NFC payment transaction” by “transmit[ting] the generated payment cryptogram and payment credentials to a point-of-sale terminal[.]” *Collinge*, [0070], [0077].



Collinge, Fig. 16.

1. *Collinge Incorporated all Provisionals for All Purposes*

Collinge claims priority benefit of and expressly “incorporated by reference in their entirety” Provisional Nos. 61/619,095 (Ex.1005) (“’095 *Provisional*”), 61/635,248 (Ex.1006) (“’248 *Provisional*”), 61/735,383 (Ex.1007) (“’383 *Provisional*”), and 61/762,098 (Ex.1008) (“’098 *Provisional*”). *Collinge*, [0001]. Thus, Collinge’s Provisionals form part of Collinge for all purposes as if explicitly contained therein. MPEP (8th Ed) §2163.07(b) (“information incorporated is as much a part of the application as filed as if the text was repeated in the application, and should be treated as part of the text of the application as filed.”); *Ultradent Prods., Inc. v. Life-Like Cosmetics, Inc.*, 127 F.3d 1065, 1069 (Fed. Cir. 1997); *Apple*

Inc. v. Koss Corporation, IPR2021-00255, Paper 54 (Final Written Decision) (P.T.A.B. May 31, 2022), at 25-30 (holding claims obvious over host reference, relying on material from two provisional applications incorporated in their entirety); *Unified Patents, LLC v. Rosen Technologies LLC*, No. IPR2022-01402, Paper 22 (Final Written Decision) (P.T.A.B. Feb. 28, 2024), at n.6 (“Because Geiwitz expressly incorporated by reference its entire provisional application [] the provisional’s disclosures are part of “Geiwitz” as asserted by Petitioner.”).

2. Obvious to Combine Provisional Features

Further, Collinge’s provisional applications are directed to the same invention. Figures, invention elements numbering, and invention descriptions substantially overlap, and a POSITA would recognize that the Provisionals provide additional implementation details relevant to Collinge’s payment system. *Compare e.g., ’098 Provisional*, Fig. 19 *with Collinge*, Fig. 6; *Collinge*, Fig. 19 *with ’095 Provisional* Fig. 9 and *’248 Provisional* Fig. 16; *Dec.*, ¶¶81-87.

Even if Collinge’s Provisionals were directed to different payment system embodiments, it would have been obvious, and a POSITA would have been motivated to apply the teachings in Collinge’s Provisionals in Collinge’s payment system. *Dec.*, ¶87. For example, Collinge’s provisional applications provide additional detail about what is shown on the graphical user interface of Collinge’s mobile device during user registration, user selection of a payment option, and an

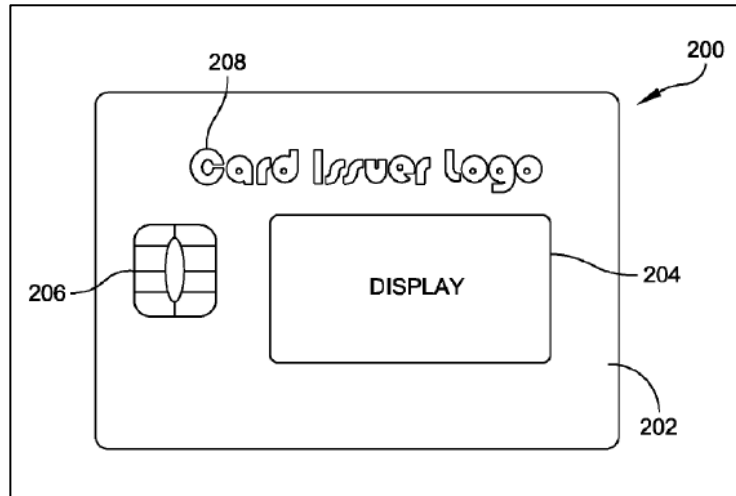
NFC transaction. *See e.g., '248 Provisional*, Fig. 2A, 2B; *'098 Provisional*, p. 96-100; *Collinge*, [0133]. A POSITA would have found it obvious and would have been motivated to incorporate these disclosures into Collinge's payment system because implementing Collinge's payment system requires various display screens with user-selectable softbuttons and Collinge's Provisional provide details regarding layout and softbutton functions that would assist a POSITA in implementing Collinge's teachings with a reasonable chance of success. *Dec.*, ¶87.

As another example, Collinge teaches use of a "CAP token" (*Collinge*, [0144]) and the provisional applications provide examples of what controls on purchases may be represented by the token. *See '095 Provisional*, Claims 9-10 (day of week, time of day, etc.). A POSITA looking to implement a CAP token would have been motivated to implement the examples of a CAP token in Collinge's Provisional application, such as spending limits and expiration date limits which were well-known and would have increased security of Collinge's payment credentials. *See Claim 15(g). Dec.*, ¶87.

In each case, a POSITA would have found a teaching, suggestion, or motivation in Collinge itself that would have led them to apply the additional details in Collinge's Provisionals to Collinge's payment system with a reasonable expectation of success. *Id.*

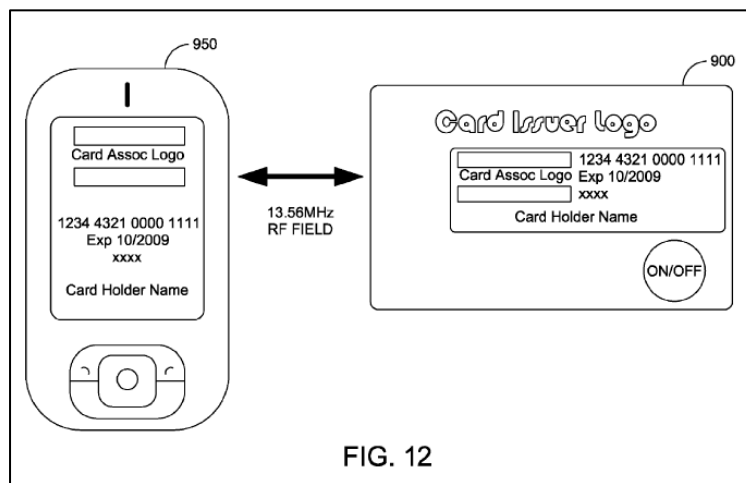
B. Bona

Bona teaches a NFC enabled companion card that “includes an on/off button 906 for powering the smart card on/off and a display 904 for displaying information to the user.” *Bona*, [0110].



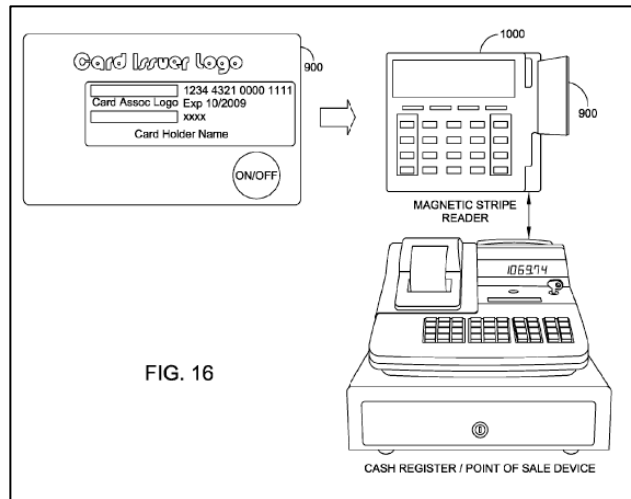
Bona, Fig. 2A.

Bona teaches using its NFC-enabled companion card in connection with a cell phone for transactions. *Bona*, [0119].



Bona, Fig. 12.

Bona's payment card device is operable for use in a payment card reader equipment, such as "contact smart card readers, contactless smart card readers and magnetic stripe readers[.]" *Bona*, [0036].



Bona, Fig. 16.

C. Smith

Smith teaches a "mobile PAN" for a "mobile device" that "may...be used...with a near field communications enabled purchasing transaction." *Smith*, Abstract.

Whenever a user wishes to open a payment account, the issuer issues a "temporary PAN...and establishes any risk parameters (e.g., for use in controlling the authorization of transactions involving the temporary PAN)" so the user is able to make purchases while awaiting an actual PAN. *Smith*, [0026]. This "temporary PAN is mapped to a mobile PAN (e.g., such as a PayPass® PAN, or PPAN)." *Smith*,

[0026]. The mobile PAN/PPAN is “assigned to the mobile device 104.” *Smith*, [0016].

600 

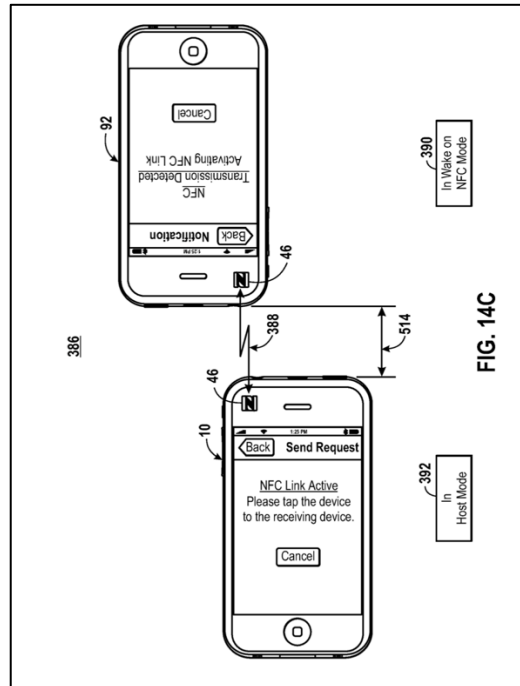
CONSUMER ID 602	TEMPORARY PAN 604	MOBILE PAN 606	ACTUAL PAN 608	RISK PARAMETER RESTRICTION(S) 610
C1001	T-PAN_0001	M-PAN_0001	NONE	NONE
C1002	T-PAN_0002	M-PAN_0002	NONE	NO TRANSACTIONS OVER \$10
C1003	T-PAN_0003	M-PAN_0003	NONE	OVERALL TRANSACTION UNDER \$100
C1004	T-PAN_0004	M-PAN_0004	NONE	NO ONLINE TRANSACTIONS
C1006	NONE	M-PAN_0006	A-PAN_0001	NONE

FIG. 6

Smith, Fig. 6, [0023] (the PPAN is associated with a “related PAN[.]”). The mobile PAN is “stored in the mobile device 204.” *Smith*, [0022]. Once an actual PAN is issued, the temporary PAN is swapped with the actual PAN. *Smith*, [0026], [0040].

D. Lin

Lin teaches “the establishment of an NFC connection 388 between two devices, namely the payee device 10 and the payor device 92, by way of the tap operation 386[.]” *Lin*, 68:10-12.



Lin, Fig. 14C.

Lin teaches that once “active device 10 is placed within an acceptable distance 514 (e.g., 2-4 cm) from the payor device 92” the devices establish an “NFC connection 388...through which the payment request may be transmitted.” *Lin*, 68:13-25.

E. Patterson

Patterson teaches allowing a cardholder to “specify blocking criteria to be associated with one or more accounts” such as credit card accounts. *Patterson*, 6:17-46. The issuer may deny a transaction based on the blocking criteria. *Patterson*, 6:28-46, Abstract. For example, the user may list a card as “lost or stolen” and the issuer “will block all transactions from that card from being authorized[.]” *Patterson*, 6:38-40.

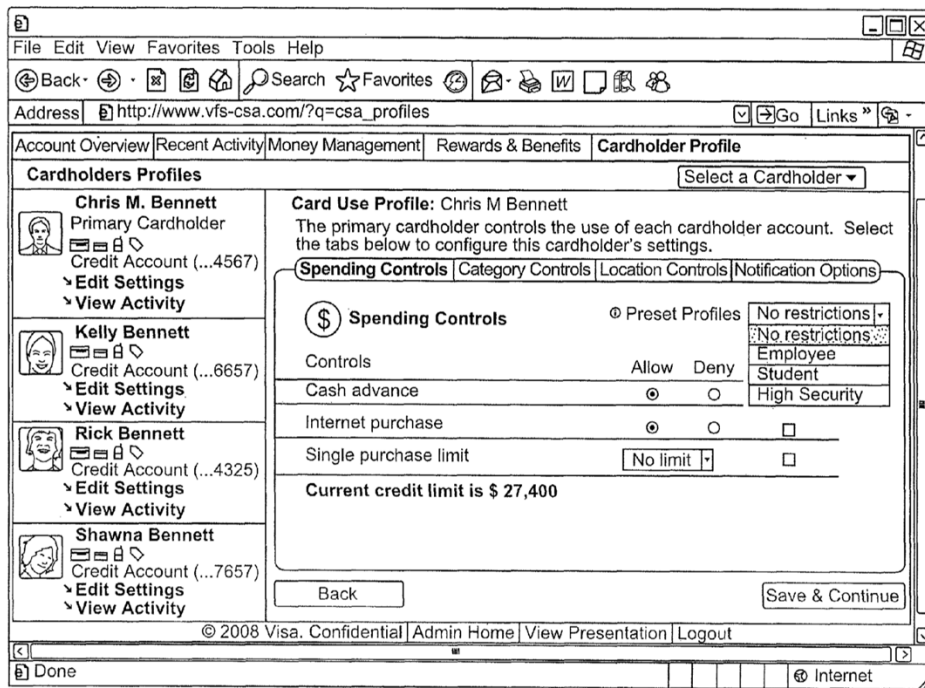


FIG. 8

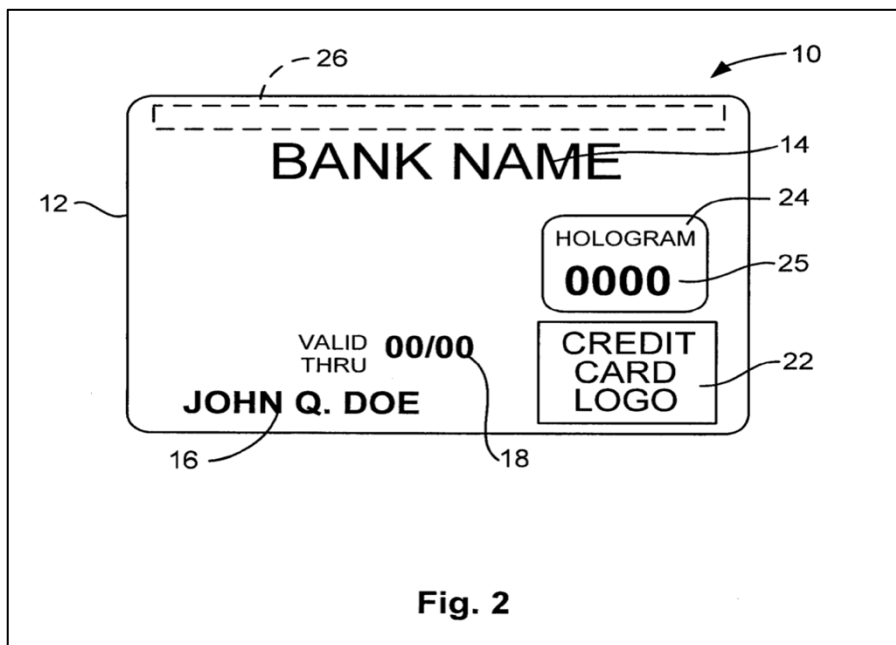
Patterson, Fig. 8.

F. Kranzley

Kranzley teaches using a virtual PAN (VPAN) in place of the PAN. The VPAN “may have its own virtual expiry date.” *Kranzley*, [0036]. Kranzley teaches displaying “the static VPAN...in plain text on a display device 14 of the mobile device 12 along with an expiry date and dynamic data[.]” *Kranzley*, [0035], [0033]-[0036].

G. Eng

Eng teaches a card with the following fixed payment information: (1) *a cardholder name*, (2) bank name (*a payment issuing logo*) among other items. *Eng*, [0020]-[0021].



Eng, Fig. 2.

H. Chin

Chin discloses “gesture based authentication for wireless payment by a mobile electronic device[.]” *Chin*, [0008]. Specifically, Chin teaches accepting a gesture on “the touch receptive input area (e.g., a touchscreen)” and “comparing the applied gesture” with a user-defined payment gesture stored locally within the device, which may be a “mobile electronic device equipped with NFC payment capabilities[.]” *Chin*, [0009]. If the gesture input by the user “matches the user-defined payment gesture stored locally within the target device, the method may include permitting the wireless transmission (e.g., using NFC technology) of protected payment data resident on the target device to an initiator device (e.g., an NFC reader, a contactless smart card reader based on RFID technology, an NFC scanner, etc.).” *Chin*, [0009].

I. Fisher

Fisher teaches a “mobile communication device” with a “mobile wallet application that executes PayPass[.]” *Fisher*, [0024]. When “a consumer (or user) is shopping online and they are ready to pay for their products, the consumer opens his mobile wallet and selects one of the payment methods (e.g., credit card, debit card, prepaid card, etc.) from their mobile wallet.” *Fisher*, [0018]. The user “waves their phone over the NFC reader present on the PC 404.” *Fisher*, [0018]. The user’s “payment credentials are transferred from the phone to the merchant website (e.g., online store application 410).” *Fisher*, [0018].

J. Hammad

Hammad teaches generating verification values on a portable consumer device for use in payment transaction. *Hammad*, 2:10-20, 2:65-3:11. The dynamically generated verification values, which are embedded in payment data sent to a service provider, are generated using two or more dynamic data elements and static data elements. *Id.*, 4:21-6:42.

K. Analogous Art

Each of the applied prior art references discloses conducting secure payment transactions and is in the same field of endeavor as the '286 Patent. *Compare '286 patent*, Abstract, 1:31-35, Fig. 1 *with Collinge*, Abstract, [0005], Fig. 1; *Bona*, Abstract, 0036-0037, Fig. 16; *Smith*, Abstract, [0021]-[0023]; *Lin*, Abstract, 68:13-25, Fig. 14C; *Patterson*, Abstract, 1:15-17, Fig. 1; *Kranzley*, Abstract, [0010], Fig.

1; *Eng*, Abstract, [0023]-[0024], Fig. 2; *Chin*, [0009], [0030]; *Fisher*, [0018], [0023]-[0025]; *Hammad*, Abstract, 2:12-20, Fig. 6; *Dec.* ¶¶78-80, 91-114, 117-20.

Further, each of the applied prior art references is reasonably pertinent to problems addressed by the '286 Patent such as increasing security of payment transactions. Compare '286 Patent, 1:31-35, 2:4-12, 9:63-10:2 with *Collinge*, [0003]-[0005]; *Dec.*, ¶¶78-80; *Bona*, 0008-0010; *Dec.*, ¶¶91-93; *Smith*, [0002], [0015], [0020]; *Dec.*, ¶¶96-97; *Lin*, 27:26-28:15; *Dec.*, ¶¶100-101; *Patterson*, 5:18-46, 11:22-25; *Dec.*, ¶¶104-05; *Kranzley*, [0003], [0065]; *Dec.*, ¶¶107-08; *Eng*, [0023], Abstract, Fig. 2; *Dec.*, ¶¶110-11; *Chin*, [0054], [0004]-[0007]; *Dec.*, ¶¶113-14; *Fisher*, [0003]-[0006]; *Dec.*, ¶¶116-17.; *Hammad*, 1:20-23; 1:45-65; *Dec.*, ¶¶119-20. Therefore, each of the applied prior art references is analogous art to the '286 Patent.

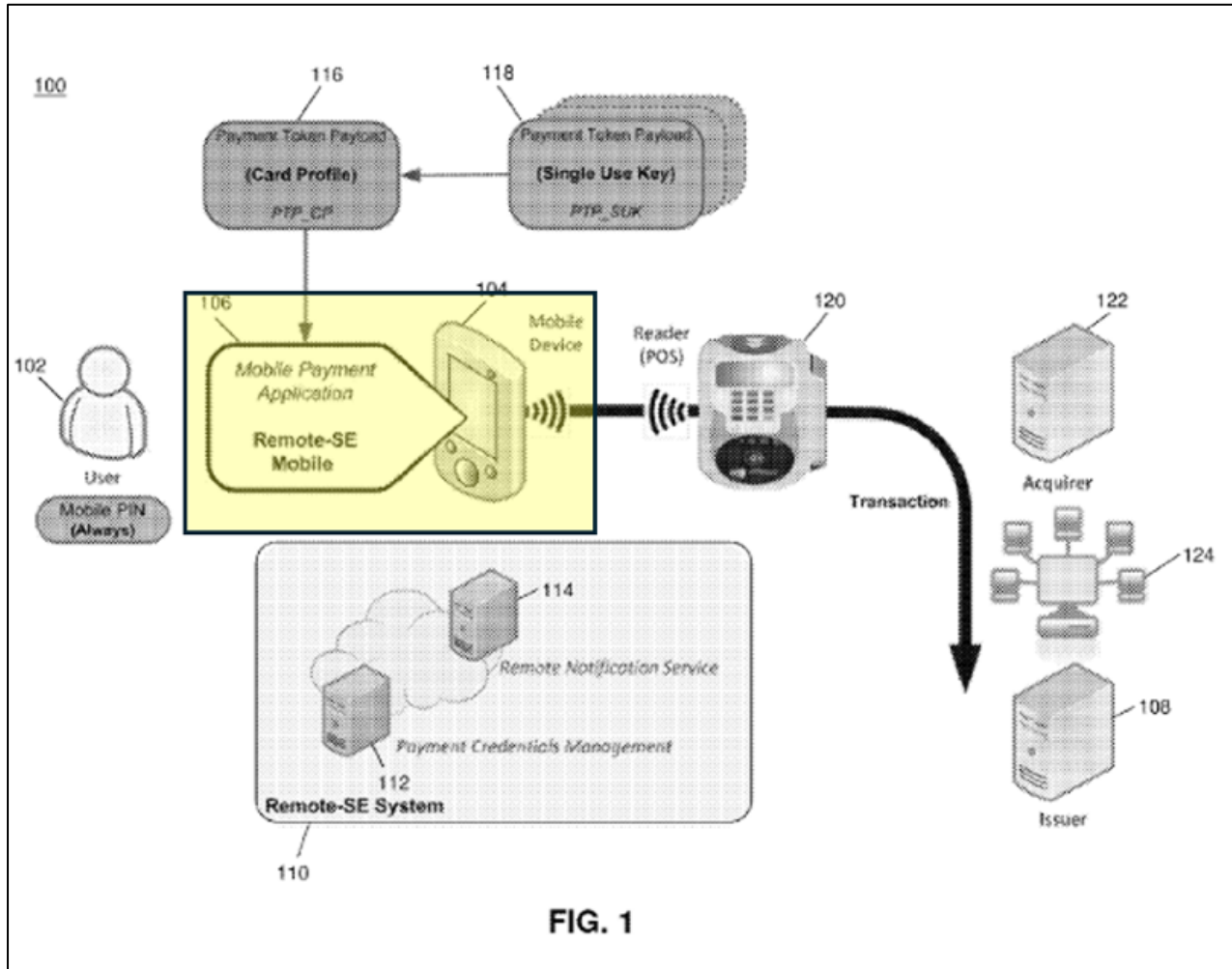
V. GROUND 1: *COLLINGS* IN VIEW OF *BONA*

A. Claim 15

1. *15(Pre): A payment system comprising:*

Collinge teaches a payment system⁷ that includes generating and “provisioning of payment credentials to a mobile device” for “use in mobile payment transactions.” *Collinge*, Abstract, [0006], [0039].

⁷ Claim language identified with *italics* and underline.



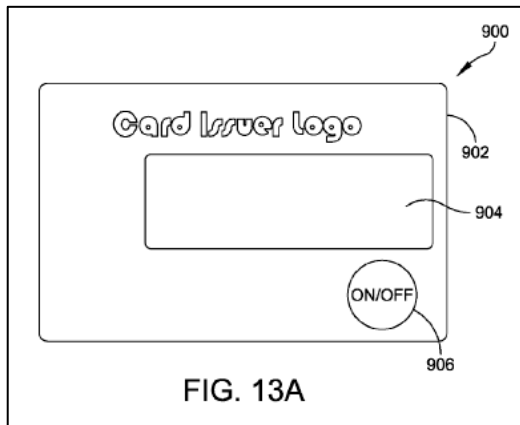
Collinge, Fig. 1 (annotated).

2. ***15(a): a payment card device that is free of any fixed payment numbers disposed thereon and wherein said payment card device is operable for use in a merchant card-reader equipment; and***

As previously discussed, (Section C.1, *supra*), the limitation that the payment card be “free of any fixed payment numbers visible thereon” is directed to printed matter that has no functional or structural relationship to the claimed card device and is entitled to no patentable weight. *Dec.*, ¶¶124-28. Nevertheless, the combination of Bona and Collinge renders this limitation obvious.

(a) Bona's Teachings

Bona teaches a payment card device (“NFC enabled companion card 900”) that is free of any fixed payment numbers visible thereon. *Bona*, Fig. 13(a), [0108]. When Bona’s card is off, there is no information on the display of the payment card device as shown below in Figure 13A. *Bona*, [0110] (“The smart card includes an on/off button 906 for powering the smart card on/off and a display 904 for displaying information to the user.”).

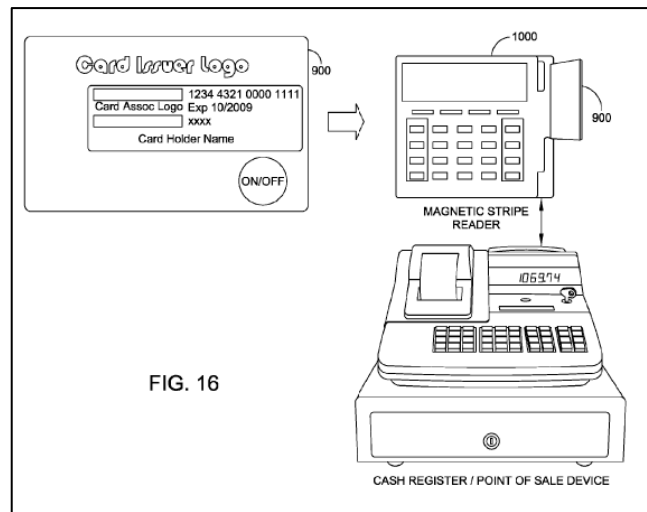


Bona, Fig. 13(a).

Even when Bona’s card is powered on, and payment numbers may be shown on the display 904, the payment numbers are not fixed. *Dec.*, ¶¶130-41. Bona teaches that a user may select from a “list of transaction applications (e.g., debit, VISA, Inc., MasterCard Inc., etc.)...and enable or activate one for use in the next transaction.” *Bona*, [0119]. “After a successful transaction, at a predetermined time limit or when the user presses the on/off button 906, the NFC enabled companion card 900 deletes any transaction data” and “retains no useful information related to the transaction.”

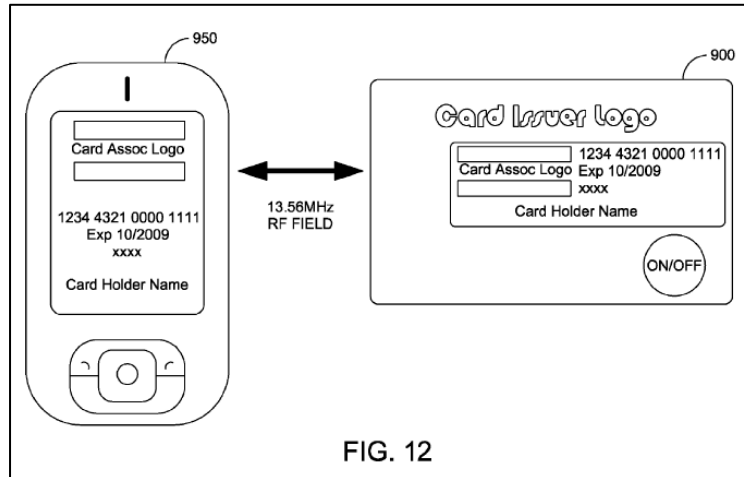
Bona, [0126]. A POSITA would have understood that the payment information associated with a VISA card would differ from the payment information associated with a MasterCard. *Dec.*, ¶138.

Bona's NFC-enabled companion card is operable for use in payment card reader equipment, such as “a traditional magnetic stripe reader” *Bona*, [0125].



Bona, Fig. 16.

Bona's card may be used in connection with a cell phone 950 that “is configured for contactless transactions (e.g., contactless credit or debit transactions) using existing NFC techniques.” *Bona*, [0108]-[0109], [0127].



Bona, Fig. 12. “[N]ecessary data for display on the NFC enabled companion card 900 for use in the transaction can also be transmitted.” *Bona*, [0109].

(b) Collinge’s Teachings

Collinge teaches that a “[a] payment card may be a physical card that may be provided to a merchant, or may be data representing the associated payment account (e.g., as stored in a communication device, such as a smart phone or computer).” *Collinge*, [0038].

(c) Motivation to Combine

A POSITA would have found it obvious and would have been motivated to use Bona’s payment card device free of any fixed payment numbers visible thereon and operable for use in payment card reader equipment with Collinge’s NFC-enabled computing device (i.e., cell phone) and payment system. *Dec.*, ¶¶142-155. A POSITA would have understood that at the time of the alleged invention, there were tens of millions of magnetic stripe readers in use and magnetic stripe

technology continued to be the “predominate point of sale reader technology deployed worldwide[.]” *Bona*, [0008], [0036], [0080]; *Dec.*, ¶143. It was well-known that many point-of-sale terminals only accepted a physical magstripe payment method. *Dec.*, ¶144. *Bona* recognized that “existing contactless transaction enabled cell phones cannot be used for magnetic stripe transactions, which is the dominant technology presently in use.” *Bona*, [109].

A POSITA would have been motivated to combine Collinge with *Bona* to allow the flexibility to make contactless payments using Collinge’s payment application on Collinge’s cell phone and also make payments at point-of-sale terminals that still only accepted a physical swipe of a magstripe card, as expressly taught by *Bona*. *Bona*, [0127]; *Dec.*, ¶¶144-46. A POSITA would have understood that providing the user with both payment options would expand the number of POS terminals where Collinge’s payment credentials could be used and provide the user with additional payment options if an NFC-enabled point-of-sale terminal was broken, not enabled, or not present. *Dec.*, ¶¶145-46.

A POSITA would have had a reasonable expectation of success in combining *Bona*’s NFC-enabled companion card with Collinge’s payment system as a combination of known elements that would yield predictable results, including greater payment flexibility. *Dec.*, ¶¶147-154. Collinge’s and *Bona*’s teachings are compatible, including because both were designed with reference to the same well-

known technical industry standards. *Dec.*, ¶¶147-50; *Bona*, [0102]; '095 *Provisional*, [0063]-[0064]. *Bona* already teaches that *Bona*'s companion card 900 receives payment credentials and dynamic information necessary to authorize the transaction from a cell phone via NFC. *Bona*, [0109], [0053]. *Collinge* likewise already teaches that *Collinge*'s mobile device is able to send payment credentials and a dynamic payment cryptogram via NFC and therefore already has the hardware necessary to communicate with *Bona*'s companion card 900. *Collinge*, [0046], [0070]. Further, *Collinge* already teaches including "magnetic stripe (mag stripe) payment credentials 204" in the card profile provisioned to the mobile device. *Collinge*, [0048], [0049].

A POSITA would have appreciated that modifying *Collinge* to send payment credentials and dynamic data (such as a payment cryptogram) to *Bona*'s payment card would not change the functionality of *Bona* and *Collinge*. *Dec.*, ¶¶152-53. In the combined system, *Collinge* would transmit the necessary transaction information to *Bona*'s companion card for use in a magnetic stripe transaction using NFC communications. *Dec.*, ¶¶153-54. Further, *Collinge* is a Mastercard patent application, and *Bona* already teaches compatibility with Mastercard-specific data. *Bona*, Fig. 15; *Collinge*, Assignee.

3. 15(b): a card-users personal computing device operable for completing a payment transaction and comprising:

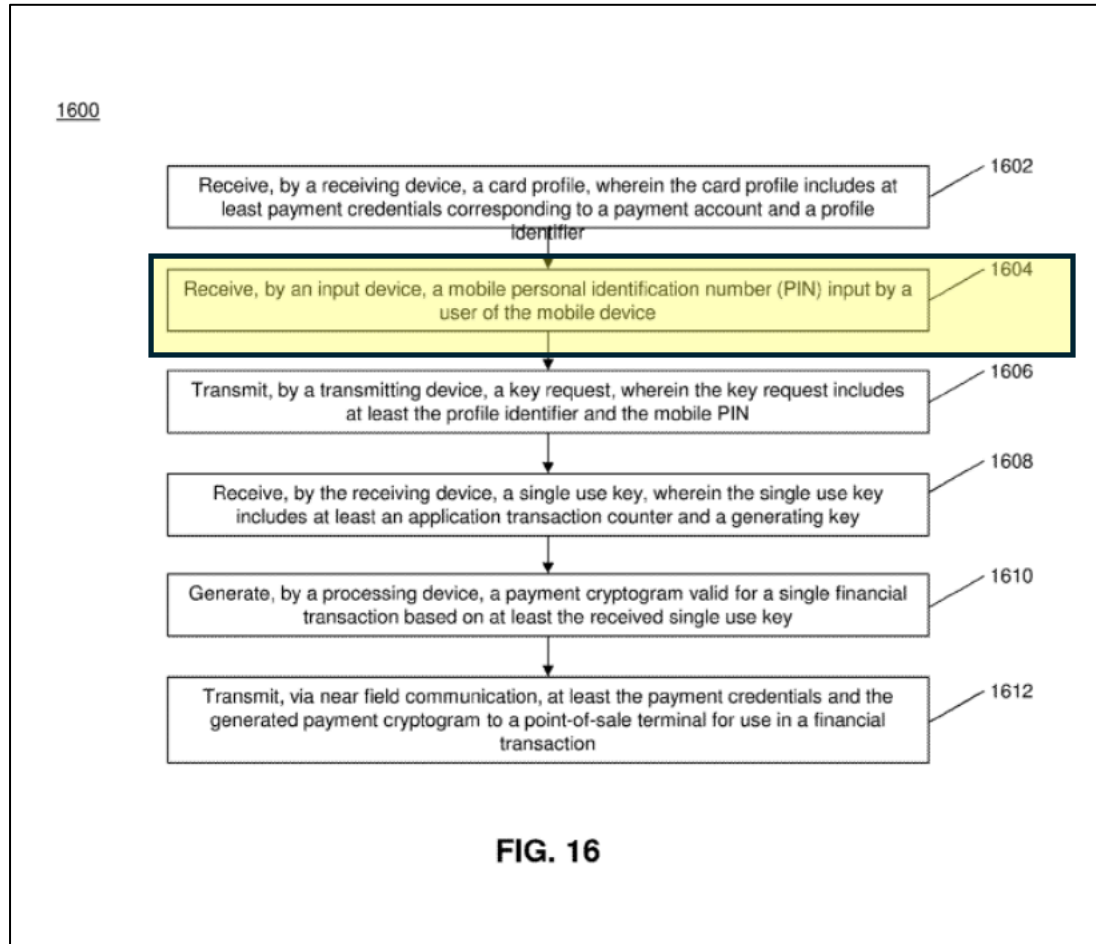
A POSITA would have understood Collinge's mobile device is a card-users personal computing device. *Dec.*, ¶156; *Collinge*, [0042] ("The user 102 may desire to use *their mobile device 104 to conduct payment transactions*"). See also *Bona*, [0117]-[0127] (describing the user cell phone associated with Bona's companion card as accepting authentication from the user).

4. 15(b)(1): a processor;

Collinge's mobile device (computing device) includes "an application program stored in data storage of the mobile device" that is "executed by a processor included in the mobile device[.]" *Collinge*, [0041], [0147] ("at least one processor device... may be used to implement the above described embodiments"). *Dec.*, ¶156.

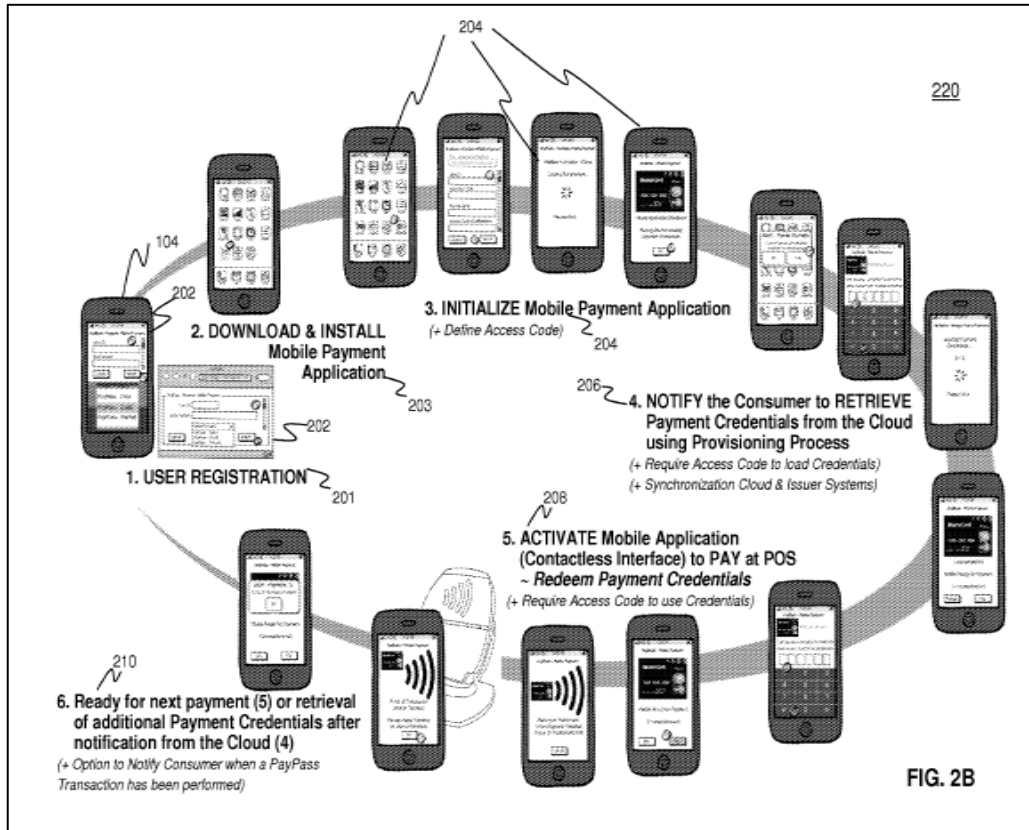
5. 15(b)(2): a touch-screen display interface;

Collinge's mobile device includes a touch-screen display user interface. *Collinge*, [0133] ("a touch screen" of "the mobile device 104"); *Dec.*, ¶¶157-62. Collinge teaches that "a touch screen" of "the mobile device 104" provides a visual user-interface for user payment interactions. *Collinge*, [0133]. Collinge teaches that the touch screen of mobile device 104 receives a user's input of a "mobile personal identification number (PIN)" prior to generation of a payment cryptogram. *Collinge*, [0133].

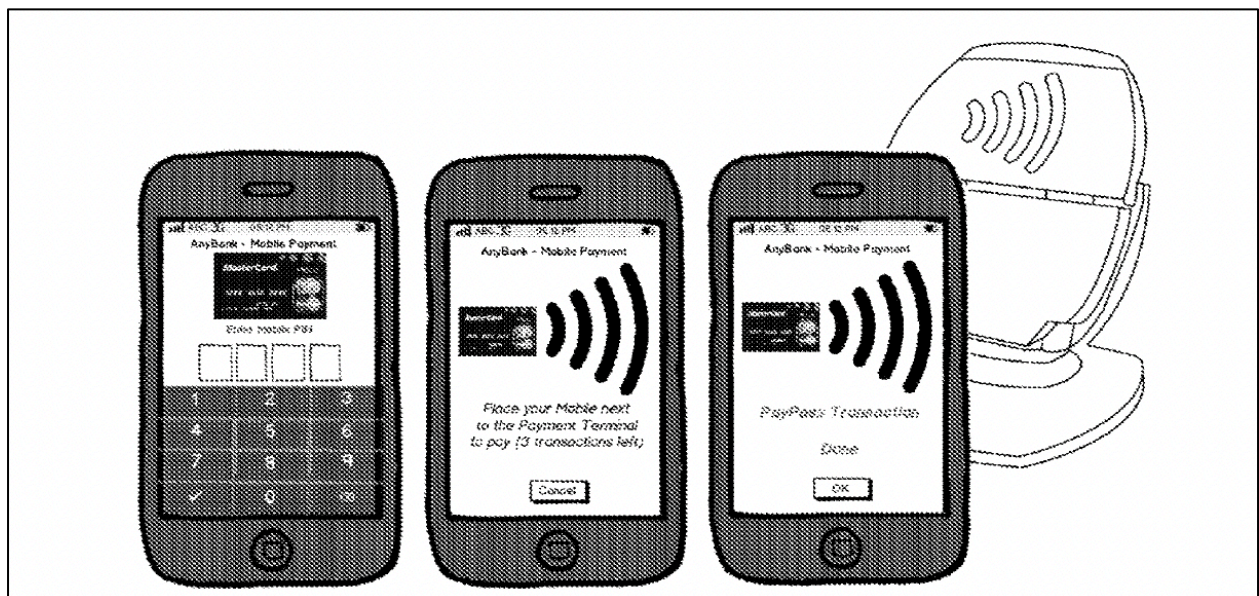


Collinge, Fig. 16 (annotated).

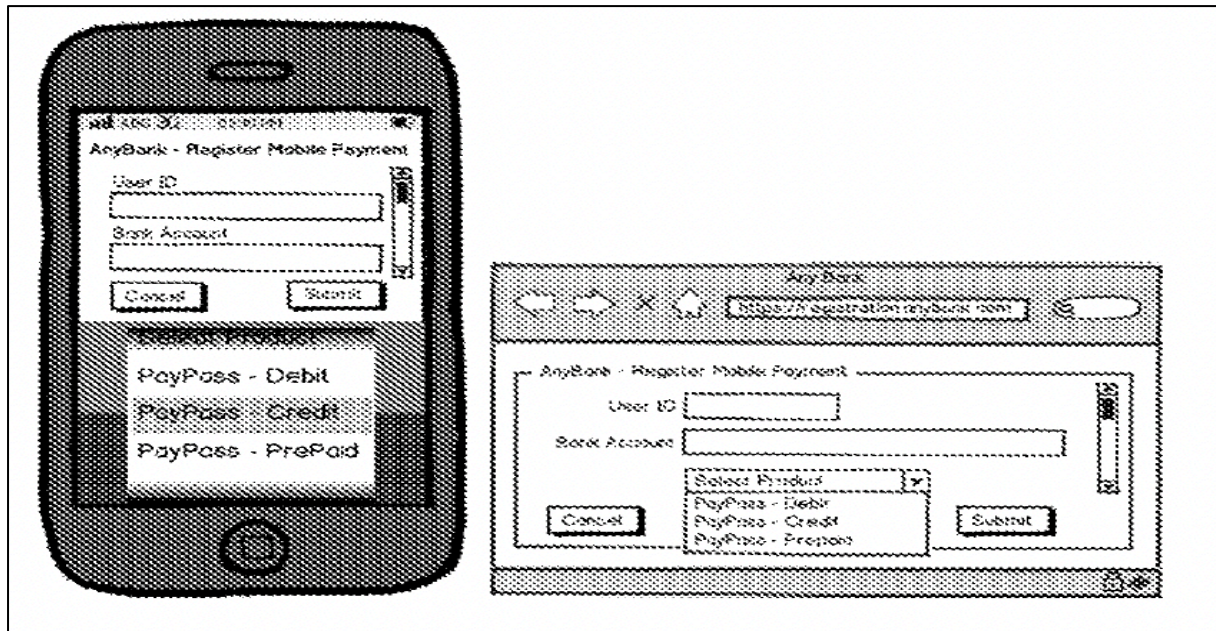
Collinge's '248 Provisional application, incorporated by reference (*see* Section IV.A.1, *supra*) provides further details of how the touch screen of *Collinge*'s mobile device provides a visual user-interface during the user registration and payment process. *Dec.*, ¶160.



'248 Provisional, Fig. 2B. As shown above, the user interface may direct the user to input a pin, direct the user to place the mobile device near a payment terminal, and provide an indication to the user when the payment transaction is complete. *Id.*



'098 Provisional, 99. The registration process steps can likewise “be accomplished using input supplied by a cardholder or user” “via a GUI” of the mobile device 104. *Id.*, p.18 at [0063]. Further, Collinge’s user-interface is operable for a user selection, of at least one of issuer-provided payment methods via the touch-screen display interface.



'098 Provisional, 96; '248 Provisional, Fig. 2B; Dec., ¶¶160-62.

6. 15(b)(3): a user-interface;

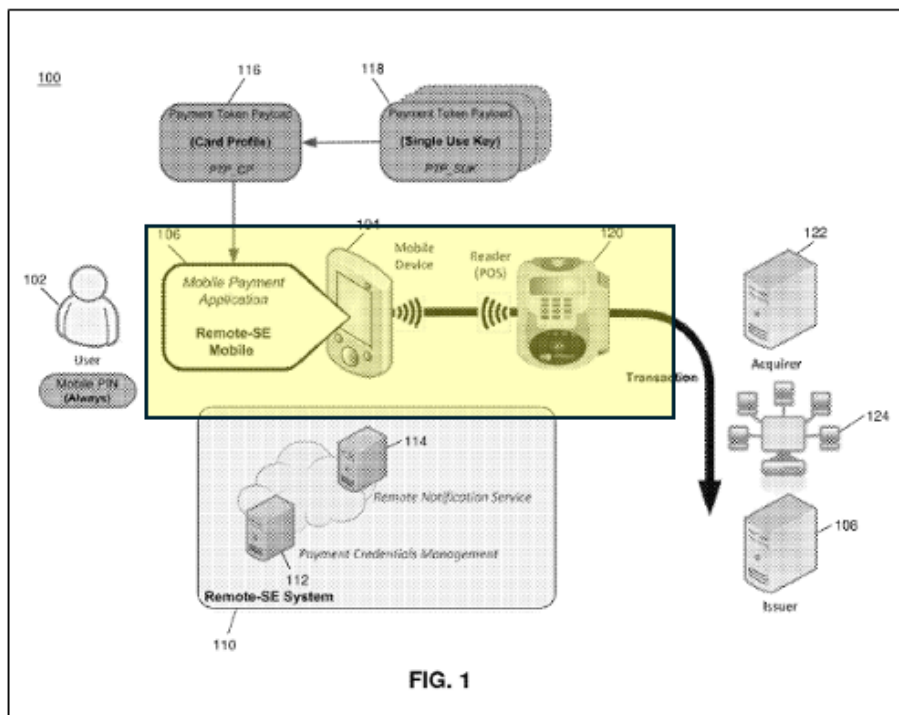
See Claim 15(b)(2).

7. 15(b)(4): a wireless interface;

Collinge teaches a wireless interface (NFC interface). Collinge’s mobile device can “conduct payment transactions via near field communication[.]” *Collinge*, [0041]. Per Collinge, a POSITA would have been familiar with methods for performing contactless payments via NFC. *Collinge*, [0041], [0044], [0070],

[0120]; [0135]; *Dec.*, ¶164. NFC had long been standardized by the time of the '286 Patent, and a POSITA would have recognized that Collinge teaches that mobile device 104 has an NFC interface, and that an NFC interface is necessarily required to conduct NFC payment transactions as taught by Collinge. *Collinge*, [0041]; '248 *Provisional*, [0067] (**NFC interface of the mobile device 104...**"), [0184]; *Dec.*, ¶165.

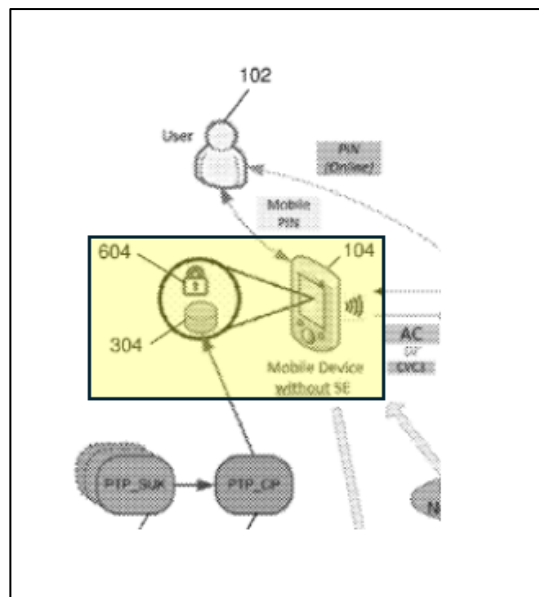
A POSITA would have understood that Collinge's NFC interface is a wireless interface because it is a short-range wireless technology that allows communication wirelessly over short distances. *Dec.*, ¶168.



Collinge, Fig. 1 (annotated excerpt).

8. 15(b)(5): and a memory for storing a payment information accessible to the processor,

Collinge's mobile device includes a memory for storing a payment information accessible to the processor. *Collinge* teaches “an application program stored in **data storage** of the mobile device[.]” *Collinge*, [0041], [0147] (“at least one processor device and **a memory**”) (emphasis added). *Collinge*'s memory includes storage 304, which may include a “local encrypted database.” *Collinge*, [0067], [0147]. Storage 304 stores “received payment credentials[.]” *Collinge*, [0063], [0048]-[0049] (describing payment credentials contents).



Collinge, Fig. 1 (annotated excerpt). *Collinge*'s mobile device includes “an application program stored in data storage of the mobile device” that is “executed by a processor included in the mobile device[.]” *Collinge*, [0041].

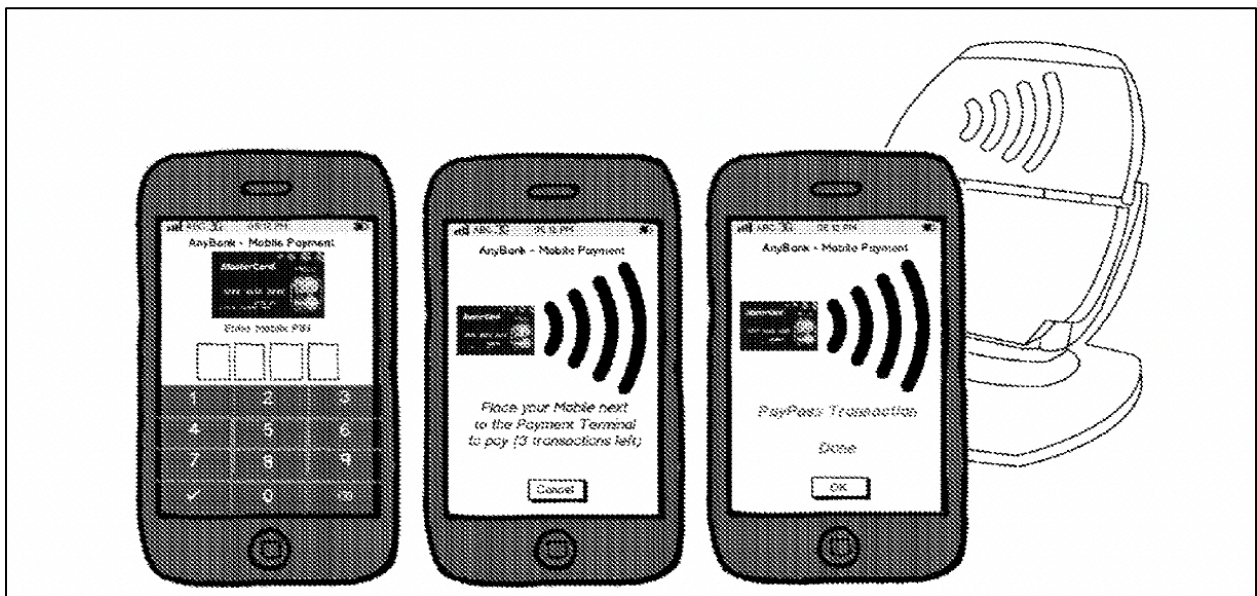
9. ***15(c): wherein the computing device is configured to dynamically generate limited-use payment information, and***

Collinge teaches a processor operable to dynamically generate at least a portion of a limited-use card payment information (payment cryptogram) for use by an authenticated card user (user authenticated by a successfully entered PIN or passcode).

Collinge's mobile payment application is "stored in data storage of the mobile device 104 and **executed by a processor** included in the mobile device 104." *Collinge*, [0041]; *Dec.*, ¶172.

The processor executing the mobile payment application of Collinge's mobile device generates a **payment cryptogram** which "may be, for example, an application cryptogram or a dynamic card validation code (CVC3)." *Collinge*, [0077]; *Dec.*, ¶¶173-75. Collinge teaches the payment cryptogram is single-use, "valid for a single financial transaction." *Collinge*, [Abstract], [0128], Fig. 16. The payment cryptogram is generated once the user "input[s] to the mobile payment application 106 that a payment transaction is to be conducted." *Collinge*, [0077]. The payment cryptogram is generated "using the generating key included in the single use key" that was previously provisioned to the mobile device. *Collinge*, [0077], [0043]. Collinge teaches generating a CVC3 based on the following values: "the supplied CVC3 value, the session key unpredictable number, the application transaction counter, and the reader unpredictable number." *Collinge*, [0145].

Collinge teaches that the generated limited-use payment information (e.g., CVC3) is for use by a card user who has been successfully authenticated with a pin or passcode. Collinge teaches that the single use key used in generating the CVC3 “may be protected based on a mobile personal identification number (PIN) value.” *Collinge*, [0051]. If the single use key is protected based on a PIN, the user “may provide a mobile PIN for authentication.” *Id.* If the mobile PIN provided is incorrect, “an incorrect value of the single use key may be used by the mobile payment application 106” and “the issuer 108 will not authorize the payment transaction” resulting in “additional security for the user 102, the issuer 108, and the merchant involved in the payment transaction.” *Id.* Therefore, the CVC3 payment information can only be used by a user authenticated by a mobile PIN. *Dec.*, ¶178.



'098 Provisional, 99.

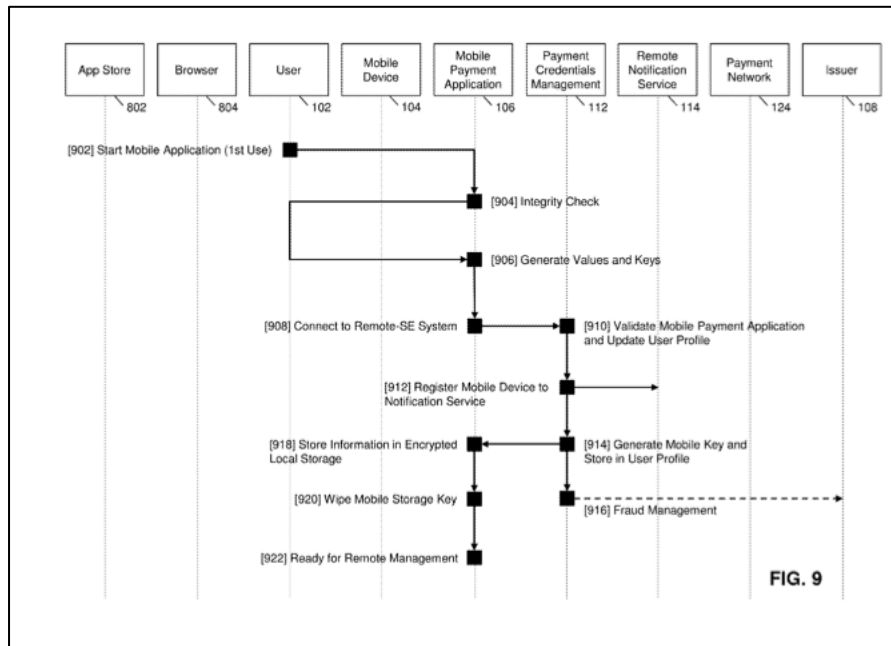
10. 15(d): wherein the computing device is configured to convey the limited-use payment information on a computing device interface upon the authorization of a valid user, and

Collinge's mobile device conveys payment information, including a payment cryptogram (limited-use payment information) via an NFC interface (interface of the computing device) to a point of sale terminal. *Dec.*, ¶179.

Collinge's "mobile device 104 may conduct a **contactless/NFC payment transaction** using the mobile payment application 106[.]" *Collinge*, [0070] (emphasis added). Collinge teaches that the mobile device transmits "generated cryptogram and payment credentials" "to a point-of-sale terminal 120 via NFC[.]" *Collinge*, [0070]; *see also Collinge*, [0145] ("the generated payment CVC3 value and the application transaction counter may be transmitted, via near field communication, to the point-of-sale terminal"), [0120] ("a NFC payment method may be executed between the user 102, the mobile device 104, the mobile payment application 106, and the point-of-sale terminal 120."). A POSITA would have understood that when a mobile device transmits payment information via NFC it is transmitting the payment information via an interface of the computing device. *Dec.*, ¶181.

Collinge further teaches conveying the limited-use card information upon the authorization of a valid user. *Collinge*, [0093], [0123].

A valid user: After the user starts the mobile payment application, “the mobile payment application 106 may perform an integrity check. As part of the integrity check, the mobile payment application 106 may authenticate the user 102 and request the activation code provided to the user 102 during the registration process (e.g., at step 812 in FIG. 8).” *Collinge*, [0093], [0123] (describing “authentication by the user 102 at both the mobile device 104 (e.g., entering of the mobile PIN) and the point-of-sale terminal 120 (e.g., entering of an online PIN or signature).”).



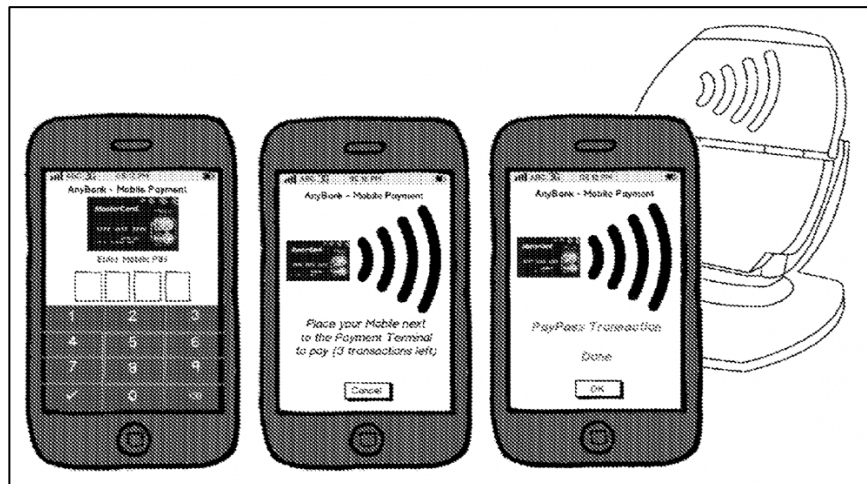
Collinge, Fig. 9. Therefore, *Collinge* identifies a user as a valid user via the correct input of an activation code. *Dec.*, ¶¶182-83.

Authorization of a payment transaction by a valid user: *Collinge* teaches a user may confirm or deny (authorize) a payment transaction after inputting the user’s

mobile PIN (Collinge, [0093], [0123]; '098 Provisional, 99) and then confirming a payment method ("quit" or "pay"):



'098 Provisional, 100. The user is then instructed to place Collinge's mobile device by a payment terminal:



'098 Provisional, 99; '248 Provisional, Fig. 2B; Dec., ¶184. Once the mobile device is placed next to the payment terminal and Collinge's NFC interface is activated

Collinge transmits payment credentials and a dynamic CVC3 to the payment terminal. *Collinge*, [0044], [0077]; '248 *Provisional*, [0073] (“For example, step 208 can comprise activating an NFC interface using the mobile payment application.”).

11. 15(e): wherein a merchant is operable to receive a payment information provided by a personal computing device, and

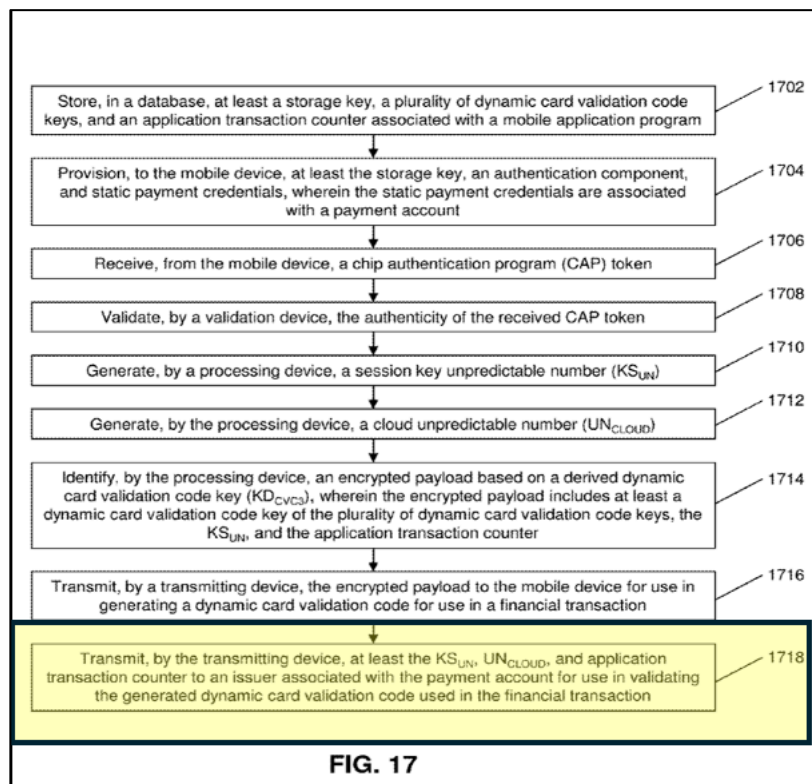
Collinge teaches that “the user 102 may shop at a merchant 306 and select goods or services for purchase.” *Collinge*, [0077] (emphasis added). Then the user “may then input to the mobile payment application 106 that a payment transaction is to be conducted.” *Id.* A payment cryptogram, (e.g., CVC3) (payment information) is generated by the mobile payment application on Collinge’s mobile device (personal computing device). See Claim 15(f). Then Collinge’s mobile payment application “may transmit the payment cryptogram to the merchant point-of-sale terminal 120.” *Id.*; *Dec.*, ¶185.

12. 15(f): wherein the limited-use payment information provided by at least one or both of: the payment card device, and the computing device, is validated by a card issuing authority when used in merchant in-store facility transactions, and

Collinge teaches an issuer 108 (card issuer authority) validates a payment cryptogram (a card payment information) that has been provided by the computing device to a point of sale terminal as authentic when received from an authenticated user of Collinge’s mobile device (an authenticated user’s computing device). *Dec.*,

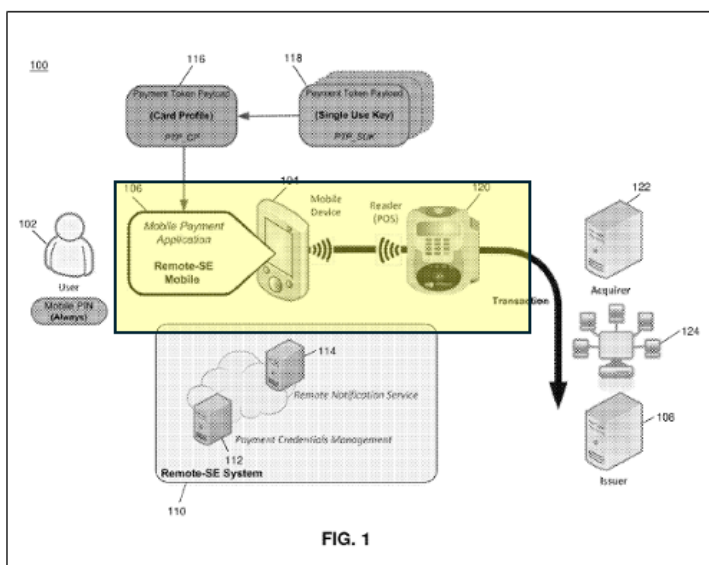
¶¶186-89. Collinge teaches authenticating the mobile device user through a pin or passcode. *See* Claim 15(d).

Collinge also teaches that the issuer 108 validates the generated payment cryptogram. *Collinge*, [0141]. Specifically, the issuer receives “at least the KS_{UN} , UN_{CLOUD} , and application transaction counter” and the issuer 108 uses that information “in validating the generated CVC3 value used in the financial transaction.” *Collinge*, [0141], [0121]; *Dec.*, ¶187.

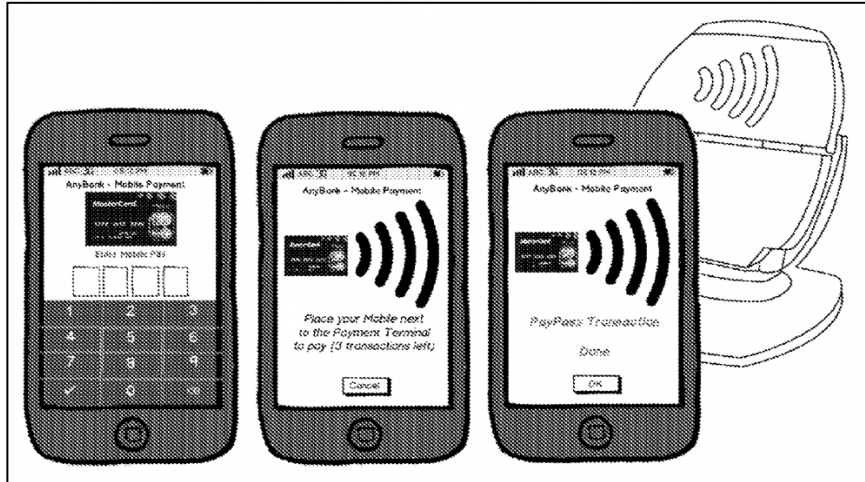


Collinge, Fig. 17 (annotated); '248 *Provisional*, 54. Based on the result, the issuer will “approve or deny the payment transaction[.]” *Collinge*, [0121].

As depicted below, a POSITA would have understood Collinge teaches performing a transaction via NFC at a physical point-of-sale terminal, which a POSITA would have understood would be a merchant in-store facility transaction. *Dec.*, ¶189; *Collinge*, [0044] (“transmit a generated payment cryptogram and payment credentials to a point-of-sale terminal120 at a merchant.”)



Collinge, Fig. 1; '098 *Provisional*, 99 (instructing the user to “[p]lace your Mobile next to the Payment Terminal to pay” at the physical terminal).



'098 Provisional, 99; '248 Provisional, Fig. 2B; Dec., ¶189.

13. 15(g): wherein a card issuing authority is operable to reject as invalid, a payment information used outside of its valid limitations of use, and

Collinge teaches that issuer 108 (card issuer authority) will “deny the payment transaction” (reject as invalid) when the received CVC3 value (a payment information) is unable to be authenticated because, for example the single-use key is not genuine based on an unsuccessfully entered mobile PIN (outside of limitations of use). Collinge, [0076]-[0077], Abstract; Dec., ¶¶190-94.

Collinge also teaches that the issuer will “deny the payment transaction” (reject as invalid) when the user’s “available credit in the payment account” does not support the “transaction amount” (outside of limitations of use). Collinge, [0121], [0077]; Dec., ¶¶191-92.

Collinge also teaches that the issuer may deny (reject as invalid) the payment transaction based on “control limits” (outside of limitations of use) synchronized between mobile payment application 106 and issuer 108. '095 Provisional, Claims

9-10 (“a day of week; a time of day; an expiration date associated with a CAP token; an expiration date associated with a payment account; a merchant category corresponding to a point-of-sale (POS) terminal; a geographic location of a merchant; a spending limit for a payment account; a spending limit for a specified merchant category; and a spending limit for a duration.”); *Collinge*, [0143]-[0144] (“a chip authentication program (CAP) token”); *Dec.*, ¶¶193-94. A POSITA would have specifically been motivated to implement Collinge’s expiration date limits to ensure that transactions with expired credentials are not authorized and cardholders whose expired cards are obtained by bad actors are protected, and further would have been motivated to implement spending limits as it was well-known for payment accounts to include a credit limit, which limits exposure in the case of fraudulent transactions. *Dec.*, ¶193.

- 14. 15(h): wherein a card issuing authority is operable to validate generated limited-use payment information provided by the computing device in an authorized transaction completed by the computing device.***

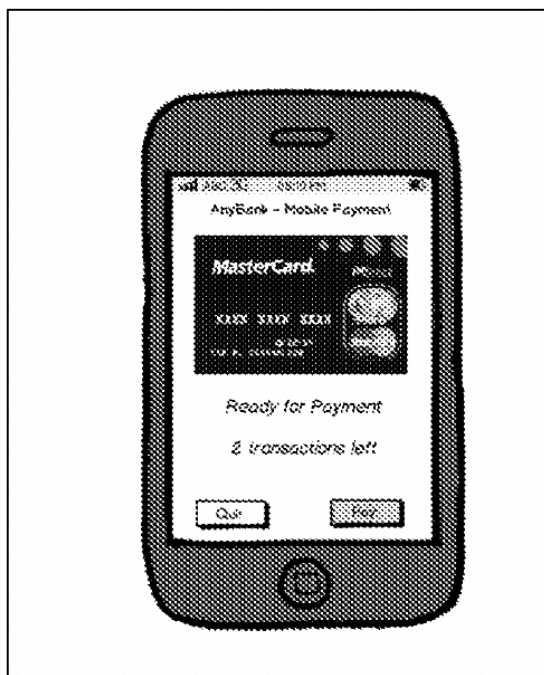
See Claim 15(f).

B. Claim 17

1. 17(a):⁸

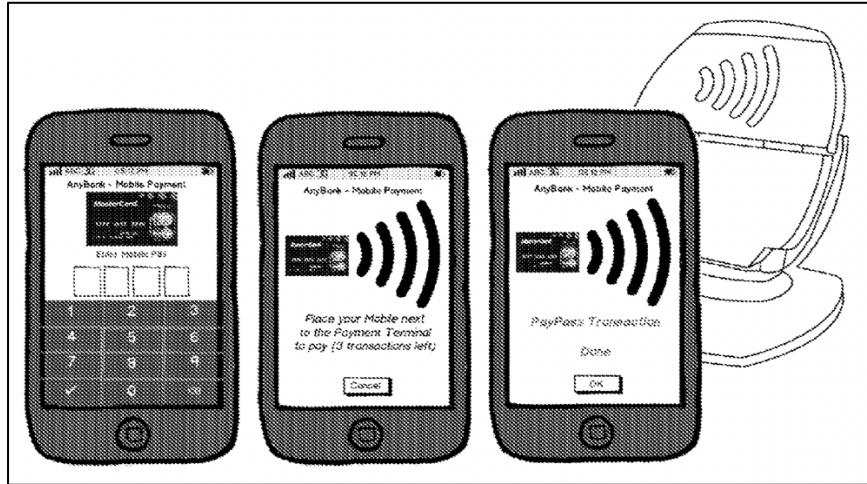
As discussed above, Collinge's touchscreen user interface is operable to accept a user approv[ing] (selecting a pay option) and deny[ing] (selecting “quit” or “cancel”) a payment transaction at a merchant facility (point-of-sale terminal).
See Claims 15(d), 11.

Collinge's mobile device is operable to display a merchant facility transaction:

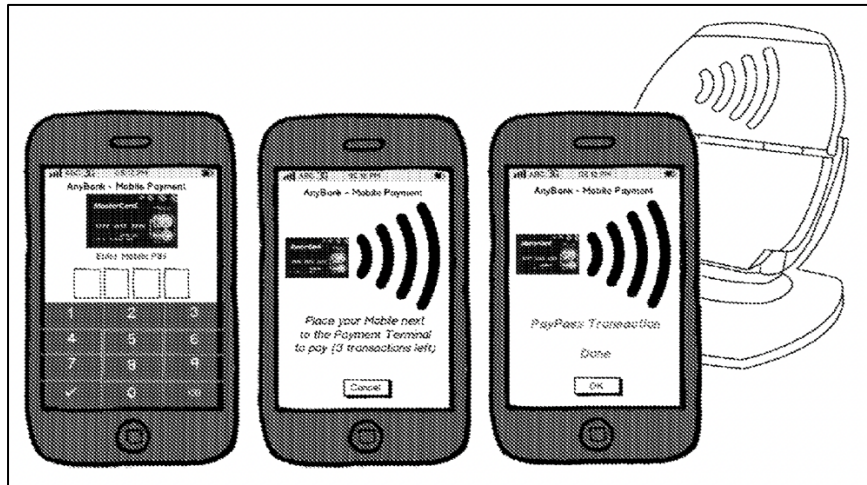


'098 Provisional, 100; '248 Provisional, Fig. 2B.

⁸ See Claim Listing Appendix.



'098 Provisional (Ex. 1008), 99; '248 Provisional (Ex. 1006), Fig. 2B.



'098 Provisional (Ex. 1008), 99; '248 Provisional (Ex. 1006), Fig. 2B. A POSITA would have understood that Collinge teaches a merchant facility transaction. *Collinge*, [0044] ("The mobile device 104 may be further configured to transmit a generated payment cryptogram and payment credentials to a point-of-sale terminal 120 at a merchant."); *Dec.*, ¶¶196-97.

2. Claim 17(b):

As discussed above, an issuer is operable to approve and deny card payment transactions. *See* Claim 15(g), (h).

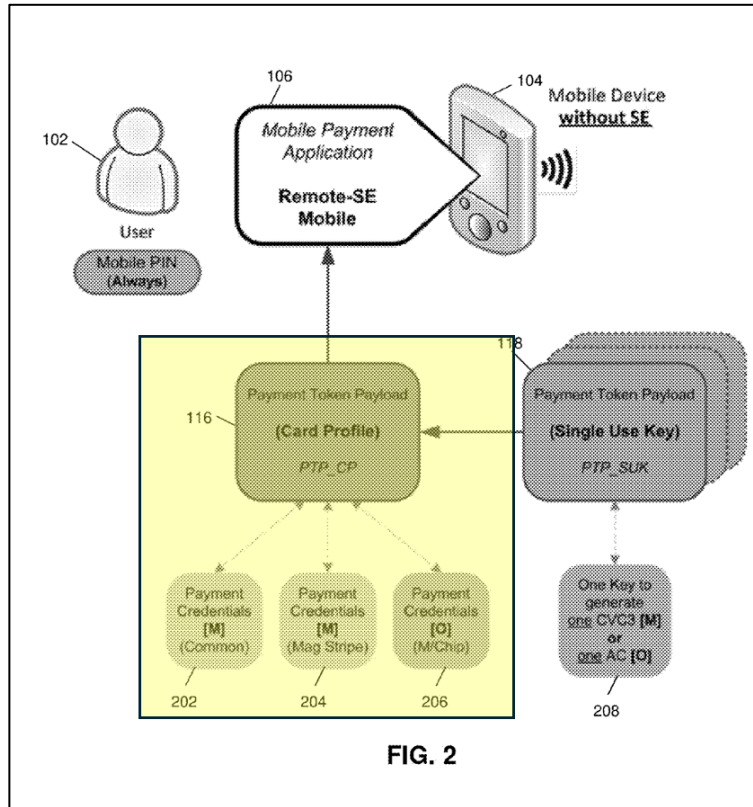
C. Claim 18

1. Claim 18(a):

Collinge teaches multiple card profiles (a plurality of issuer-provided payment information) are wirelessly downloaded into Collinge's mobile (personal computing) device. *Collinge*, [0074] (“the card profile 116 is ready to be downloaded to the mobile payment application 106.”).

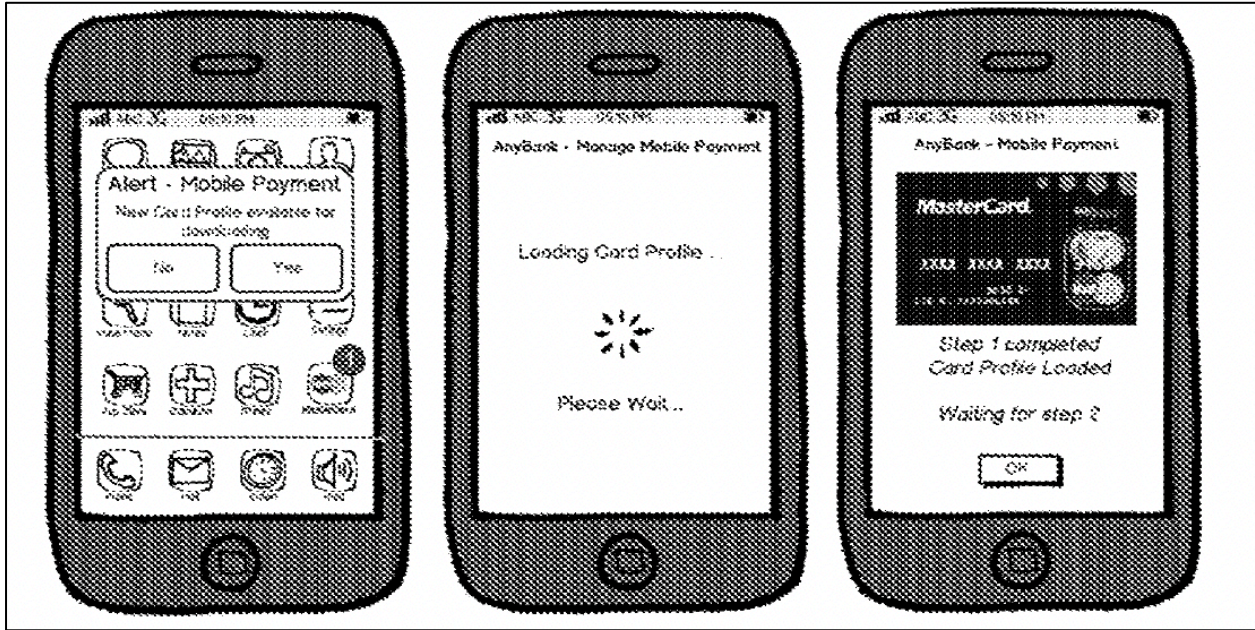
Each Collinge card profile includes a plurality of issuer-provided payment information such as the “PAN, PSN + Track Data[.]” ’098 *Provisional*, p.101; *Collinge*, [0127] (“the card profile 116 includes at least payment credentials corresponding to the associated payment account and a profile identifier.”).

Collinge teaches that a card profile includes multiple payment credentials. *Collinge*, Fig. 2; [0038], [0048], [0051] (referencing multiple card profiles).



Collinge, Fig. 2 (annotated); *Dec.*, ¶201.

Collinge teaches that “[t]he mobile payment application 106 may then...receive the card profile 116 from the remote-SE system.” *Collinge*, [0074]. Once the card profile is received *Collinge* “store[s] the received card profile 116 in the local encrypted database 304.” *Id.* *Collinge*’s “communications interface” “allow[s] software and data to be transferred between the computer system 1900 and external devices.” *Collinge*, [0154]. The “communications interfaces 1924 may include ...a network interface [.]” *Id.* *Collinge* teaches “[t]he network may be any network suitable for performing the functions as disclosed herein and may include...a wireless network...” *Collinge*, [0150].



'098 Provisional, 97.

2. **Claim 18 (b):**

See Claim 15(b)(3).

3. **Claim 18 (c):**

See Claim 15(d).

VI. GROUND 2: COLLINGE IN VIEW OF BONA, AND SMITH

A. Claim 1

1. **Claim 1(Pre):**

See Claim 15(Pre).

2. **Claim 1(a):**

See Claim 15(a).

3. **Claim 1(b):**

See Claim 15(b).

4. ***Claim 1(b)(1):***

See Claim 15(b)(5).

5. ***Claim 1(b)(2):***

See Claim 15(b)(4).

6. ***Claim 1(b)(3):***

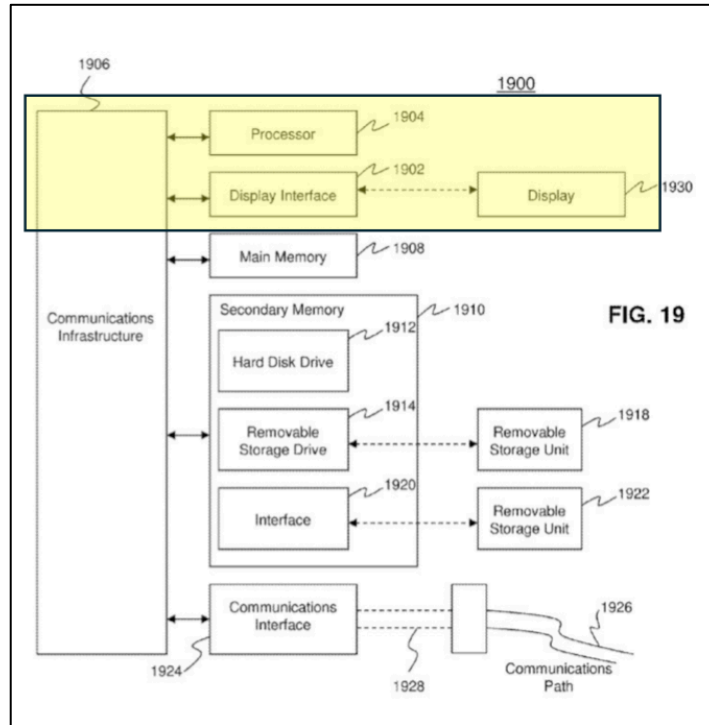
See Claim 15(b)(3).

7. ***Claim 1(c):***

Collinge teaches that the user-input device (e.g., touch screen) of Collinge's mobile device 104 is coupled to the processor. Collinge identifies the "touch screen" of "mobile device 104" as "an input device[.]" *Collinge*, [0133]. Collinge teaches that its touch screen receives a **user's input** of a "mobile personal identification number (PIN)" during generation of a payment cryptogram. *Id.*

Collinge further teaches that the touch screen of mobile device 104 is coupled to the processor. Collinge teaches that "at least one processor device" is used to implement Collinge's payment system. *Collinge*, [0147]. Collinge teaches and a POSITA would have understood that for the touch screen in Collinge's mobile device 104 to display information and receive and act on user input as taught by Collinge, the touch screen must necessarily be coupled to a processor. *Collinge*, [0147], Fig. 16; *Dec.*, ¶¶211-13.

Collinge teaches that the payment system comprises a display interface and display that is "coupled" to the processor via the communication interface:



Collinge, Fig. 19 (annotated). *Collinge* teaches that the communications infrastructure may be a “bus, message queue, network, multi-core message-passing scheme, etc.” *Collinge*, [0150]. *Collinge* teaches and a POSITA would have found it obvious that *Collinge*’s mobile device 104 would be implemented as the computer system 1900. Dec., ¶¶ 212. This figure teaches “the computer programs, when executed, enable the **processor 1604** to implement the processes of the present disclosure” including methods expressly taught as being carried out by “mobile device 104[.]” ’248 *Provisional* at [0246], [0017], [0048]. For this additional reason, *Collinge* teaches that a display interface (the touchscreen) is coupled to a processor. Dec., ¶¶214-16. A POSITA would have understood that *Collinge*’s display interface is *Collinge*’s touchscreen. Dec., ¶216.

8. Claim 1(d):

Collinge teaches an application transaction counter (ATC) (transaction sequence count) which is a “count of transactions used for fraud management and authentication[.]” *Collinge*, [0050]; *Dec.*, ¶217. Collinge teaches that the ATC is provisioned from the cloud system to the mobile device and stored in storage 304, “an encrypted local database.” *Collinge*, [0050], [0063], [0076], [0134].

Collinge teaches that its processor is operable to store an ATC (i.e., transaction sequence count) because Collinge’s ATC is stored in the storage 304 (encrypted local database) and at least transitorily stored by the processor when the application transaction counter is used by the mobile device to generate a cryptogram or dynamic card validation code to make a payment. *Collinge*, [0050], [0063], [0076], [0134]; *Dec.*, ¶¶218-221. Collinge teaches that the ATC is included in a single use key 118 and that the “single use key 118 may be a payment token used one time to generate a payment cryptogram to be used in a payment transaction.” *Collinge*, [0050]. Collinge teaches generating a CVC3 based on at least: “the supplied CVC3 value, the session key unpredictable number, the application transaction counter, and the reader unpredictable number.” *Collinge*, [0145].

9. Claim 1(d)(1):

The combination of Collinge and Smith teaches a device account number. *Dec.*, ¶¶222-27.

(a) Collinge's Teachings

Collinge teaches that its mobile device is provisioned with a “card profile” that includes “static payment credentials” that “are associated with a payment account[.]” *Collinge*, [0043], [0143]. Collinge teaches that the payment credentials include, for example, a primary account number (PAN). *Collinge*, [0049] (“payment account number”); *'098 Provisional*, p.101; *Dec.*, ¶228. Collinge’s card profile which includes the PAN is stored in the storage 304 (encrypted local database) and at least transitorily stored by the processor when the PAN is received by the mobile device and when it is used by the mobile device to make a payment. *Collinge*, [0048]-[0049], [0063], [0068]; *Dec.*, ¶246.

Collinge teaches that a virtual primary account number (VPAN) can be used as an alternative to the card PAN. *'098 Provisional*, 159-160. Collinge teaches that using a VPAN is safer and can “mitigate the risk of any misuse of a PAN value” but provides limited implementation details. *'098 Provisional*, 159-160; *Dec.*, ¶¶229-31.

(b) Smith's Teachings

In related art, Smith (also assigned to MasterCard) teaches a “mobile device” that “may...be used...with a near field communications enabled purchasing transaction.” *Smith*, Abstract. Whenever a user wishes to open a payment account, the issuer issues a “temporary PAN...and establishes any risk parameters (e.g., for

use in controlling the authorization of transactions involving the temporary PAN)” so the user is able to make purchases while awaiting an actual PAN. *Smith*, [0026].

This “temporary PAN is mapped to a **mobile PAN (e.g., such as a PayPass® PAN, or PPAN).**” *Smith*, [0026] (emphasis added). The PPAN (device account number) is “assigned to the mobile device 104.” *Smith*, [0016]. The PPAN is “stored in the mobile device 204.” *Smith*, [0022]. The PPAN is, therefore, a *device* account number. *Dec.*, ¶¶232-35.

Once an actual PAN is issued, the temporary PAN is swapped with the actual PAN. *Smith*, [0026], [0040]. The PPAN (device account number) is then associated with a “related PAN[.]” *Smith*, [0023]. The PPAN is “initially...mapped to the temporary PAN” but whenever the issuer issues the “actual PAN” the actual PAN “replace[s] the temporary PAN” so the PPAN is now an alternate number mapped to the actual PAN. *Smith*, [0040]; *Dec.*, ¶234. The PPAN is a different number from the actual PAN. *Id.*, *Dec.*, ¶234.

600

CONSUMER ID 602	TEMPORARY PAN 604	MOBILE PAN 606	ACTUAL PAN 608	RISK PARAMETER RESTRICTION(S) 610
C1001	T-PAN_0001	M-PAN_0001	NONE	NONE
C1002	T-PAN_0002	M-PAN_0002	NONE	NO TRANSACTIONS OVER \$10
C1003	T-PAN_0003	M-PAN_0003	NONE	OVERALL TRANSACTION UNDER \$100
C1004	T-PAN_0004	M-PAN_0004	NONE	NO ONLINE TRANSACTIONS
C1006	NONE	M-PAN_0006	A-PAN_0001	NONE

FIG. 6

Smith, Fig. 6. During a transaction “the point of sale device is provided with information including the PPAN stored in the mobile device 204” by using NFC. *Smith*, [0022]. Once the PPAN is sent the “payment network 218 identifies the PPAN and requests a look up of the related PAN from the PAN mapping/account generation service 210.” *Smith*, [0023].

The issuer can “implement dual account number structures” for “multiple NFC-enabled handsets may be managed for a single account.” *Smith*, [0029]. It was well known that a dual account number has separate and distinct numbers for each device an account is used with. *Dec.*, ¶237. Accordingly, *Smith*’s PPAN is a distinct account number for a payment account on a particular “mobile device.” *Dec.*, ¶237.

Even if the same user wants to register a new device, a user will get a different PPAN for that device to use because the PPAN is assigned immediately upon registering the device. *Smith*, [0026] (“an instantly-issued payment account that may be used by the customer almost immediately after submitting a request for a new payment account.”); *Dec.*, ¶238.

Smith’s PPAN is a static number; Smith teaches the expiration date associated with the account may be updated without updating the PPAN. *Smith*, [0041] (“update an NFC-enabled payment account (e.g., to update an expiration month and/or year”) Therefore, a POSITA would have understood that Smith’s PPAN is static. *Dec.*, ¶239.

(c) Motivation to Combine

A POSITA would have found it obvious and been motivated to use Smith’s PPAN in place of Collinge’s PAN in Collinge’s payment credential, akin to the Virtual PAN already taught by Collinge. *'098 Provisional*, 159-160; *Dec.*, ¶¶240-49.

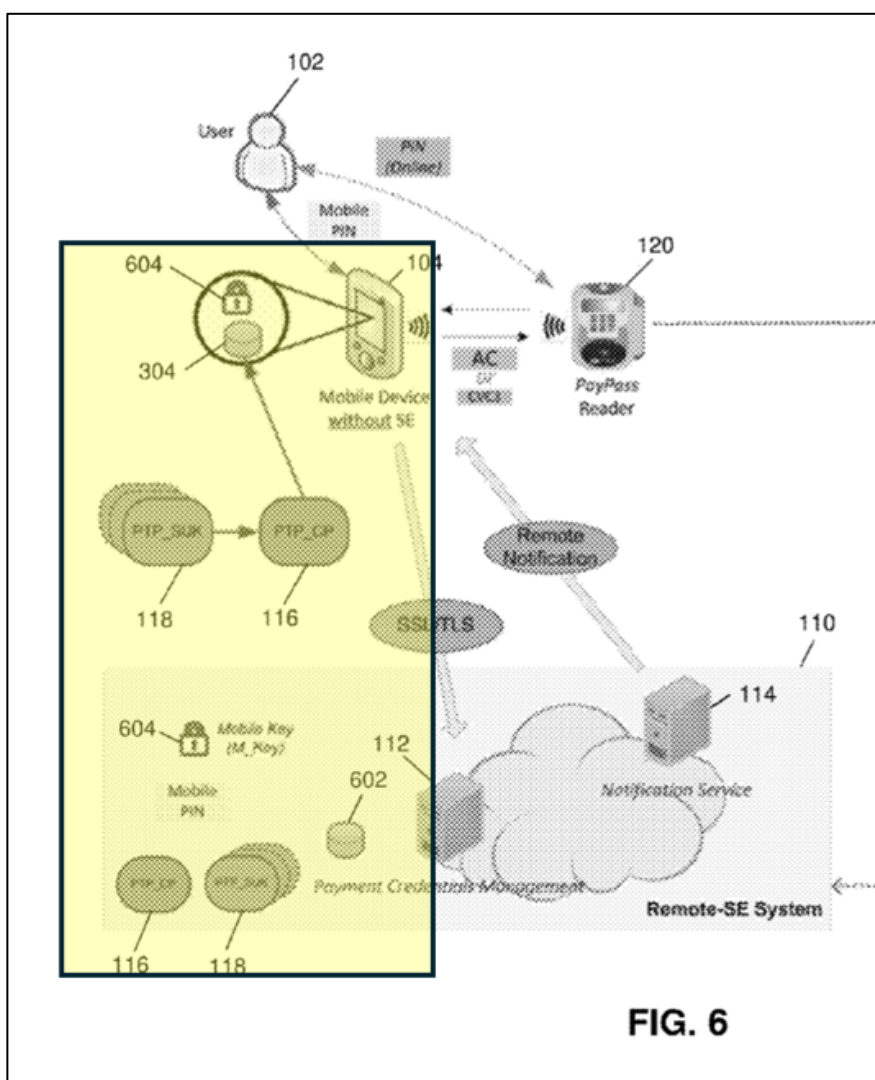
A POSITA would have been motivated to use Smith’s PPAN in place of Collinge’s PAN so that Collinge’s mobile device would not be required to store the PAN, which is a sensitive financial number. *Dec.*, ¶242. It was well known in the art that a device without a secure element (SE), such as Collinge’s mobile device, could be vulnerable to malicious attacks and therefore storing Smith’s PPAN instead of

the PAN on Collinge's mobile device would have increased security for the user's account. *Dec.*, ¶243. For example, a POSITA would have understood that it is valuable to remove all traditional payment device account numbers from a user device so that if the device were stolen, the thief would have access only to PayPass PAN(s). *Bona*, [0074]; *Dec.*, ¶243. A POSITA would have recognized that this is beneficial because if a user's device is lost or stolen, only the PPAN(s) would have to be cancelled; automatic transactions using the traditional payment credentials (such as the credit card PAN) would not be impacted. *Dec.*, ¶243; *Bona*, [0007], [0014], [0074], Fig. 6.

A POSITA would have had a reasonable expectation of success in implementing Smith's PPAN in Collinge's mobile payment application without undue experimentation because Collinge already teaches use of a Virtual PAN and a POSITA would have been familiar with using PAN-alternatives, particularly when making mobile PayPass payments. *Dec.*, ¶244. In the combination, Smith's PPAN would perform the same function—provide an alternative account number that can be used for a payment transaction. *Dec.*, ¶244; *Smith*, [0023]. A POSITA would have understood that using Smith's PPAN in place of Collinge's PAN would be combining prior art elements according to known methods to yield the predictable result of increased security. *Dec.*, ¶244. A POSITA would have been motivated to apply Collinge and Smith's teachings and appreciated the compatibility of their

teachings because both discuss payment systems that rely on MasterCard PayPass functionalities. *Dec.*, ¶244.

In the proposed combination of Collinge and Smith, Collinge's mobile device would receive the assigned PPAN(s) taught by Smith, in place of PAN information in Collinge's payment credentials provisioned to the mobile payment application as part of Collinge's card profile 116. *Collinge*, [0048], Fig. 6, [0104] (card profile (PTP_CP)); '098 *Provisional*, p.101 ("Payment Token Payload – Card Profile (PTP_CP_ contains the Payment Credentials required to perform a [MasterCard] *PayPass* transaction" including "data elements such as: **PAN**, PSN + Track Data."); *Dec.*, ¶245.



Collinge, Fig. 6 (annotated excerpt).

Smith's PPAN would then be stored in Collinge's storage 304 within the card profile as a replacement for Collinge's PAN and in the same manner that Collinge's PAN was stored. *Collinge*, [0068]; *Smith*, [0022] (The PPAN is "stored in the mobile device 204. "). The PPAN would also be at least transitorily stored by Collinge's processor when received by Collinge's mobile device and when it is used by Collinge's mobile device to make a payment. *Collinge*, [0048]-[0049], [0063]; *Dec.*,

¶246 (discussing use of the PPAN when generating a payment cryptogram). It was well known in the art that storing sensitive information such as a PAN in fewer locations can lessen the risks of the sensitive information being compromised. *Dec.*, ¶247.

Likewise, a POSITA would have substituted Smith's PPAN for Collinge's PAN when making payment transactions, as taught by Smith. *Smith*, [0018] ("the process of personalizing the mobile device 104 with the software (including the PPAN...[o]nce the personalization or loading of the payment application is complete, the customer 102 may use the mobile device **104** to complete payment transactions"); *Dec.*, ¶248. A POSITA would again have recognized that substitution of a PayPass PAN would have increased security since sensitive information like a PAN would therefore not be transmitted. *Smith*, [0023] ("the payment network 218 identifies the PPAN and requests a look up of the related PAN"); *Dec.*, ¶248. Smith already teaches using "the PayPass® standard" when completing a transaction where "the point of sale device is provided with information including the PPAN stored in the mobile device 204" by using NFC. *Smith*, [0022].

The simple substitution of Collinge's PAN with Smith's PPAN is a substitution of one known element for another and a POSITA would have understood that the substitution would have predictably increased the security of Collinge's payment system and protected the user's sensitive PAN information.

Dec., ¶249. Likewise, the same simple substitution would have predictably allowed the POSITA to provision Smith's PPAN to Bona's payment card device in place of the PAN to better protect sensitive financial information. *Dec.*, ¶249.

10. Claim 1(d)(2):

Collinge's processor is operable to store a local storage encryption key, unique identifier, single use key, and key request (secrets limited to the computing device). *Dec.*, ¶¶250-59.

Collinge's local storage encryption key is "generated by the mobile payment application" and used to "provide the storage 304 as an encrypted local database." *Collinge*, [0063]. Collinge's mobile payment application also generates "a unique identifier and additional values and keys, such as a local database storage key (e.g., mobile storage key)." *Collinge*, [0093]. Collinge's mobile device also generates a "key request, wherein the key request includes at least a mobile identification number (PIN) and the profile identifier." *Collinge*, [0011]. A POSITA would have understood those values (secrets) are limited to Collinge's computing device. *Collinge*, [0093], [0062], [0099]; *Dec.*, ¶¶251-52.

Collinge's "local storage encryption key", "unique identifier", and "key request" are therefore private information (secrets). *Dec.*, ¶¶251, 253, 255. Collinge's local storage encryption key, unique identifier, and key request are

likewise limited to the computing device because they are generated by Collinge's mobile device. *Dec.*, ¶¶251, 253, 255.

Collinge is provisioned a single use key that “includes at least the profile identifier, an application transaction counter, and a generating key for use in generating a payment cryptogram” by Collinge's “mobile payment application” *Collinge*, [0011], [0070]. Collinge's single use key and the components within the single use key, are likewise limited to the computing device because the single use key is used by Collinge's “mobile payment application” for generating a payment cryptogram. *Collinge*, [0011], [0070], [0145].

Collinge teaches the processor is operable to store secrets limited to the computing device (e.g., local storage encryption key) because Collinge's local storage encryption key is stored in memory (storage 304) and at least transitorily stored by the processor when the local storage encryption key is used by the mobile device to encrypt the storage 304 as an encrypted local database. *Collinge*, [0067]; *Dec.*, ¶259. Collinge also stores “the single use key 118 in the local encrypted database 304.” *Collinge*, [0076]. Collinge's single use key is at least transitorily stored by the processor when the single use key is used by the mobile device to generate a payment cryptogram. *Collinge*, [0011], [0070]; '248 *Provisional*, Table 1; *Dec.*, ¶259. Since Collinge's device generates the key request and unique identifier a POSITA would have understood that those values must be at least

transitorily stored by the processor when generated by the mobile device. *Collinge*, [0011], [0093]; *Dec.*, ¶259.

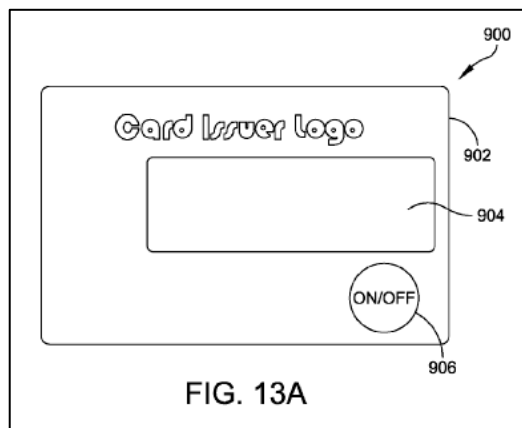
11. Claim 1(e):

As discussed above, (Section C.1, *supra*), the limitation “card payment information not visible on the payment card device” is directed to printed matter that has no functional or structural relationship to the claimed card device and is entitled to no patentable weight. *Dec.*, ¶260. Nevertheless, the combination of Bona and Collinge renders this limitation obvious.

In the combination of Collinge and Bona, Collinge’s mobile device receives, stores, and transmits card payment information (Collinge’s payment credentials (as modified by Smith to include a PayPass PAN in place of the PAN) and Collinge’s ATC), not visible on the payment card device (Bona’s companion card 900).

(a) Bona’s Teachings

As described above at claim 1(a), when Bona’s card is off, there is no information on the display of the payment card device as shown below in Figure 13A. *Bona*, [0110] (“The smart card includes an on/off button 906 for powering the smart card on/off and a display 904 for displaying information to the user.”).

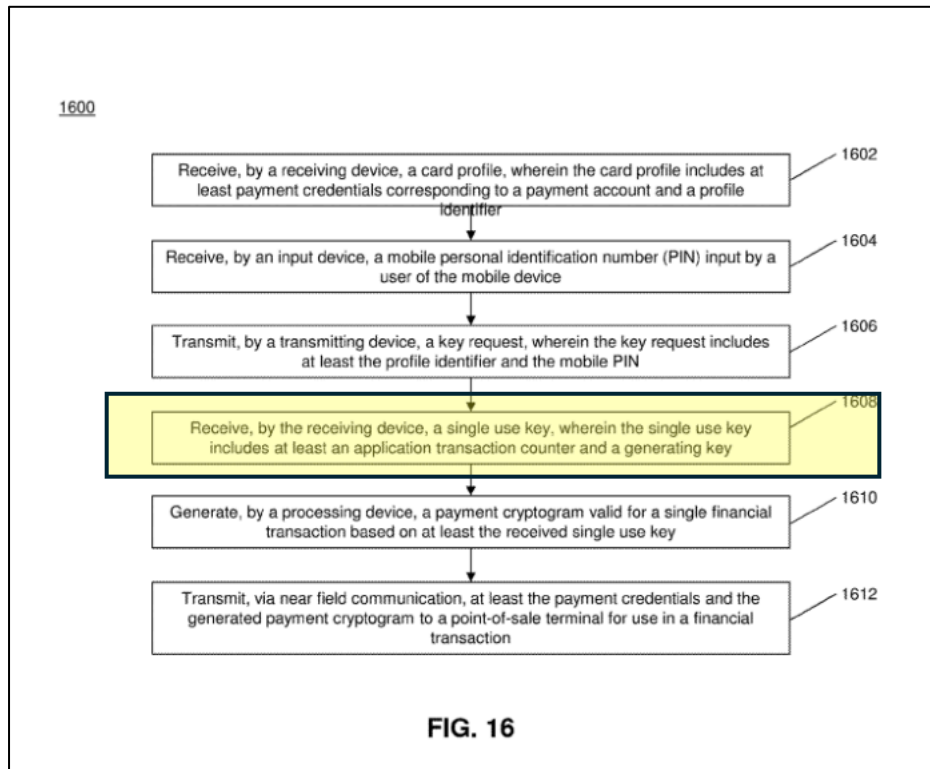


Bona, Fig. 13(a). Further, *Bona* teaches transmission of only “necessary data for display on the NFC enabled companion card 900 for use in the transaction” and a POSITA would have understood that showing payment information on the face of *Bona*’s card is not necessary when conducting a magstripe transaction. *Bona*, [0109]; *Dec.*, ¶262; *see also* claim 1(a).

(b) Collinge’s Teachings

Collinge’s mobile device receives, stores and transmits a card payment information not visible on *Bona*’s payment card device, including payment credentials and an ATC.

Collinge’s mobile device receives “**payment credentials**” and an “**application transaction counter**” from “the remote-SE system[.]” *Collinge*, [0068] (emphasis added), [0134]; Fig. 16; *Dec.*, ¶¶264, 267-68.



Collinge, Fig. 16 (annotated).

Collinge’s mobile device stores “**payment credentials**” and a single use key which includes an **application transaction counter** in “...the storage 304[.]” *Collinge*, [0063] (emphasis added), [0076], [0134]; *Dec.*, ¶¶265, 267-68.

Collinge’s mobile device transmits “the generated cryptogram and **payment credentials** to a point-of-sale terminal 120.” *Collinge*, [0070] (emphasis added); *Dec.*, ¶266-68. *Collinge* also teaches that “the **application transaction counter** may be transmitted, via near field communication, to the point-of-sale terminal 120 for including in an authorization request in a financial transaction.” *Collinge*, [0145].

(c) Motivation to Combine

See Claim 1(a).

12. Claim 1(f):

See Claim 15(c).

13. Claim 1(g):

See Claim 15(d).

14. Claim 1(h):

See Claim 15(g).

15. Claim 1(i):

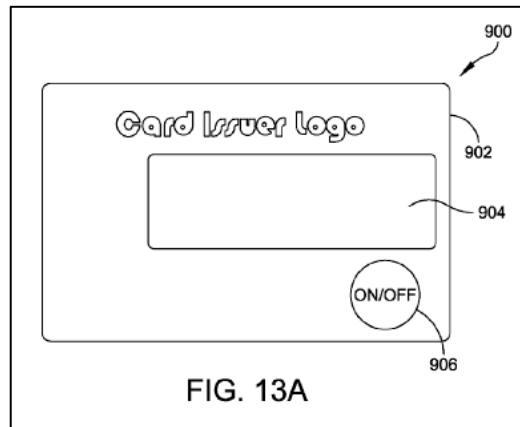
See Claim 15(h).

16. Claim 1(j):

As described above, Collinge teaches that a transaction from a valid user within the limitations of use of the payment method (authentic transactions) will be approved by the issuer 108 (card issuer authority) and permit[ted]...to complete. See Claim 1(i). Collinge teaches that issuer 108 validates the payment cryptogram and if validation/authentication is successful “approve the payment transaction” or if validation/authentication is unsuccessful, the may “deny the payment transaction.” Collinge, [0077]; Dec., ¶¶274-75.

B. Claim 5

Collinge, in view of Bona, renders obvious a payment card device (Bona’s companion card 900) without any information on the display (absent a payment number information) and with magstripe transaction information limited to use in an in-store transaction. See Claim 1(e); Bona, [0109].



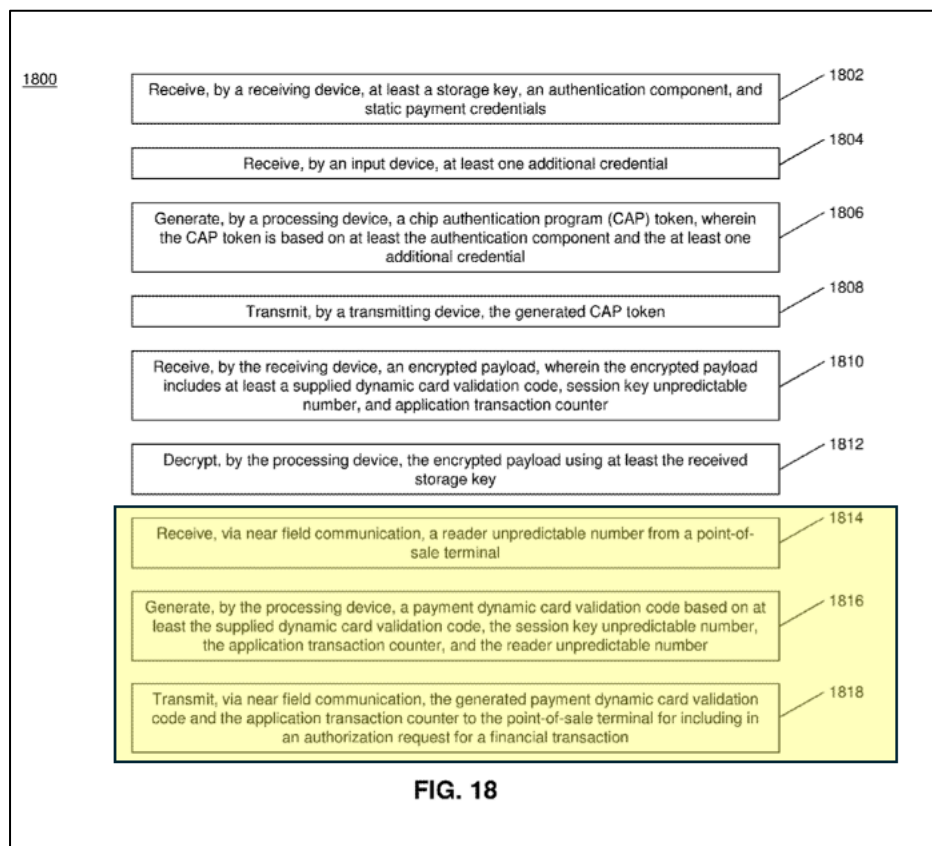
Bona, Fig. 13(a).

For example, Collinge’s mobile device receives “a reader unpredictable number...via near field communication, from a point-of-sale terminal (e.g., the point-of-sale terminal 120).” *Collinge*, [0145]. As discussed above, Collinge generates the CVC3 based in part on a reader unpredictable number. *See* Claim 1(f). A POSITA would have understood Collinge’s CVC3 is limited to an in-store transaction and therefore the information Bona’s companion card 900 presents during a magnetic stripe transaction is limited to an in-store merchant card reader facility use only (e.g., magnetic card reader). *Dec.*, ¶277. Bona teaches transmission of only “necessary data for display on the NFC enabled companion card 900 for use in the transaction” and a POSITA would have understood that showing payment information on the face of Bona’s card is not necessary when conducting a magstripe transaction. *Bona*, [0109]; *Dec.*, ¶278; *see also* claim 1(a).

C. Claim 8:

Collinge teaches transceiving the payment cryptogram (*limited-use payment information*) via Collinge's NFC interface in an in-store NFC reader facility transaction. *See* Claim [1(k)].

Collinge further teaches receiving a reader unpredictable number (UN_{READER}) from a “point-of-sale terminal” via “near field communication” which is then used to generate the payment cryptogram (e.g., CVC3 value). *Collinge*, [0145].



Collinge, Fig. 18 (annotated).

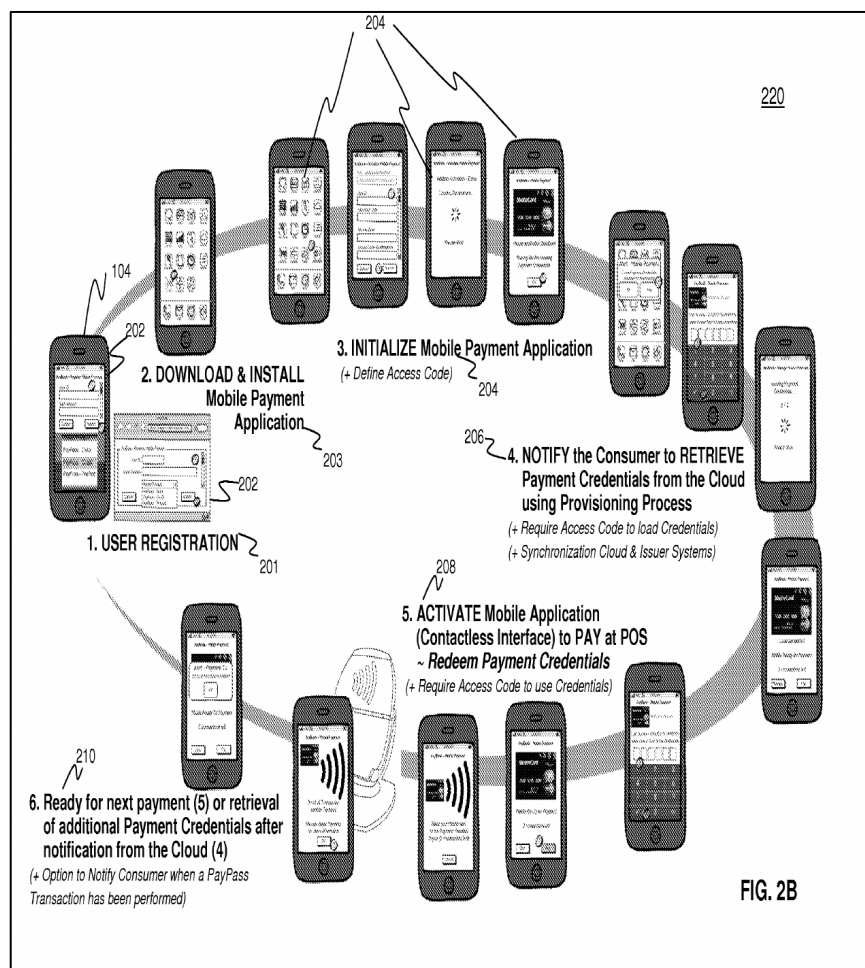
D. Claim 11

1. Claim 11(a):

Collinge's touchscreen user interface is operable to accept a user approving (selecting a pay option) and denying a payment transaction (canceled payment) from a user approved facility transaction (point-of-sale terminal).

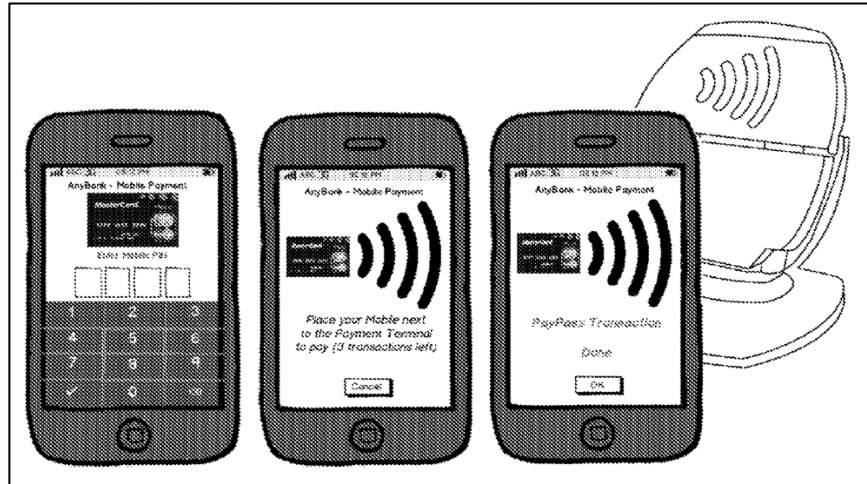
(a) Collinge's Teachings

As discussed in Claim 1(b)(3)-1(c), Collinge's touch screen is a user interface:



'248 Provisional, Fig. 2B(excerpt).

Collinge's user interface instructs the user to provide a pin and then "Place your Mobile next to the Payment Terminal to pay":



'098 Provisional, 99; Dec., ¶282; see Claim [15(d)].

Collinge teaches that the user may cancel (deny) the NFC transaction.



'098 Provisional, 99; '248 Provisional, Fig. 2B (annotated excerpt); Dec., ¶283.

Collinge further teaches the user may "quit" or "pay" during a transaction.



'098 Provisional, 100; '248 Provisional, Fig. 2B. A POSITA would have further understood that by selecting “pay” a user would approve the transaction and by selecting “quit” the user would deny the transaction. *Dec.*, ¶284.

2. Claim 11(b):

Collinge teaches that a transaction is approved as authentic when a user provides an accurate mobile PIN and denied as inauthentic when an incorrect mobile PIN is provided. *See* Claim 1(i)-1(j).

E. Claim 14

Collinge in view of Bona teaches that the payment issuing authority can decline transactions performed by Bona's companion card 900 (payment card device) when a user fails a security challenge presented to a user by Collinge's mobile device (e.g., a request for a mobile PIN).

(a) Bona’s Teachings

Bona teaches that “the user is authenticated, such as using biometrics if the cell phone (or smart card) has biometric capabilities or a PIN or password authentication scheme.” *Bona*, [0120].

(b) Collinge’s Teachings

Collinge teaches that a payment issuing authority can decline transactions when a user fails to accurately “provide a mobile PIN for authentication” via “an input device (e.g., of the mobile device 104, such as a touch screen)[.]” *Collinge*, [0051], [0076]-[0077], [0133].

(c) Motivation to Combine

It would have been obvious and a POSITA would have been motivated to decline a transaction performed by Bona’s companion card where the user input an incorrect mobile PIN on Collinge’s mobile device. *Dec.*, ¶289. Collinge and Bona both expressly teach requiring user authentication with a PIN. *Bona*, [0120]; *Collinge*, [0051], [0076]-[0077]. Collinge teaches that in the case of an incorrect PIN, the issuer would “not authorize” the transaction. *Id.* Collinge and Bona teach and it would have been well-known to a POSITA that in a secure payment system, an unauthenticated user should not be permitted to make any payment via card or via the mobile device. *Dec.*, ¶289-90.

A POSITA would have had a reasonable expectation of success implementing Collinge’s teaching of an issuer declining a payment transaction when an incorrect

PIN is entered to payment transactions conducted using Bona's companion card because in either case the issuer receives payment information indicating that the PIN-based authentication challenge failed. *Dec.*, ¶290. Such an application of Collinge's teachings would have predictably improved the security of Bona's card. *Id.*

F. Claim 20

1. Claim 20(Pre)

See Claim 1(Pre).

2. Claim 20(a):

See Claim 1(a).

3. Claim 20(b):

See Claim 1(b).

4. Claim 20(b)(1):

See Claim 1(b).

5. Claim 20(b)(2):

See Claim 1(b)(1).

6. Claim 20(b)(3):

See Claim 1(b)(2).

7. Claim 20(b)(4):

See Claim 1(b)(3).

8. Claim 20(b)(5):

See Claim 1(c).

9. Claim 20(c): wherein the memory is operable to store a transaction sequence count, a static device account number and secrets limited to the computing device;

In the combination, Collinge stores an ATC (transaction sequence count), PPAN (static device account number) and a local storage encryption key, unique identifier, single use key, and key request (secrets limited to the computing device) in Collinge's memory (storage 304). See Claims 1(d), 1(d)(1), and 1(d)(2).

10. Claim 20(d):

See Claim 1(e). A POSITA would have understood that Collinge's payment credentials (modified by Smith to include a PPAN in place of the PAN) comprise issuer-provided payment information. 300Smith's PPAN is assigned by the issuer and is issuer-provided payment information. *Smith*, [0012], [0016]; *Dec.*, ¶300.

11. Claim 20(e):

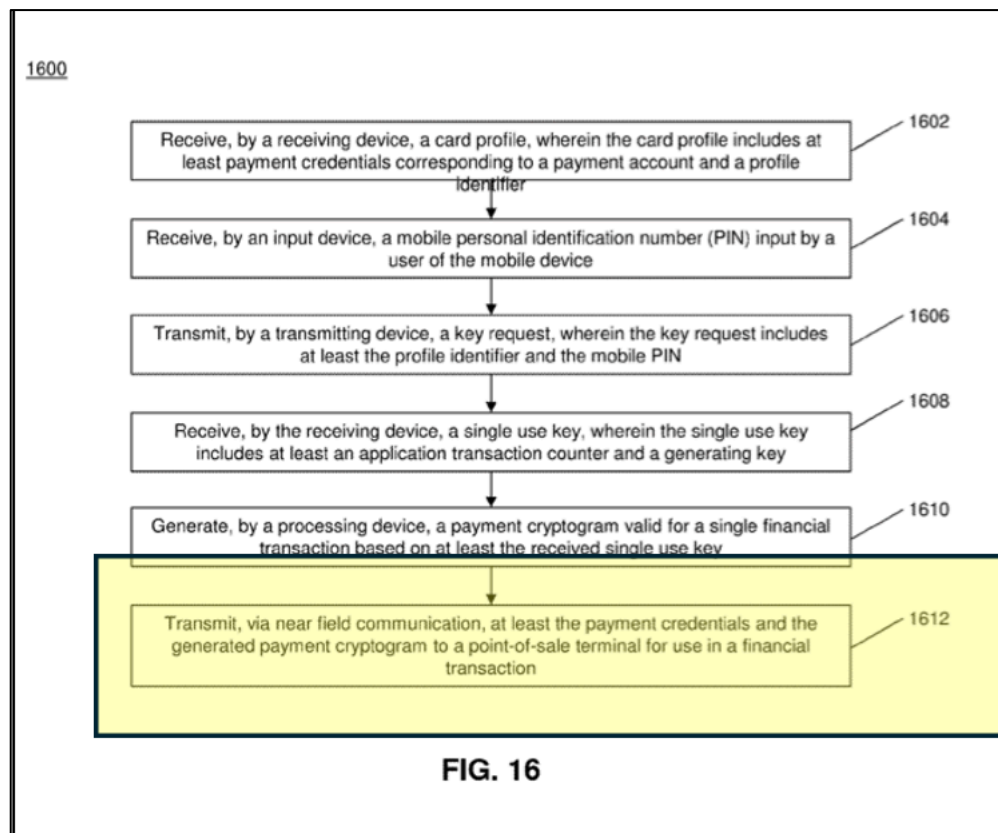
See Claim 1(f).

12. Claim 20(f):

Collinge, in view of Smith, renders obvious creating combined payment information, including a CVC3 (limited-use payment information) and PPAN (static device account number) when sending complete payment information to a POS terminal via Collinge's NFC interface. See Claims 1(d)(1).

Collinge teaches generating limited-use payment information (payment cryptogram/CVC3). *See* Claim 1(f).

As shown below, Collinge teaches sending the dynamically generated CVC3 and payment credentials (which include the PAN, among other items) to a point-of-sale terminal in a payment transaction. *Collinge*, [0070], [0077].



Collinge, Fig. 16 (annotated); *Collinge*, [0048], Fig. 6, [0104] (card profile (PTP_CP)); '098 *Provisional*, 101 (“Payment Token Payload – Card Profile (PTP_CP_ contains the Payment Credentials required to perform a [MasterCard] *PayPass* transaction” including “data elements such as: **PAN**, PSN + Track Data.”).

Therefore, Collinge in view of Smith teaches combining a CVC3 (limited-use payment information) and PPAN (static device account number) to create combined payment information which is collectively transmitted via NFC to a point-of-sale terminal for use in a financial transaction at step 1612. *Dec.*, ¶304.

(a) Motivation to Combine

As discussed above, Smith's PPAN would be used instead of a PAN in Collinge's payment system. *Dec.*, ¶305; *see* Claim 1(d)(1).

13. Claim 20(g):

See Claim 20(f).

14. Claim 20(h):

See Claims 1(i)-1(j).

G. Claim 21

See Claim 7.

H. Claim 22

Collinge teaches generating the payment cryptogram (a dynamic single-use CVC3) using an application transaction counter (transaction sequence counter count). *See* Claims 1(j)-1(k).

I. Claim 23

As discussed above, Collinge teaches that the payment cryptogram (limited-use payment information) is generated by the processor of Collinge's mobile phone based, in part, on a ATC, UN_{CLOUD} , and the KS_{UN} (secrets). *See* Claim 1(f). Collinge

further teaches that the ATC, UN_{CLOUD} , and the KS_{UN} (secrets) are shared with an issuer (payment processing authority). *Dec.*, ¶310.

As discussed in Claim 1(i), the issuer uses the ATC, UN_{CLOUD} , and the KS_{UN} to authenticate the payment cryptogram. *Collinge*, [0077], [0145]. Therefore, these values are also issuer secrets (payment processing authority secrets). *Dec.*, ¶311.

J. Claim 24

See Claim 20(k).

K. Claim 25

See Claim 21.

L. Claim 26

See Claim 20(k).

M. Claim 27

See Claim 21.

VII. GROUND 3: COLLINGE IN VIEW OF BONA, SMITH, AND PATTERSON

A. Claim 2

As discussed above, *Collinge*, in view of *Bona*, teaches that the touch-screen user interface of *Collinge*'s mobile device is used to (1) control the provisioning of payment credentials to *Bona* (control access for payment transactions) (*Bona*, [0123], Fig. 12) and (2) authenticate payment transactions using, for example, a PIN

or password. *Bona*, [0120]; *Collinge*, [0093], [0123]. *See* Claims 15(c)-(d), and 14; *Dec.*, ¶316.

Alternatively, Collinge-Bona in view of Patterson teaches Collinge's touch-screen user interface is operable to control access for payment transactions by Bona's companion card (card device) by applying blocking criteria.

(a) Bona's Teachings

As discussed in Claim 15(a), Collinge's mobile device allows Bona's companion card to perform a transaction by provisioning Bona's payment card payment credentials and a payment cryptogram. As discussed in Claim 14, Collinge in view of Bona teaches that the payment issuing authority (issuer) can decline transactions performed by Bona's companion card 900 (payment card device) when a user fails a security challenge presented to a user by Collinge's mobile device (e.g., a request for a mobile PIN). Therefore, if the PIN is validated, the transaction is authentic. *See* Claim 1(f); 14; 15(c); *Dec.*, ¶319.

(b) Patterson's Teachings

Patterson teaches that through a registration process, the user "may then specify blocking criteria to be associated with one or more accounts." *Patterson*, 6:17-27. The registration process may take place on a "client computer" such as "a wireless phone. *Id.*, 3:51-53.

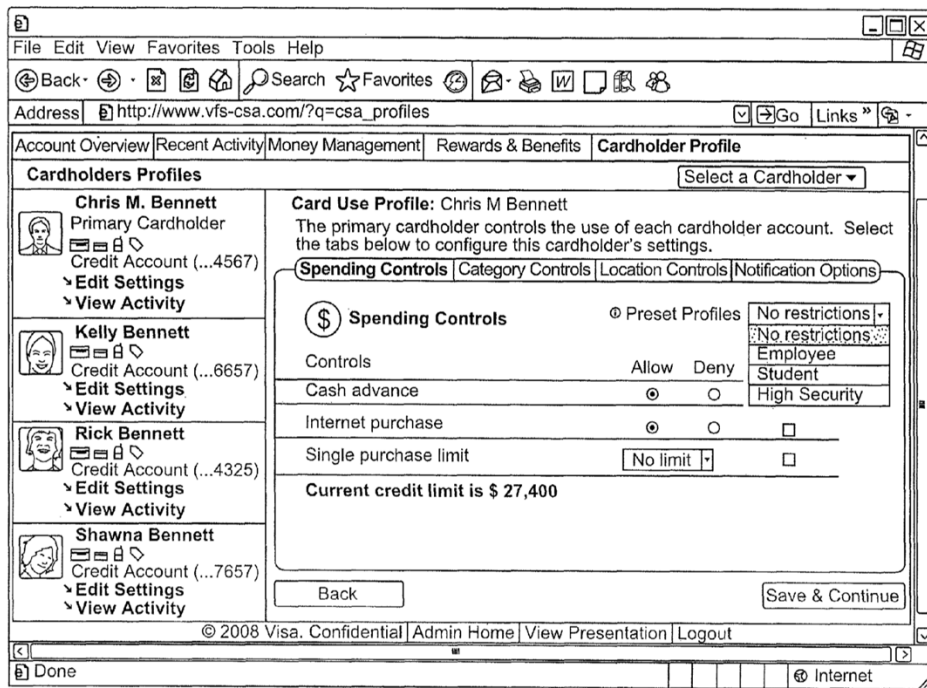


FIG. 8

Patterson, Fig. 8. *Patterson* notes that:

Blocking criteria may include ... payment channel (e.g., face-to-face, card not present, e-commerce), terminal ID (e.g., deny transactions that originate from specific terminals), transaction type (e.g., cash, POS purchase, quasi-cash, account funding transaction (AFT), original credit, payment), lost or stolen card (e.g., a “hotcard” list which will block all transactions from that card from being authorized)[.]

Patterson, 6:28-46. A POSITA would have understood that a card designated as “lost or stolen” would be locked, as *Patterson* teaches that the issuer “will block all transactions from that card from being authorized.” *Patterson*, 6:38-40; *Dec.*, ¶321.

Likewise, terminal ID and transaction type restrictions control an access for payment transactions by the card device. *Dec.*, ¶321

When a user attempts to perform a transaction, the transaction request will be “den[ied], using the server computer” (issuer), “if the transaction satisfies the stored blocking parameter.” *Patterson*, Abstract, 4:35-38.

(c) Motivation to Combine

It would have been obvious, and a POSITA would have been motivated to modify Collinge’s payment system to allow a user to input blocking criteria for payment cards using Collinge’s touchscreen (such as during Collinge’s registration process), as taught by Patterson. *Dec.*, ¶323-25. A POSITA would have been further motivated to have Collinge’s issuer deny a transaction if “the transaction satisfies the stored blocking parameter” as proposed by Patterson. *Patterson*, 4:35-38; *Dec.*, ¶324. Collinge already suggests assigning control limits on purchases, but provides limited details on how they would be applied. *’095 Provisional*, Claims 9-10; *Dec.*, ¶325. A POSITA would have recognized that applying blocking criteria is useful to users who want to prevent overspending (by themselves or children), reduce fraud by preventing purchases on stores they do not frequent, or temporarily lock a card that may be stolen, or may be simply misplaced (rather than wholly cancel the card). *Dec.*, ¶325. Modifying Collinge’s payment system to include Patterson’s blocking criteria would have been combining prior art elements according to known methods

to yield the predictable result of increased security in Collinge's payment system and a POSITA would have had a reasonable expectation of success in making such a modification. *Dec.*, ¶325.

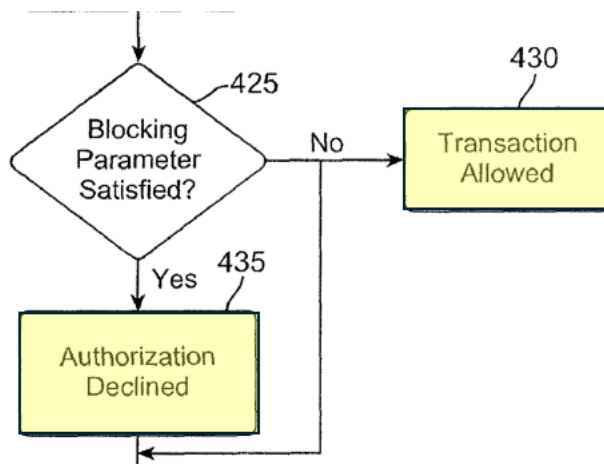
B. Claim 3

See Claim 2; *Patterson*, 6:28-46 (blocking criteria is “payment channel (e.g., face-to-face, card not present, e-commerce)” and “terminal ID (e.g., deny transactions that originate from specific terminals)[.]”

C. Claim 4

Collinge-Bona as modified by *Patterson* teaches applying blocking criteria (locking and unlocking payment transactions) through the touch-screen user-interface of Collinge's mobile device and that the card issuer authority will deny[] a payment transaction based on the blocking criteria (from a locked card device). *See* Claim 2.

In the combined system, if Bona's card is unlocked (e.g., has no associated blocking criteria), a card issuer authority permits as authorized, a card payment transaction. *See* Claims 1(i)-1(j); *Dec.*, ¶¶327-28; *Patterson*, Fig. 4.



Patterson, Fig. 4 (annotated excerpt).

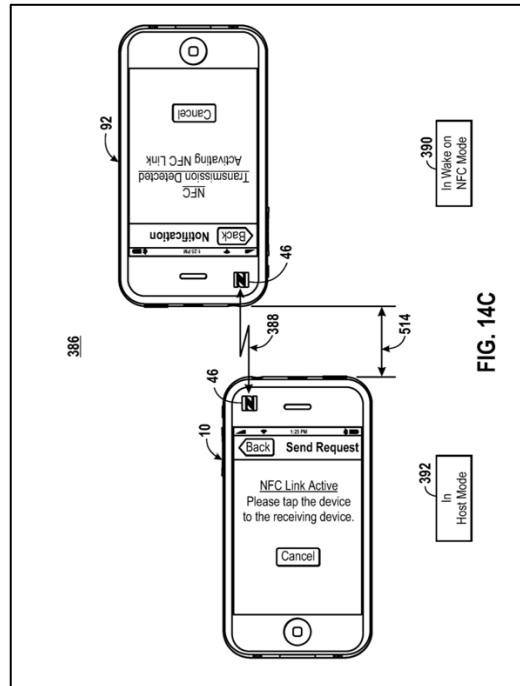
VIII. GROUND 4: *COLLINGS* IN VIEW OF *BONA*, *SMITH* AND *LIN*

A. Claim 9

Collings in view of Lin teaches transceiving limited-use payment information wirelessly with another device via the NFC interface (a wireless interface) of Collings's mobile device, in a device-to-device transaction.

(a) Lin's Teachings

Lin depicts in Fig. 14C "the establishment of an NFC connection 388 between two devices, namely the payee device 10 and the payor device 92, by way of the tap operation 386[.]" *Lin*, 68:10-12.



Lin, Fig. 14C.

Lin teaches that once “active device 10 is placed within an acceptable distance 514 (e.g., 2-4 cm) from the payor device 92...the payor device 92 may transition from the passive to an active mode in which the NFC device 46 within the payor device 92 is powered on, thus enabling the payor device’s 92 corresponding NFC interface 60 and providing the establishment of the NFC connection 388 between the payee device 10 and the payor device 92 through which the payment request may be transmitted.” *Lin*, 68:12-25.

(b) Motivation to Combine

It would have been obvious and a POSITA would have been motivated to modify Collinge’s mobile phone to wirelessly receive and transmit limited-use payment information in a device-to-device transaction as taught by Lin. *Dec.*, ¶¶329-

32. A POSITA would have recognized peer-to-peer payments options on mobile phones were becoming increasingly popular. *Dec.*, ¶332. A POSITA would have recognized that Collinge already teaches transmitting and receiving limited-use payment information from Collinge's mobile phone (*see* Claim 1(f)), and a POSITA would have recognized the value of the same payment information in a peer-to-peer transaction. *Collinge*, [0044]; *Lin*, Abstract, Fig. 14C; *Dec.*, ¶332. A POSITA would have appreciated that Lin's device-to-device payment was a known technique that could be used to improvise similar devices, like Collinge's mobile phone, in the same way, and therefore a POSITA would have had a reasonable expectation of success without undue experimentation in making such a combination. *Dec.*, ¶332.

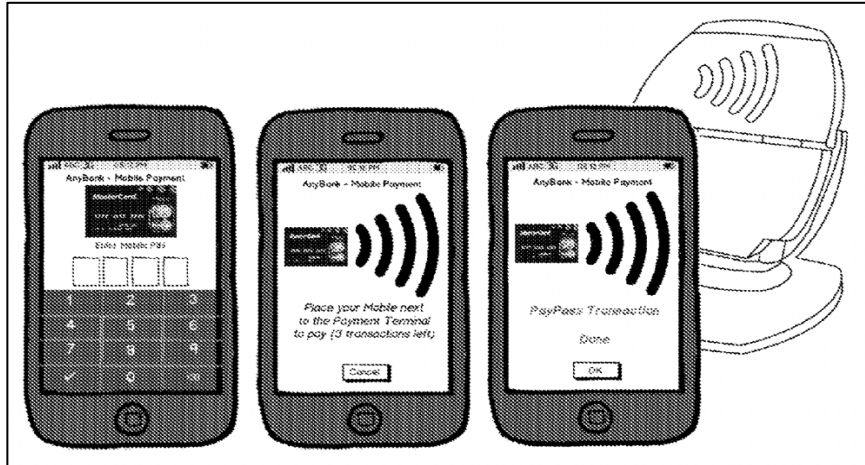
IX. GROUND 5: COLLINGE IN VIEW OF BONA, SMITH, AND KRANZLEY

A. Claim 10

Collinge in view of Kranzley teaches Collinge's mobile device (computing device) is further operable to transmit a payment information visually, in alphanumeric code, barcode (graphical) and an image of a card (iconography) via Collinge's touch screen user interface.

(a) Collinge

Collinge teaches a touch-screen user interface. *See* Claim 1(b)(3). Collinge further teaches graphically depicting a payment card:



'098 Provisional, 99; '248 Provisional, Fig. 2B; Dec., ¶334.

(b) Kranzley

Kranzley teaches that “[t]he payment application of the mobile device 12 converts the data (including the PAN, expiry, and dynamic data) into a bar code image 13.” *Kranzley*, [0028]. A POSITA would have understood that one example of Kranzley’s dynamic data would have included a CVC3, such as Collinge’s single use dynamic payment cryptogram. *Dec.*, ¶335. “Other bar code image formats may also be used (e.g., such as two-dimensional bar codes or other image formats that can hold at least 38 numeric digits of data and that are commonly used at merchant point of sale terminals).” *Kranzley*, [0028]. The bar code image is “displayed on a display device 14 of the mobile device 12.” *Kranzley*, [0033]-[0034]. “By allowing merchants to use their existing scanning equipment, embodiments allow ready adoption of payments using mobile devices configured pursuant to the present invention.” *Kranzley*, [0028].

Kranzley teaches displaying “the static VPAN...in plain text on a display device 14 of the mobile device 12 along with an expiry date and dynamic data)” *Kranzley*, [0035], [0033]-[0036]. “The VPAN 502 may be, for example, an alphanumeric code (typically, in current systems, a sixteen digit numeric code)[.]” *Kranzley*, [0065].

(c) Motivation to Combine

A POSITA would have been motivated to modify Collinge’s mobile device to display payment information visually as an alphanumeric code, barcode and an image of a card via Collinge’s touch screen user interface such that the displayed information can be accepted at a merchant facility, as taught by Kranzley. *Dec.*, ¶338. A POSITA would have recognized that providing payment information visually as taught by Kranzley would provide the user and merchant with flexibility to accept payment in a variety of ways in the event that traditional card reader equipment is unavailable or nonfunctional. *Id.* A POSITA would have had a reasonable expectation of success in modifying Collinge based on Kranzley’s teachings because these analogous references are both concerned with performing financial transactions with a mobile phone, both are assigned to Mastercard, and a POSITA would have been well-familiar with the operation of a GUI on a mobile device and how to modify that GUI to display various information, including payment information. *Kranzley*, Abstract; [0036]; *Collinge*, [0006]; *Dec.*, ¶339.

X. GROUND 6: *COLLINGE* IN VIEW OF *BONA AND KRANZLEY*

A. Claim 16

See Claim 10.

XI. GROUND 7: *COLLINGE* IN VIEW OF *BONA AND ENG*

A. Claim 19

1. Claim 19(a):

To the extent this limitation is entitled to any patentable weight, Collinge, in view of Bona and Eng, teaches Bona's companion card (payment card device) comprises fixed payment information comprising only: a card-holder name, card issuer logo (payment issuing logo), card payment network logo, and a magnetic stripe and chip (card reader interface icon).

(a) Bona's Teachings

See Claim 1(a). As depicted below Bona teaches card issuer logo (payment issuing logo) and magnetic stripe 214 and chip 206 (a card reader interface icon) on Bona's payment card. *Dec.*, ¶¶342-43.

Bona teaches "[t]he card 200 may include the logo 208 of the card issuer or other source indicia." *Bona*, [0045].



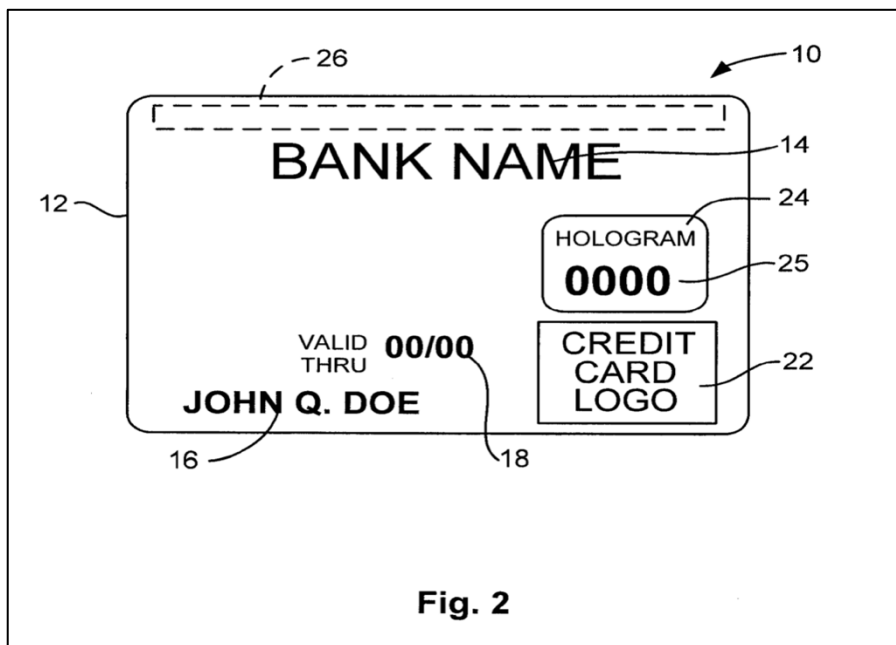
Bona, Fig. 2A.



Bona, Fig. 2B.

(b) Eng's Teachings

Eng teaches a card that has: (1) a card-holder name, (2) credit card logo (a card payment network logo), (3) Bank Name (payment issuing logo). Eng, [0020]-[0021].



Eng, Fig. 2.

(c) Motivation to Combine

It would have been obvious and a POSITA would have been motivated to modify Bona's card to include a fixed cardholder name and credit card logo as taught by Eng. *Dec.*, ¶345. A POSITA would have understood that a user would have found it valuable to distinguish their cards from each other (for example, with a credit card logo) and from similar cards that others in their household might have (with a cardholder name). *Id.* Each of these pieces of information was well-known to a POSITA and common on payment cards. A POSITA would have had a reasonable expectation of success in making this combination of known elements without undue experimentation. *Id.*

2. Claim 19(b):

To the extent this limitation is entitled to any patentable weight, Bona's card is free of any fixed account numbers, expiration dates, card security codes, or other fixed payment numbers. See Claim 1(a), 19(a).

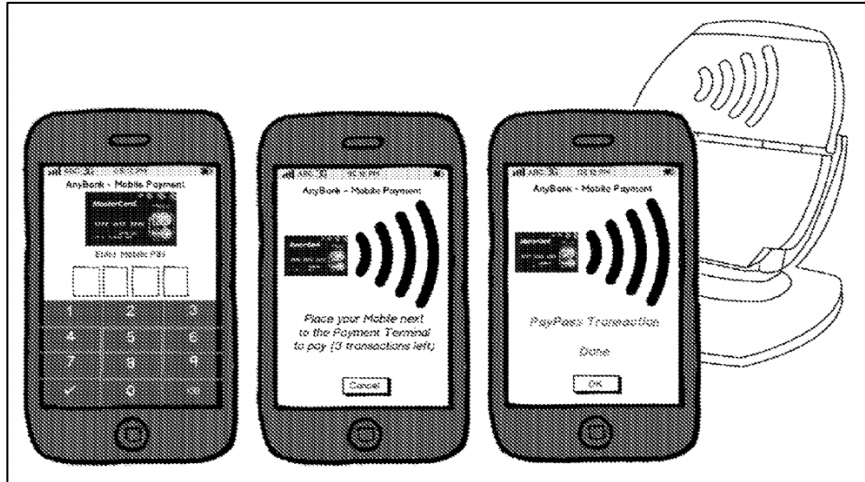
XII. GROUND 8: COLLINGE IN VIEW OF BONA, SMITH, AND CHIN

A. Claim 12

1. Claim 12(a):

Collinge's mobile device presents at least one security challenge, such as a PIN (a user touch-screen entry), user gesture, user passcode entry, or biometric sensing. For example, Collinge teaches that “[t]he mobile payment application 106 may transmit the activation code and any other additional user authentication information (e.g., a user identifier, a password, etc.) as a method of authentication.” *Collinge*, [0094]. Collinge also teaches that the user “may provide a mobile PIN for authentication” via “an input device (e.g., of the mobile device 104, such as a touch screen) [.]” *Collinge*, [0051], [0133].

Collinge teaches the user will “provide the Mobile PIN for all *PayPass* transactions...when using Remote-SE Mobile *PayPass* solution.” ’098 Provisional, 99.



'098 Provisional, 99; '248 Provisional, Fig. 2B.

2. Claim 12(b):

Collinge in view of Chin renders obvious where Collinge's mobile device is operable to reject and accept a user authorization to use Collinge's device based on the input gesture (security challenge response). *Dec.*, ¶¶349-354.

(a) Collinge's Teachings

Collinge teaches the issuer will decline transactions performed by the computing device when a user inputs an incorrect PIN because a fake single-use key would be provided, therefore the issuer cannot successfully validate the payment cryptogram. *See* Claim 1(i); *Collinge*, [0076] ("In some instances, the single use key 118 may be incorrect (e.g., fake, not genuine, etc.) if the key request includes a mobile PIN for which authentication is unsuccessful."), [0077] ("If the validation is unsuccessful, the issuer may deny the payment transaction."); '248 *Provisional*, 15-16.

(b) Chin's Teachings

Chin teaches accepting a gesture on “the touch receptive input area (e.g., a touchscreen) of the target device [.]” *Chin*, [0009]. The “target device is associated with a user-defined payment gesture (for e.g., a designated payment gesture defined by the user of the mobile device).” *Chin*, [0008]. If the gesture input by the user “matches the user-defined payment gesture stored locally within the target device, the method may include permitting the wireless transmission (e.g., using NFC technology) of protected payment data resident on the target device to an initiator device (e.g., an NFC reader, a contactless smart card reader based on RFID technology, an NFC scanner, etc.).” *Chin*, [0009].

However, “if the applied gesture on the touch receptive input area of the target device does not match the user-defined payment gesture stored locally within the target device, the method may include denying the wireless transmission of the protected payment data resident on the target device to the initiator device.” *Chin*, [0009].

(c) Motivation to Combine

A POSITA would have been motivated to modify Collinge to decline transactions based on a security challenge, such as a gesture as taught by Chin. *Dec.*, ¶353. Collinge already teaches a gesture to identify a user. *Collinge*, [0139] (“the additional credential may be at least one of: a gesture, a password, a passcode, and a biometric identifier.”). Collinge already teaches the issuer will decline transactions

based on an incorrectly entered PIN by a user, but a POSITA would have been motivated to expand upon that teaching so Collinge's device would deny transactions if the user is not able to authenticate themselves via a gesture as well. *Dec.*, ¶353. To decide if the gesture matches or not, processing would need to happen at the mobile device as taught by Chin. *Dec.*, ¶354. A POSITA would have appreciated that such a modification would have saved power, and a POSITA would have had a reasonable expectation of success in making such a modification since Collinge teaches being able to receive a gesture. *Id.* A POSITA would have appreciated that such a modification was obvious to try. *Id.*

3. Claim 12(c):

See Claim 12(b).

4. Claim 12(d):

See Claim 12(b).

B. Claim 13

Collinge teaches that the issuer is operable to decline transactions performed by Collinge's mobile device when a user inputs an incorrect PIN (*fails at least one security challenge*). *See* Claim 12.

XIII. GROUND 9: *COLLINGE, BONA, SMITH, AND FISHER*

A. Claim 7

Collinge in view of Fisher renders obvious transceiving Smith's PPAN (card payment information) via Collinge's wireless interface (NFC) for completing an online transaction.

(a) Collinge's Teachings

Collinge teaches receiving the card profile from the remote-SE system and storing the card profile “by the mobile payment application 106 in the local encrypted database 304.” *Collinge*, [0068]. Collinge teaches that the communication network may be “wireless[.]” *Collinge*, [0150].

As discussed in Claim 1(d)(1), a POSITA would have been motivated to send and receive Smith's PPAN to Collinge's mobile device with the card profile since account information was already included in Collinge's card profile. *Collinge*, Abstract (“wherein the card profile includes at least payment credentials corresponding to the associated payment account”); *Dec.*, ¶¶359-60.

(b) Fisher's Teachings

Fisher teaches a “mobile communication device” with a “mobile wallet application that executes PayPass[.]” *Fisher*, [0024]. When “a consumer (or user) is shopping online and they are ready to pay for their products, the consumer opens his mobile wallet and selects one of the payment methods (e.g., credit card, debit card,

prepaid card, etc.) from their mobile wallet.” *Fisher*, [0018]. The user “waves their phone over the NFC reader present on the PC 404.” *Fisher*, [0018]. The user’s “payment credentials are transferred from the phone to the merchant website (e.g., online store application 410).” *Fisher*, [0018].

(c) Motivation to Combine

For the reasons discussed above, a POSITA would have been motivated to modify Collinge’s mobile device to transceive the Collinge-Smith payment credentials via an NFC interface to complete an online payment transaction, as taught by Fisher. *See* Claim 1(d)(1); *Dec.*, 362-63. It was well known that mobile wallets could be used in online transactions, and Fisher demonstrated the feasibility of using PayPass in an online system. *Dec.*, ¶363. Fisher teaches transceiving payment credentials to an “NFC reader” to complete the online transaction, explaining that a “PayPass or other payment authorization protocol” would be used. *Fisher*, [0024]. A POSITA would have appreciated that performing an online transaction using Smith’s PPAN would have provided the user with flexibility to shop in more places while still protecting sensitive PAN information. *Dec.*, ¶363. A POSITA would have had a reasonable chance of success in making the combination, as it combines known elements and would yield predictable results, including increased security due to greater protection of a PAN during an online transaction. *Id.*

XIV. GROUND 10: *COLLINGE, SMITH, BONA, AND HAMMAD*

A. Claim 6

1. Claim 6(a):

Collinge-Smith-Bona in view of Hammad renders obvious the issuer receiving transacted payment information (Claim 1(h), 1(i); *Collinge*, [0076]-[0077]) and computing a limited-use payment information (payment cryptogram) from a transaction information (transaction amount), a merchant (merchant ID), a facility information (terminal ID), a sequence counter (ATC), a payment card account information (track data), secrets (UN_{CLOUD} and KS_{UN}), and an information limited to said card device and to said computing device (expiration date). *Dec.*, ¶364. As discussed above, Collinge in view of Smith teach a PPAN (alternative to the PAN). *See* Claim 1.

(a) Hammad's Teachings

Hammad teaches dynamically generating a dCVV (cryptogram number) using a mobile payment transaction. *Hammad*, 2:65-3:11, 3:51-4:6. The DCV is generated from “at least two...dynamic data elements,” including an “application transaction counter (ATC),” “a cryptogram, digital signature, or hash value based on transaction data,” “a time of day, a current transaction amount, a terminal ID, a merchant ID, and a randomly generated number from a terminal, etc.,” or information “relat[ing] to a consumer’s portable consumer device.” *Id.*, 4:21-56,

4:62-7:5, Fig. 1. The dynamic data elements can also be used with “static data elements,” including “telephone number, a SIM card number, an account number, birthday, home address, expiration date, etc.” and “service code” to generate a dCVV. *Id.*, 4:52-60, 5:2-5.

The service provider uses the dCVV to determine the authenticity of the payment. *Id.*, 7:29-8:50, Fig. 6; *Dec.*, ¶366.

(b) Collinge’s Teachings

Collinge teaches that the issuer validates a payment cryptogram as authentic. *See* Claim 1(i). A POSITA would have been well-familiar with methods of validating a payment cryptogram. *Collinge*, [0077]; *Dec.*, ¶367. Typically, the issuer will recompute the payment cryptogram and compare the issuer-generated payment cryptogram to the cryptogram received from the merchant. *Dec.*, ¶367. When generating the cryptogram, the issuer will use the KS_{UN} , UN_{CLOUD} , and ATC. *Collinge*, [0141]; Claim 1(i). A POSITA would have understood that the cloud unpredictable number (UN_{CLOUD}) and KS_{UN} are private information (*secrets*) that is shared between Collinge and the issuer specifically used by Collinge’s mobile device to generate a payment cryptogram and the issuer to validate Collinge’s generated payment cryptogram. *Dec.*, ¶¶367-69. The issuer also computes $Cloud_CVC3_{TRACK1/2}$:

The Issuer system is able to compute Cloud_CVC3_{TRACK1/2} using: ◊ IVCVC3_{TRACK1/2} (2 bytes) ◊ UN_{CLOUD} (4 bytes) ◊ ATC (2 bytes)
--

'095 Provisional, 24. The issuer also uses $IVCVC3_{TRACK1/2}$ which is a message authentication code (MAC) calculated over track 1 and 2 data using KD_{CVC3} which is “kept in the Cloud/Issuer” '095 Provisional, 21.

(c) Motivation To Combine

A POSITA would have recognized that using additional data elements to generate Collinge's cryptogram (e.g., transaction information (transaction amount), a merchant (merchant ID), a facility information (terminal ID), and an information limited to said card device and to said computing device (expiration date) would decrease the likelihood that, even if payment data were intercepted, that it could be used in a fraudulent manner. *Dec.*, ¶370. Therefore, a POSITA would have been motivated to include more data elements in Collinge generating a payment cryptogram, as taught by Hammad. *Id.* A POSITA would have further recognized that modifications to Collinge-Bona would be minimal as it would simply require additional inputs to Collinge's payment cryptogram generation. *Id.* As taught by Hammad, a POSITA would have been motivated to modify Collinge so that the issuer would therefore validate Collinge's payment cryptogram based on Hammad's

data elements, as well as the data elements already taught by Collinge. *Hammad*.,

7:29-8:50, Fig. 6.

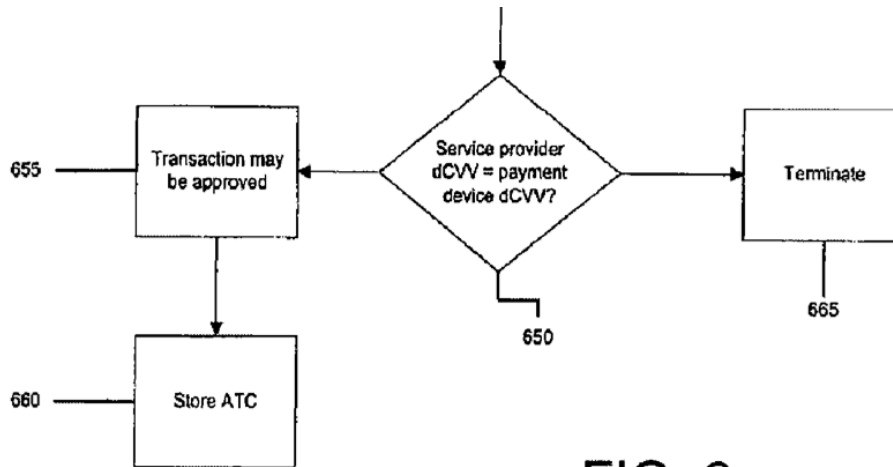


FIG. 6

Hammad, Fig. 6 (excerpt). Incorporating Hammad's data elements to generate a dynamic verification value is an application of known techniques to improve similar devices (e.g., mobile devices used in payment transactions) in the same way and would have yielded the predictable result of increasing security of the transaction. *Dec.*, ¶370.

2. Claim 6(b):

See Claim 1(i).

3. Claim 6(c):

See Claim 1(h).

4. Claim 6(d)

See Claim 1(i) and 1(h).

XV. DISCRETIONARY DENIAL

Pursuant to the Office's Interim Process Concerning Institution published March 26, 2025, Petitioners reserve the right to address in further briefing any discretionary denial issues raised by Cardware.

XVI. CONCLUSION

For the forgoing reasons, Petitioner respectfully requests *inter partes* review of the Challenged Claims.

Respectfully submitted,

ERISE IP, P.A.

BY: /s/ Adam P. Seitz
Adam P. Seitz, Reg. No. 52,206
adam.seitz@eriseip.com
7015 College Boulevard, Suite 700
Overland Park, Kansas 66211
(913) 777-5600 Telephone
(913) 777-5601 Facsimile

COUNSEL FOR PETITIONER

XVII. MANDATORY NOTICES UNDER 37 C.F.R. § 42.8

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

Petitioner is the real party-in-interest.

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

The '286 Patent is the subject of a civil action in *CardWare Inc. v. Apple Inc.*, 1:25-cv-00446 (W.D. Tex.).

The '286 patent was previously the subject of a Post-Grant Review petitions in *Samsung Electronics Co., Ltd., v. CardWare Inc.*, PGR2023-00012 and PGR2023-00013, which are no longer pending.

C. Lead and Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3)

Petitioner provides the following designation and service information for lead and back-up counsel. 37 C.F.R. § 42.8(b)(3) and (b)(4).

Lead Counsel	Back-Up Counsel
Adam Seitz (Reg. No. 52,206) Adam.seitz@eriseip.com PTAB@eriseip.com <u>Postal and Hand-Delivery Address:</u> ERISE IP, P.A. 7015 College Blvd., Suite 700 Overland Park, Kansas 66211 Telephone: (913) 777-5600 Fax: (913) 777-5601	Mark Lang (Reg. No. 55,356) Mark.Lang@eriseip.com Lydia Raw (Reg. No. 76,436) Lydia.raw@eriseip.com PTAB@eriseip.com <u>Postal and Hand-Delivery Address:</u> ERISE IP, P.A. 7015 College Blvd., Suite 700 Overland Park, Kansas 66211 Telephone: (913) 777-5600 Fax: (913) 777-5601

D. 37 C.F.R. 42.8(b)(4) – Service Information

Please address all correspondence to the lead and back-up counsel as shown above. Petitioners consent to electronic service by e-mail at the e-mail addresses provided above.

APPENDIX OF EXHIBITS

Exhibit 1001	U.S. Patent No. 11,328,286 (“’286 Patent”)
Exhibit 1002	File History of the ’286 Patent (“’286 File History”)
Exhibit 1003	Declaration of Dr. Neuman (“Dec.”)
Exhibit 1004	U.S. Patent Publication No. 2013/0262317 to Collinge et al. (“Collinge”)
Exhibit 1005	U.S. Provisional Patent Application No 61/619,095 to Collinge et al. (“’095 Provisional”)
Exhibit 1006	U.S. Provisional Patent Application No 61/635,248 to Collinge et al. (“’248 Provisional”)
Exhibit 1007	U.S. Provisional Patent Application No 61/735,383 to Collinge et al. (“’383 Provisional”)
Exhibit 1008	U.S. Provisional Patent Application No 61/762,098 to Collinge et al. (“’098 Provisional”)
Exhibit 1009	U.S. Patent Publication No. 2011/0140841 to Bona et al. (“Bona”)
Exhibit 1010	U.S. Patent Publication No. 2010/0125508 to Smith (“Smith”)
Exhibit 1011	US. Patent No. 8,103,588 to Patterson (“Patterson”)
Exhibit 1012	WIPO International Publication No. WO 2010/039337 to Lin et al. (“Lin”)
Exhibit 1013	U.S. Patent Publication No. 2010/0125509 to Kranzley et al. (“Kranzley”)
Exhibit 1014	U.S. Patent Publication No. 2013/0068366 to Eng (“Eng”)
Exhibit 1015	U.S. Patent Publication No. 2011/0282785 to Chin (“Chin”)
Exhibit 1016	U.S. Patent Publication No. 2013/0097040 to Fisher (“Fisher”)
Exhibit 1017	U.S. Patent No. 7,740,168 to Hammad (“Hammad”)
Exhibit 1018	Intentionally Left Blank
Exhibit 1019	Intentionally Left Blank
Exhibit 1020	IBM, <i>The Magnetic Stripe</i> , IBM, https://www.ibm.com/history/magnetic-stripe . (“IBM”)
Exhibit 1021	Vedat Coskun, <i>Near Field Communication: Theory To Practice</i> (John Wiley & Sons, 1st ed. 2012) (“Coskun”)
Exhibit 1022	MagTek, <i>Magnetic Stripe Card Standards</i> , (MagTek Inc. eds., 2011) (“MagTek”)
Exhibit 1023	EMVCo, LLC, <i>EMV Integrated Circuit Card Specifications for Payment Systems: Book 2 – Security and Key Management</i> (EMVCo, LLC eds., Version 4.3 2011) (“EMV”)
Exhibit 1024	Klaus Finkenzeller, <i>RFID Handbook</i> (John Wiley & Sons, 3rd ed. 2010) (“Finkenzeller”)

Exhibit 1025	MasterCard, <i>MasterCard PayPass™ in Action</i> , MASTERCARD (Jun. 11, 5:35 PM), https://www.mastercard.com/us/company/en/ourbusiness/paypass_in_action.html#:~:text=MasterCard%20PayPass%E2%84%A2%20in%20Action&text=Developed%20to%20replace%20the%20need,the%20way%20they%20view%20cash. (“ <i>PayPass</i> ”)
Exhibit 1026	Smart Card Alliance, <i>EMV And NFC: Complementary Technologies That Deliver Secure Payments And Value-Added Functionality</i> (Smart Card Alliance, Inc. eds., 2012) (“ <i>Smart</i> ”)
Exhibit 1027	U.S. Patent Publication No. 2012/0011058 to Pitroda et al. (“ <i>Pitroda</i> ”)
Exhibit 1028	MasterCard, <i>MasterCard Approved Mobile Devices</i> , MASTERCARD (Aug. 3, 2012), http://www.mastercard-mobilepartner.com/docs/MasterCard_Aproved_Mobile_Devices.pdf , [https://web.archive.org/web/20120906234255/http://www.mastercard-mobilepartner.com:80/docs/MasterCard_Aproved_Mobile_Devices.pdf] (“ <i>MasterCard Mobile Partner</i> ”)
Exhibit 1029	U.S. Patent Publication No. 2013/0054474 to Yeager (“ <i>Yeager</i> ”)
Exhibit 1030	EMVCo, LLC, <i>EMV Chip At-a-Glance: Enabling Seamless and Secure Contact and Contactless Payments Around the World</i> , EMVCo (2002), https://www.emvco.com/wp-content/uploads/2022/09/EMV%C2%AE-Chip-At-A-Glance-EMVCo-eBook.pdf (“ <i>EMVCo</i> ”)
Exhibit 1031	Scoping SIG & Tokenization Taskforce PCI Security Standards Council, <i>PCI Data Security Standard (PCI DSS) – Information Supplement: PCI DSS Tokenization Guidelines</i> (pci Security Standards Council eds., Version 2.0 2011) (“ <i>PCI SSC</i> ”)
Exhibit 1032	Alessandro Vizzarri et al., <i>Security in Mobile Payments</i> (2013) (“ <i>Vizzarri</i> ”)
Exhibit 1033	U.S. Patent Publication No. 2008/00110983 to Ashfield (“ <i>Ashfield</i> ”)
Exhibit 1034	Intentionally Left Blank
Exhibit 1035	WIPO International Publication No. WO 1994/17498 to Labaton et al. (“ <i>Labaton</i> ”)
Exhibit 1036	Geoffrey R. Gerdes et al., <i>The 2013 Federal Reserve Payment Study – Recent and Long-Term Trends in the United States: 2003-2012</i> (Federal Reserve System, Rev. 2014) (“ <i>Study Summary</i> ”)

Exhibit 1037	Geoffrey R. Gerdes et al., <i>The 2013 Federal Reserve Payment Study – Recent and Long-Term Trends in the United States: 2000-2012</i> (Federal Reserve System, 2014) (“ <i>Study</i> ”)
Exhibit 1038	ConsumerWorld, <i>Two Months After the Deadline, Most Major Retailers Still Can't Read Chipped Credit Cards</i> , CONSUMERWORLD (Dec. 7, 2015), https://www.consumerworld.org/pages/creditcardreaders.htm (“ <i>ConsumerWorld Survey</i> ”)
Exhibit 1039	Ann Cavoukian, <i>Mobile Near Field Communications (NFC)</i> (“ <i>Tap ‘n Go</i> ” <i>Keep it Secure & Private</i> , IPC (2011), https://www.ipc.on.ca/sites/default/files/legacy/Resources/mobile-nfc.pdf (“ <i>Cavoukian</i> ”)
Exhibit 1040	Annika Paus, <i>Near Field Communication in Cell Phones</i> (2017) (“ <i>Paus</i> ”)
Exhibit 1041	Ashis K. Mahapatra, <i>Touch Screen Systems</i> , ORISSA REVIEW (2005), https://magazines.odisha.gov.in/orissareview/jun2005/engpdf/touch_screen_system.pdf (“ <i>Mahapatra</i> ”)
Exhibit 1042	U.S. Patent Publication No. 2006/0097991 to Hotelling et al. (“ <i>Hotelling</i> ”)
Exhibit 1043	U.S. Patent Publication No. 2008/0122796 to Jobs et al. (“ <i>Jobs</i> ”)
Exhibit 1044	U.S. Patent No. 10,181,121 (“ <i>Roberts</i> ”)
Exhibit 1045	U.S. Patent Publication No. 2013/0151292 to Van Deloo et al. (“ <i>Deloo</i> ”)
Exhibit 1046	U.S. Patent Publication No. 2006/0186195 to Gray (“ <i>Gray</i> ”)
Exhibit 1047	U.S. Patent Publication No. 2014/0006276 to Grigg et al. (“ <i>Grigg</i> ”)
Exhibit 1048	Anup K. Ghosh & Tara M. Swaminatha, <i>Software Security and Privacy Risks in Mobile E-Commerce</i> , 44 CACM 51 (2001) (“ <i>Ghosh</i> ”)
Exhibit 1049	Josh Constine, <i>Bump Pay Lets You PayPal Someone With A Tap, But Only In-Person</i> , TECHCRUNCH (Mar. 29, 2012, 5:01 AM), https://techcrunch.com/2012/03/29/bump-pay/#:~:text=Now%20it's%20as%20easy%20as,to%20anyone%20in%20arm's%20reach. (“ <i>Tech</i> ”)
Exhibit 1050	U.S. Patent Publication No. 2009/0083850 to Fadell et al. (“ <i>Fadell</i> ”)

CLAIM LISTING APPENDIX
U.S. Patent No. 11,328,286 for Claims 1-27

Claim Designation	Claim Language
Claim 1(Pre)	1. A payment system comprising:
Claim 1(a)]	a payment card device free of any fixed payment numbers visible thereon and wherein said payment card device is operable for use in payment card reader equipment; and
Claim 1(b)	a computing device comprising: a processor;
Claim 1(b)(1)	a memory;
Claim 1(b)(2)	a wireless interface;
Claim 1(b)(3)	a touch-screen user interface operable to provide a visual user-interface for user payment interactions; and
Claim 1(c)	a user-input device coupled to the processor, and
Claim 1(d)	wherein the processor is operable to store a transaction sequence count,
Claim 1(d)(1)	a device account number and
Claim 1(d)(2)	secrets limited to the computing device, and
Claim 1(e)	wherein the computing device is operable to receive, store and transmit a card payment information not visible on the payment card device, and
Claim 1(f)	wherein the processor is operable to generate at least a portion of a limited-use card payment information for use by an authenticated card user, and
Claim 1(g)	wherein the computing device is operable to convey said limited-use card payment information via an interface of the computing device, and
Claim 1(h)	wherein a card issuer authority is operable to reject as invalid a transaction attempt outside of its limitations of use,
Claim 1(i)	wherein a card issuer authority is operable to validate a card payment information as authentic when received from at least one of: an authenticated users payment card; and an authenticated users computing device, and
Claim 1(j)	wherein the card issuer authority is operable to permit the authentic transactions to complete.
Claim 2	2. The system of claim 1, wherein the touch-screen user interface is operable to control an access for payment

Claim Designation	Claim Language
	transactions by the card device, and is operable to enable as authentic payment transactions by the card device.
Claim 3	3. The system of claim 1, wherein the touch-screen user interface is operable to control an access of the card device for payment transactions at an NFC Card Reader facility, and is operable to enable and disable NFC payment transactions by the card device.
Claim 4	4. The system of claim 3, wherein the touch-screen user-interface is configurable for a locking and unlocking of payment transactions, and wherein a card issuer authority is further operable for denying a payment transaction from at least one of: a locked card device; and a locked card-users computing device, and wherein a card issuer authority is further operable to permit as authorized, a card payment transaction from an unlocked device.
Claim 5	5. The system of claim 1, wherein the payment card device is absent a payment number information necessary for completing an online transaction, and wherein the information presented on an interface of said card device, are limited to an in-store merchant card reader facility use only.
Claim 6(a)	6. A system of claim 1, wherein: the card issuer authority is operable to receive said transacted payment information, and wherein a card issuer authority is operable to compute a limited-use payment information from a transaction information, a merchant, a facility information, a sequence counter, a payment card account information, secrets and an information limited to said card device and to said computing device,
Claim 6(b)	and wherein a card issuer authority is operable to compare said computed payment information to said device transacted information,
Claim 6(c)	and wherein a card issuer authority is operable to reject as invalid a device transaction used outside of a valid range of device limitations,
Claim 6(d)	and wherein a card issuer authority is operable to authenticate as valid, a device transaction use within valid range of device limitations.

Claim Designation	Claim Language
Claim 7	7. The system of claim 1, wherein the computing device is further operable to transceive the card payment information via the wireless interface for completing an online transaction.
Claim 8	8. The system of claim 1, wherein the computing device is further operable to transceive the limited-use card payment information via an NFC interface of the computing device in an in-store NFC reader facility transaction.
Claim 9	9. The system of claim 1, wherein the computing device is further operable to transceive the limited-use payment information wirelessly with another device via a wireless interface of the computing device, in a device-to-device transaction.
Claim 10	10. The system of claim 1, wherein the computing device is further operable to transmit a payment information visually, in alphanumeric, graphical and iconography via the touch screen user interface.
Claim 11(a)	11. The system of claim 1, further comprising a touch-screen user interface control for a user approving and denying a transaction, and
Claim 11(b)	and wherein a card issuer authority is further operable to deny as authentic, a card payment transaction from a user-denied transaction, and to approve as authentic a card payment transaction from a user-approved transaction.
Claim 12(a)	12. The system of claim 1, wherein the computing device is further operable to present at least one challenge, of a set of security challenges comprising: a card user personal information question, a card issuer authority security question, a user touch-screen entry, a user touch-screen swipe, a user gesture of a device, a user passcode entry, a biometric sensing of a user touch, a biometric sensing of a recognized user proximity, and a biometric sensing of a recognized user, and
Claim 12(b)	wherein the computing device is operable to reject and accept a user authorization to use the device based on the security challenge response, and
Claim 12(c)	wherein the computing device is operable to decline performing a payment transaction in the possession of an unauthorized user,

Claim Designation	Claim Language
Claim 12(d)	and wherein the computing device is operable to perform a payment transaction while in the possession of a user correctly passing the at least one challenge.
Claim 13	13. The user computing device of claim 12, wherein a payment issuing authority is operable to decline transactions performed by the computing device when a user fails the at least one security challenge.
Claim 14	14. The system of claim 1, wherein a payment issuing authority is operable to decline transactions performed by the payment card device when a user fails at least one security challenge presented to a user by the computing device.
Claim 15(Pre)	15. A payment system comprising:
Claim 15(a)	a payment card device that is free of any fixed payment numbers disposed thereon and wherein said payment card device is operable for use in a merchant card-reader equipment; and
Claim 15(b)	a card-users personal computing device operable for completing a payment transaction and comprising:
Claim 15(b)(1)	a processor;
Claim 15(b)(2)	a touch-screen display interface;
Claim 15(b)(3)	a user-interface;
Claim 15(b)(4)	a wireless interface;
Claim 15(b)(5)	and a memory for storing a payment information accessible to the processor,
Claim 15(c)	wherein the computing device is configured to dynamically generate limited-use payment information,
Claim 15(d)	and wherein the computing device is configured to convey the limited-use payment information on a computing device interface upon the authorization of a valid user, and
Claim 15(e)	wherein a merchant is operable to receive a payment information provided by a personal computing device, and
Claim 15(f)	wherein the limited-use payment information provided by at least one or both of: the payment card device, and the computing device, is validated by a card issuing authority when used in merchant in-store facility transactions, and
Claim 15(g)	wherein a card issuing authority is operable to reject as invalid, a payment information used outside of its valid limitations of use, and

Claim Designation	Claim Language
Claim 15(h)	wherein a card issuing authority is operable to validate generated limited-use payment information provided by the computing device in an authorized transaction completed by the computing device.
Claim 16	16. The system of claim 15, wherein the touch-screen user interface is operable for displaying the limited-use payment information, and wherein a merchant is operable to accept the displayed payment card information in a transaction at a merchant facility.
Claim 17(a)	17. The system of claim 15, wherein the touch-screen display interface is operable to display a merchant facility transaction, and wherein the touch-screen display interface is operable to accept a user approval and denial of a payment transaction,
Claim 17(b)	and wherein a card issuer authority is further operable to deny a card payment transaction from a user-denied merchant facility transaction, and to approve as authentic a card payment transaction from a user-approved facility transaction.
Claim 18(a)	18. The system of claim 15, wherein a plurality of issuer-provided payment information is wirelessly downloaded into the personal computing device, and
Claim 18(b)	wherein the user-interface is operable for a user selection, of at least one of issuer-provided payment methods via the touch-screen display interface, and
Claim 18(c)	wherein the payment card device is operable for a transaction with a user-selected payment method.
Claim 19(a)	19. The card device of claim 15, wherein the payment card device comprises fixed payment information disposed thereon, and wherein the fixed payment information comprises only: a card-holder name; a payment issuing logo; a card payment network logo, and a card reader interface icon, and
Claim 19(b)	wherein the payment card device is free of any account numbers, expiration dates, card security codes, or other fixed payment numbers, disposed thereon.
Claim 20(Pre)	20. A payment system comprising:
Claim 20(a)	a payment card device, free of any depictions of fixed payment numbers thereon, and operable for use in payment card reader equipment; and

Claim Designation	Claim Language
Claim 20(b)	a computing device comprising:
Claim 20(b)(1)	a processor;
Claim 20(b)(2)	a memory;
Claim 20(b)(3)	a wireless interface;
Claim 20(b)(4)	a touch-screen user interface operable to provide a visual user-interface for user payment interactions; and
Claim 20(b)(5)	a user-input device coupled to the processor; and
Claim 20(c)	wherein the memory is operable to store a transaction sequence count, a static device account number and secrets limited to the computing device;
Claim 20(d)	wherein the computing device is operable to receive, store, display and transmit issuer-provided payment information, associated with, but not depicted on, the payment card device;
Claim 20(e)	wherein the processor is operable to dynamically generate at least a portion of a limited-use payment information for use by an authenticated card user,
Claim 20(f)	and to combine said at least a portion of the limited-use payment information with at least said static device account number to create combined payment information;
Claim 20(g)	wherein the computing device is operable to convey said combined payment information via an interface of the computing device; and
Claim 20(h)	wherein the computing device is operable to receive information, from an issuer, in response to the conveyed combined payment information, indicating that a payment transaction is valid.
Claim 21	21. The system of claim 20 wherein the computing device is operable to wirelessly receive the static device account number.
Claim 22	22. The system of claim 20, wherein the processor is operable to dynamically generate the at least a portion of a limited-use payment information based on a transaction sequence counter count, and further wherein the generated limited-use payment information is valid for a single use.
Claim 23	23. The system of claim 22 wherein the processor is operable to dynamically generate the at least a portion of a limited-use payment information further based on payment processing authority secrets.

Claim Designation	Claim Language
Claim 24	24. The system of claim 23 wherein the processor is operable to dynamically generate the at least a portion of a limited-use payment information further based on the static device account number.
Claim 25	25. The system of claim 24 wherein the computing device is operable to wirelessly receive the static device account number.
Claim 26	26. The system of claim 22 wherein the processor is operable to dynamically generate the at least a portion of a limited-use payment information further based on the static device account number.
Claim 27	27. The system of claim 26 wherein the computing device is operable to wirelessly receive the static device account number.

CERTIFICATION OF WORD COUNT

The undersigned certifies pursuant to 37 C.F.R. §42.24 that the foregoing Petition for *Inter Partes* Review, excluding any table of contents, mandatory notices under 37 C.F.R. §42.8, certificates of service or word count, or appendix of exhibits, contains 13,891 words according to the word-processing program used to prepare this document (Microsoft Word).

Dated: June 20, 2025

Respectfully submitted,

ERISE IP, P.A.

BY: /s/ Adam P. Seitz
Adam P. Seitz, Reg. No. 52,206
adam.seitz@eriseip.com
7015 College Boulevard, Suite 700
Overland Park, Kansas 66211
(913) 777-5600 Telephone
(913) 777-5601 Facsimile

COUNSEL FOR PETITIONER

CERTIFICATE OF SERVICE ON PATENT OWNER
UNDER 37 C.F.R. § 42.105(a)

Pursuant to 37 C.F.R. §§ 42.6(e) and 42.105(b), the undersigned certifies that on June 20, 2025, a complete and entire copy of this Petition for *Inter Partes* Review and Exhibits were provided via Federal Express to the Patent Owner by serving the correspondence address of record for the '286 patent:

David Wyatt
c/o Murabito, Hao & Barnes
1500 E Hamilton Ave, Suite 118
Campbell, CA 95008

A courtesy copy of the Petition for *Inter Partes* Review was emailed to counsel of record in the parallel litigation:

Caroline M. Walters (cwalters@reichmanjorgensen.com)
Navid Cyrus Bayar (nbayar@reichmanjorgensen.com)
Timothy A. Trost (ttrost@reichmanjorgensen.com)
Khue V. Hoang (khoang@reichmanjorgensen.com)
Matthew G. Berkowitz (mberkowitz@reichmanjorgensen.com)
Patrick R. Colsher (pcolsher@reichmanjorgensen.com)
Yue (Joy) Wang (ywang@reichmanjorgensen.com)
Eric H. Findlay (efindlay@findlaycraft.com)

Respectfully submitted,

ERISE IP, P.A.

BY: /s/ Adam P. Seitz
Adam P. Seitz, Reg. No. 52,206
adam.seitz@eriseip.com
7015 College Boulevard, Suite 700
Overland Park, Kansas 66211

IPR2025-01151

U.S. Patent No. 11,328,286

(913) 777-5600 Telephone

(913) 777-5601 Facsimile

COUNSEL FOR PETITIONER