

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. IPR2025-01152
U.S. Patent No. 11,620,634

**PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 11,620,634**

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	THE '634 PATENT	1
	A. DESCRIPTION OF THE '634 PATENT	1
	B. FIELD OF ENDEAVOR AND PROBLEM SOLVED BY THE INVENTORS	1
	C. PRIORITY AND PROSECUTION HISTORY	2
	D. LEVEL OF SKILL OF A POSITA	2
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)	3
	C. CLAIM CONSTRUCTION UNDER 37 C.F.R § 42.104(B)(3).....	5
IV.	SHOWING OF ANALOGOUS PRIOR ART	6
	A. COLLINGE	6
	1. <i>Collinge Incorporated all Provisionals for All Purposes</i>	8
	2. <i>Obvious to Combine Provisional Features</i>	9
	B. LIN.....	10
	C. SMITH	12
	D. SAHOTA	13
	E. KRANZLEY	14
	F. FADELL	14
	G. YU	15
	A. ANALOGOUS ART.....	16
V.	GROUND 1: <i>COLLINGE</i> IN VIEW OF LIN IN VIEW OF SAHOTA	17
	1. <i>1(Pre): “A method of generating and using limited-use payment information for performing a payment transaction, the method comprising:”</i>	17

2.	<i>1(a): “receiving an input at an electronic device, wherein the input comprises a priming operation, and, wherein the electronic device comprises:”</i>	19
3.	<i>1(a)(1): “a processor;”</i>	23
4.	<i>1(a)(2): “a touch-screen display coupled to the processor; and”</i>	23
5.	<i>1(a)(3): “a near field communications (NFC) interface coupled to the processor;”</i>	26
6.	<i>1(b): “responsive to said priming operation, readying said device to perform a payment transaction by an identified user;”</i>	29
7.	<i>1(c): “receiving a payment request for the payment transaction at said electronic device;”</i>	31
	(a) Collinge’s Teachings	31
	(b) Lin’s Teachings	33
	(c) Motivation to Combine	33
8.	<i>1(d): “displaying, on the touch-screen display, information reflecting the payment request, and an image representing a selected issued payment account;”</i>	34
	(a) Lin’s Teachings	36
	(b) Motivation to Combine	37
9.	<i>1(e): “dynamically generating, by the processor, limited-use payment information;”</i>	38
10.	<i>1(f): “wherein said limited-use payment information is dynamically generated based on a per-transaction sequential parameter originating from the electronic device;”</i>	41
	(a) Collinge’s Teachings	41
	(b) Sahota’s Teachings	41
	(c) Motivation to Combine	42
11.	<i>1(g): “using said limited-use payment information in connection with the payment transaction in place of</i>	

	<i>issued payment information associated with said selected issued payment account;”</i>	42
12.	<i>1(h): “transmitting said limited-use payment information from said electronic device via said NFC interface for receipt by an NFC recipient;”</i>	43
13.	<i>1(i): “responsive to the transmitting the limited-use payment information, receiving via the NFC interface information reflecting a status of said payment transaction; and displaying the status of said payment transaction via said touch-screen display.”</i>	43
14.	<i>Claim 2:</i>	46
15.	<i>Claim 7:</i>	46
16.	<i>8(a): The method of claim 7, wherein said readying said device to perform a payment transaction comprises: identifying said proximity NFC recipient is an NFC payment facility; successfully validating the identified user as authorized to perform the payment transaction via said electronic device; and</i>	46
17.	<i>8[b]: receiving a user approval for performing the payment transaction.</i>	47
18.	<i>9[Pre]: The method of claim 8, wherein said user approval for performing a payment transaction comprises displaying a request for user input at said electronic device, for both said identifying and said user approval of said payment transaction, and further comprising:</i>	47
19.	<i>9[a]: the processor identifying that said user input matches a known authorized user of the electronic device, before said readying said device to perform a payment transaction; and,</i>	48
20.	<i>9[b]: disallowing the payment transaction by the device until said readying said device to perform the payment transaction is successfully completed.</i>	48
21.	<i>10.1: The method of claim 8, wherein said successfully validating the identified user comprises the processor successfully determining a match between: firstly, a user</i>	

	<i>input received via at least one of a set of user input sensors of the electronic device; and, secondly, at least one of the set consisting of: predetermined user characteristics, and challenge-responses of an authorized user, as stored in the electronic device.</i>	<i>49</i>
(a)	Collinge’s Teachings.....	50
(b)	Smith’s Teachings	51
(c)	Motivation to Combine	51
22.	<i>Claim 11:</i>	<i>53</i>
23.	<i>Claim 15:</i>	<i>53</i>
24.	<i>Claim 27:</i>	<i>53</i>
25.	<i>28[Pre]: The method of claim 27 wherein the limited-use payment information is based on at least one secret information shared by both the electronic device and the payment processing authority; and</i>	<i>53</i>
26.	<i>28[a]: further wherein the at least one secret information is not exchanged when [performing] the payment transaction.</i>	<i>53</i>
27.	<i>39(Pre): “An electronic device for completing a payment transaction, the electronic device comprising:”</i>	<i>54</i>
28.	<i>39(a): “a processor;”</i>	<i>54</i>
29.	<i>39(b): “a memory coupled to the processor,”</i>	<i>54</i>
30.	<i>39(b)(1): “wherein the memory is operable to store information associated with use of an issued payment account and wherein the payment authority information comprises a secret information;”</i>	<i>56</i>
31.	<i>39(c): “a near field communications (NFC) interface coupled to the processor and operable to receive a payment request associated with the payment transaction;”</i>	<i>57</i>
32.	<i>39(d): “a user interface coupled to the processor;”</i>	<i>57</i>
33.	<i>“39(e): “a user input device coupled to the processor; and,”</i>	<i>59</i>

34.	39(f): “wherein said processor is operable to: responsive to a priming operation, wherein the priming operation is operable to ready the device to perform the payment transaction,”	59
35.	39(g): “cause the display of information associated with the payment request;”	59
36.	39(h): “cause the display of an image representing at least one user-selectable issued payment account; and,”	59
37.	39(i): “dynamically generate a limited-use payment information based on a per-transaction sequential parameter originating from the electronic device, and secret information associated with a selected issued payment account; and,”	59
38.	39(j): “cause the transmission, via said NFC interface, a payment information combination comprising the dynamically generated limited-use payment information and said payment authority information, for receipt by an NFC recipient;”	60
39.	39(k): “wherein the NFC interface is operable, in response to transmitting said payment information combination, to receive status information reflecting a transaction processing status of said payment transaction; and wherein the user interface is operable to provide an indication of the status information.”	60
40.	Claim 41:	60
41.	Claim 44:	60
42.	Claim 45:	61
43.	Claim 46:	61
44.	Claim 49:	61
45.	Claim 50:	61
46.	55[a]: The device of claim 39, wherein the processor is operable to: receive a user-selection of an issued payment account presented on the user interface, received the user input device coupled to the processor, and	61

47.	<i>55[b]: responsive thereto, select from the memory a specific processing authority information corresponding to the user-selected issued payment account information, and</i>	<i>62</i>
48.	<i>55[c]: use at least a portion of said specific processing authority information in place of at least a portion of the issued payment account information to generate a combined payment information to complete a payment transaction per the input user-selection.</i>	<i>63</i>
49.	<i>Claim 56(Pre):.....</i>	<i>63</i>
50.	<i>Claim 56(a):</i>	<i>63</i>
51.	<i>Claim 56(b):</i>	<i>63</i>
52.	<i>Claim 56(b)(1):.....</i>	<i>63</i>
53.	<i>Claim 56(c):.....</i>	<i>63</i>
54.	<i>Claim 56(d):</i>	<i>63</i>
55.	<i>Claim 56(e):.....</i>	<i>64</i>
56.	<i>Claim 56(f):</i>	<i>64</i>
57.	<i>Claim 56(g):</i>	<i>64</i>
58.	<i>Claim 56(h):</i>	<i>64</i>
59.	<i>Claim 56(i):</i>	<i>64</i>
60.	<i>Claim 56(j):</i>	<i>64</i>
61.	<i>Claim 56(k):.....</i>	<i>64</i>
62.	<i>Claim 60:</i>	<i>64</i>
63.	<i>Claim 61:.....</i>	<i>64</i>
64.	<i>Claim 62:.....</i>	<i>64</i>
65.	<i>Claim 63:.....</i>	<i>65</i>
66.	<i>Claim 66:.....</i>	<i>65</i>
67.	<i>Claim 67:.....</i>	<i>65</i>
68.	<i>Claim 72[Pre]:</i>	<i>65</i>
69.	<i>Claim 72[a]:.....</i>	<i>65</i>
70.	<i>Claim 72[b]:.....</i>	<i>65</i>

VI. GROUND 2: COLLINGE IN VIEW OF LIN, SAHOTA, AND SMITH	65
1. 29(Pre): “A system for completing a payment transaction, the system comprising:”	65
2. 29(a): “an electronic device operable to receive a priming operation, wherein the priming operation is operable to ready said device for performing a payment transaction by an identified user, and, wherein the electronic device further comprises:”	66
3. 29(b):” a processor;”	66
5. 29(d): “a touch-screen display coupled to the processor, and”	67
6. 29(e): “wherein the electronic device is operable to cause the display of information reflecting device-readiness, the payment request, and an image representing at least one selected issued payment account;”	67
7. 29(f): “wherein the electronic device is operable to dynamically generate limited-use payment information based on a sequential counter count from the electronic device;”	67
8. 29(g): “wherein the electronic device is operable to store a static device-specific user account information;”	67
(a) Collinge’s Teachings	68
(b) Smith’s Teachings	68
(c) Motivation to Combine	72
9. 29(h): “wherein the electronic device is operable to transmit a combination of said dynamically generated limited-use payment information and said static device-specific user account information to an NFC recipient via, said NFC interface for use in connection with payment transaction in place of information associated with said selected issued payment account;”	76
(a) Motivation to Combine	78

10.	<i>29(i): “wherein the electronic device is operable, subsequent to transmission of said combination, to receive a status information reflecting a status of said payment transaction; and, wherein the touch-screen display is operable to display as indication of said status information.”</i>	78
11.	<i>3[a]: The method of claim 2, further comprising: prior to the priming operation, transmitting the issued payment information for receipt by a payment processing authority; and,</i>	78
12.	<i>3[b]: in response to said transmitting issued payment information, receiving a static device account information that is unique to the electronic device.</i>	79
13.	<i>Claim 4[a]:</i>	80
14.	<i>Claim 4[b]:</i>	80
15.	<i>Claim 4[c]:</i>	80
16.	<i>5: The method of claim 3, wherein the dynamically generating [further] comprises dynamically generating the limited-use payment information based on payment processing authority secret information.</i>	80
17.	<i>Claim 6:</i>	81
18.	<i>Claim 17[a]:</i>	81
19.	<i>Claim 17[b]:</i>	81
20.	<i>Claim 18[a]:</i>	81
21.	<i>Claim 18[b]:</i>	81
22.	<i>Claim 18[c]:</i>	82
23.	<i>Claim 19:</i>	82
24.	<i>Claim 20:</i>	82
25.	<i>Claim 21:</i>	82
26.	<i>Claim 22:</i>	82
27.	<i>23[a]: The method of claim 1, further comprising: prior to the priming operation, transmitting the issued payment</i>	

	<i>information, user information and device-specific information; and, ...</i>	82
(a)	Collinge's Teachings	82
(b)	Smith's Teachings	83
(c)	Motivation to Combine	84
28.	<i>23[b]: in response to transmitting said issued payment information, user information and device-specific information, receiving a payment processing authority supplied secret information.</i>	85
29.	<i>Claim 24:</i>	85
30.	<i>Claim 30:</i>	85
31.	<i>Claim 31:</i>	85
32.	<i>Claim 32:</i>	86
33.	<i>Claim 34:</i>	86
34.	<i>Claim 35:</i>	86
35.	<i>Claim 36[Pre]:</i>	86
36.	<i>Claim 36[a]:</i>	86
37.	<i>Claim 37:</i>	86
38.	<i>Claim 38:</i>	86
39.	<i>Claim 40:</i>	86
40.	<i>Claim 42:</i>	86
41.	<i>Claim 47:</i>	86
42.	<i>Claim 57:</i>	86
43.	<i>Claim 58:</i>	87
44.	<i>Claim 64:</i>	87

VII. GROUND 3: COLLINGE IN VIEW OF LIN, SAHOTA, SMITH, AND KRANZLEY 87

1.	<i>Claim 25: The method of claim 24 wherein said static device account information comprises a static device account number and a static device-specific expiration date.</i>	87
----	--	----

(a)	Motivation to Combine	87
2.	<i>Claim 26:</i>	88
3.	<i>Claim 33:</i>	88
4.	<i>Claim 43:</i>	88
5.	<i>Claim 48:</i>	89
6.	<i>Claim 59:</i>	89
7.	<i>Claim 65:</i>	89
VIII.	GROUND 4: COLLINGE IN VIEW OF LIN, SAHOTA, AND	
	FADELL.....	89
1.	<i>10.2: The method of claim 8, wherein said successfully validating the identified user comprises the processor successfully determining a match between: firstly, a user input received via at least one of a set of user input sensors of the electronic device; and, secondly, at least one of the set consisting of: predetermined user characteristics, and challenge-responses of an authorized user, as stored in the electronic device.</i>	<i>89</i>
(a)	Collinge’s Teachings.....	89
(b)	Fadell’s Teachings.....	90
(c)	Motivation to Combine	91
2.	<i>Claim 12:</i>	92
3.	<i>Claim 13:</i>	92
4.	<i>16[Pre]: The method of claim 15, wherein said readying said device to perform a payment transaction comprises:</i>	<i>92</i>
5.	<i>16[a]: successfully identifying said identified user from said user input; and, ...</i>	<i>92</i>
6.	<i>16[b]: wherein said user input further comprises a user approval for performing the payment transaction received from said identified user; and, ...</i>	<i>92</i>
7.	<i>16[c]: wherein said successfully identifying further comprises said electronic device validating an authorized user of said electronic device by comparing a user-touch input received via a touch input sensor on the electronic</i>	

	<i>device with a recognized valid user-touch, stored in a memory of the electronic device; and,.....</i>	<i>93</i>
8.	<i>16[d]: wherein said user approval for performing the payment transaction further comprises:.....</i>	<i>93</i>
9.	<i>16[e]: visually presenting information of the payment transaction on the touch screen display of said electronic device;.....</i>	<i>93</i>
	(a) Lin’s Teachings	93
	(b) Motivation to Combine	94
10.	<i>Claim 16[ff]: visually presenting a request for user approval of the payment transaction via touch input at said electronic device; and, ...</i>	<i>95</i>
11.	<i>Claim 16[g]: subsequent to receiving a user-touch input from an identified user, approving performance of said payment transaction via said electronic device.....</i>	<i>95</i>
12.	<i>Claim 51:.....</i>	<i>95</i>
13.	<i>Claim 52:.....</i>	<i>95</i>
14.	<i>Claim 53:.....</i>	<i>95</i>
15.	<i>Claim 68:.....</i>	<i>95</i>
16.	<i>Claim 69:.....</i>	<i>95</i>
17.	<i>Claim 70:.....</i>	<i>95</i>
IX.	GROUND 5: COLLINGE IN VIEW OF LIN, SAHOTA, AND YU.....	95
1.	<i>10.3: The method of claim 8, wherein said successfully validating the identified user comprises the processor successfully determining a match between: firstly, a user input received via at least one of a set of user input sensors of the electronic device; and, secondly, at least one of the set consisting of: predetermined user characteristics, and challenge-responses of an authorized user, as stored in the electronic device.</i>	<i>95</i>
	(a) Collinge’s Teachings.....	96
	(b) Yu’s Teachings.....	96
	(c) Motivation to Combine	97

2.	<i>Claim 14:</i>	98
3.	<i>Claim 54:</i>	98
4.	<i>Claim 71:</i>	98
X.	DISCRETION UNDER 35 U.S.C. § 325(D)	99
XI.	CONCLUSION	99
XII.	MANDATORY NOTICES UNDER 37 C.F.R. § 42.8	100
A.	REAL PARTY-IN-INTEREST UNDER 37 C.F.R. § 42.8(B)(1).....	100
B.	RELATED MATTERS UNDER 37 C.F.R. § 42.8(B)(2)	100
C.	LEAD AND BACK-UP COUNSEL UNDER 37 C.F.R. § 42.8(B)(3).....	100
	ADAM SEITZ (REG. No. 52,206)	101
	ADAM.SEITZ@ERISEIP.COM.....	101
	PTAB@ERISEIP.COM	101
D.	37 C.F.R. 42.8(B)(4) – SERVICE INFORMATION.....	101

I. INTRODUCTION

Apple Inc., (“Petitioner”) respectfully requests *inter partes* review (“IPR”) of claims 1-72 (“Challenged Claims”) of U.S. Patent No. 11,620,634 (“’634 Patent”).

II. THE ’634 PATENT

A. Description of the ’634 Patent

The ’634 Patent describes emulating a standard credit card with a device “capable of generating a programmed magnetic field of alternating polarity...when used in electronic credit card readers.” ’634 Patent (Ex. 1001), 2:17-23. The ’634 Patent also describes “generating a limited-duration payment number...which is limited in scope of use to a predetermined number of authorized transactions.” *Id.* at 2:28-32.

B. Field of Endeavor and Problem Solved by the Inventors

The ’634 Patent defines the “FIELD OF THE INVENTION” as relating to “electronic or smart payment devices and, more specifically, to more secure, smart multi-function smart tokenizing electronic payment devices and transaction processing thereof.” ’634 Patent, 1:25-31, 1:66-2:3 (criticizing existing systems as “susceptible to theft and/or compromise”). A POSITA would have understood that the field of endeavor of the ’634 Patent includes more secure payment cards, devices, and systems, and the ’634 Patent is trying 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 '634 Patent claims priority to Provisional Application No. 61/794,891, filed March 15, 2013. Because the '634 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.

The '634 Patent did not face any prior art rejections during prosecution. '634 *File History* (Ex. 1002).

D. Level of Skill of a POSITA

A POSITA at the time of the '634 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

¹ Petitioner does not concede that any of the Challenged Claims are entitled to claim priority to March 15, 2013. Multiple claims of the '634 Patent recite features not described in CardWare's provisional application.

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

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 '634 Patent is eligible for IPR.

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	1-2, 7-11 15, 27-28, 39, 41, 44-46, 49-50, 55-56, 60-63, 66-67, 72	Collinge (Ex. 1004), Lin (Ex. 1012), and Sahota (Ex. 1011)
2	3-6, 17-24, 29-32, 34-38, 40, 42, 47, 57-58, 64	Collinge, Lin, Sahota, Smith (Ex. 1010)
3	25-26, 33, 43, 48, 59, 65	Collinge, Lin, Sahota, Smith, and Kranzley (Ex. 1013)
4	10, 12-13, 16, 51-53, 68-70	Collinge, Lin, Sahota, Fadell (Ex. 1015)
5	10, 14, 54, 71	Collinge, Lin, Sahota, Yu (Ex. 1014)

The earliest claimed priority date of the '634 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 '634 Patent as shown:

³ Petitioner does not concede that any of the Challenged Claims are entitled to claim priority to March 15, 2013. Multiple claims of the '634 Patent recite features not described in the provisional application. Unless specifically noted, the analysis

Reference	Filed	Published	Prior Art Basis
Collinge	3/14/2013	10/3/2013	§102(e) ⁴
Lin	8/11/2009	4/8/2010	§102(b)
Sahota	8/18/2003	2/24/2005	§102(b)
Smith	11/17/2009	5/20/2010	§102(b)
Kranzley	6/1/2009	5/20/2010	§102(b)
Fadell	9/9/2008	3/26/2009	§102(b)
Yu	6/20/2008	12/24/2009	§102(b)

None of these references were cited or discussed during prosecution of the '634 Patent.

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 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.*, ¶¶80-86. *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).

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

For purposes of this proceeding only, Petitioner adopts the following constructions, proposed by Patent Owner in the underlying litigation. Ex. 1016.

Claim language	Patent Owner's Construction
Claim 4: “reduce”	“produce”
Claim 4: “via said NFC for receipt by an NFC recipient”	“via said NFC interface for receipt by an NFC recipient”
Claim 5: “Lather”	“further”
Claim 18: “in place of the issued payment account information said NFC interface”	“in place of the issued payment account information via said NFC interface”
Claim 28: “preforming”	“performing”

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

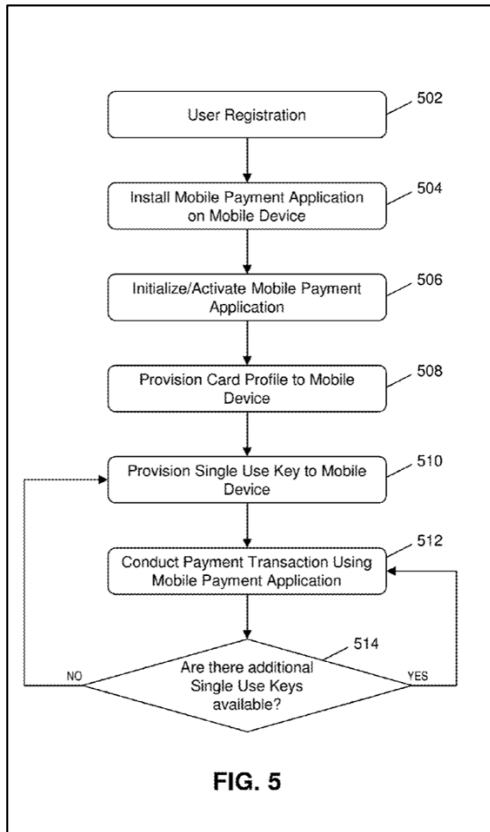
⁵ Petitioner's application of prior art to the Challenged Claims is not a waiver of any argument in litigation that any claim is indefinite, invalid, or requires claim construction.

IV. SHOWING OF ANALOGOUS PRIOR ART

A. Collinge

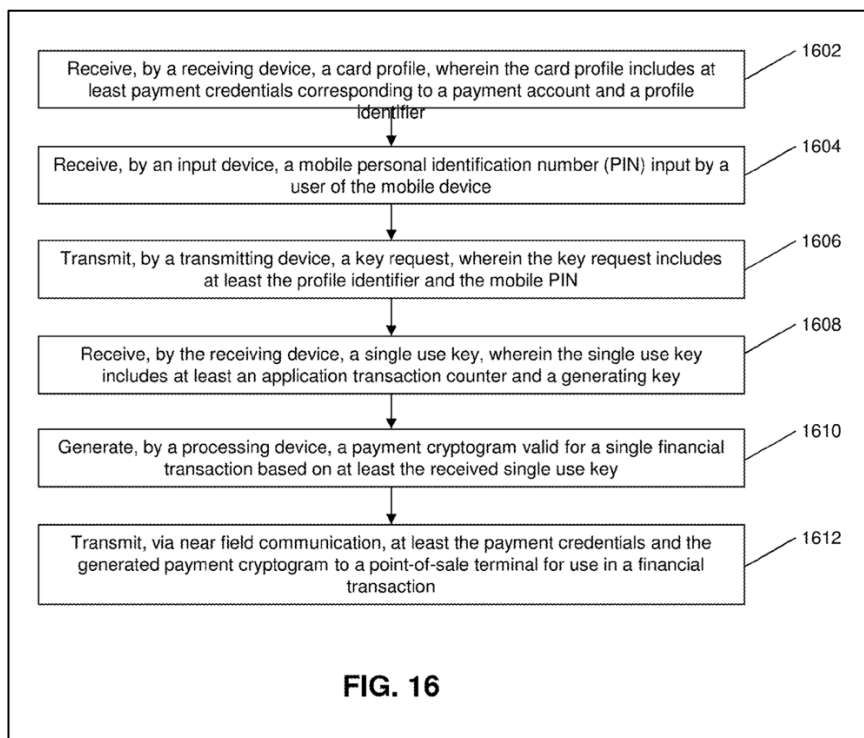
Collinge teaches “[a] method for generating and provisioning payment credentials to a mobile device lacking a secure element” which payment credentials may be used “in conducting a near field financial transaction.” *Collinge*, Abstract; [0002].

Collinge teaches 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 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 generated 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

Collinge’s provisional applications are directed to the same invention. Figures, invention elements numbering, and invention descriptions substantially overlap, and a POSITA would recognize 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.*, ¶¶81-86.

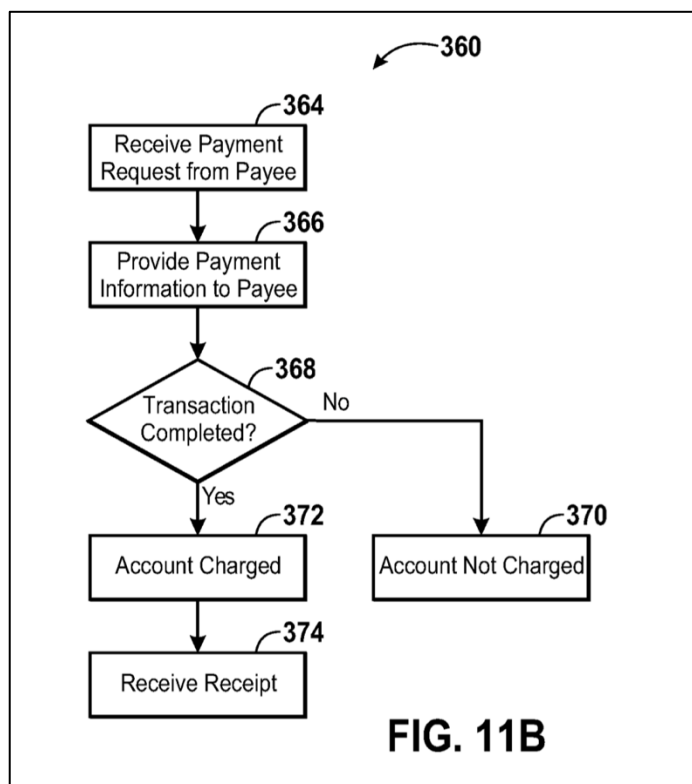
Even if Collinge’s Provisionals were directed to different payment system embodiments, it would have been obvious, and a POSITA would have been motivated to apply the teachings in Collinge’s Provisionals in Collinge’s payment system. *Dec.*, ¶¶81-86. For example, Collinge’s provisional applications provide 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.*, ¶¶81-86.

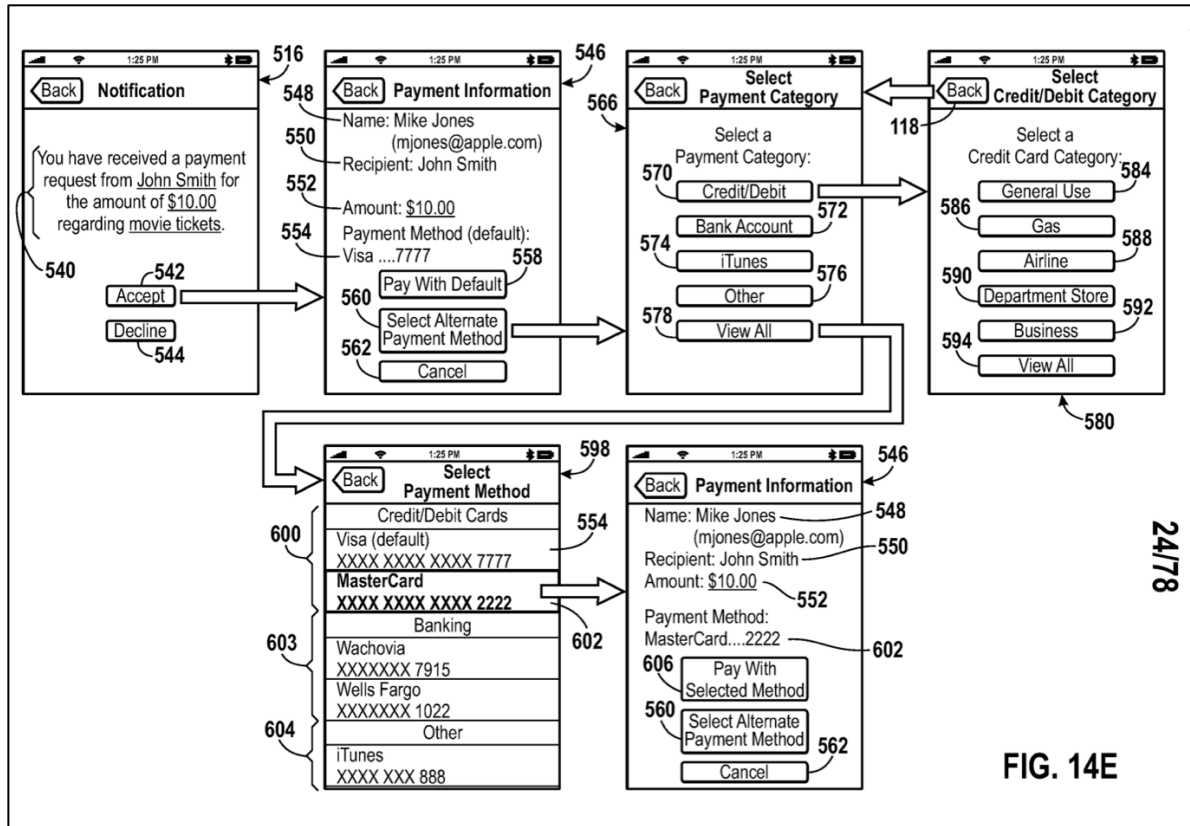
In each case, a POSITA would have found a teaching, suggestion, or motivation in Collinge itself that would have led them to apply the additional details in Collinge's *Provisionals* to Collinge's payment system with a reasonable expectation of success. *Dec.*, ¶¶81-86.

B. Lin

Lin teaches "payee device 10 may first transmit a payment request 384 to the payor device 92...payment request 384 may include the amount of the requested payment, the identity of the payee, as well as additional information with regard to the nature or reason for the payment request." *Lin*, 56:21-57:2. This "request for payment is transmitted from a first device IO to a second device 92 using a near field communication (NFC) interface 46." *Lin*, Abstract. Specifically, in method step 364, payor electronic device receives a request for payment via its wireless NFC interface from a payee device. *Id.*, Fig. 11B, 55:7-15; *see also, id.* at Fig. 14B, 70:8-27.



Lin, Fig. 11B. *Lin* teaches displaying, on the touch-screen display, information reflecting the payment request.



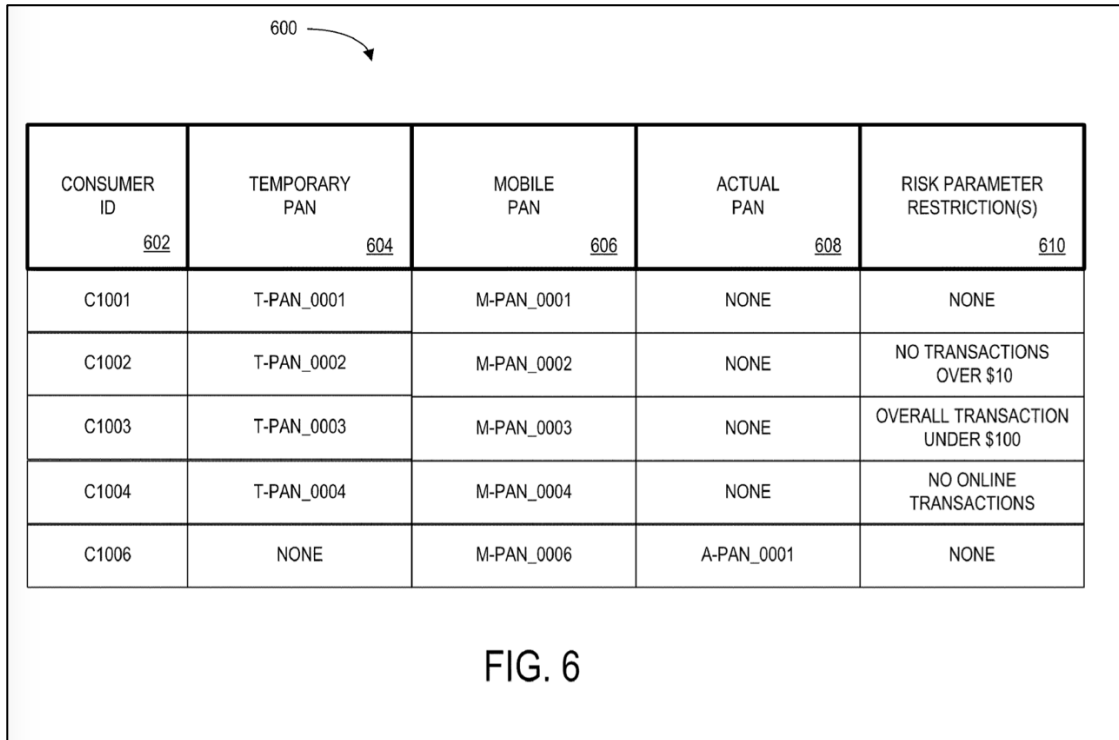
Lin, Fig. 14E.

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].



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. Sahota

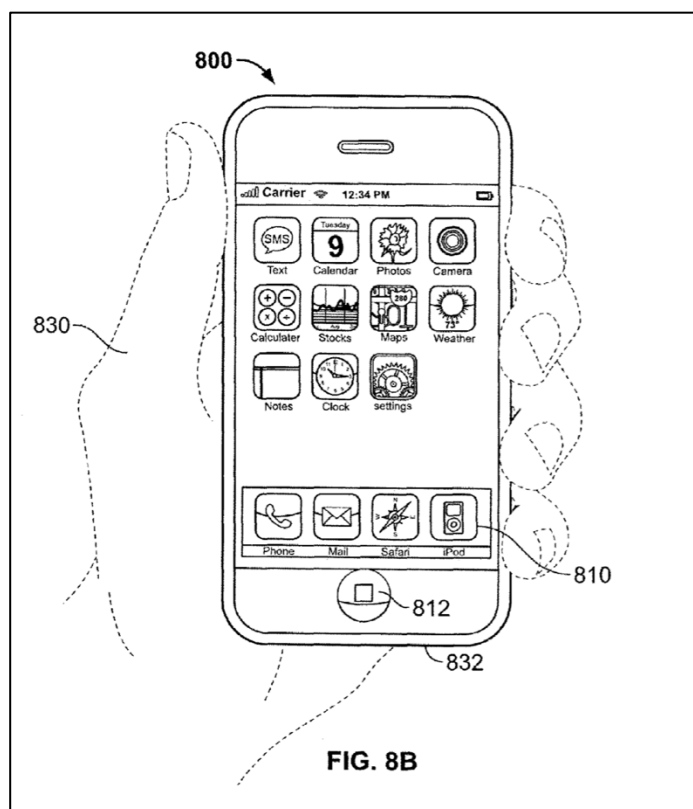
Sahota teaches the “payment device will also maintain an application transaction counter (ATC).” *Sahota*, [0028]. The “service provider computer compares the ATC received from the payment device to the corresponding ATC stored on the service provider computer to determine if the received ATC is the expected next ATC 635.” *Sahota*, [0038].

E. Kranzley

Kranzley teaches using a virtual PAN (VPAN) in place of the PAN. The VPAN “may have its own virtual expiry date.” *Kranzley*, [0036].

F. Fadell

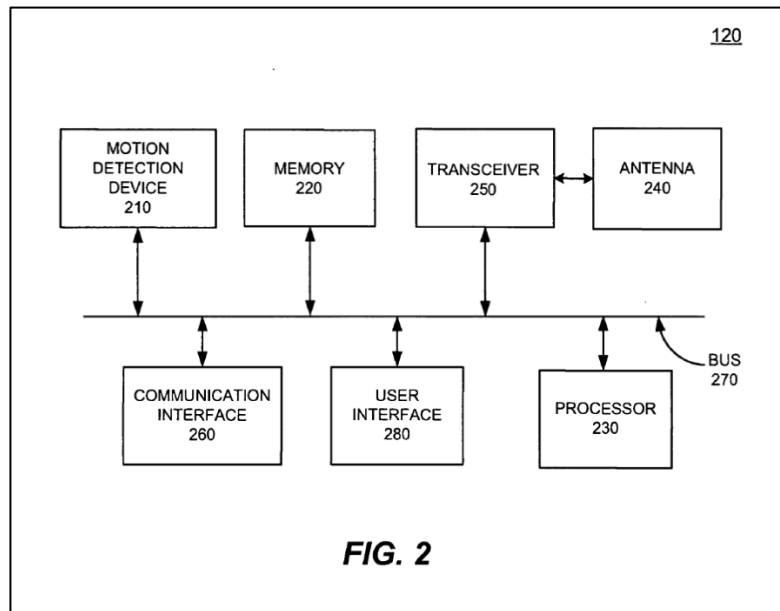
Fadell teaches “a sensor 720 may be placed behind a home button of a portable media player or cellular telephone (e.g., button 812, FIG. 8B)” used to “detect the features of the user’s finger for authenticating the user.” *Fadell*, [0065]-[0066].



Fadell, Fig. 8B. The user is “authenticated by comparing the detected biometric attributes with a library of biometric attributes stored by or accessible to the electronic device.” *Fadell*, [0006].

G. Yu

Yu teaches a “mobile device” that includes a “motion detection device 210[.]”
Yu, [0027].



Yu, Fig. 2.

Yu’s mobile phone motion detection device “can comprise one or more accelerometers, gyros, inclinometers, cameras, tilt sensors, or any other sensors that can determine the motion of a device within N degrees of freedom[.]” *Yu*, [0028]. The output of the “motion detection device 210 can be processed by processor 230 with instructions in memory 220 to extract features from the movement of the mobile device to verify both the identity and presence of a mobile user.” *Yu*, [0028]. If the user is verified “control passes to action 410 for further processing. In action 410 access to the service or device is granted. Access includes providing admission to mobile internet services, mobile banking or e-commerce, usage of the mobile

communication device 120, usage of selected services or software in the device, or right to use selected hardware resources.” *Yu*, [0038].

A. Analogous Art

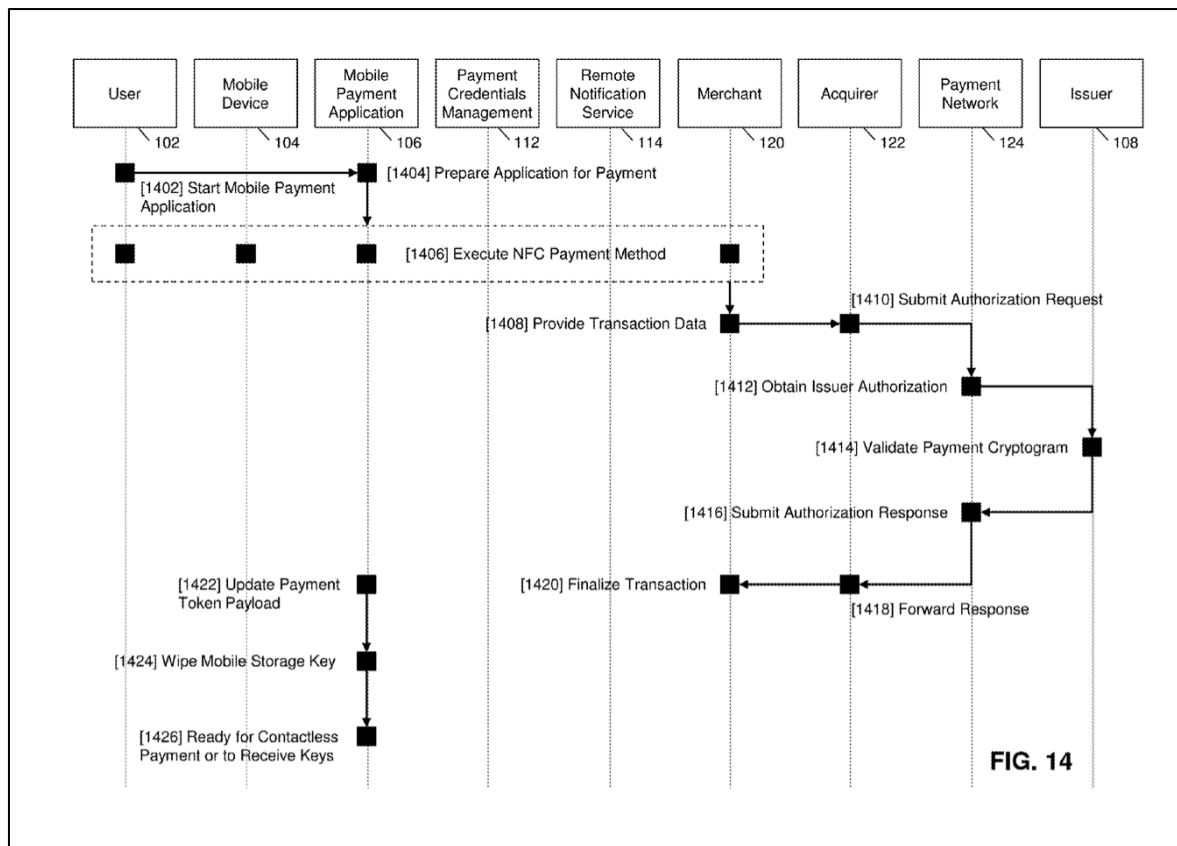
The applied prior art references disclose conducting secure payment transactions, secure systems for accessing payment credentials, and authentication systems for accessing restricted payment information on a mobile device and are in the same field of endeavor as the '634 Patent. *Compare '634 Patent*, Abstract, 1:26-31, 11:63-12:12, Fig. 1 *with Collinge*, Abstract, [0005], Fig. 1; *Smith*, Abstract, [0021]-[0023]; *Lin*, Abstract, 68:13-25, Fig. 14C; *Sahota*, Abstract, [0008], Fig. 1; *Kranzley*, Abstract, [0010], Fig. 1; *Fadell*, Abstract, [0031]; *Yu*, [0004], [0025], [0038]; *Dec.* ¶¶78-79, 90-91, 94-95, 98-99, 101-102, 105-106, 109-110.

Further, each of the applied prior art references is reasonably pertinent to problems addressed by the '634 Patent such as increasing security of payment transactions or providing secure access to mobile applications through specific user interactions with a user interface. *Compare '634 Patent*, 1:26-31, 1:66-2:3, 11:63-12:12, *with Collinge*, [0003]-[0005]; *Dec.*, ¶¶78-79; *Smith*, [0002], [0015], [0020]; *Dec.*, ¶¶90-91; *Lin*, 27:26-28:15; *Dec.*, ¶¶94-95; *Sahota*, [0004], [0021], [0028]; *Dec.*, ¶¶98-99; *Kranzley*, [0003], [0065]; *Dec.*, ¶¶101-102; *Fadell*, [0004], [0054], [0064]; *Dec.*, ¶¶105-106; *Yu*, [0007]-[0008], [0018], [0038]; *Dec.*, ¶¶109-110. Therefore, each of the applied prior art references is analogous art to the '634 Patent.

V. GROUND 1: *COLLIGE* IN VIEW OF LIN IN VIEW OF SAHOTA

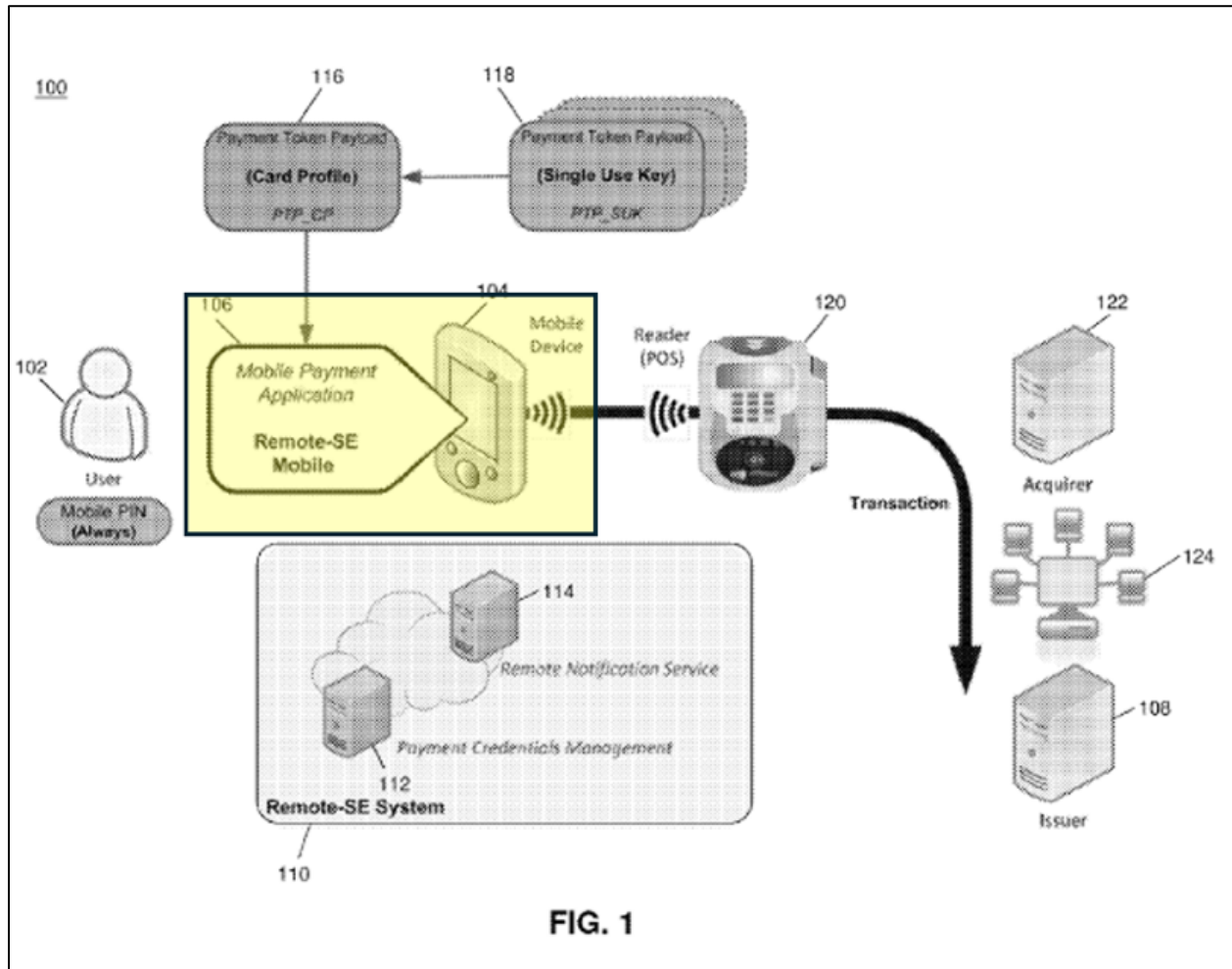
1. *1(Pre): “A method of generating and using limited-use payment information for performing a payment transaction, the method comprising:”*

Collinge teaches a method of generating and using a single-use payment cryptogram (*limited-use payment information*⁶) for performing a payment transaction. *Collinge*, [0029] (Collinge teaches “a *method* for conducting a payment transaction using the mobile device[.]”).



⁶ Claim language identified with *italics* and underline.

Collinge, Fig. 14. Collinge's mobile device's "mobile payment application 106 may generate a payment cryptogram...and may transmit the generated cryptogram and payment credentials to a point-of-sale terminal 120." *Collinge*, [0070]. Collinge's payment cryptogram is "valid for a single financial transaction." *Collinge*, [0128].

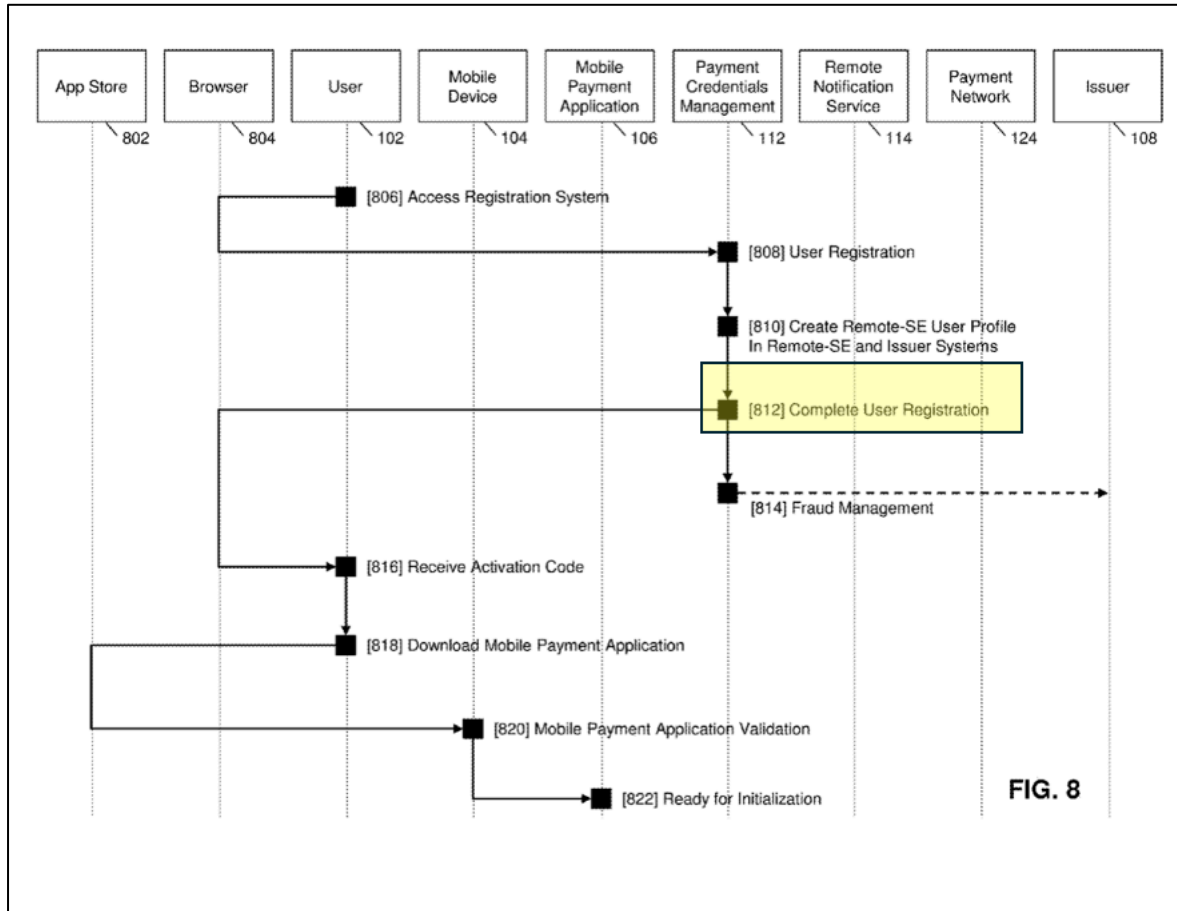


Collinge, Fig. 1 (annotated).

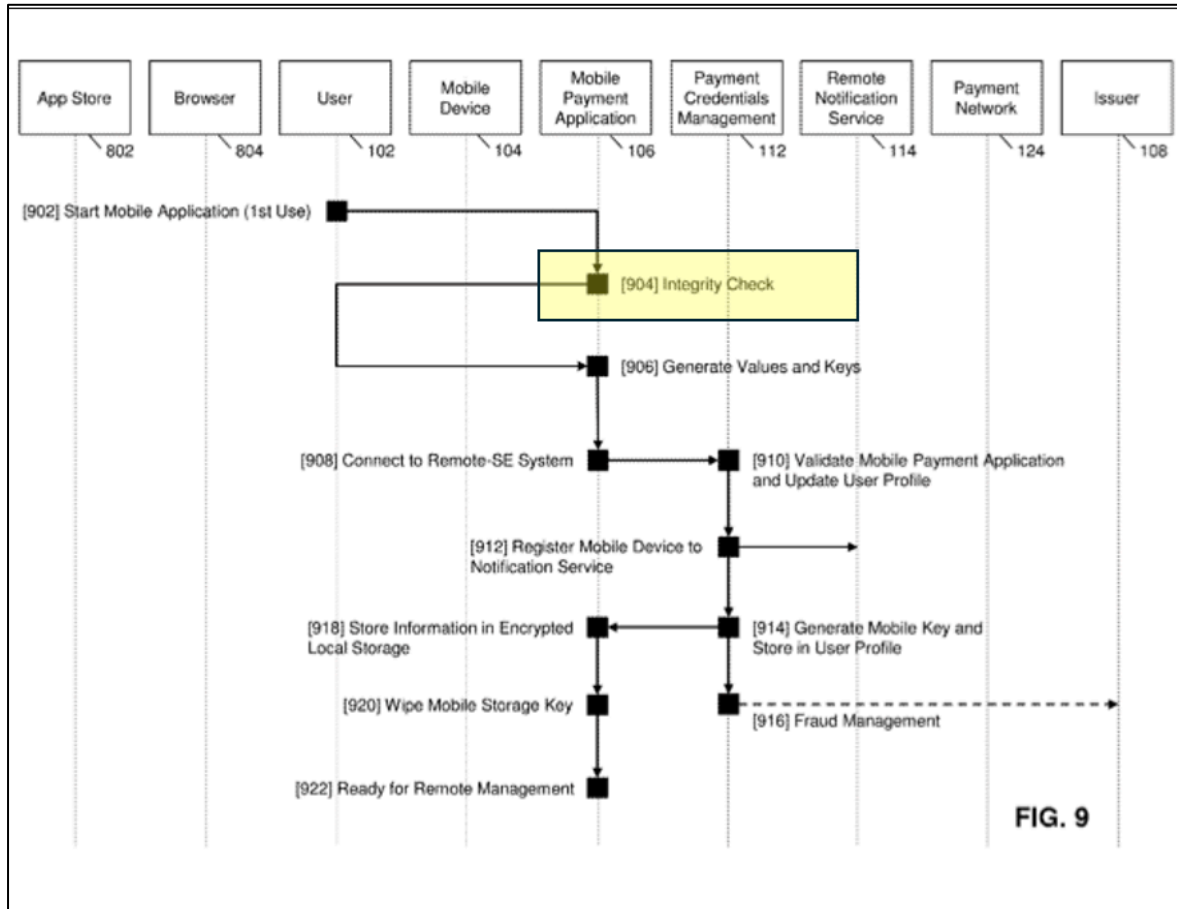
2. *1(a): “receiving an input at an electronic device, wherein the input comprises a priming operation, and, wherein the electronic device comprises:”*

The touch screen of Collinge’s mobile device 104 (*electronic device*) receives input that corresponds to a *priming operation* (which may include a user inputting an activation code, PIN, or bringing the mobile device within receiving proximity of an NFC reader) of the electronic device by an *identified user* (an authenticated user).

Collinge teaches in the registration process, the user “receive[s] an activation code and...a unique identifier used to identify the user 102.” *Collinge*, [0065]. Then when the user is ready to make a payment, the user will start the mobile payment application, and an integrity check is performed (a *priming operation*) before the user is allowed to access payment credentials. *Collinge*, Fig. 8, [0092]-[0093]. During 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] (emphasis added).

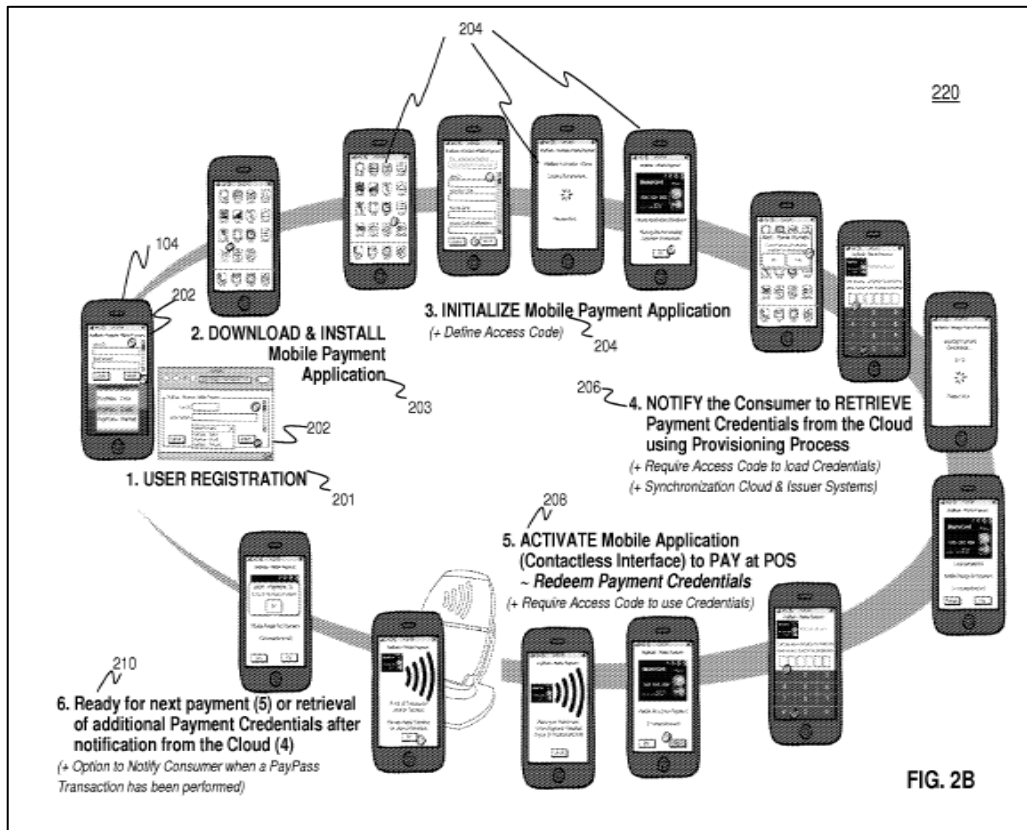


Collinge, Fig. 8 (annotated).



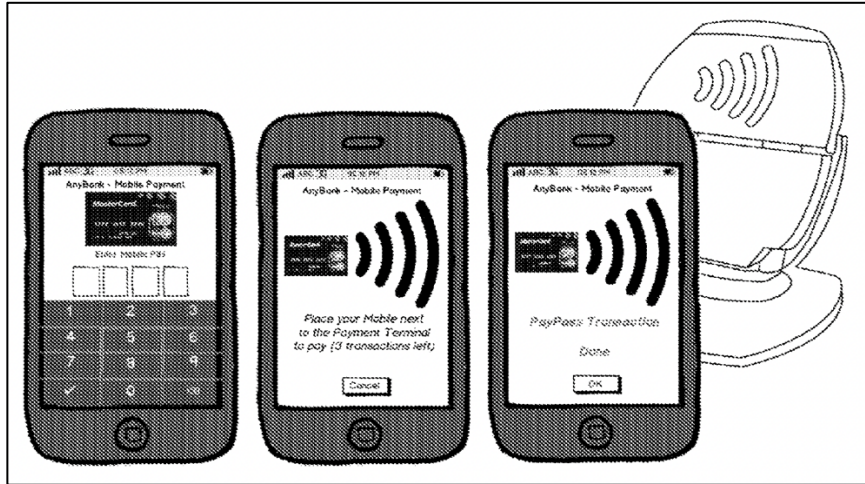
Collinge, Fig. 9 (annotated). A POSITA would have understood Collinge’s process of a user inputting an activation code into Collinge’s mobile device as a priming operation. *Dec.*, ¶¶120-123.

Figure 2B (below) which Collinge incorporates by reference further describes a code used to identify a user and to prime the electronic device for payment. For example, in Step 4 the user must provide their access code in order to load payment credentials, and in Step 5 the user must provide an access code in order to use payment credentials—each of these steps is a priming operation. ’248 *Provisional*, Fig. 2B; *Dec.*, ¶122.



'248 *Provisional*, Fig. 2B. Collinge teaches the correct access code is required to load credentials. '248 *Provisional*, Fig. 2B. *Dec.*, ¶122.

Collinge teaches 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, which is likewise a priming operation. *Collinge*, [0133]. *Dec.*, ¶¶124-125. Collinge teaches the user "must always provide the Mobile PIN for all PayPass transactions[.]" '098 *Provisional*, 99.



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

In addition, the user must place Collinge's mobile device within range of the payment terminal, as directed by the UI (see '098 Provisional, 99; '248 Provisional, Fig. 2B), which may form part of a priming operation. '248 Provisional, Fig. 14. ("NFC tap"); Ex.1001, Claim 7. Dec., ¶¶126.

3. ***1(a)(1): "a processor;"***

Collinge's mobile device (electronic 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").

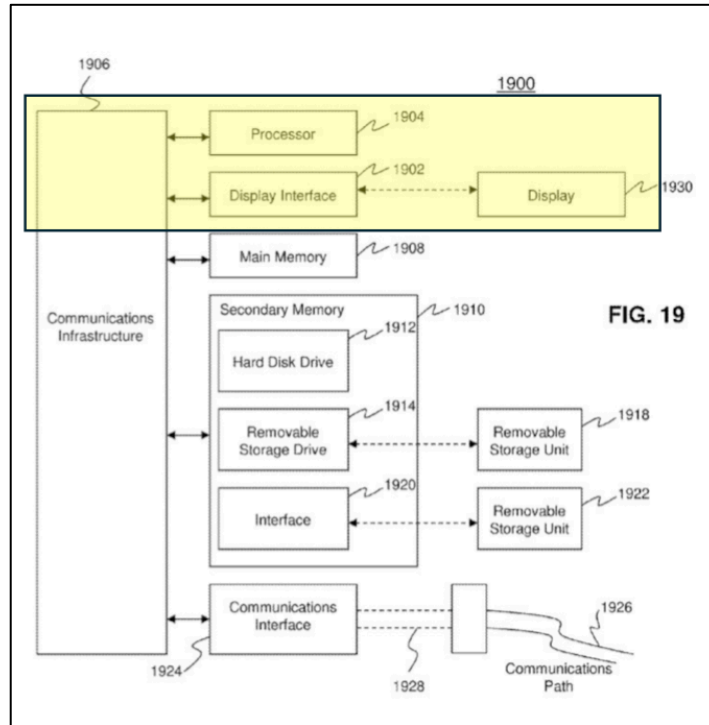
4. ***1(a)(2): "a touch-screen display coupled to the processor; and"***

Collinge teaches mobile device 104 includes a touch screen display. Collinge identifies the "touch screen" of "mobile device 104" as "an input device." Collinge, [0133]. Collinge teaches its touch screen receives a **user's input** of a "mobile

personal identification number (PIN)” during generation of a payment cryptogram. *Collinge*, [0133]. Therefore, Collinge’s touch screen is a user input device. *Dec.*, ¶¶128, 210.

Collinge further teaches the touch screen of mobile device 104 is coupled to the processor. Collinge teaches “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 the processor, as further shown in Fig. 16 below. *Collinge*, [0147], Fig. 16., *Dec.*, ¶¶129-137.

Collinge’s payment system comprises a display interface and display that is “coupled” to the processor via the communication interface:



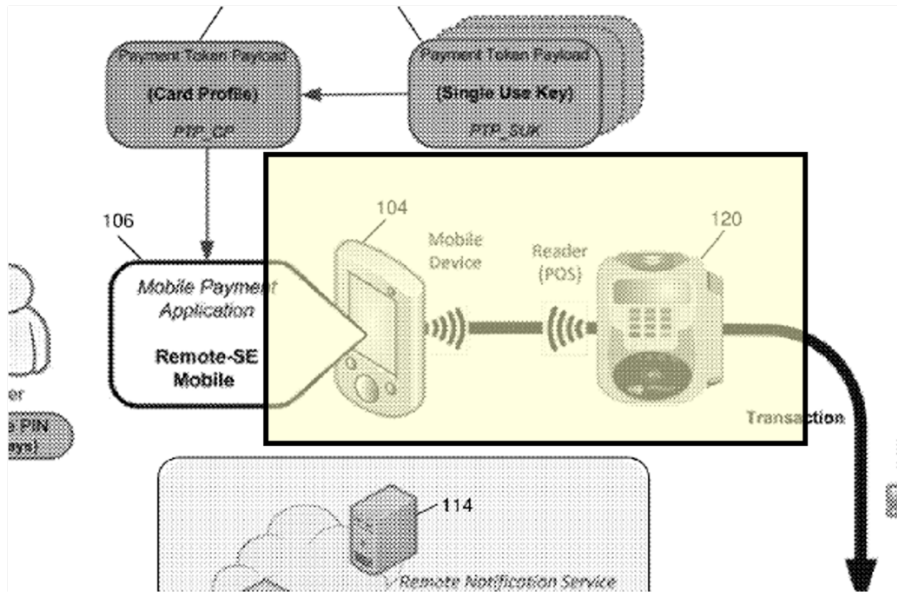
Collinge, Fig. 19. (annotated). *Collinge* teaches the communications infrastructure may be a “bus, message queue, network, multi-core message-passing scheme, etc.” *Collinge*, [0150]. For this additional reason, *Collinge* teaches a display interface (the touchscreen) and the display is coupled to a processor. *Dec.*, ¶¶129-137.

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.*, ¶¶133-137. 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*, [0246], [0017], [0048].

A POSITA would have understood Collinge's display interface is Collinge's touchscreen. *Dec.*, ¶¶133-137.

5. *1(a)(3): “a near field communications (NFC) interface coupled to the processor;”*

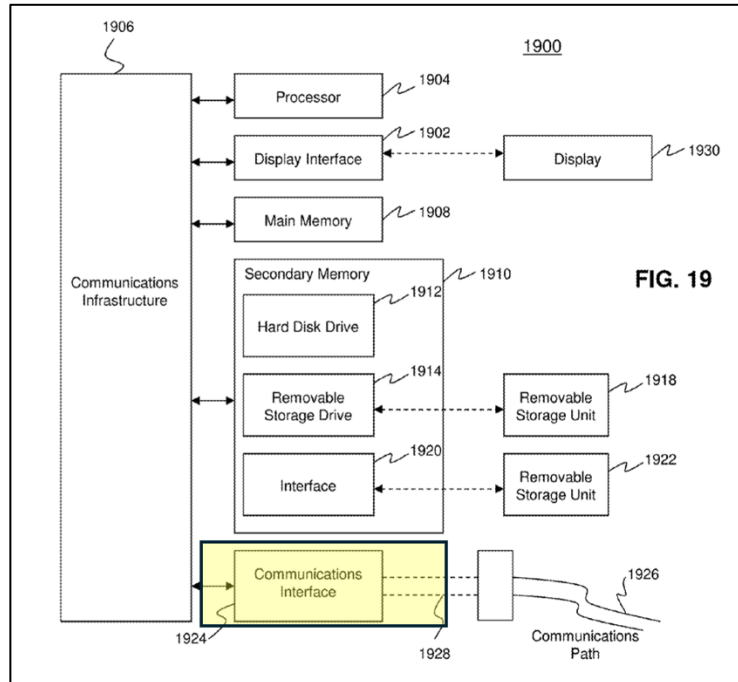
Collinge teaches a near field communications (NFC) interface. *Collinge*, [0041] (Collinge's mobile device can “conduct payment transactions via near field communication[.]”). Per Collinge, a person having skill in the relevant art would have been familiar with methods for performing contactless payments via NFC. *Collinge*, [0041], [0044], [0070], [0086], [0120]. NFC had long been standardized by the time of the '634 Patent, Collinge teaches mobile device 104 has an NFC interface, and a POSITA would have recognized that an NFC interface is required to conduct NFC payment transactions as taught by Collinge. *Collinge*, [0041]; '248 *Provisional*, [0067] (**NFC interface of the mobile device 104...**”), [0184]. *Dec.*, ¶¶138-140.



Collinge, Fig. 1 (annotated excerpt).

Collinge further teaches the near-field communication interface is coupled to the processor. Collinge teaches, and a POSITA would have understood to transmit payment information to a POS terminal via NFC in Collinge's mobile device, the NFC interface must necessarily be coupled to a processor. *Collinge*, [0135], [0147], Fig. 16., *Dec.*, ¶¶141-144.

As shown below, Collinge teaches the payment system comprises a communications interface that is “coupled” to the processor:



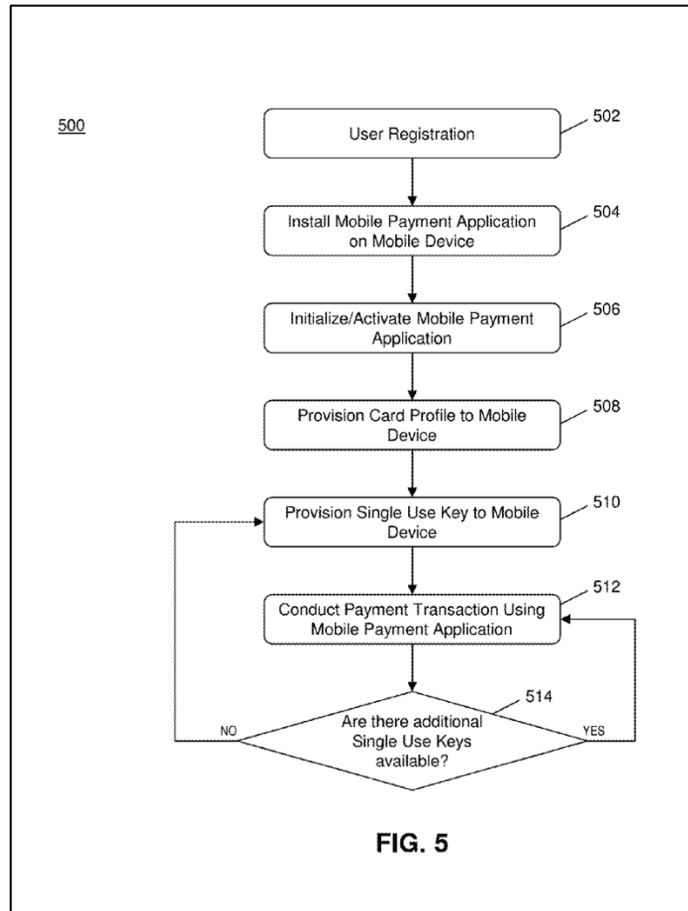
Collinge, Fig. 19 (annotated).

Collinge teaches “[s]oftware and data transferred via the communications interface 1924 may be in the form of signals, which may be electronic, electromagnetic...The signals may travel via a communications path 1926, which may be configured to carry the signals and may be implemented using...a radio frequency link...” *Collinge*, [0154]. It was well known in the art that NFC uses a radio frequency link. *Dec.*, ¶144. It was well known in the art that NFC uses electromagnetic signals, and specifically radio waves and magnetic fields to transmit data. *Dec.*, ¶144. *Collinge* teaches that the communications infrastructure may be a “bus, message queue, network, multi-core message-passing scheme, etc.” *Collinge*, [0150]. Therefore, a POSITA would have understood that *Collinge*’s NFC interface (communications interface) is coupled to the processor. *Dec.*, ¶144.

6. *1(b): “responsive to said priming operation, readying said device to perform a payment transaction by an identified user;”*

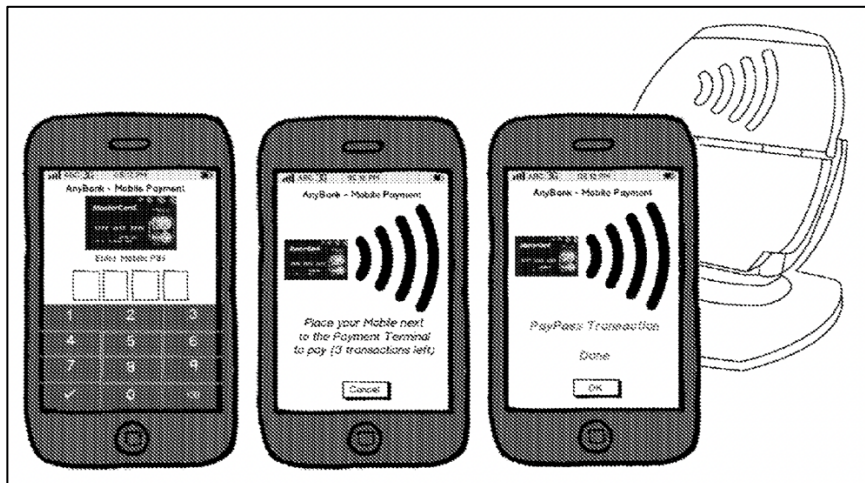
As discussed above in Claim 1(a), Collinge teaches identifying a user via an integrity check. Collinge teaches responsive to a priming operation (see Claim 1(a)), provisioning the card profile and single use keys to Collinge’s mobile device (readying said device to perform a payment transaction) by an identified user.

Collinge teaches “[i]n step 506, the user 102 may initialize/activate the mobile payment application 106” by “enter[ing] the activation code received in step 502 into the mobile payment application 106.” *Collinge*, [0067]. After this integrity check during the initialization process, the “remote-SE system may transmit both the card profile 116 and a single use key 118 to the mobile payment application 106[.]” *Collinge*, [0069]. Collinge’s payment cryptogram is then generated “using the generating key included in the single use key” that was previously provisioned to the mobile device. *Collinge*, [0077], [0043]. Collinge’s device therefore readied to perform a payment transaction responsive to the user inputting the activation code. *Dec.*, ¶¶146-148.



Collinge, Fig. 5. *See also* Figs. 9, 14.

Collinge further teaches instructing the user to bring the electronic device near an NFC recipient and inputting a PIN, which each form part of priming operations and also ready the device to perform a payment transaction by an authorized user. '098 *Provisional*, 99; *Collinge*, [0094], [0128], [0133].



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

7. ***1(c): “receiving a payment request for the payment transaction at said electronic device;”***

Collinge, in view of Lin, renders obvious receiving a payment request for the payment transaction at Collinge’s electronic device via Collinge’s NFC interface. Dec., ¶¶149-154.

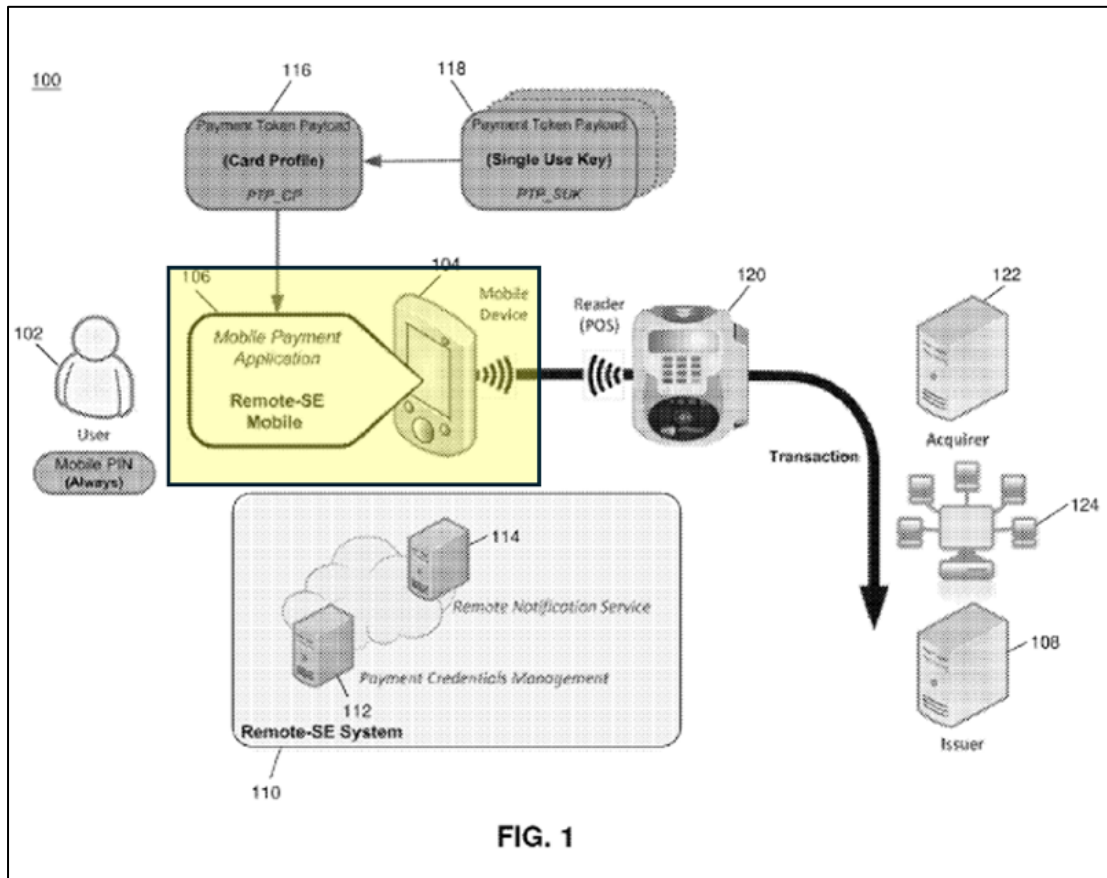
(a) Collinge’s Teachings

Collinge’s mobile device receives data from a POS terminal during a payment transaction. 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].

Collinge also teaches conducting a payment transaction involves NFC communications between the mobile device and a POS terminal, but does not describe how the transaction is initiated. *Collinge*, [0145] (“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.”); [0135].

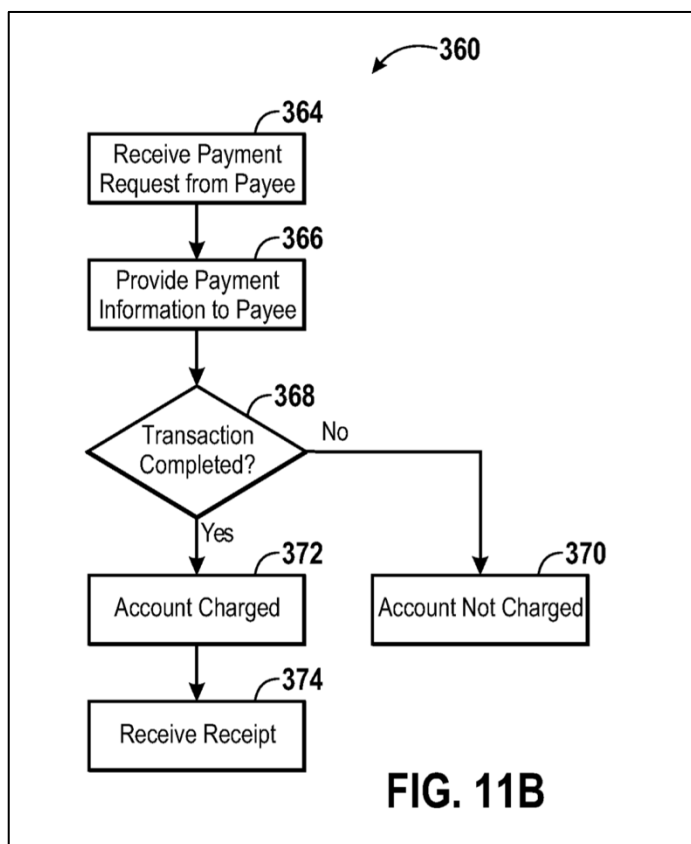
Collinge also teaches conducting a payment transaction involves NFC communications between the mobile device and a POS terminal. *Collinge*, [0145]. (“the application transaction counter may be transmitted, via near field communication, to the point-of-sale terminal 120 for including in an authorization request in a financial transaction.”)



Collinge, Fig. 1. (annotated).

(b) Lin's Teachings

In analogous art, Lin teaches a payment method where “a request for payment is transmitted from a first device 10 to a second device 92 using a near field communication (NFC) interface 46.” *Lin*, Abstract. Specifically, in method step 364, payor electronic device receives a request for payment via its wireless NFC interface from a payee device. *Id.*, Fig. 11B, 55:7-15; *see also, id.* at Fig. 14B, 70:8-27.



Lin, Fig. 11B.

(c) Motivation to Combine

It would have been obvious, and a POSITA would have been motivated to configure Collinge's mobile device to receive a request for payment via the mobile

device's NFC interface, as taught by Lin. *Lin*, 4:3-5; *Dec.*, ¶153. At the time, it was common for an NFC point-of-sale (POS) terminal to initialize a transaction by sending a data request and for an NFC-enabled mobile phone to respond by providing payment credentials, as taught by Lin. *Dec.*, ¶153. A POSITA would have recognized this method allows the point of sale terminal greater control over the payment session, making it easier to enforce security measures, including session timeout. *Dec.*, ¶153. A POSITA would have further recognized when the POS terminal initiates the transaction, the POS terminal can send the mobile phone the payment amount (which the user can then verify before sending their payment credentials) as well as data that can be used by the mobile phone to generate a payment cryptogram. *Dec.*, ¶153; *Collinge*, [0145].

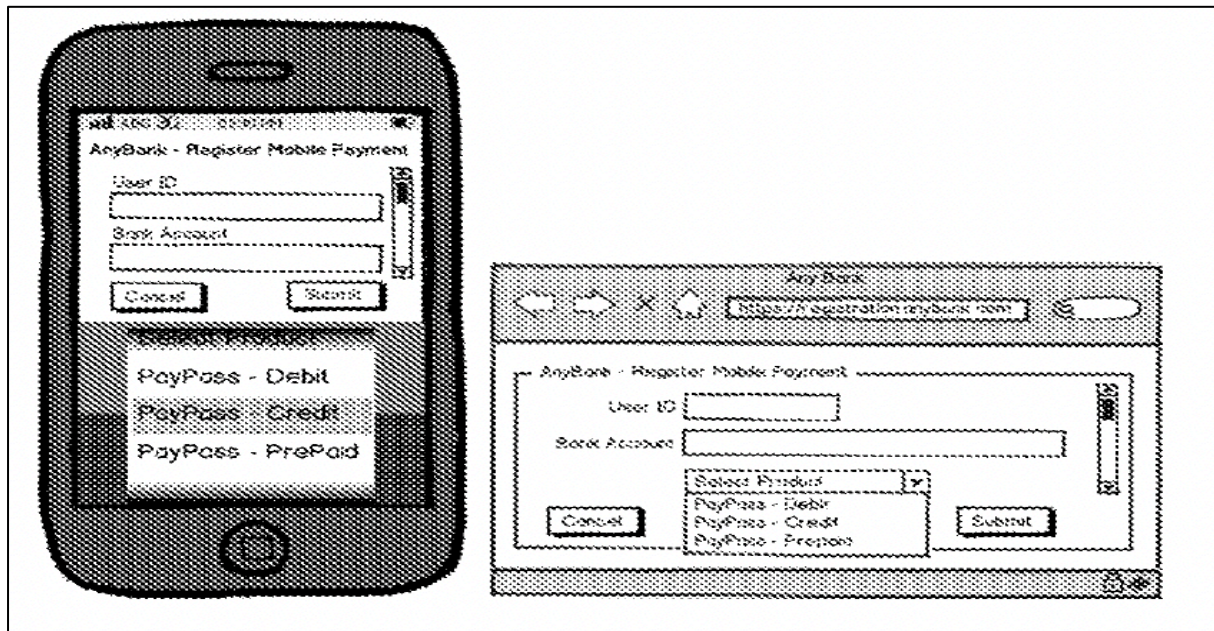
A POSITA would have been motivated to combine the prior art elements of *Collinge*'s mobile device having a wireless NFC interface with Lin's method step of a device receiving a payment request to yield the predictable result of increased security to verify transaction details and a POSITA would have had a reasonable expectation of success in making such a modification to *Collinge*. *Dec.*, ¶153.

8. ***1(d): "displaying, on the touch-screen display, information reflecting the payment request, and an image representing a selected issued payment account;"***

Collinge in view of *Lin* teaches displaying, on the touch-screen display of *Collinge*'s mobile device, the payment amount and payee (information reflecting the

payment request), and an image of the payment card used in the transaction (an image representing a selected issued payment account).

Collinge teaches “[p]ayment cards may include credit cards, debit cards, charge cards, stored-value cards, prepaid cards, fleet cards, virtual payment numbers, virtual card numbers, controlled payment numbers, etc.” *Collinge*, [0038]. Collinge teaches the user may select a card issuer payment method (i.e. Debit, Credit or Prepaid) on Collinge’s touch screen display:



'098 Provisional, 96; '248 Provisional, Fig. 2A-2B; Dec., ¶154.

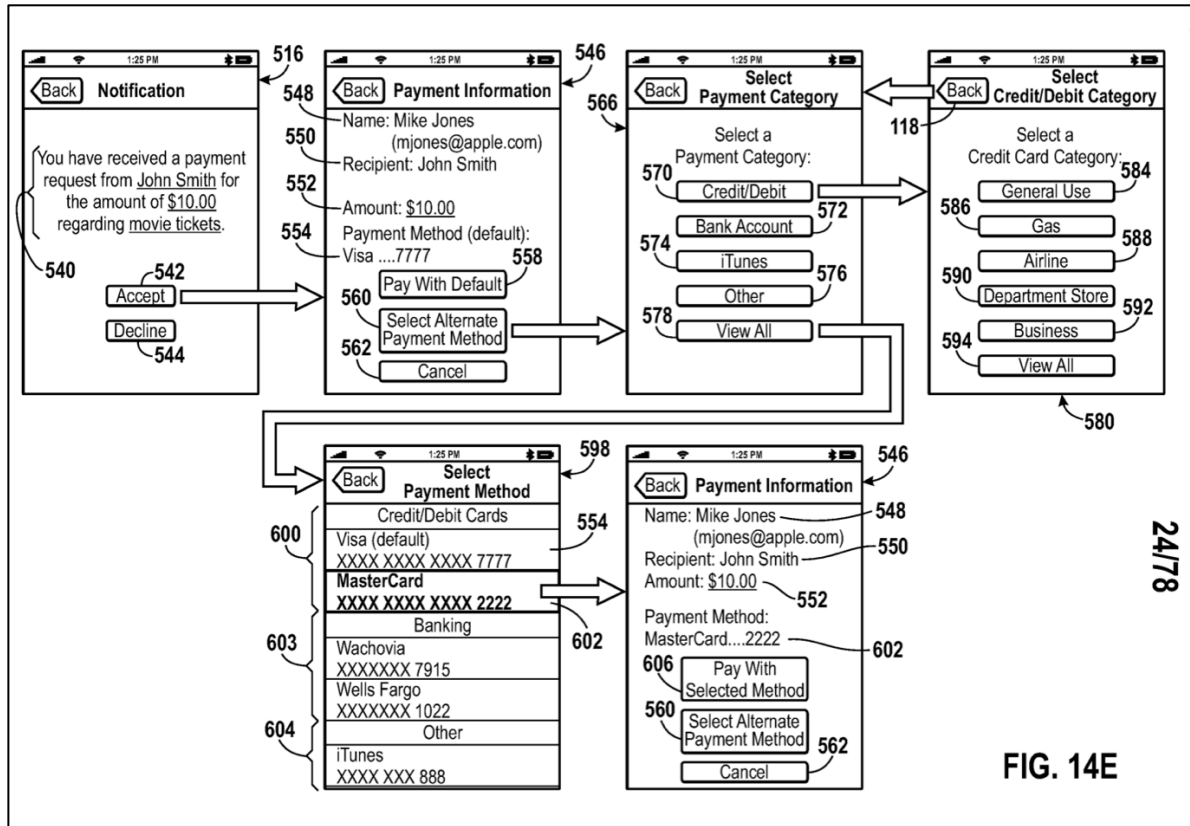
Collinge further teaches displaying on Collinge’s mobile device touch screen a payment card image including a logo and other card iconography (an image representing a selected issued payment account):



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

(a) Lin's Teachings

Lin teaches displaying, on the touch-screen display, information reflecting the payment request (amount). Lin teaches "payee device 10 may first transmit a payment request 384 to the payor device 92...payment request 384 may include the amount of the requested payment, the identity of the payee, as well as additional information with regard to the nature or reason for the payment request" which is information reflecting the payment request. Lin, 56:21-57:2.



Lin, Fig. 14E.

(b) Motivation to Combine

It would have been obvious, and a POSITA would have been motivated to configure Collinge's mobile payment application to display information reflecting the payment request (such as the payment amount and payee) as taught by Lin. *See* Lin, Fig. 22C; Claim 1(c). A POSITA would have been motivated to combine the prior art elements of Collinge's mobile device having a GUI and touchscreen interface with Lin's teaching of displaying information reflecting a payment request to yield the predictable result of a user being able to view the selected payment card, the payment amount, and the payee associated with the transaction. *Dec.*, ¶157. A

POSITA would have understood that showing the user the payee and payment on the touchscreen user interface would have provided an additional security feature by allowing the user to check again that the information is accurate, and immediately address any discrepancies or attempted fraud, such as the payment amount being increased without the user's knowledge. *Dec.*, ¶157. A POSITA would have had a reasonable expectation of success in making such a modification because displaying additional known information relating to a transaction on a display would have been well-within the capabilities of a POSITA. *Dec.*, ¶157. The combination is application of a known technique (displaying payment transaction information) to improve similar devices (mobile devices for conducting payment transactions) in the same way. *Dec.*, ¶157.

9. *1(e): “dynamically generating, by the processor, limited-use payment information;”*

Collinge teaches a processor operable to dynamically generate at least a limited-use payment information (payment cryptogram) and using said limited-use payment information in place of said card issuer supplied payment information (CVC).

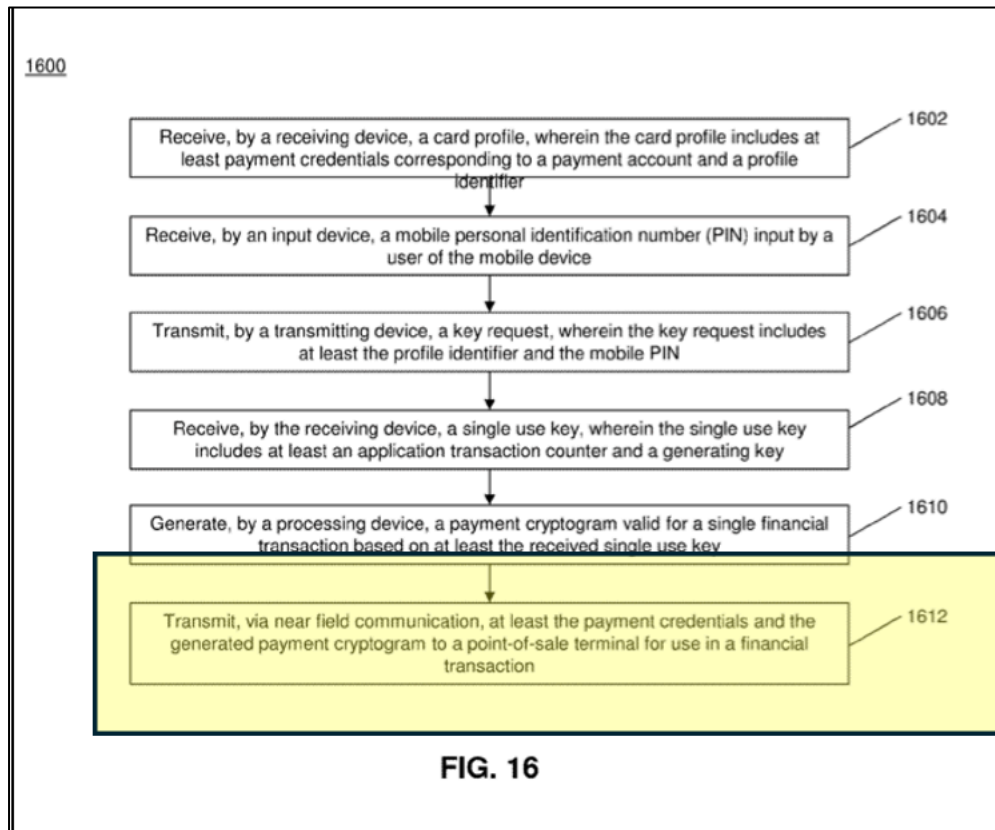
Collinge's mobile payment application is “stored in data storage of the mobile device 104 and **executed by a processor** included in the mobile device 104.” *Collinge*, [0041] (emphasis added). *Dec.*, ¶161.

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] (emphasis added); *Dec.*, ¶158-160. 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 at least: "the supplied CVC3 value, the session key unpredictable number, the application transaction counter, and the reader unpredictable number." *Collinge*, [0145]; '248 Provisional, Table 1.

The Mobile Payment Application use a specific process to generate the CVC3 using (KS _{UN} , Cloud_CVC3 _{TRACK1/2} , ATC and UN _{READER})
--

Collinge teaches and a POSITA would have understood Collinge's CVC3 is used instead of the card issuer's CVC in a transaction, including because it was well known in the art that Mastercard uses a CVC3 value to replace a conventional static CVC. *Dec.*, ¶160-161. Likewise, Collinge's CVC3 is combined with additional payment credentials, and the combined complete payment information (which is also

limited-use payment information) is used in place of an issuer-provided PAN and CVC.



Collinge, Fig. 16. (annotated), [0048], [0104] (card profile (PTP_CP); '098 *Provisional*, [0101] (“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.”).

10. 1(f): “wherein said limited-use payment information is dynamically generated based on a per-transaction sequential parameter originating from the electronic device;”

Collinge in view of Sahota teaches dynamically generating a payment cryptogram (limited-use payment information) based on an application transaction counter originating from Collinge’s mobile device.

(a) Collinge’s Teachings

Collinge teaches dynamically generating a payment cryptogram (limited-use payment information) based on an application transaction counter provisioned from the cloud system and stored on Collinge’s mobile device. *See* Claim 1(e); *Collinge*, [0145].

The cloud system “identify[ies] an encrypted payload based on a derived CVC3 key (KD_{CVC3}), wherein the encrypted payload includes...the application transaction counter.” *Collinge*, [0140]. The encrypted payload is transmitted “to the mobile device 104 for use in generating a CVC3 value for use in a financial transaction.” *Collinge*, [0141]. Collinge then stores the ATC in storage 304. *Collinge*, [0063]; [0076]; [0134]. *Dec.*, ¶162.

A POSITA would have understood that Collinge’s ATC corresponds to the claimed “per-transaction sequential parameter” and is updated each transaction. *Collinge*, [0050]; *Dec.*, ¶162.

(b) Sahota’s Teachings

In related art, Sahota teaches the “payment device will also maintain an application transaction counter (ATC).” *Sahota*, [0028].

(c) Motivation to Combine

A POSITA would have been motivated to modify Collinge’s mobile device to maintain an ATC as taught by Sahota. *Dec.*, ¶164. Collinge teaches that the ATC “may be a count of transactions used for **fraud management and authentication**[.]” *Collinge*, [0050]. A POSITA would have been motivated to modify mobile device 104 to maintain its own application transaction counter for use in generating the CVC3 in order to enhance the security of Collinge’s payment system. *Dec.*, ¶164. Having an ATC in sync in two different places was a known technique, and would have prevented possible fraud in Collinge’s payment system in the same way as in Sahota’s payment system. *Sahota*, [0038] (“service provider computer compares the ATC received from the payment device to the corresponding ATC stored on the service provider computer to determine if the received ATC is the expected next ATC 635.”). A POSITA would have had a reasonable chance of success in including ATC tracking in Collinge’s mobile device because at the time it was already common for devices to track an ATC and a POSITA would have been well-familiar with how a device-tracked ATC would be implemented. *Dec.*, ¶¶164-165.

- 11. 1(g): “using said limited-use payment information in connection with the payment transaction in place of issued payment**

information associated with said selected issued payment account;”

Collinge’s CVC3 is used instead of the card issuer’s CVC in a transaction.

See Claim 1(e).

12. 1(h): “transmitting said limited-use payment information from said electronic device via said NFC interface for receipt by an NFC recipient;”

Collinge’s mobile device conveys payment information, including a payment cryptogram (*limited-use payment information*) via Collinge’s *NFC interface* to a point of sale terminal (*NFC recipient*).

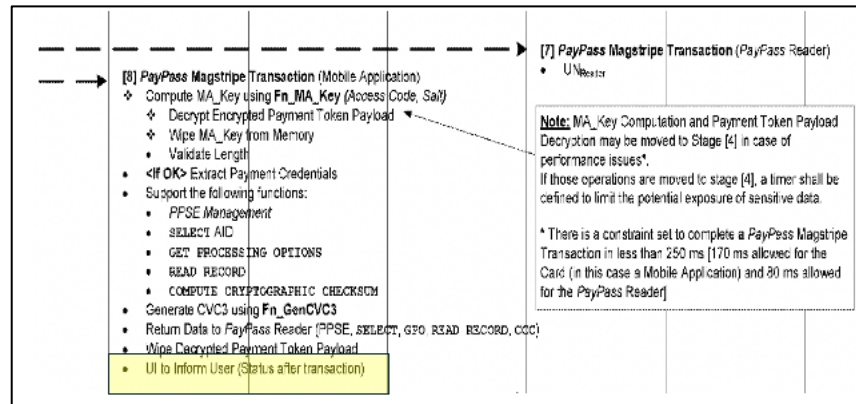
Collinge’s “mobile device 104 may conduct a **contactless/NFC payment transaction** using the mobile payment application 106[.]” *Collinge*, [0070] (emphasis added). Collinge’s mobile device transmits “the generated cryptogram and payment credentials to a point-of-sale terminal 120...via NFC.” *Collinge*, [0070], [0145] (“the generated payment CVC3 value and the application transaction counter may be transmitted, via near field communication, to the point-of-sale terminal 120”); [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.”).

13. 1(i): “responsive to the transmitting the limited-use payment information, receiving via the NFC interface information reflecting a status of said payment transaction; and displaying

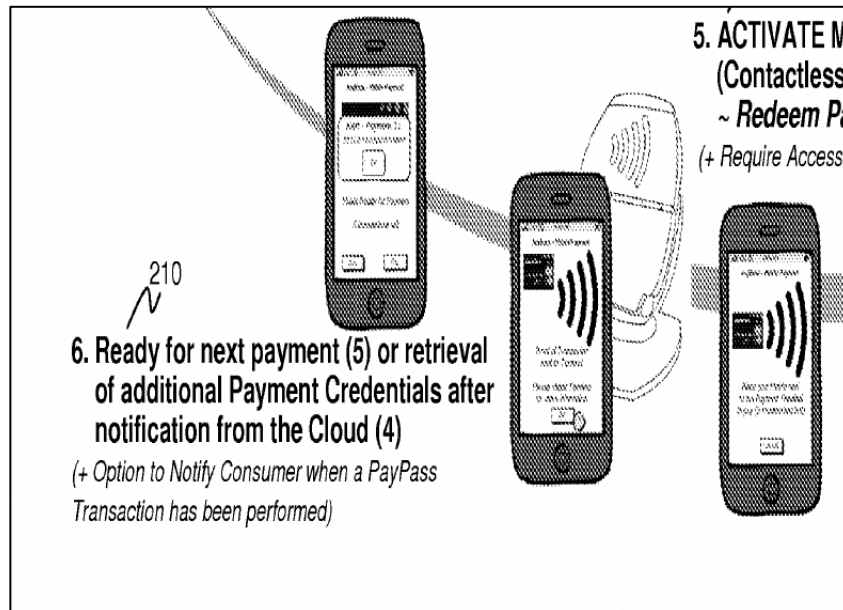
the status of said payment transaction via said touch-screen display.”

After Collinge’s mobile device transmits payment credentials and payment cryptogram (*limited-use payment information*) to a POS terminal, Collinge’s mobile device receives via Collinge’s NFC interface a status of the payment transaction and this status of the transaction is displayed on Collinge’s touch-screen display.

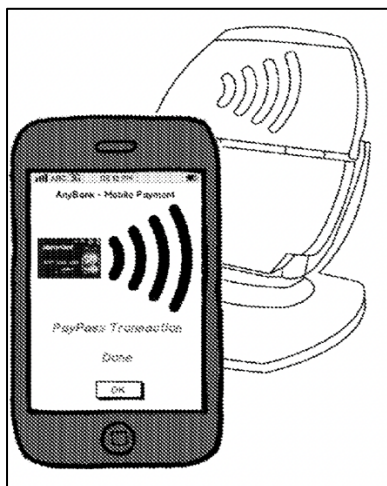
Collinge teaches “the mobile payment application 106 may display a notification to the user 102 via a user interface to indicate that the mobile payment application 106 is ready to conduct a contactless payment transaction.” *Collinge*, [0112]. Collinge further teaches that the UI will “notify[] the user 113 when a PayPass® transaction has been performed.” *’248 Provisional*, [0074].



’248 Provisional, Fig. 14 (annotated excerpt). As discussed above at Claim 1(c), Collinge’s mobile device communicates with the POS terminal and receives transaction information via the NFC interface, including transaction status as shown in Fig. 2B.



'248 Provisional, Fig. 2B.



'098 Provisional, 99 (excerpt); '248 Provisional, Fig. 2A-2B. Therefore, Collinge teaches and a POSITA would have understood that the UI notification of a status of a transaction is based on information received by Collinge's mobile device via the NFC interface. *Dec.*, ¶¶170-172.

14. Claim 2:⁷

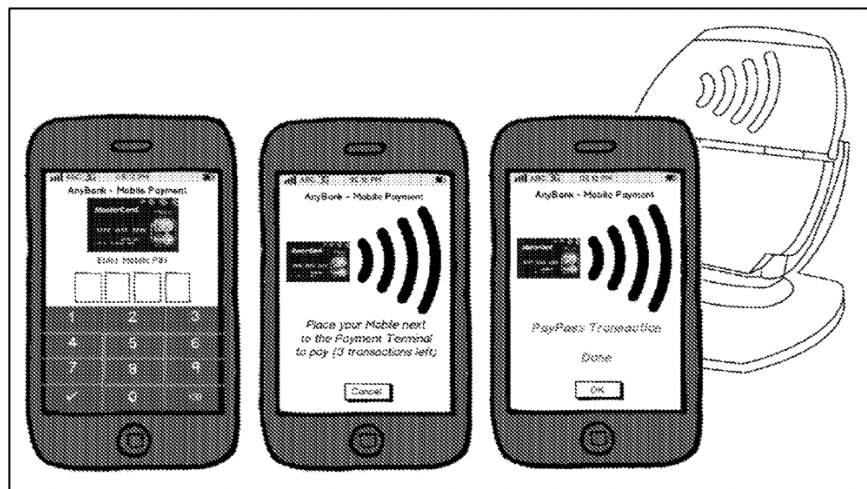
See Claim 1(e).

15. Claim 7:

See Claim 1(a).

- 16. 8(a): The method of claim 7, wherein said readying said device to perform a payment transaction comprises: identifying said proximity NFC recipient is an NFC payment facility; successfully validating the identified user as authorized to perform the payment transaction via said electronic device; and**

See Claim 1(a). Collinge's user interface instructs the user to provide a PIN (validating the identified user as authorized to perform the payment transaction via said electronic device) and then "place your Mobile next to the Payment Terminal to pay" (identifying said proximity NFC recipient is an NFC payment facility).



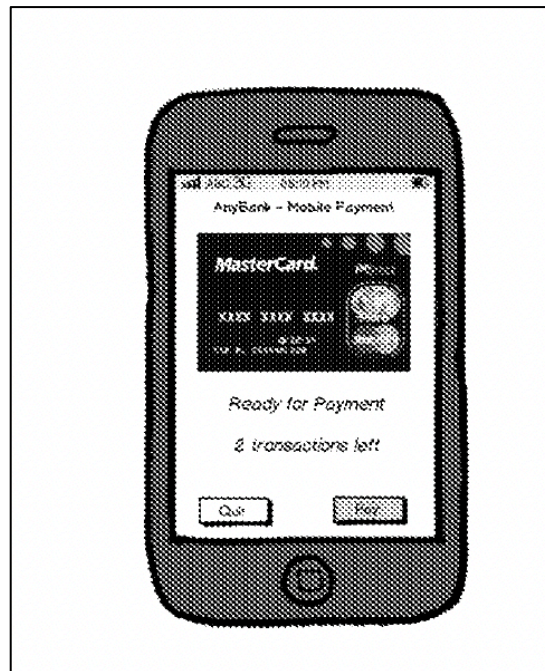
'098 Provisional, 99; '248 Provisional, Fig. 2B. Dec., ¶¶176-178. The user "must always provide the Mobile PIN for all PayPass transactions[.]" '098 Provisional, 99.

⁷ See Claim Appendix.

Dec., ¶179 (discussing how NFC payment standards handle determining the device is by a payment terminal).

17. 8[b]: receiving a user approval for performing the payment transaction.

Collinge receives a user approval for performing the payment transaction when a user selects “pay” during a transaction on Collinge’s touch screen display.



'098 Provisional, 100; '248 Provisional, Fig. 2B. Collinge teaches and a POSITA would have found it obvious that by selecting “pay,” a user would approve the transaction and by selecting “quit” the user would deny the transaction. Dec., ¶180.

18. 9[Pre]: The method of claim 8, wherein said user approval for performing a payment transaction comprises displaying a request for user input at said electronic device, for both said identifying

and said user approval of said payment transaction, and further comprising:

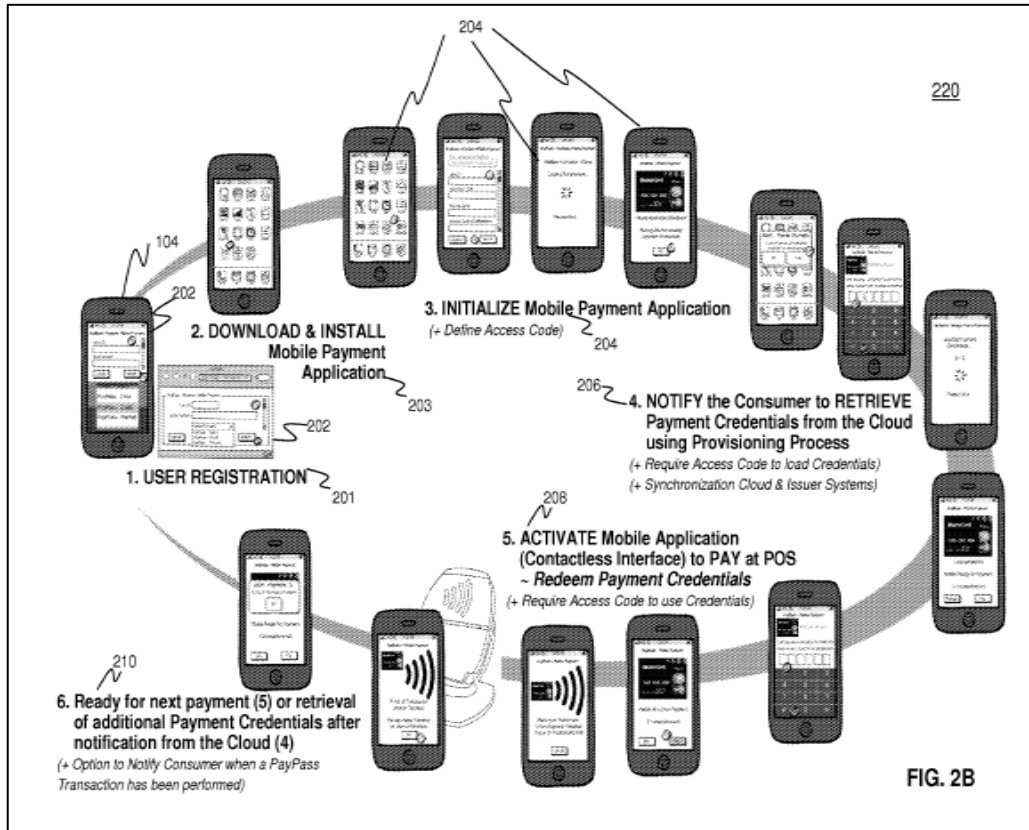
Collinge teaches displaying a request for user input at Collinge's mobile device for both inputting a PIN/code (identifying) and selecting a pay button (user approval of said payment transaction). See Claims 8 and 1(a).

19. 9[a]: the processor identifying that said user input matches a known authorized user of the electronic device, before said readying said device to perform a payment transaction; and,

As discussed in Claim 1(a), Collinge teaches the correct PIN/code is required to load credentials, thus Collinge's processor identifies that said user input matches a known authorized user (via a correct PIN/code) of the electronic device, before said readying said device to perform a payment transaction. '248 Provisional, Fig. 2B. Dec., ¶182.

20. 9[b]: disallowing the payment transaction by the device until said readying said device to perform the payment transaction is successfully completed.

Collinge teaches, if the user does not input the correct PIN/code the user will not be allowed to load credentials (disallowing the payment transaction by the device) until the user inputs the correct access/activation code (until said readying said device to perform the payment transaction is successfully completed) Dec., ¶183.



'248 Provisional, Fig. 2B ("Require Access Code to load Credentials").

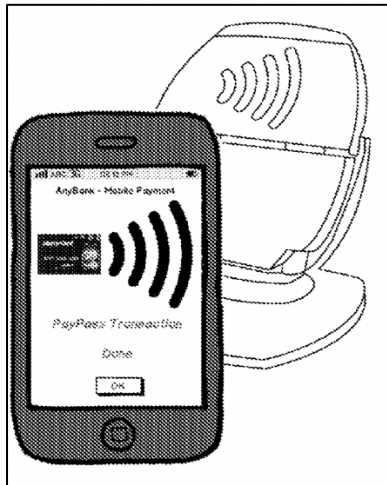
21. *10.1: The method of claim 8, wherein said successfully validating the identified user comprises the processor successfully determining a match between: firstly, a user input received via at least one of a set of user input sensors of the electronic device; and, secondly, at least one of the set consisting of: predetermined*

***user characteristics, and challenge-responses of an authorized user, as stored in the electronic device.*⁸**

Collinge in view of Smith teaches validating a user when Collinge's processor successfully determines a match between a user's input of a PIN/password and a stored PIN/password (*challenge-responses of an authorized user*).

(a) Collinge's Teachings

Collinge's mobile device has a button ('098 *Provisional*, 99) and a touchscreen, which are *user input sensors*. *Dec.*, ¶185. See Claim 39(d).

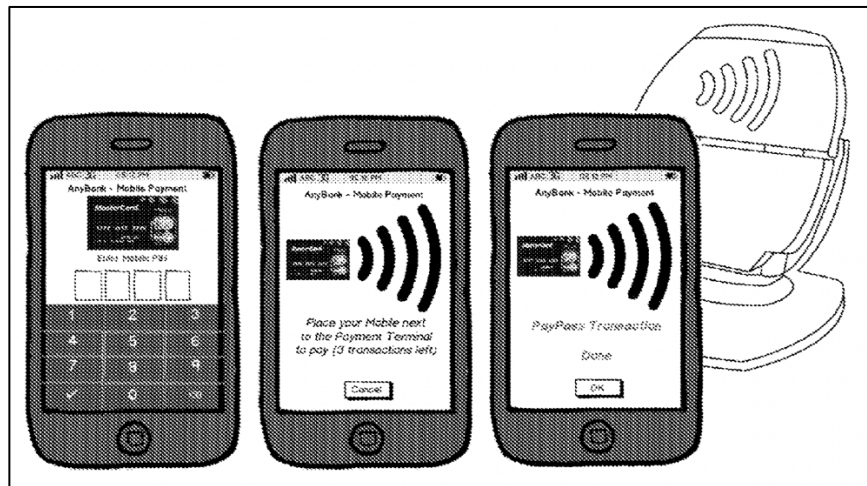


'098 *Provisional*, 99 (excerpt); see Collinge, Fig. 1.

Collinge teaches validating a user via the input of a PIN via “an input device (e.g., of the mobile device 104, such as a touch screen)” that may “receive a mobile

⁸ Claim 10 appears in three places in this IPR due to the differences in the dependent claims which depend from claim 10. The designation 10.1, 10.2 and 10.3 will be used to distinguish the mappings when “see above” is used.

personal identification number (PIN) input by a user (e.g., the user 102) of the mobile device 104.” *Collinge*, [0133]. Collinge teaches a user “must always provide the Mobile PIN for all PayPass transactions[.]” *’098 Provisional*, 99. *Collinge*, [0123] (“require 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).”) *Dec.*, ¶186.



’098 Provisional, 99; *’248 Provisional*, Fig. 2B. Collinge does not specifically teach where the PIN is validated or stored.

(b) Smith’s Teachings

Smith teaches a transaction may be “offline” and in an offline transaction “the transaction is authorized by the payment application in the mobile device without transmission of an authorization request to the issuer 206[.]” *Smith*, [0022], [0029] (discussing code “selected by the consumer during the registration process”).

(c) Motivation to Combine

A POSITA would have been motivated to modify Collinge so that Collinge's mobile PIN is stored in Collinge's mobile device and can be validated by Collinge's processor, as taught by Smith. Collinge already teaches requiring a user to provide a PIN for transactions. *'098 Provisional*, 99; *Collinge*, [0123]. A POSITA would have understood that by storing a PIN in Collinge's mobile device storage, Collinge's processor could validate the PIN (and therefore the user) and advantageously halt a transaction or even halt a request for payment credentials. *Dec.*, ¶188. A bad actor would have no chance of obtaining useful payment credentials if there are none to be found on the device. *Id.* Further, the phone could verify a PIN more quickly, and a POSITA could have advantageously taken advantage of Smith's offline payment mode. *Id.* Using Collinge's device to verify the PIN would be combining prior art elements according to known methods to yield the predictable results of increasing security within Collinge's device and would have had a reasonable expectation of success in making such a modification. *Id.* The combination is nothing more than the use of a known technique (verifying a PIN known to the device) to improve similar devices (electronic devices) in the same way. *Id.* The modification is straightforward and would have required storing the PIN in Collinge's memory, which is already accessible to Collinge's processor. *See* Claim 39(b).

22. Claim 11:

See Claim 10.1.

23. Claim 15:

See Claim 1(a).

24. Claim 27:

See Claim 5.

25. 28[Pre]: The method of claim 27 wherein the limited-use payment information is based on at least one secret information shared by both the electronic device and the payment processing authority; and

See Claim 5.

26. 28[a]: further wherein the at least one secret information is not exchanged when [performing] the payment transaction.

Collinge teaches the generating key within the single use key (secret information) is not exchanged (sent or received) to or from the POS terminal. See Collinge, [0050], [0070], [0077], Fig. 12, Fig. 18. Dec., ¶¶193-197, Alternatively, to the extent this claim requires shared secret information to not be exchanged with an issuer, Collinge teaches wherein at least one secret information (CVC) shared with Collinge and the issuer is not exchanged when performing the payment transaction since Collinge uses a dynamic CVC instead of the static CVC. Collinge, [0065], [0145]. Dec., ¶¶193-197.

27. **39(Pre): “An electronic device for completing a payment transaction, the electronic device comprising:”**

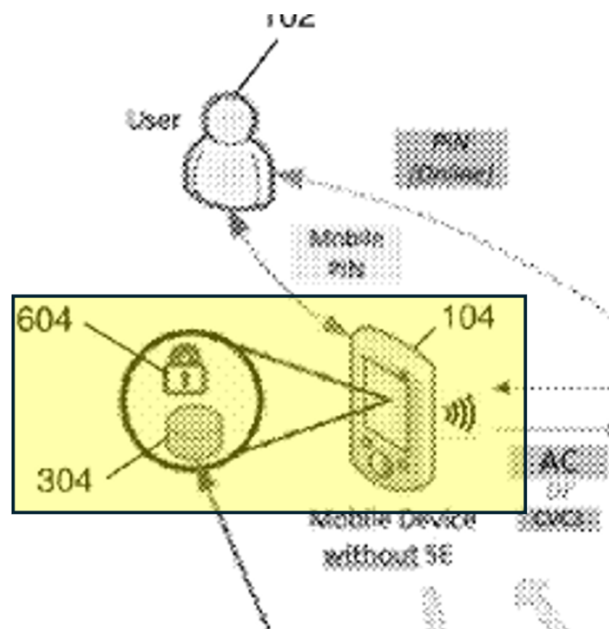
Collinge teaches mobile device 104 (*electronic device*) which includes a mobile payment application 106 for completing a payment transaction. *Collinge*, [0041].

28. 39(a): “a processor;”

See Claim 1(a)(1).

29. 39(b): “a memory coupled to the processor,”

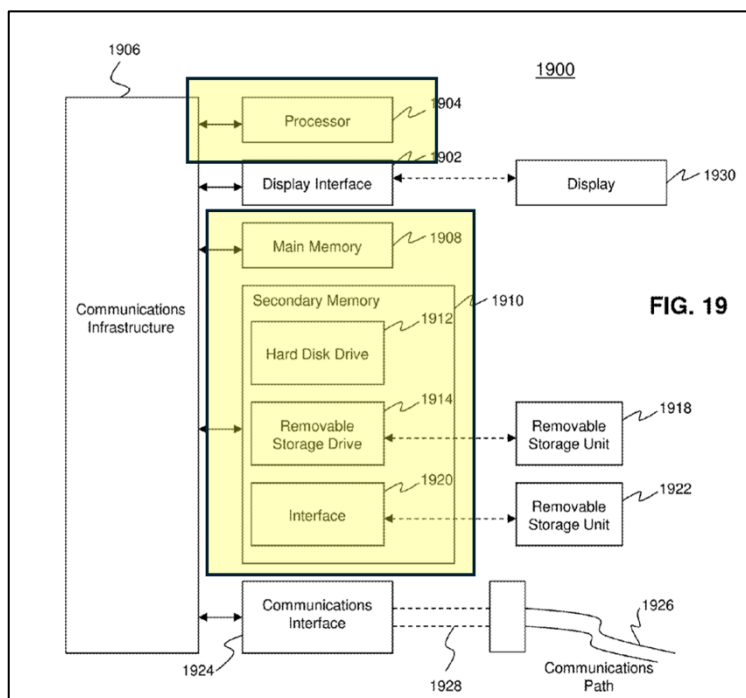
Collinge’s mobile device includes a memory. Collinge teaches “an application program stored in **data storage** of the mobile device[.]” *Collinge*, [0041], [0147] (“at least one processor device and **a memory**”) (emphasis added). Collinge’s memory includes storage 304, which may include a “local encrypted database.” *Collinge*, [0067], [0147].



Collinge, Fig. 6 (annotated excerpt).

Collinge further teaches the memory of mobile device 104 is coupled to the processor. *Collinge* teaches that “at least one processor device and a memory” is used to implement the payment system taught by *Collinge*. *Collinge*, [0147]. *Collinge* teaches and a POSITA would have understood that for *Collinge* to be able to execute an application program stored in the memory, the processor must necessarily be coupled to *Collinge*’s memory. *Collinge*, [0041], [0147], Fig. 16., Dec., ¶¶201-202.

As shown below, *Collinge* teaches the payment system comprises a memory that is “coupled” to the processor:



Collinge, Fig. 19 (annotated). Fig. 19 depicts a computer system including “memory that will configure associated processors to implement” *Collinge*’s teachings can “be

carried out e.g., by processing capability on mobile device 104[.]” ’248 *Provisional*, [0234]. Collinge teaches that the communications infrastructure may be a “bus[.]” *Collinge*, [0150]. For this additional reason, Collinge teaches that a memory is coupled to a processor. *Dec.*, ¶¶200-202.

30. 39(b)(1): “wherein the memory is operable to store information associated with use of an issued payment account and wherein the payment authority information comprises a secret information;”

Collinge’s memory stores payment credentials (information associated with use of an issued payment account) and a single use key (secret) that is shared with an issuer (payment authority) in storage 304.

Collinge teaches that “[t]he mobile payment application 106 may then...receive the card profile116 from the remote-SE system.” *Collinge*, [0074]. Once the card profile is received Collinge “store[s] the received card profile116 in the local encrypted database 304.” *Collinge*, [0074], [0048], Fig. 6, [0104] (card profile (PTP_CP)); ’098 *Provisional*, [0101] (“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.”).

Collinge’s mobile device stores a single use key in “...the storage 304.” *Collinge*, [0063], [0076], [0134].

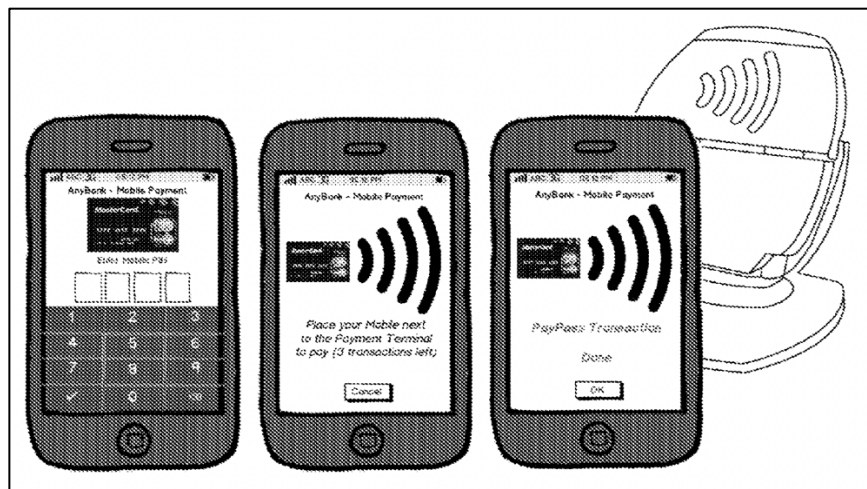
Collinge further teaches that the single use key (*secret*) is shared with an issuer (*payment processing authority*). *Dec.*, ¶204. *Collinge*, [0128]. (“transmitting the generated single use key 118 to an issuer associated with the payment account.”).

31. 39(c): “a near field communications (NFC) interface coupled to the processor and operable to receive a payment request associated with the payment transaction;”

See Claims 1(a)(3) and 1(c).

32. 39(d): “a user interface coupled to the processor;”

Collinge’s mobile phone includes touch screen display that provides a graphical visual *user interface*. *Collinge*, [0133].

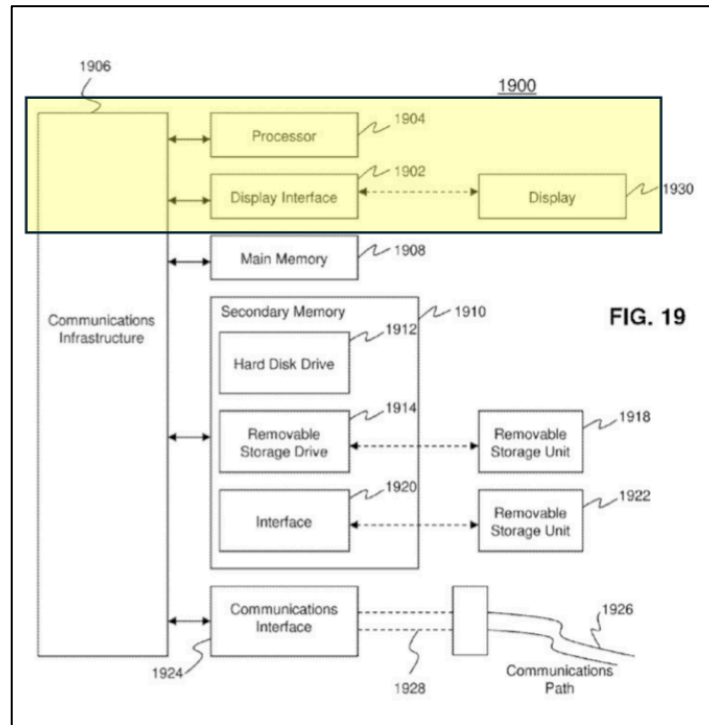


'098 Provisional, 99; '248 Provisional, Fig. 2B.

The display of Collinge’s mobile device 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.*, ¶208.

Collinge teaches that the display interface is “coupled” to the processor via the communication interface:



Collinge, Fig. 19. (annotated). Fig. 19 depicts a computer system including “memory that will configure associated processors to implement” Collinge’s teachings can “be carried out e.g., by processing capability on mobile device 104[.]” ’248 *Provisional*, [0234]. *Dec.*, ¶208. Collinge’s communications infrastructure may be a “bus, message queue, network, multi-core message-passing scheme, etc.” *Collinge*, [0150]. For this additional reason, Collinge’s display interface (the touchscreen) is

coupled to a processor. *Dec.*, ¶208. A POSITA would have understood that Collinge's display interface is Collinge's touchscreen. *Dec.*, ¶208.

33. ***“39(e): “a user input device coupled to the processor; and,”***

See Claim 1(a)(2).

34. ***39(f): “wherein said processor is operable to: responsive to a priming operation, wherein the priming operation is operable to ready the device to perform the payment transaction,”***

See Claim 1(b).

35. ***39(g): “cause the display of information associated with the payment request;”***

See Claim 1(d).

36. ***39(h): “cause the display of an image representing at least one user-selectable issued payment account; and,”***

See Claim 1(d).

37. ***39(i): “dynamically generate a limited-use payment information based on a per-transaction sequential parameter originating from the electronic device, and secret information associated with a selected issued payment account; and,”***

Collinge in view of Sahota teaches using a ATC (per-transaction sequential parameter) originating from Collinge's device. *See* Claim 1(f). Collinge further teaches dynamically generating a limited-use payment information based on ATC (per-transaction sequential parameter) and secret information (a session key unpredictable number (KS_{UN}) or single use key) associated with a selected issued payment account. *See* Claim 1(e).

38. **39(j): “cause the transmission, via said NFC interface, a payment information combination comprising the dynamically generated limited-use payment information and said payment authority information, for receipt by an NFC recipient;”**

Collinge teaches generating the payment cryptogram by combining multiple values one of which is the session key unpredictable number (KS_{UN}). *See* Claim 1(e); *Collinge*, [0145].

Therefore, Collinge combines the KS_{UN} (payment authority information) when generating the payment cryptogram for receipt by an NFC point of sale terminal. *Dec.*, ¶¶215-216. As discussed above Collinge’s mobile device conveys payment information, including a single use payment cryptogram (dynamically generated limited-use payment information) via Collinge’s NFC interface to a point of sale terminal (NFC recipient).

39. **39(k): “wherein the NFC interface is operable, in response to transmitting said payment information combination, to receive status information reflecting a transaction processing status of said payment transaction; and wherein the user interface is operable to provide an indication of the status information.”**

See Claim 1(i).

40. **Claim 41:**

See Claim 5.

41. **Claim 44:**

See Claim 3.

42. Claim 45:

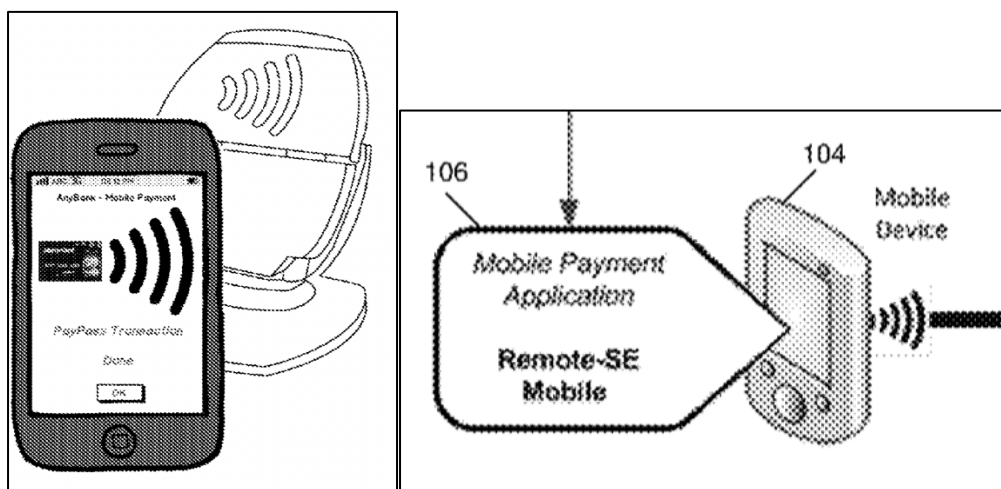
See Claims 1(e) and 1(h).

43. Claim 46:

See Claim 3.

44. Claim 49:

As discussed above, Collinge teaches multiple priming operations, for example inputting a PIN or passcode (security challenge question). See Claims 1(a) and 11. Collinge's touch panel is adjacent to said display. *Dec.*, ¶¶222-223.



'098 Provisional, 99. (excerpt); Collinge, Fig. 1 (except).

45. Claim 50:

As discussed above, Collinge teaches multiple priming operations, for example inputting a PIN or passcode (security challenge question presented on the display). See Claims 1(a) and 39(d).

46. 55[a]: *The device of claim 39, wherein the processor is operable to: receive a user-selection of an issued payment account*

presented on the user interface, received the user input device coupled to the processor, and

See Claim 1(d).

47. *55[b]: responsive thereto, select from the memory a specific processing authority information corresponding to the user-selected issued payment account information, and*

Collinge, in response to the user selecting a payment account, selecting from memory the issuer card profile (payment authority information) corresponding to selected user-selectable issued payment account. *Dec.*, ¶¶226-228.

After the user performs a payment section as discussed in Claim 1(d), “[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*, [0048], Fig. 6, [0104] (card profile (PTP_CP)); *'098 Provisional*, [0101] (“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.”); *Collinge*, [0048] (“payment credentials included in the card profile 116 may include common payment credentials 202, magnetic stripe (mag stripe) payment credentials 204, and m/chip payment credentials 206.”)

When the user is ready to perform a transaction, 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]. Therefore, because the PAN is stored in the memory of mobile device 104 as part of the payment credentials, and because the PAN is sent to POS 120, the PAN must be selected from memory. *Dec.*, ¶¶226-228.

48. 55[c]: use at least a portion of said specific processing authority information in place of at least a portion of the issued payment account information to generate a combined payment information to complete a payment transaction per the input user-selection.

Collinge's payment cryptogram (CVC3) is generated based in part on the KS_{UN}, and the CVC3 is used in place of the issuer provided CVC. *See* Claim 1(e).

49. Claim 56(Pre):

See Claim 39(Pre).

50. Claim 56(a):

See Claim 39(a).

51. Claim 56(b):

See Claim 39(b).

52. Claim 56(b)(1):

See Claim 39(b)(1).

53. Claim 56(c):

See Claim 39(c).

54. Claim 56(d):

See Claim 39(d).

55. Claim 56(e):

See Claims 1(a)(2); 39(e).

56. Claim 56(f):

See Claims 1(b); 39(f).

57. Claim 56(g):

See Claims 1(d); 39(g).

58. Claim 56(h):

See Claims 1(d); 39(h).

59. Claim 56(i):

See Claim 39(i).

60. Claim 56(j):

See Claim 39(j).

61. Claim 56(k):

See Claim 39(k).

62. Claim 60:

See Claim 5

63. Claim 61:

See Claim 3.

64. Claim 62:

Collinge's payment cryptogram (CVC3) is used in place of the issuer provided CVC. *See* Claim 1(e).

65. Claim 63:

See Claim 3.

66. Claim 66:

See Claims 39(g); 1(a)-1(b).

67. Claim 67:

As discussed above, Collinge teaches multiple priming operations, for example inputting a PIN or passcode (security challenge question). See Claims 1(a); 11; 39(d).

68. Claim 72[Pre]:

See Claim 1(d).

69. Claim 72[a]:

See Claim 55(b).

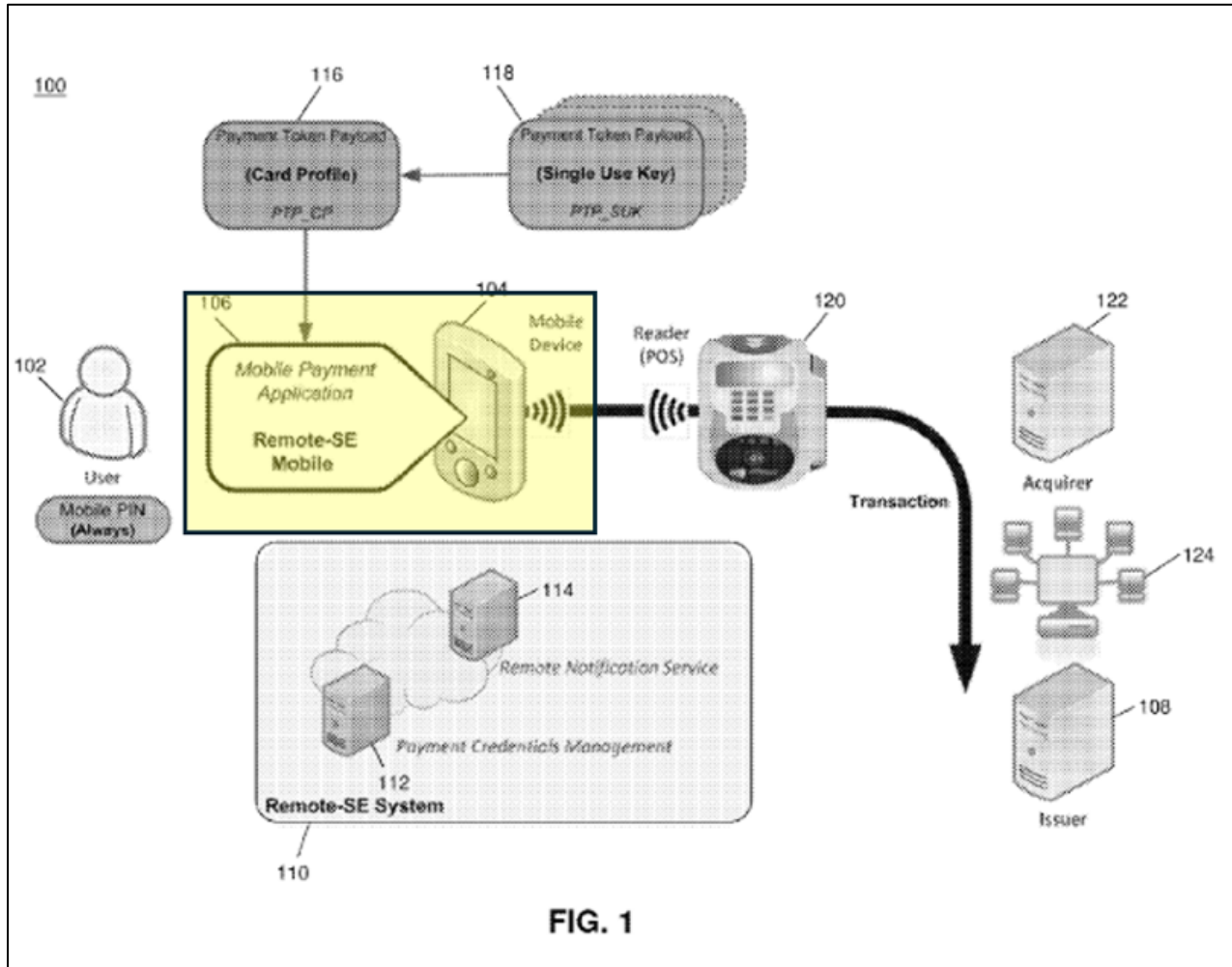
70. Claim 72[b]:

Collinge's payment cryptogram (CVC3) is used in place of the issuer provided CVC. See Claims 1(e); 55(c).

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

1. 29(Pre): "A system for completing a payment transaction, the system comprising:"

Collinge teaches a payment system that includes generating and "provisioning of payment credentials to mobile devices" for "use in mobile payment transactions." (completing a payment transaction) Collinge, *Abstract*, [0006], [0039].



Collinge, Fig. 1. (annotated).

2. **29(a):** “an electronic device operable to receive a priming operation, wherein the priming operation is operable to ready said device for performing a payment transaction by an identified user, and, wherein the electronic device further comprises:”

See Claims 1(a) and 1(b).

3. **29(b):**” a processor;”

See Claim 1(a)(1).

4. ***29(c): “a near field communications (NFC) interface coupled to the processor and operable to receive a payment request associated with the payment transaction; and,”***

See Claims 1(a)(3) and 1(c).

5. ***29(d): “a touch-screen display coupled to the processor, and”***

See Claim 1(a)(2).

6. ***29(e): “wherein the electronic device is operable to cause the display of information reflecting device-readiness, the payment request, and an image representing at least one selected issued payment account;”***

Collinge in view of Lin teaches Collinge’s device can display the payment request. See Claim 1(d). Collinge teaches displaying an image representing at least one selected issued payment account. *Id.*

Collinge further teaches displaying that Collinge’s mobile device is “ready to conduct a contactless payment transaction” via “display[ing]” a “notification to the user 102 via a user interface[.]” (information reflecting device-readiness) Collinge, [0112].

7. ***29(f): “wherein the electronic device is operable to dynamically generate limited-use payment information based on a sequential counter count from the electronic device;”***

See Claims 1(e), 1(f).

8. ***29(g): “wherein the electronic device is operable to store a static device-specific user account information;”***

The combination of Collinge and Smith teaches static device-specific user account information.

(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). *'098 Provisional*, [0101]. Collinge's 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].

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.*, ¶¶261-64.

(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. When 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-specific user account information) 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-specific* account number. *Dec.*, ¶¶265-70.

Once an actual PAN is issued, the temporary PAN is swapped with the actual PAN. *Smith*, [0026], [0040]. The PPAN 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]. Therefore the PPAN is a different number from the actual PAN. *Dec.*, ¶¶271-73.

600

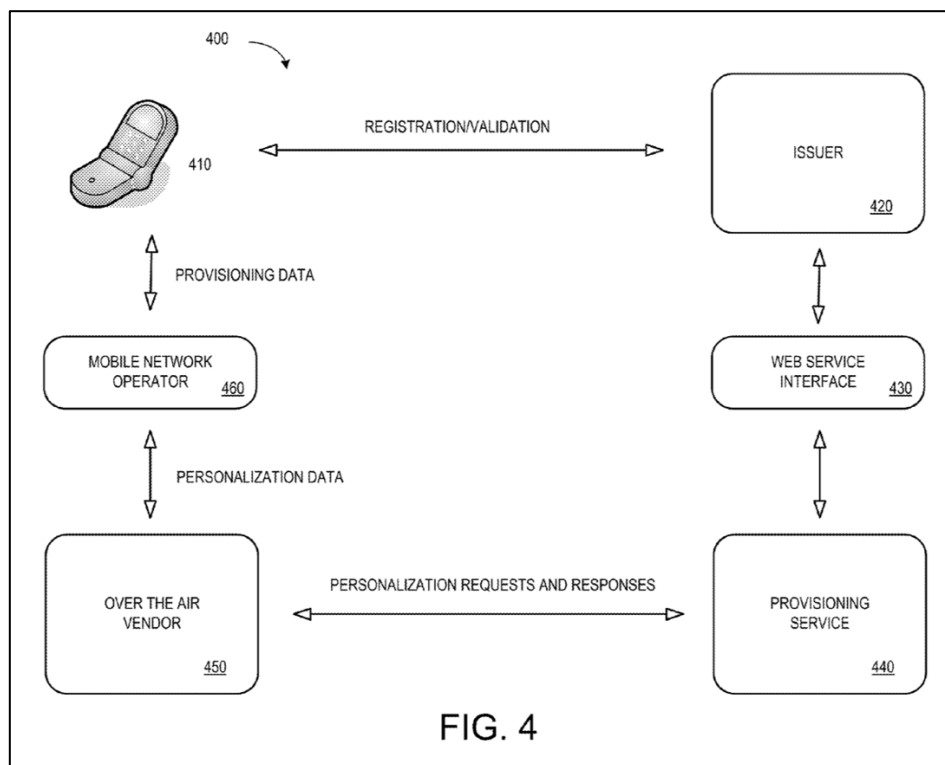
CONSUMER ID 602	TEMPORARY PAN 604	MOBILE PAN 606	ACTUAL PAN 608	RISK PARAMETER RESTRICTION(S) 610
C1001	T-PAN_0001	M-PAN_0001	NONE	NONE
C1002	T-PAN_0002	M-PAN_0002	NONE	NO TRANSACTIONS OVER \$10
C1003	T-PAN_0003	M-PAN_0003	NONE	OVERALL TRANSACTION UNDER \$100
C1004	T-PAN_0004	M-PAN_0004	NONE	NO ONLINE 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*, [0024]. 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].

Smith teaches during a registration process the consumer will “access a web site operated by issuer 420 and enter details, including his or her personal information, a model number of the mobile telephone 410, a phone number of the mobile telephone 410, and/or an indication of a mobile network operator associated with the telephone 410.” *Smith*, [0028].

In response the card issuer transmits a response back to the mobile device that includes “a record identifier, an issuer code, a PPAN, an expiration date (e.g., an expiration month and year), a mobile phone number and carrier identifier, a verification code (e.g., selected by the consumer during the registration process), and/or an encryption key for security purposes.” *Smith*, [0029]-[0030].



Smith, Fig. 4.

The issuer can “implement dual account number structures” for “multiple NFC-enabled handsets ... managed for a single account.” *Smith*, [0029]. It was well known that a dual account number has separate and distinct numbers for each device the account is used on. *Dec.*, ¶270. Accordingly, *Smith*’s PPAN is a distinct account number for a payment account on a particular “mobile device.” *Dec.*, ¶¶268-271.

Even if the same user wanted to register a new device, a user would 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.”)

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.*, ¶¶272-73.

(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.*, ¶¶274-84.

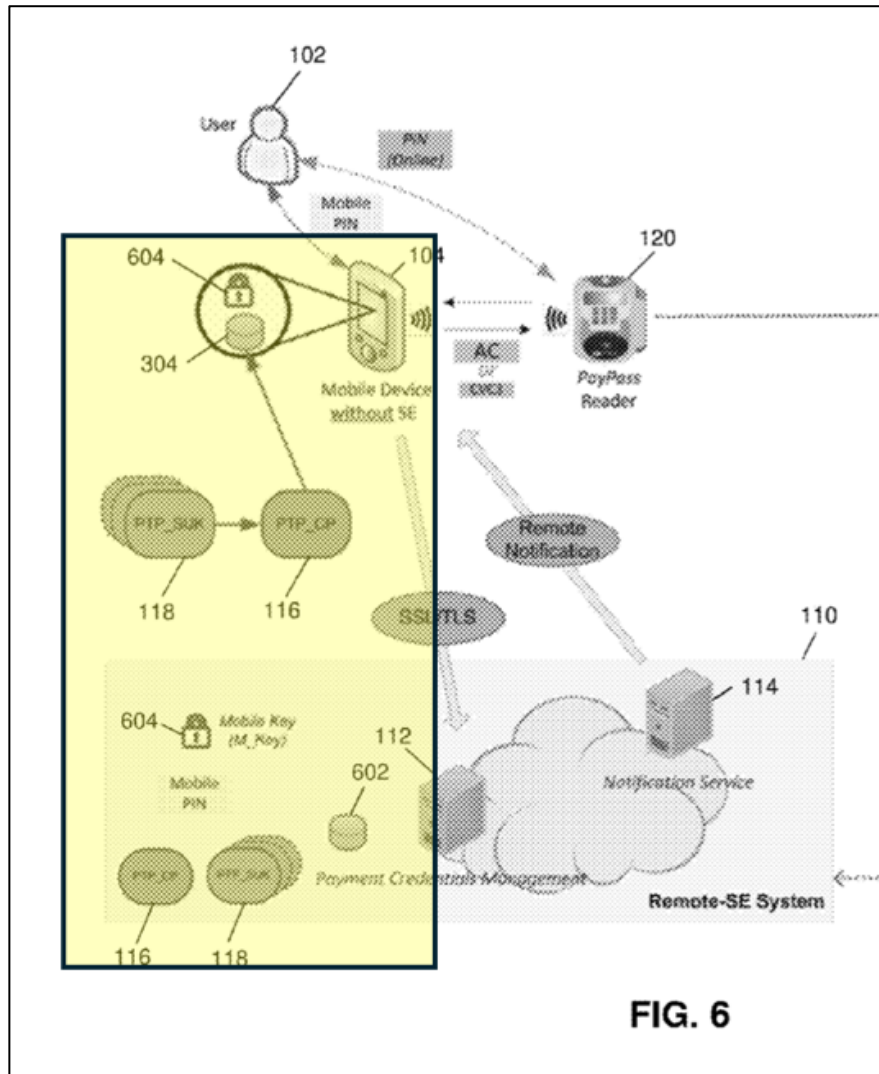
A POSITA would have been motivated to use Smith’s PPAN in place of Collinge’s PAN so that Collinge’s mobile device would not be required to store the PAN, which is a sensitive financial number. *Dec.*, ¶276. It was well known in the art that a device without a secure element (SE), such as Collinge’s mobile device, could be vulnerable to malicious attacks and therefore using Smith’s PPAN instead of the

PAN on Collinge's mobile device would have increased security for the user's account. *Dec.*, ¶277. A POSITA would have appreciated that storing Smith's PPAN would be safer than storing the literal PAN on Collinge's device. *Dec.*, ¶282.

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.*, ¶278. 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.*, ¶¶279-281; *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, and the PPAN would perform the same function in the combination. *Id.* 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. *Id.*

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*, [0101] (“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.”); *Smith*, [0029]-[0030].



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 generate a cryptogram and to make a payment. *Collinge*, [0048]-[0049], [0063]; *Dec.*, ¶281. 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.*, ¶282.

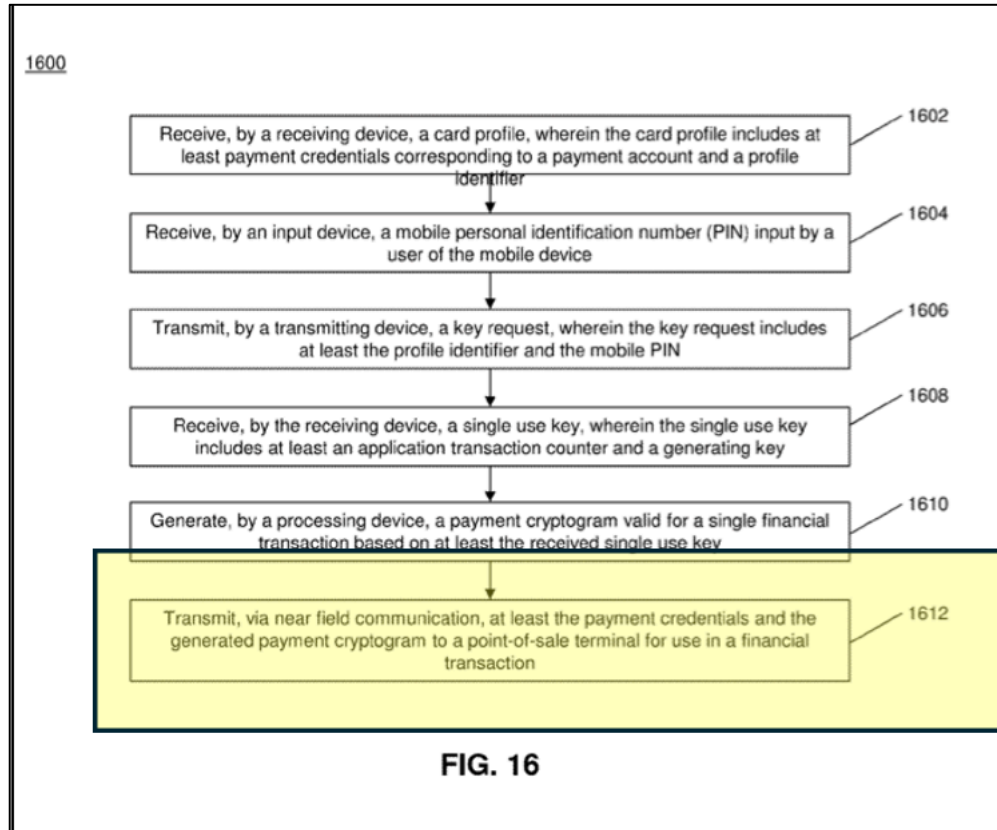
Likewise, a POSITA would have substituted Smith’s PPAN for Collinge’s PAN when making payment transactions, as taught by Smith. *Smith*, [0018] (“the process of personalizing the mobile device 104 with the software (including the PPAN...[o]nce the personalization or loading of the payment application is complete, the customer 102 may use the mobile device **104** to complete payment transactions”). A POSITA would again have recognized that substitution of a PPAN 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.*, ¶¶283-84. 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.*, ¶284.

9. ***29(h): “wherein the electronic device is operable to transmit a combination of said dynamically generated limited-use payment information and said static device-specific user account information to an NFC recipient via, said NFC interface for use in connection with payment transaction in place of information associated with said selected issued payment account;”***

See Claim 1(h). Collinge, in view of Smith, renders obvious transmitting a combination of said dynamically generated limited-use payment information and said static device-specific user account information, including a CVC3 (limited-use payment information) and PPAN (static device-specific user account information) when sending complete payment information to a POS terminal via Collinge's NFC interface, in place of the static CVC and PAN (information associated with said selected issued payment account). Collinge teaches generating limited-use payment information (payment cryptogram). See Claim 1(e).

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*, [0101] (“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* teaches transmitting a combination of said dynamically generated limited-use payment information and said static device-specific user account information, including a CVC3 (limited-use payment information) and PPAN (static device account number) which is collectively transmitted via NFC to a point-of-sale terminal for use in a financial transaction at step 1612. *Dec.*, ¶¶285-89.

(a) Motivation to Combine

See Claim 29(g).

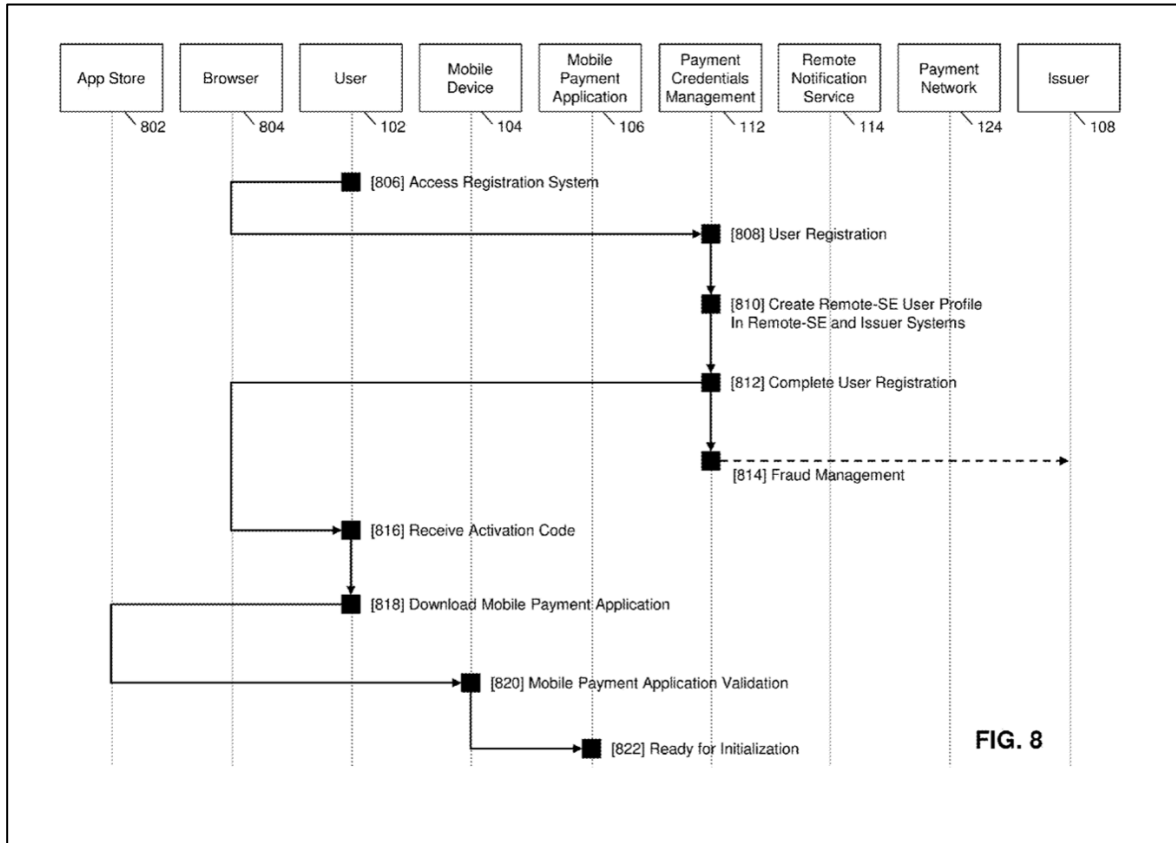
- 10. 29(i): “wherein the electronic device is operable, subsequent to transmission of said combination, to receive a status information reflecting a status of said payment transaction; and, wherein the touch-screen display is operable to display as indication of said status information.”**

See Claim 1(i).

- 11. 3[a]: The method of claim 2, further comprising: prior to the priming operation, transmitting the issued payment information for receipt by a payment processing authority; and,**

Prior to Collinge’s payment system transmits the user-provided issued payment account information from Collinge’s mobile phone to the issuer (payment processing authority) during the registration process. The registration process occurs prior to Collinge’s priming operation (e.g., inputting a PIN; bringing Collinge’s mobile device within proximity of an NFC recipient, *see* Claim 1(a)).

Collinge teaches in step 806 “[a]s part of the registration, the user 102 may provide account details for a payment account, and the payment credentials management service 112 may ensure the payment account is eligible for remote payment transactions.” *Collinge*, [0089].



Collinge, Fig. 8. The user input account details are used to create “a user profile for the user 102 in the remote-SE system 110.” *Collinge*, [0090]. *Collinge* teaches that at “step 814, the payment credentials management service 112 may synchronize information (e.g., the user profile, activation code status, etc.) with the issuer 108 for fraud management.” *Collinge*, [0090].

12. ***3[b]: in response to said transmitting issued payment information, receiving a static device account information that is unique to the electronic device.***

Collinge in view of *Smith* teaches a PPAN (static device account information) unique to *Collinge*’s mobile device and received in place of PAN information in

Collinge's payment credentials provisioned to the mobile payment application as part of Collinge's card profile 116. *See* Claim 29(g); Smith, Fig. 4; [0029]-[0030].

The receipt of the payment credentials located within Collinge's card profile occur after the initially input account information by the user that is transmitted to the issuer. *Collinge*, Figs. 11, 15-16, [0104].

13. Claim 4[a]:

See Claim 29(h).

14. Claim 4[b]:

See Claim 29(h).

15. Claim 4[c]:

See Claim 1(i).

16. 5: The method of claim 3, wherein the dynamically generating [further] comprises dynamically generating the limited-use payment information based on payment processing authority secret information.

Collinge teaches the payment cryptogram (limited-use payment information) is based on at least the single use key and KS_{UN} (secret information) shared by both the electronic device and the issuer (payment processing authority).

Collinge teaches generating a payment cryptogram such as a CVC3 based on at least: “the supplied CVC3 value, the session key unpredictable number [(KS_{UN})], the application transaction counter, and the reader unpredictable number. *Collinge*, [0145]. Collinge generates the CVC3 by using the single use key “used one time to

generate a payment cryptogram to be used in a payment transaction.” *Collinge*, [0050].

A POSITA would have been very familiar with methods of validating a payment cryptogram, as recognized by *Collinge*. *Collinge*, [0077]. 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]. The issuer also receives “the generated single use key[.]” *Collinge*, [0128]. A POSITA would have understood that KS_{UN} and single use key is private information shared between two parties (*secrets*). *Dec.*, ¶¶300-305.

17. Claim 6:

See Claim 5.

18. Claim 17[a]:

See Claim 3(a).

19. Claim 17[b]:

See Claims 29(g), 3(b).

20. Claim 18[a]:

See Claim 29(h).

21. Claim 18[b]:

See Claim 29(h).

22. Claim 18[c]:

See Claim 1(i).

23. Claim 19:

See Claim 5.

24. Claim 20:

See Claim 5.

25. Claim 21:

See Claim 5.

26. Claim 22:

See Claim 5.

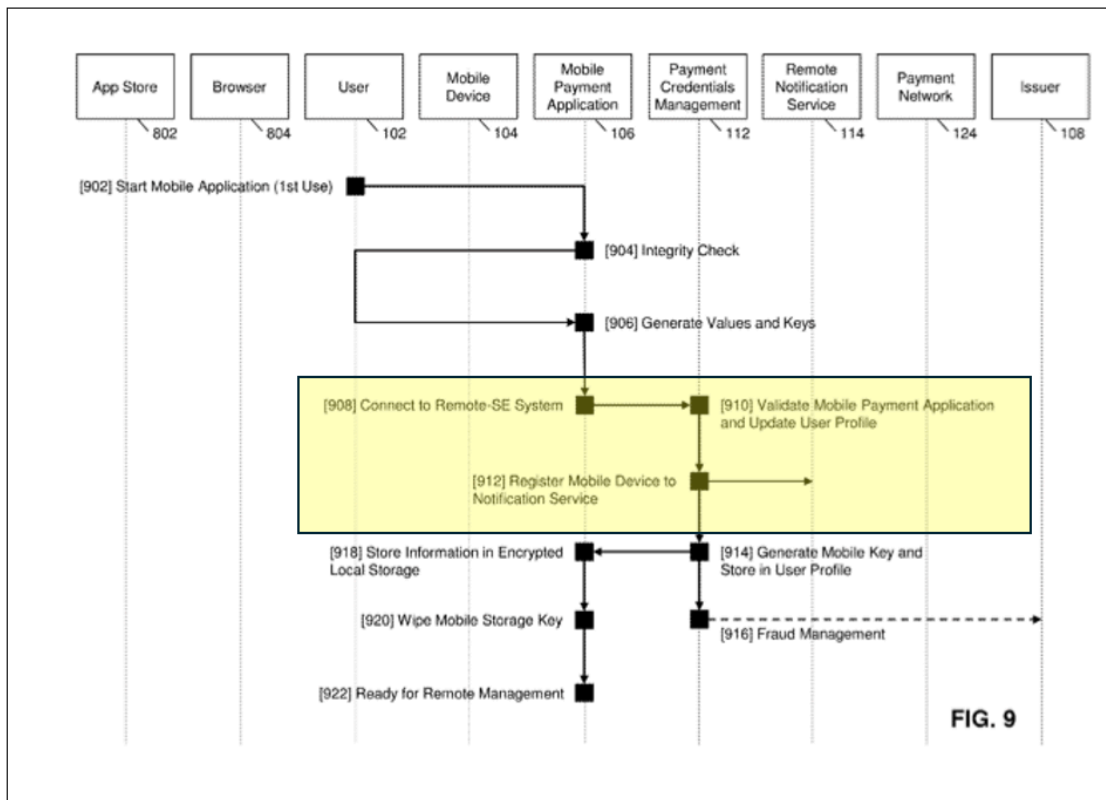
27. 23[a]: The method of claim 1, further comprising: prior to the priming operation, transmitting the issued payment information, user information and device-specific information; and,

See Claims 3(a) and 29. Collinge in view of Smith teach prior to the priming operation, transmitting the issued payment information, user information (his or her personal information) and device-specific information (a model number and phone number).

(a) Collinge's Teachings

As discussed in Claim 3(a), Collinge's payment system transmits the user-provided issued payment account information from Collinge's mobile phone to the issuer (payment processing authority) during the registration process.

Collinge also already teaches transmitting information that will “uniquely identify the mobile device 104” called a “unique identifier[.]” *Collinge*, [0062], [0095].

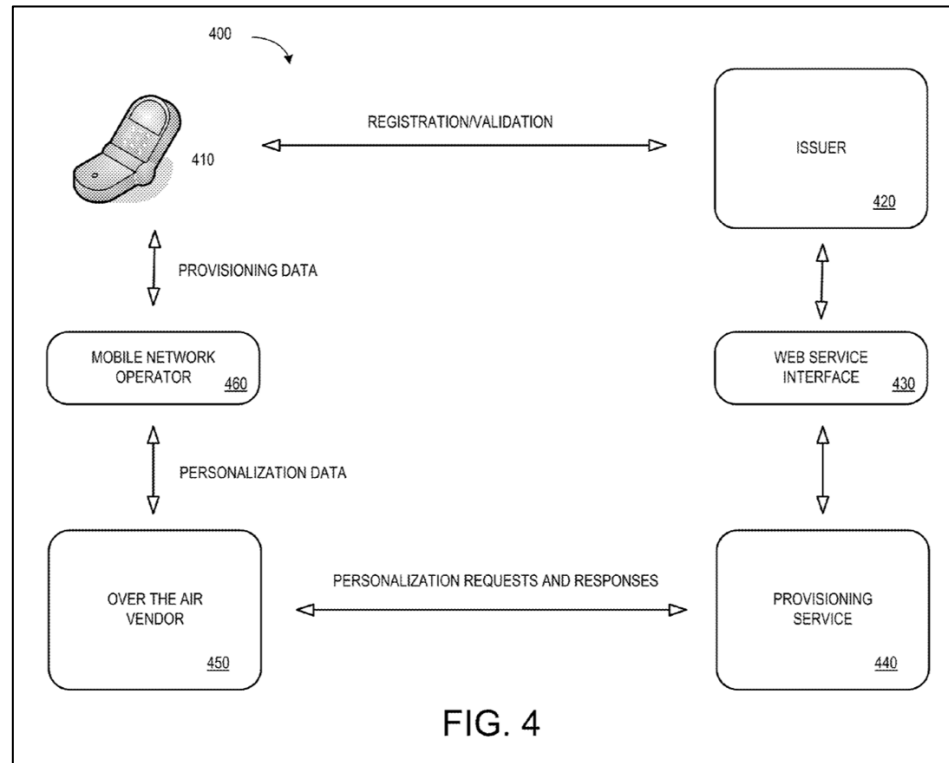


Collinge, Fig. 9. (annotated)

(b) Smith’s Teachings

Smith teaches during a registration process the consumer will “access a web site operated by issuer 420 and enter details, including his or her personal information [*user information*], a model number of the mobile telephone 410 [*device-specific information*], a phone number of the mobile telephone 410 [*device-*

specific information], and/or an indication of a mobile network operator associated with the telephone 410.” *Smith*, [0028].



Smith, Fig. 4.

(c) Motivation to Combine

It would have been obvious and a POSITA would have been motivated to transmit “his or her personal information, a model number of the mobile telephone 410, a phone number of the mobile telephone 410[.]” as taught by *Smith* during Collinge’s registration process. *Dec.*, ¶321. In the combination, the user information and device-specific information would be transmitted along with Collinge’s card information as discussed in Claim 3(a) prior to the priming operation. *Smith*, [0028]. Collinge already teaches that “register[ing] the mobile

device 104 with the remote notification service 114 using the unique identifier” that is used to “uniquely identify the mobile device 104[.]” *Collinge*, [0062], [0095]. A POSITA would have been motivated to transmit user information and device-specific information in Collinge’s registration process as taught by Smith so that the issuer can correctly identify the device when it generates and transmits Smith’s device-specific PPAN and would have had a reasonable expectation of success in doing so. *Id.* A POSITA would have recognized that this would have been a use of a known technique (sending device identifying information during registration) to improve Collinge’s mobile payment system in the same way. *Id.*

28. 23[b]: in response to transmitting said issued payment information, user information and device-specific information, receiving a payment processing authority supplied secret information.

Collinge-Smith teaches receiving a PPAN from an issuer in response to which is a payment processing authority supplied secret information. See Claims 3(b); 29(g).

29. Claim 24:

See Claim 3.

30. Claim 30:

See Claim 2.

31. Claim 31:

See Claim 29(g).

32. Claim 32:

See Claims 29(g), 3(b).

33. Claim 34:

See Claims 1(f); 29(f).

34. Claim 35:

See Claim 3.

35. Claim 36[Pre]:

See Claims 5, 29(h).

36. Claim 36[a]:

See Claim 5.

37. Claim 37:

See Claim 5.

38. Claim 38:

See Claim 5.

39. Claim 40:

See Claims 29(g); 3(b).

40. Claim 42:

See Claims 24; 29(g).

41. Claim 47:

See Claims 24; 29(g).

42. Claim 57:

See Claims 29(g), 5.

43. Claim 58:

See Claims 24; 29(g).

44. Claim 64:

See Claims 24; 29(g).

VII. GROUND 3: COLLINGE IN VIEW OF LIN, SAHOTA, SMITH, AND KRAZLEY

1. Claim 25: *The method of claim 24 wherein said static device account information comprises a static device account number and a static device-specific expiration date.*

As discussed in Claim 29, Collinge-Smith teaches a card issuing authority provides a device-specific account number (PPAN) for use by Collinge's mobile in place of the PAN in performing payment transactions. Smith teaches an expiration date but is not specific as to if that is assigned to the PPAN (static device account number). Collinge, [0124], Smith, [0029] ("PPAN, an expiration date (e.g., an expiration month and year)").

Kranzley teaches using a virtual PAN (VPAN) in place of the PAN and that the VPAN "may have its own virtual expiry date." Kranzley, [0036].

(a) Motivation to Combine

It would have been obvious and a POSITA would have been motivated to modify the Collinge-Smith's payment system to assign a static device-specific expiration date to the static device account number, as taught by Kranzley. Dec., ¶¶343-44. A POSITA would have been motivated to associate the PPAN with an

expiration date (such as the expiration date of the associated payment card) for increased security.) *See Smith*, [0029] (“PPAN, an expiration date (e.g., an expiration month and year)”). *Dec.*, ¶344. A POSITA would have recognized that, as with traditional credit cards, allowing cards to regularly expire prevents cards that have been inadvertently lost or cards that are little used from falling into the wrong hands and being used without authorization. *Id.* A POSITA would have recognized that allowing a payment number to remain valid indefinitely increases the chances of fraud. *Id.* A POSITA would have been motivated to apply the known technique described in Kranzley—a VPAN with an expiration date—to the static device-specific account number in the Collinge-Smith combination to improve a similar device in the same way to obtain the same benefits of increased security. *Id.* A POSITA would have had a reasonable expectation of success in adding an expiration date to the static device-specific account number including because a POSITA would have been well-familiar with using payment credential expiration dates. *Id.*

2. Claim 26:

See Claims 3 and 29.

3. Claim 33:

See Claim 25.

4. Claim 43:

See Claim 25.

5. Claim 48:

See Claim 25.

6. Claim 59:

See Claim 25.

7. Claim 65:

See Claim 25.

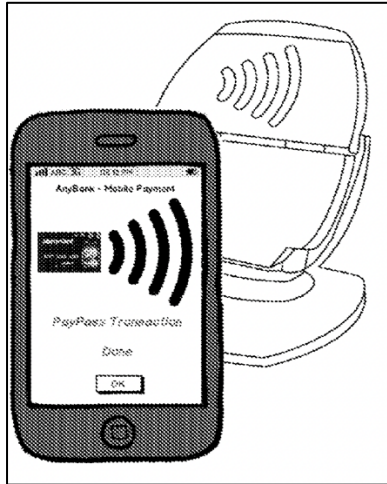
VIII. GROUND 4: COLLINGE IN VIEW OF LIN, SAHOTA, AND FADELL

- 1. 10.2: *The method of claim 8, wherein said successfully validating the identified user comprises the processor successfully determining a match between: firstly, a user input received via at least one of a set of user input sensors of the electronic device; and, secondly, at least one of the set consisting of: predetermined user characteristics, and challenge-responses of an authorized user, as stored in the electronic device.***

Collinge in view of Fadell teaches validating a user when Collinge's processor successfully determines a match between a user fingerprint (detected on a fingerprint sensor, one of Collinge's mobile device's user input sensors) and stored biometric fingerprints (predetermined user characteristics) within Collinge's mobile device.

(a) Collinge's Teachings

Collinge teaches a user supplying a "biometric identifier." *Collinge*, [0143]. As shown below Collinge's mobile device has a button. Collinge also includes a touchscreen, which is a user input sensor. See Claim 39(d).



'098 Provisional, 99 (excerpt); see Collinge, Fig. 1.

(b) Fadell's Teachings

Fadell teaches electronic device (e.g., phone) with a sensor 620 “operative to detect features of the user’s skin when the skin is held immobile over the sensor.” *Fadell*, [0059]. Therefore, Fadell requires the user to hold their finger on the fingerprint sensor until they are authenticated. *Dec.*, ¶¶353-55. The sensor “may be placed at any suitable location within the electronic device” including “in the [touchscreen] display[.]” *Fadell*, [0060]-[0062]. Specifically, “sensor 620 may include an existing component of...the display stack for a touch screen display” which “may include a capacitance sensor.” *Fadell*, [0061]. In that case, “the authentication system may use the detected output of a capacitance sensing component of the display stack (e.g., in a touch screen display) that has a sufficient resolution for distinguishing ridges and valleys of a user’s skin.” *Fadell*, [0061]. The user is “authenticated by comparing the detected biometric attributes with a library

of biometric attributes stored by or accessible to the electronic device.” *Fadell*, [0006].

(c) Motivation to Combine

It would have been obvious and a POSITA would have been motivated to modify Collinge’s mobile device to authenticate a user via a fingerprint sensor and to store a library of fingerprint scans for authentication purposes in Collinge’s storage 304, as taught by Fadell. *Dec.*, ¶354. Collinge already teaches a user supplying a “biometric identifier” for authentication purposes. *Collinge*, [0139]. By the Critical Date, it was already well-known that fingerprint sensors could be added to mobile devices. *Dec.*, ¶355 (discussing the Pantech GI100 released in 2004 and Motorola Atrix released in 2011). A POSITA would have understood that a fingerprint scan was a more secure way to authenticate a user than a pin or password, which can be used by another who acquires it or guesses it. *Dec.*, ¶355. Therefore, a POSITA would have understood that adding a fingerprint sensor and library, as taught by using Fadell would have been combining prior art elements according to known methods to yield the predictable results of increasing security within Collinge’s device, and a POSITA would have had a reasonable expectation of success in making such a modification. *Dec.*, ¶354-55. When combined with Collinge’s mobile device Fadell’s fingerprint sensor and library would function the same way as it does on Fadell’s phone. *Id.* The combination is nothing more than

the use of a known technique (applying fingerprint sensors for user authentication) to improve similar devices (electronic devices) in the same way. *Id.*

2. Claim 12:

See Claim 10.2.

3. Claim 13:

Collinge teaches validating a user via the input of a PIN on Collinge's mobile device touch screen sensor (known user touch gesture) or a user's fingerprint touch gesture. Fadell, [0058] ("detect features of user's finger as it slides or rolls over the sensor"). *See* Claim 10.1, 10.2.

4. 16[Pre]: The method of claim 15, wherein said readying said device to perform a payment transaction comprises:

See Claim 1(b).

5. 16[a]: successfully identifying said identified user from said user input; and,

See Claims 1(b) and 1(a). Collinge teaches a user inputting a PIN (a priming operation) and Collinge's mobile device identifying a user when the PIN is accepted (readying the device). Collinge, [0133]; '098 Provisional, 99; '248 Provisional, Fig. 2A-2B.

6. 16[b]: wherein said user input further comprises a user approval for performing the payment transaction received from said identified user; and,

See Claim 8(b).

7. ***16[c]: wherein said successfully identifying further comprises said electronic device validating an authorized user of said electronic device by comparing a user-touch input received via a touch input sensor on the electronic device with a recognized valid user-touch, stored in a memory of the electronic device; and,***

Collinge in view of Fadell teach this claim limitation. See Claim 10.1, 10.2.

8. ***16[d]: wherein said user approval for performing the payment transaction further comprises:***

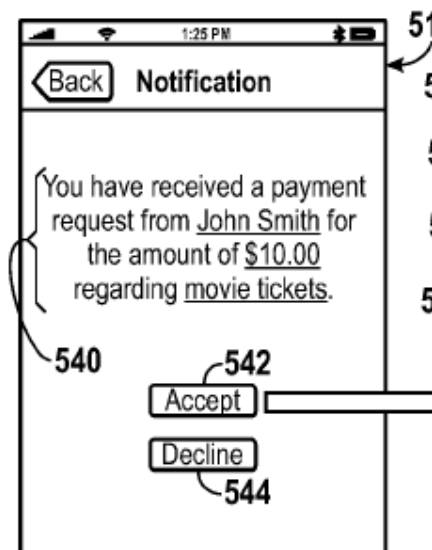
See Claim 8(b).

9. ***16[e]: visually presenting information of the payment transaction on the touch screen display of said electronic device;***

Collinge in view of Lin teaches visually presenting a payment request information (*information of the payment transaction*) on Collinge's touch screen display of Collinge's mobile device.

(a) Lin's Teachings

Referring to Fig. 14E, Lin teaches that "once the payment request information has been received by the payor device, the screen 516 may be updated to display the details 540 of the payment request[.]" *Lin*, 71:7-9, Fig. 14E. As illustrated below details 540 displayed on the screen 516 include who the payment request is from, for what amount, and what the payment is for (*visually presenting information of the payment transaction*).



Lin, Fig. 14E (excerpt).

(b) Motivation to Combine

A POSITA would have found it obvious and been motivated to modify Collinge's mobile device 104 to display details 540 of a payment request as taught by Lin. In the combination, Lin's details 540 would be displayed on the display/touch screen of Collinge's mobile device 104 (visually presenting information of the payment transaction on the touch screen display of said electronic device). A POSITA would have been motivated to make such a modification and would have had a reasonable chance of success for the same reasons addressed in Claim 1(d). Dec., ¶¶ 364-626.

- 10. Claim 16[ff]: visually presenting a request for user approval of the payment transaction via touch input at said electronic device; and,**

See Claim 8(b).

- 11. Claim 16[g]: subsequent to receiving a user-touch input from an identified user, approving performance of said payment transaction via said electronic device.**

Collinge teaches if the user clicks pay, the transaction will proceed. See Claim 8(b).

- 12. Claim 51:**

See Claim 10.2.

- 13. Claim 52:**

See Claims 10.2; 49.

- 14. Claim 53:**

See Claims 10.2; 49.

- 15. Claim 68:**

See Claim 10.2.

- 16. Claim 69:**

See Claims 10.2; 39(d).

- 17. Claim 70:**

See Claims 10.2; 39(d).

IX. GROUND 5: COLLINGE IN VIEW OF LIN, SAHOTA, AND YU

- 1. 10.3: The method of claim 8, wherein said successfully validating the identified user comprises the processor successfully**

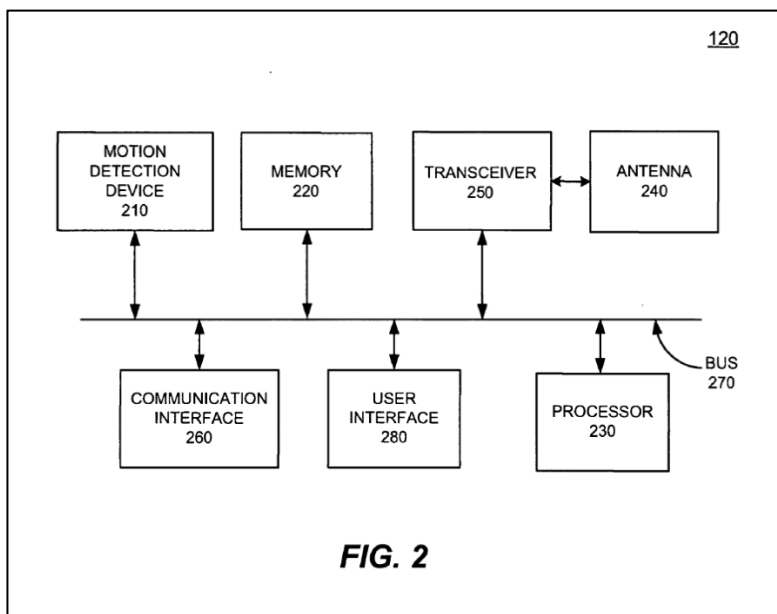
determining a match between: firstly, a user input received via at least one of a set of user input sensors of the electronic device; and, secondly, at least one of the set consisting of: predetermined user characteristics, and challenge-responses of an authorized user, as stored in the electronic device.

(a) Collinge's Teachings

Collinge teaches processing “a gesture” as an authentication “credential.” Collinge, [0143]. Collinge does not specifically teach how a gesture is detected or processed.

(b) Yu's Teachings

Yu teaches a “mobile communication device” that includes a “motion detection device 210” (*user input sensors*). Yu, [0027].



Yu, Fig. 2.

Yu's mobile phone motion detection device 210 “can comprise one or more accelerometers, gyros, inclinometers, cameras, tilt sensors, or any other sensors that

can determine the motion of a device [*user input*] within N degrees of freedom[.]” *Yu*, [0028] (an array of motion sensors); *Dec.*, ¶375. The output of the “motion detection device 210 can be processed by processor 230 with instructions in memory 220 to extract features from the movement of the mobile device to verify both the identity and presence of a mobile user” (*predetermined user characteristics*). *Yu*, [0028]. If the user is verified “control passes to action 410 for further processing. In action 410 access to the service or device is granted. Access includes providing admission to mobile internet services, mobile banking or e-commerce, usage of the mobile communication device 120, usage of selected services or software in the device, or right to use selected hardware resources.” *Yu*, [0038].

Yu teaches that the “extracted motion features are used to construct a motion password. The “motion password shadow 370 is stored so it can later be used to authenticate a user. *Yu*, [0040].

(c) Motivation to Combine

It would have been obvious and a POSITA would have been motivated to modify Collinge to include an array of motion sensors and to use those motion sensors to identify an authorized user by detecting a recognized user displacement of the array of motion sensors as taught by *Yu*. *Dec.*, ¶¶379-81. Collinge already teaches processing “a gesture” as an authentication “credential” and motion detection hardware was already commonly found in mobile devices at the time.

Collinge, [0143]. A POSITA would have been motivated to modify *Collinge* to identify a user via a known user's motion to increase accessibility and security of *Collinge*'s mobile payment application. *Id.* A POSITA would have been motivated to store the users' motion credential(s) in *Collinge*'s storage 304, to quickly authenticate a user as taught by Yu. *Yu*, [0040]. *Id.* A POSITA would have recognized that Yu's motion-based authentication was a known technique that could have improved *Collinge*'s mobile device in the same way, and it would have predictably resulted in the ability to use a motion or gesture to authenticate a user, increasing security. *Id.* A POSITA would have had a reasonable expectation of success in making this modification, including because motion sensor arrays were already standard in mobile devices and because *Collinge* already teaches gesture-based authentication. *Id.*

2. Claim 14:

See Claim 10.3.

3. Claim 54:

See Claim 10.3.

4. Claim 71:

See Claim 10.3.

X. DISCRETION UNDER 35 U.S.C. § 325(d)

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

XI. 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

XII. 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 '634 Patent is the subject of a civil action in *CardWare Inc. v. Apple Inc.*, 1:25-cv-00446 (W.D. Tex.) and *CardWare Inc. v. Google LLC*, 7:24-cv-00278 (W.D. Tex.).

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. Petitioner consents to electronic service by e-mail at the e-mail addresses provided above.

CLAIM LISTING APPENDIX
U.S. PATENT NO. 11,620,634 FOR CLAIMS 1-72

Claim Designation	Claim Language
Claim 1(Pre)	A method of generating and using limited-use payment information for performing a payment transaction, the method comprising:
Claim 1(a)	receiving an input at an electronic device, wherein the input comprises a priming operation, and, wherein the electronic device comprises:
Claim 1(a)(1)	a processor;
Claim 1(a)(2)	a touch-screen display coupled to the processor; and
Claim 1(a)(3)	a near field communications (NFC) interface coupled to the processor;
Claim 1(b)	responsive to said priming operation, readying said device to perform a payment transaction by an identified user;
Claim 1(c)	receiving a payment request for the payment transaction at said electronic device;
Claim 1(d)	displaying, on the touch-screen display, information reflecting the payment request, and an image representing a selected issued payment account;
Claim 1(e)	dynamically generating, by the processor, limited-use payment information;
Claim 1(f)	wherein said limited-use payment information is dynamically generated based on a per-transaction sequential parameter originating from the electronic device;
Claim 1(g)	using said limited-use payment information in connection with the payment transaction in place of issued payment information associated with said selected issued payment account;
Claim 1(h)	transmitting said limited-use payment information from said electronic device via said NFC interface for receipt by an NFC recipient;
Claim 1(i)	responsive to the transmitting the limited-use payment information, receiving via the NFC interface information reflecting a status of said payment transaction; and displaying the status of said payment transaction via said touch-screen display.

Claim Designation	Claim Language
Claim 2	The method of claim 1, wherein the limited-use payment information comprises a cryptogram number.
Claim 3(a)	The method of claim 2, further comprising: prior to the priming operation, transmitting the issued payment information for receipt by a payment processing authority; and,
Claim 3(b)	in response to said transmitting issued payment information, receiving a static device account information that is unique to the electronic device.
Claim 4(a)	The method of claim 3 further comprising: combining said limited-use payment information and said static device account information, to reduce a combined payment information;
Claim 4(b)	transmitting said combined payment information, in place of the issued payment account information, via said NFC for receipt by an NFC recipient; and
Claim 4(c)	receiving, via the NFC interface, and in response to transmitting said combined payment information, transaction processing information reflecting a status of said payment transaction.
Claim 5	The method of claim 3, wherein the dynamically generating Lather comprises dynamically generating the limited-use payment information based on payment processing authority secret information.
Claim 6	The method of claim 5, wherein the limited-use payment information is based on at least one secret information shared by both the electronic device and the payment processing authority.
Claim 7	The method of claim 1, wherein the priming operation comprises bringing the electronic device within receiving proximity of an NFC recipient.
Claim 8(a)	The method of claim 7, wherein said readying said device to perform a payment transaction comprises: identifying said proximity NFC recipient is an NFC payment facility; successfully validating the identified user as authorized to perform the payment transaction via said electronic device; and

Claim Designation	Claim Language
Claim 8(b)	receiving a user approval for performing the payment transaction.
Claim 9(Pre)	The method of claim 8, wherein said user approval for performing a payment transaction comprises displaying a request for user input at said electronic device, for both said identifying and said user approval of said payment transaction, and further comprising:
Claim 9(a)	the processor identifying that said user input matches a known authorized user of the electronic device, before said readying said device to perform a payment transaction; and,
Claim 9(b)	disallowing the payment transaction by the device until said readying said device to perform the payment transaction is successfully completed.
Claim 10	The method of claim 8, wherein said successfully validating the identified user comprises the processor successfully determining a match between: firstly, a user input received via at least one of a set of user input sensors of the electronic device; and, secondly, at least one of the set consisting of: predetermined user characteristics, and challenge-responses of an authorized user, as stored in the electronic device.
Claim 11	The method of claim 10, wherein said user input received via at least one of a set of user input sensors of the electronic device comprises a passcode entry sequence performed by a user input via the touch-screen display.
Claim 12	The method of claim 10, wherein said predetermined user characteristics stored within the electronic device comprise known user biometric touch characteristics.
Claim 13	The method of claim 10, wherein said predetermined user characteristics stored within the electronic device comprise a known user touch gesture.
Claim 14	The method of claim 10, wherein said predetermined user characteristics stored within the electronic device comprise a known user motion of the device.
Claim 15	The method of claim 1, wherein the input comprising a priming operation is a user input.
Claim 16(Pre)	The method of claim 15, wherein said readying said device to perform a payment transaction comprises:

Claim Designation	Claim Language
Claim 16(a)	successfully identifying said identified user from said user input; and,
Claim 16(b)	wherein said user input further comprises a user approval for performing the payment transaction received from said identified user; and,
Claim 16(c)	wherein said successfully identifying further comprises said electronic device validating an authorized user of said electronic device by comparing a user-touch input received via a touch input sensor on the electronic device with a recognized valid user-touch, stored in a memory of the electronic device; and,
Claim 16(d)	wherein said user approval for performing the payment transaction further comprises:
Claim 16(e)	visually presenting information of the payment transaction on the touch screen display of said electronic device;
Claim 16(f)	visually presenting a request for user approval of the payment transaction via touch input at said electronic device; and,
Claim 16(g)	subsequent to receiving a user-touch input from an identified user, approving performance of said payment transaction via said electronic device.
Claim 17(a)	The method of claim 1, further comprising: prior to the priming operation, transmitting the issued payment information for receipt by a payment processing authority; and,
Claim 17(b)	in response to said transmitting issued payment information, receiving a static device account information that is unique to the electronic device.
Claim 18(a)	The method of claim 17 further comprising: combining said limited-use payment information and said static device account information, to produce a combined payment information;
Claim 18(b)	transmitting said combined payment information, in place of the issued payment account information said NFC interface for receipt by an NFC recipient; and
Claim 18(c)	receiving, via the NFC interface, and in response to transmitting said combined payment information, transaction processing information reflecting a status of said payment transaction.

Claim Designation	Claim Language
Claim 19	The method of claim 18, wherein the dynamically generating further comprises dynamically generating the limited-use payment information based on payment processing authority secret information.
Claim 20	The method of claim 19, wherein the limited-use payment information is based on at least one secret information shared by both the electronic device and the payment processing authority.
Claim 21	The method of claim 17, wherein the dynamically generating further comprises dynamically generating the limited-use payment information based on payment processing authority secret information.
Claim 22	The method of claim 21, wherein the limited-use payment information is based on at least one secret information shared by both the electronic device and the payment processing authority.
Claim 23(a)	The method of claim 1, further comprising: prior to the priming operation, transmitting the issued payment information, user information and device-specific information; and,
Claim 23(b)	in response to transmitting said issued payment information, user information and device-specific information, receiving a payment processing authority supplied secret information.
Claim 24	The method of claim 23 wherein said payment processing authority supplied secret information comprises static device account information.
Claim 25	The method of claim 24 wherein said static device account information comprises a static device account number and a static device-specific expiration date.
Claim 26	The method of claim 25 wherein the static device account number is associated with the selected issued payment account on said electronic device.
Claim 27	The method of claim 1, wherein the dynamically generating further comprises dynamically generating the limited-use payment information based on payment processing authority secret information.

Claim Designation	Claim Language
Claim 28(Pre)	The method of claim 27 wherein the limited-use payment information is based on at least one secret information shared by both the electronic device and the payment processing authority; and
Claim 28(a)	further wherein the at least one secret information is not exchanged when performing the payment transaction.
Claim 29(Pre)	A system for completing a payment transaction, the system comprising:
Claim 29(a)	an electronic device operable to receive a priming operation, wherein the priming operation is operable to ready said device for performing a payment transaction by an identified user, and, wherein the electronic device further comprises:
Claim 29(b)	a processor;
Claim 29(c)	a near field communications (NFC) interface coupled to the processor and operable to receive a payment request associated with the payment transaction; and,
Claim 29(d)	a touch-screen display coupled to the processor, and
Claim 29(e)	wherein the electronic device is operable to cause the display of information reflecting device-readiness, the payment request, and an image representing at least one selected issued payment account;
Claim 29(f)	wherein the electronic device is operable to dynamically generate limited-use payment information based on a sequential counter count from the electronic device;
Claim 29(g)	wherein the electronic device is operable to store a static device-specific user account information;
Claim 29(h)	wherein the electronic device is operable to transmit a combination of said dynamically generated limited-use payment information and said static device-specific user account information to an NFC recipient via, said NFC interface for use in connection with payment transaction in place of information associated with said selected issued payment account;
Claim 29(i)	wherein the electronic device is operable, subsequent to transmission of said combination, to receive a status information reflecting a status of said payment transaction; and, wherein the touch-screen display is operable to display as indication of said status information.

Claim Designation	Claim Language
Claim 30	The system of claim 29, wherein the dynamically generated limited-use payment information comprises a cryptogram number.
Claim 31	The system of claim 29, wherein the device-specific user account information comprises static device account information.
Claim 32	The system of claim 31, wherein the static device account information comprises a static device account number that is unique to the electronic device.
Claim 33	The system of claim 32 wherein the static device account information further comprises a static device account expiration date.
Claim 34	The system of claim 32 wherein the sequential counter count is changed per payment transaction.
Claim 35	The system of claim 34 wherein the electronic device is operable to transmit issued payment account information and in response thereto, to receive the static device account information.
Claim 36(Pre)	The system of claim 29 wherein the electronic device is further operable to dynamically generate the limited-use payment information based on a shared information: from said user, information associated with said electronic device, information associated with said selected, issued payment account, and at least one secret; and,
Claim 36(a)	wherein said shared information is shared by both the electronic device and a payment processing authority.
Claim 37	The system of claim 36 wherein the electronic device is further operable to dynamically generate the limited-use payment information based on payment processing authority secrets.
Claim 38	The system of claim 29 wherein the electronic device is further operable to dynamically generate the limited-use payment information based on payment processing authority secrets.
Claim 39(Pre)	An electronic device for completing a payment transaction, the electronic device comprising:
Claim 39(a)	a processor;
Claim 39(b)	a memory coupled to the processor,

Claim Designation	Claim Language
Claim 39(b)(1)	wherein the memory is operable to store information associated with use of an issued payment account and wherein the payment authority information comprises a secret information;
Claim 39(c)	a near field communications (NFC) interface coupled to the processor and operable to receive a payment request associated with the payment transaction;
Claim 39(d)	a user interface coupled to the processor;
Claim 39(e)	a user input device coupled to the processor; and,
Claim 39(f)	wherein said processor is operable to: responsive to a priming operation, wherein the priming operation is operable to ready the device to perform the payment transaction,
Claim 39(g)	cause the display of information associated with the payment request;
Claim 39(h)	cause the display of an image representing at least one user-selectable issued payment account; and,
Claim 39(i)	dynamically generate a limited-use payment information based on a per-transaction sequential parameter originating from the electronic device, and secret information associated with a selected issued payment account; and,
Claim 39(j)	cause the transmission, via said NFC interface, a payment information combination comprising the dynamically generated limited-use payment information and said payment authority information, for receipt by an NFC recipient;
Claim 39(k)	wherein the NFC interface is operable, in response to transmitting said payment information combination, to receive status information reflecting a transaction processing status of said payment transaction; and wherein the user interface is operable to provide an indication of the status information.
Claim 40	The device of claim 39 wherein the payment authority information comprises information that is unique to the electronic device.
Claim 41	The device of claim 39 wherein the payment authority information comprises a secret information shared by both the electronic device and a payment processing authority.
Claim 42	The device of claim 41 wherein the processing authority information comprises a static device account number.

Claim Designation	Claim Language
Claim 43	The device of claim 42 wherein the processing authority information further comprises a static device account expiration date.
Claim 44	The device of claim 39 wherein the processor is operable to cause the transmission of issued payment account information and in response thereto, to receive the processing authority information.
Claim 45	The device of claim 39 wherein the dynamically generated limited-use payment information comprises a cryptogram number, and further wherein the processor is operable to cause transmission, via said NFC interface, of a payment information combination comprising the dynamically generated limited-use payment information and at least a portion of said payment authority information in connection with the payment transaction in place of at least a portion of the payment information associated with said selected issued payment account.
Claim 46	The device of claim 45 wherein the processor is operable to cause the transmission of issued payment account information and in response thereto, receive the processing authority information.
Claim 47	The device of claim 46 wherein the processing authority information comprises a static device account number.
Claim 48	The device of claim 47 wherein the processing authority information further comprises a static device account expiration date.
Claim 49	The device of claim 39, wherein said user interface comprises a display and wherein said user input device comprises a touch panel disposed adjacent to said display and wherein further the processor is operable to identify an authorized user by validating a valid user passcode input to the touch panel.
Claim 50	The device of claim 39, wherein said user interface comprises a display and wherein said user input device comprises a touch panel disposed adjacent to said display and wherein further the processor is operable to identify an authorized user by displaying a security challenge question presented on the display and receiving a correct user response thereto.

Claim Designation	Claim Language
Claim 51	The device of claim 39, wherein said user input device comprises a biometric sensor operable to detect a user touch of said electronic device and wherein further the processor is operable to identify an authorized user by biometric sensing of a continuous user touch.
Claim 52	The device of claim 39, wherein said user interface comprises a display and wherein said user input device comprises a touch panel disposed adjacent to said display and wherein further the processor is operable to identify an authorized user by biometric sensing of a user touch at the touch panel.
Claim 53	The device of claim 39, wherein said user interface comprises a display and wherein said user input device comprises a touch panel disposed adjacent to said display and wherein further the processor is operable to identify an authorized user by biometric recognition of a valid user identification.
Claim 54	The device of claim 39, wherein said user input device comprises an array of motion sensors and wherein further the processor is operable to identify an authorized user by detecting a recognized user displacement of the array of motion sensors.
Claim 55(a)	The device of claim 39, wherein the processor is operable to: receive a user-selection of an issued payment account presented on the user interface, received the user input device coupled to the processor, and
Claim 55(b)	responsive thereto, select from the memory a specific processing authority information corresponding to the user-selected issued payment account information, and
Claim 55(c)	use at least a portion of said specific processing authority information in place of at least a portion of the issued payment account information to generate a combined payment information to complete a payment transaction per the input user-selection.
Claim 56(Pre)	An electronic device for completing a payment transaction, the electronic device comprising:
Claim 56(a)	a processor;
Claim 56(b)	a memory coupled to the processor,

Claim Designation	Claim Language
Claim 56(b)(1)	wherein the memory stores a payment authority information associated with a user-selectable issued payment account, and wherein the payment authority information includes a secret information;
Claim 56(c)	a near field communications (NFC) interface coupled to the processor and operable to receive a payment request associated with the payment transaction;
Claim 56(d)	a user interface coupled to the processor;
Claim 56(e)	a user input device coupled to the processor; and,
Claim 56(f)	wherein said processor is operable to: responsive to a priming operation, wherein the priming operation is operable to ready the device to perform the payment transaction,
Claim 56(g)	cause the display of information associated with the payment request;
Claim 56(h)	cause the display of an image representing the user-selectable issued payment account; and,
Claim 56(i)	dynamically generate a limited-use payment information based on a per-transaction sequential parameter originating from the electronic device, and the secret information associated with the user-selectable issued payment account; and,
Claim 56(j)	cause the transmission, via said NFC interface, of a payment information combination comprising, the dynamically generated limited-use payment information and at least a portion of said payment authority information, for receipt by an NFC recipient;
Claim 56(k)	wherein the NFC interface is operable, in response to transmitting said payment information combination, to receive status information reflecting a transaction processing status of said payment transaction; and wherein the user interface is operable to provide an indication of the transaction status information.
Claim 57	The device of claim 56, wherein the payment authority information comprises information that is unique to the electronic device.
Claim 58	The device of claim 57, wherein the payment authority information comprises a static device account number.

Claim Designation	Claim Language
Claim 59	The device of claim 58, wherein the payment authority information further comprises a static device account expiration date.
Claim 60	The device of claim 56, wherein the secret information is shared by both the electronic device and a payment processing authority.
Claim 61	The device of claim 56, wherein the processor is operable to cause the transmission of issued payment account information and in response thereto, to receive the payment authority information.
Claim 62	The device of claim 56, wherein the dynamically generated limited-use payment information comprises a cryptogram number, and further payment information combination is used in place of at least a portion of fixed payment information associated with said user-selectable issued payment account.
Claim 63	The device of claim 62, wherein the processor is operable to cause the transmission of issued payment account information and in response thereto, receive the payment authority information.
Claim 64	The device of claim 63, wherein the payment authority information comprises a static device account number.
Claim 65	The device of claim 64, wherein the payment authority information further comprises a static device account expiration date.
Claim 66	The device of claim 56, wherein said user interface comprises a display and wherein said user input device comprises a touch screen interface of the display, and wherein further the processor is operable to identify an authorized user by validating a valid user passcode input to the touch screen interface.
Claim 67	The device of claim 56, wherein said user interface comprises a display and wherein said user input device comprises a touch screen interface of the display, and wherein further the processor is operable to identify an authorized user by displaying a security challenge question presented on the display and receiving a correct user response via said touch screen interface of the display.

Claim Designation	Claim Language
Claim 68	The device of claim 56, wherein said user input device comprises a biometric sensor operable to detect a user touch of said electronic device and wherein further the processor is operable to identify an authorized user by biometric sensing of said user touch.
Claim 69	The device of claim 56, wherein said user interface comprises a display and wherein said user input device comprises a touch screen interface of the display and wherein further the processor is operable to identify an authorized user by biometric sensing of a user touch at the touch screen interface.
Claim 70	The device of claim 56, wherein said user interface comprises a display and wherein said user input device comprises a touch input of the electronic device and wherein further the processor is operable to identify an authorized user by biometric recognition of a valid user identification via the touch input.
Claim 71	The device of claim 56, wherein said user input device comprises an array of motion sensors and wherein further the processor is operable to identify an authorized user by detecting a recognized user displacement of the array of motion sensors.
Claim 72(Pre)	The device of claim 56, wherein the processor is operable to receive, via the user input device, a user-selection of said user-selectable issued payment account presented on the user interface, and
Claim 72(a)	in response thereto, is further operable to select from memory the payment authority information corresponding to selected user-selectable issued payment account, and
Claim 72(b)	is further operable to use said payment information combination in place of at least a portion of fixed payment information associated with said selected user-selectable issued payment account.

APPENDIX OF EXHIBITS

Exhibit 1001	U.S. Patent No. 11,620,634 (the “’634 Patent”)
Exhibit 1002	File History of the ’634 Patent (“the ’634 File History”)
Exhibit 1003	Declaration of Dr. Neuman
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	Intentionally left blank
Exhibit 1010	U.S. Patent Publication No. 2010/0125508 to Smith (“Smith”)
Exhibit 1011	U.S. Patent Publication No. 2005/0043997 to Sahota et al. (“Sahota”)
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. 2009/0320123 to Yu et al. (“Yu”)
Exhibit 1015	U.S. Patent Publication No. 2009/0083850 to Fadell et al. (“Fadell”)
Exhibit 1016	CardWare Inc.’s Preliminary Proposed Claim Constructions
Exhibit 1017	Intentionally Left Blank
Exhibit 1018	Intentionally Left Blank
Exhibit 1019	Intentionally Left Blank
Exhibit 1020	IBM, The Magnetic Stripe, IBM, https://www.ibm.com/history/magnetic-stripe . (“IBM”)
Exhibit 1021	Vedat Coskun, Near Field Communication: Theory to Practice (John Wiley & Sons, 1st ed. 2012) (“Coskun”)
Exhibit 1022	MagTek, Magnetic Stripe Card Standards, (MagTek Inc. eds., 2011) (“MagTek”)
Exhibit 1023	EMVCo, LLC, EMV Integrated Circuit Card Specifications for Payment Systems: Book 2 – Security and Key Management (EMVCo, LLC eds., Version 4.3 2011) (“EMV”)

Exhibit 1024	Klaus Finkenzeller, RFID Handbook (John Wiley & Sons, 3rd ed. 2010) (“Finkenzeller”)
Exhibit 1025	MasterCard, MasterCard PayPass TM in Action, 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 . (“PayPass”)
Exhibit 1026	Smart Card Alliance, EMV and NFC: Complementary Technologies that Deliver Secure Payments and Value-Added Functionality (Smart Card Alliance, Inc. eds., 2012) (“Smart”)
Exhibit 1027	U.S. Patent Publication No. 2012/0011058 to Pitroda et al. (“Pitroda”)
Exhibit 1028	MasterCard, MasterCard Approved Mobile Devices, 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] (“MasterCard Mobile Partner”)
Exhibit 1029	U.S. Patent Publication No. 2013/0054474 to Yeager (“Yeager”)
Exhibit 1030	EMVCo, LLC, EMV Chip At-a-Glance: Enabling Seamless and Secure Contact and Contactless Payments Around the World, EMVCo (2002), https://www.emvco.com/wp-content/uploads/2022/09/EMV%C2%AE-Chip-At-A-Glance-EMVCo-eBook.pdf (“EMVCo”)
Exhibit 1031	Scoping SIG & Tokenization Taskforce PCI Security Standards Council, PCI Data Security Standard (PCI DSS) – Information Supplement: PCI DSS Tokenization Guidelines (pci Security Standards Council eds., Version 2.0 2011) (“PCI SSC”)
Exhibit 1032	Alessandro Vizzarri et al., Security in Mobile Payments (2013) (“Vizzarri”)
Exhibit 1033	U.S. Patent Publication No. 2008/00110983 to Ashfield (“Ashfield”)
Exhibit 1034	U.S. Patent Publication No. 2014/0310113 to Sengupta et al. (“Sengupta”)
Exhibit 1035	U.S. Patent Appl. No. 2012/0169593 to Mak et al. (“Mak”)
Exhibit 1036	U.S. Patent Appl. No. 2012/0148115 to Birdwell et al. (“Birdwell”)
Exhibit 1037	U.S. Patent Appl. No. 2007/0076923 to Chiu et al. (“Chiu”)
Exhibit 1038	Intentionally left blank

Exhibit 1039	Ann Cavoukian, Mobile Near Field Communications (NFC) “Tap ‘n Go” Keep it Secure & Private, IPC (2011), https://www.ipc.on.ca/sites/default/files/legacy/Resources/mobile-nfc.pdf (“Cavoukian”)
Exhibit 1040	Annika Paus, Near Field Communication in Cell Phones (2017) (“Paus”)
Exhibit 1041	Intentionally left blank
Exhibit 1042	U.S. Patent Publication No. 2006/0097991 to Hotelling et al. (“Hotelling”)
Exhibit 1043	U.S. Patent No. 7,580,898 to Brown et al. (“Brown”)
Exhibit 1044	U.S. Patent No. 10,181,121 (“Roberts”)
Exhibit 1045	U.S. Patent Publication No. 2013/0151292 to Van Deloo et al. (“Deloo”)
Exhibit 1046	U.S. Patent Publication No. 2006/0186195 to Gray (“Gray”)
Exhibit 1047	U.S. Patent Publication No. 2014/0006276 to Grigg et al. (“Grigg”)
Exhibit 1048	Anup K. Ghosh & Tara M. Swaminatha, Software Security and Privacy Risks in Mobile E-Commerce, 44 CACM 51 (2001) (“Ghosh”)
Exhibit 1049	U.S. Patent Appl. No. 2011/0140841 to Bona et al. (“Bona”)

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 13,932 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 '634 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

IPR2025-01152

U.S. Patent No. 11,620,634

(913) 777-5600 Telephone

(913) 777-5601 Facsimile

COUNSEL FOR PETITIONER