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. IPR2025-01148
U.S. Patent No. 10,810,579

PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT NO. 10,810,579

TABLE OF CONTENTS

I. INTRODUCTION 1
II. THE '579 PATENT 1
A. DESCRIPTION OF THE '579 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. Collinge Incorporated all Provisionals for All Purposes 8
2. Obvious to Combine Provisional Features 9
B. LIN 11
C. SMITH 13
D. KRANZLEY 14
E. PHILLIPS 15
F. AABYE 16
G. PISULA 17
H. FADELL 17
I. ANALOGOUS ART 18
V. GROUND 1: COLLINGE IN VIEW OF LIN AND PHILLIPS 19
1. 1(Pre): "A method of performing a transaction, the method comprising:" 19

2. 1(a): "receiving an input at an electronic device, wherein the input corresponds to a priming operation of the electronic device by an identified user" *21*

3. 1(b): "and wherein the electronic device comprises a processor;" *25*

4. 1(b)(1): "a touch screen display coupled to the processor; and;" *25*

5. 1(b)(2): "a near field communications (NFC) interface coupled to the processor;" *28*

6. 1(c): "receiving a request for a transaction payment at said electronic device via the NFC interface;" *30*

(a) Collinge's Teachings 31

(b) Lin's Teachings 32

(c) Motivation to Combine 32

7. 1(d): "displaying, on the touch-screen display, images of: a card issuer payment method selection, including a last 4-digit partial number of a card issuer supplied account number of a payment card; a card logo; and other iconography of the payment card;" *33*

(a) Collinge's Teachings 34

(b) Phillips' Teachings 35

(c) Motivation to Combine 37

(d) Lin's Teachings 39

8. 1(e): "generating, by the processor, a limited-use payment information, and using said limited-use payment information in place of said card issuer supplied payment information;" *41*

9. 1(f): "transmitting said limited-use payment information from said electronic device to an NFC recipient of the transaction via said NFC interface; and" *42*

10. 1(g): "visually conveying a status of said transaction via a user-interface displayed on said touch-screen display." *43*

11. Claim 2 ..... *44*

12. Claim 3: *46*
13. Claim 7: *47*
14. Claim 10: *48*
15. Claim 11: *50*
(a) Collinge's Teachings 50
(b) Phillips' Teachings 52
(c) Motivation to Combine 52
16. Claim 12(a): *54*
17. Claim 12(b): *54*
(a) Phillips' Teachings 54
(b) Motivation to Combine 54
18. Claim 19(Pre): *55*
19. Claim 19(a): *55*
20. Claim 19(b): *55*
21. Claim 19(b): *57*
22. 19(b)(1): *59*
23. 19(b)(2): *60*
24. 19(b)(3): *60*
25. 19(c): *61*
26. 19(d): *62*
27. 19(e): *62*
28. Claim 19(f): *62*
29. Claim 19(g): *62*
30. Claim 19(h): *62*
31. Claim 19(i): *62*
32. Claim 19(j): *62*
33. Claim 20: *62*
34. Claim 23: *63*

VI. GROUND 2: COLLINGE IN VIEW OF PHILLIPS, LIN AND KRANZLEY 64

1. Claim 5(a): 64

2. Claim 5(b): 64

(a) Motivation to Combine 64

3. Claim 6: 65

(a) Collinge's Teachings 66

(b) Kranzley's Teachings 68

(c) Motivation to Combine 68

VII. GROUND 3: COLLINGE IN VIEW OF COLLINGE, LIN, PHILLIPS, SMITH, AND KRANZLEY 70

1. Claim 4(Pre): 70

(a) Collinge's Teachings 70

(b) Smith's Teachings 71

(c) Motivation to Combine 73

2. Claim 4(a): 77

(a) Motivation to Combine 77

3. Claim 4(b): 78

4. Claim 4(c): 80

(a) Smith's Teachings 81

(a) Motivation to Combine 81

5. Claim 4(d): 82

6. Claim 21: 82

7. Claim 22: 82

VIII. GROUND 4: COLLINGE IN VIEW OF PHILLIPS, LIN, AND AABYE 82

1. Claim 8(a): 82

2. Claim 8(b): 83

(a) Collinge's Teachings 83

(b) Aabye's Teachings 84
(c) Motivation to Combine 85
3. Claim 9(a): *87*
4. Claim 9(b): *88*
5. Claim 9(c): *88*
IX. GROUND 5: COLLINGE IN VIEW OF LIN AND AABYE 89
1. Claim 15(Pre): *89*
2. Claim 15(a): *89*
3. Claim 15(b): *89*
4. Claim 15(c): *89*
5. Claim 15(d): *89*
6. Claim 15(e): *89*
7. Claim 15(f): *90*
8. Claim 15(h): *90*
9. Claim 15(i): *90*
10. Claim 15(j): *90*
11. Claim 16: *90*
12. Claim 17: *90*
13. Claim 18: *91*
X. GROUND 6: COLLINGE IN VIEW OF LIN, PHILLIPS, AABYE AND PISULA 91
1. Claim 13(a): *91*
(a) Pisula's Teachings 91
(b) Motivation to Combine 92
2. Claim 13(b): *94*
3. Claim 13(c): *95*
4. Claim 13(d): *95*
5. Claim 13(e): *96*

XI. GROUND 7: *COLLINGE* IN VIEW OF LIN, PHILLIPS, AABYE, PISULA AND FADELL 96

1. Claim 14(a): 96

(a) Collinge's Teachings 96

(b) Fadell's Teachings 98

(c) Motivation to Combine 98

2. Claim 14(b): 100

3. Claim 14(c): 101

XII. DISCRETION UNDER 35 U.S.C. § 325(d) 102

XIII. CONCLUSION 102

XIV. MANDATORY NOTICES UNDER 37 C.F.R. § 42.8 103

A. REAL PARTY-IN-INTEREST UNDER 37 C.F.R. § 42.8(B)(1) 103

B. RELATED MATTERS UNDER 37 C.F.R. § 42.8(B)(2) 103

C. LEAD AND BACK-UP COUNSEL UNDER 37 C.F.R. § 42.8(B)(3) 103

A. 37 C.F.R. 42.8(B)(4) – SERVICE INFORMATION 104

I. INTRODUCTION

Apple Inc., ("Petitioner") respectfully requests *inter partes* review ("IPR") of claims 1-23 ("Challenged Claims") of U.S. Patent No. 10,810,579 ("'579 Patent").

II. THE '579 PATENT

A. Description of the '579 Patent

The '579 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." *'579 Patent* (Ex. 1001), 2:13-19. The '579 Patent also describes "generating a limited-duration credit card number…which is limited in scope of use to a predetermined number of authorized transactions." *Id.* at 2:23-30.

B. Field of Endeavor and Problem Solved by the Inventors

The '579 Patent defines the "FIELD OF THE INVENTION" as relating to "multi-function electronic devices or smart cards and, more particularly, to systems and methods of smart tokenizing payment cards and devices and transaction processing thereof." *'579 Patent* at 1:23-27, 1:62-2:3 (criticizing existing systems as "susceptible to theft and/or compromise"). A POSITA would have understood that the field of endeavor of the '579 Patent includes more secure payment cards, devices, and systems, and the '579 Patent is trying to solve the problem of providing payment

solutions that limit opportunities for theft or compromise of payment credentials. *Dec.*, ¶¶32-37. [1]

C. Priority and Prosecution History

The '579 Patent claims priority to Provisional Application No. 61/794,891, filed March 15, 2013. Because the '579 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.[2] Unless noted, the below analysis would not change under the AIA.

D. Level of Skill of a POSITA

A POSITA at the time of the '579 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. Additional industry experience or technical training may offset less

[1] All references to "*Dec.*" are to Exhibit 10003, Declaration of Dr. Neuman.

[2] Petitioner does not concede that any of the Challenged Claims are entitled to claim priority to March 15, 2013. Multiple claims of the '579 Patent recite features not described in CardWare's provisional application.

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 '579 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	1-3, 7, 10-12, 19-20, 23	Collinge (Ex. 1004), Lin (Ex. 1012), and Phillips (Ex. 1009)
2	5-6	Collinge, Lin, Phillips, and Kranzley (Ex. 1013)
3	4, 21-22	Collinge, Lin, Phillips, Smith (Ex. 1010), and Kranzley
4	8-9	Collinge, Lin, Phillips, and Aabye (Ex. 1011)
5	15-18	Collinge, Lin, and Aabye
6	13	Collinge, Lin, Phillips, Aabye, and Pisula (Ex. 1014)
7	14	Collinge, Lin, Phillips, Aabye, Pisula, Fadell (Ex. 1015)

The earliest claimed priority date of the '579 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 '579 Patent:

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

[3] Petitioner does not concede that any of the Challenged Claims are entitled to claim priority to March 15, 2013. Multiple claims of the '579 Patent recite features not described in the provisional application. Unless specifically noted, the analysis presented in this petition remains the same regardless of whether March 15, 2013 or some later date is used as the Critical Date.

[4] Collinge is prior art of its filing date. Should CardWare attempt to establish an earlier date of reduction to practice, Apple will show that Collinge is entitled to a 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*., ¶¶82-87. *See also Dynamic Drinkware, LLC v. Nat'l Graphics, Inc.,* 800 F.3d 1375, 1381 (Fed. Cir. 2015) (holding Petitioner did not have the burden of producing evidence relating to earlier effective filing date based on provisional application until Patent Owner argued for an earlier date of reduction to practice).

Lin	8/11/2009	4/8/2010	§102(b)
Smith	11/17/2009	5/20/2010	§102(b)
Aabye	9/21/2009	8/26/2010	§102(b)
Kranzley	6/1/2009	5/20/2010	§102(b)
Pisula	9/5/2008	12/25/2012	§102(a), (e)
Fadell	9/9/2008	3/26/2009	§102(b)
Phillips	5/13/2009	12/10/2009	§102(b)

None of these references were cited or discussed during prosecution of the '579 Patent.

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

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

[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.

Claim 6: "rejecting a limited-use number, by the payment processing authority, on at least one"	"rejecting a limited-use number, by the payment processing authority, based on at least one"
Claim 9: "a device biometric sensing the electronic device is continuously remaining in the proximity contact of a valid user"	"a device biometric sensing that the electronic device is continuously remaining in the proximity contact of a valid user"

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

IV. SHOWING OF ANALOGOUS PRIOR ART

A. Collinge

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

Collinge teaches that a user may register their mobile device for use in contactless payments and install a mobile payment application on the mobile device. *Collinge,* [0065]-[0066]. Collinge teaches that after registration, the mobile payment application of the mobile device is provisioned with a card profile and single use key from a remote secure element. *Collinge*, [0068]-[0069]; Fig. 5.

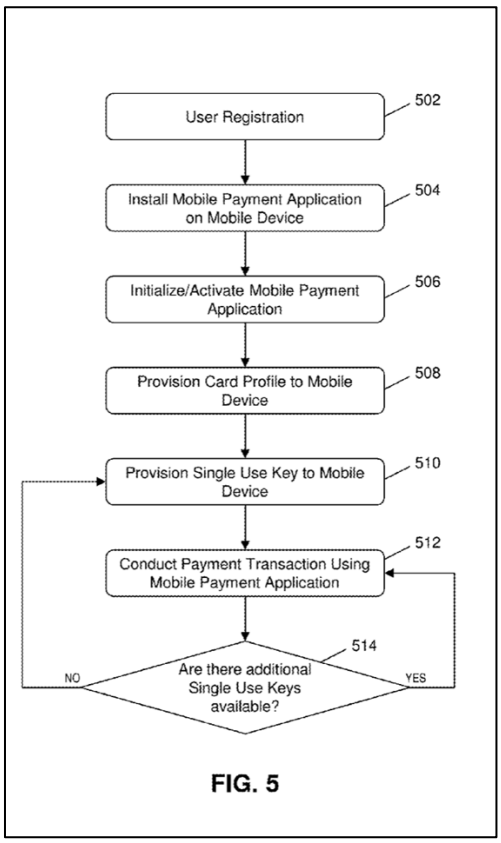
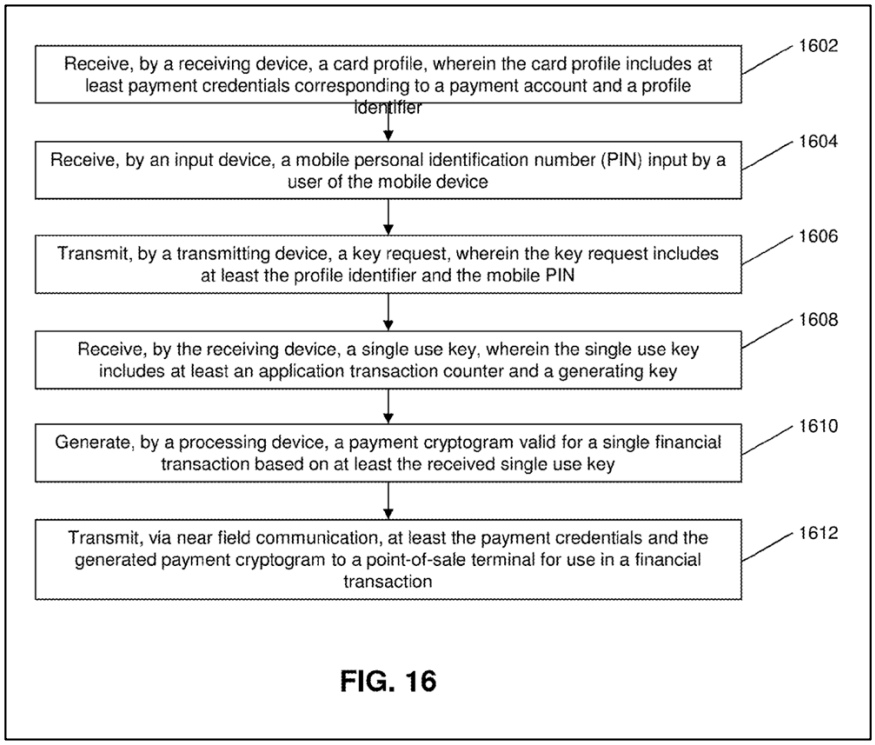


FIG. 5

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 that the Provisionals provide additional implementation details relevant to Collinge's payment system. *Compare e.g., '098 Provisional*, Fig. 19 *with Collinge,* Fig. 6; *Collinge,* Fig. 19 *with* '095 Provisional Fig. 9 and '248 Provisional Fig. 16; *Dec.*, ¶¶81-87.

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

NFC transaction. *See e.g., '248 Provisional*, Fig. 2A, 2B; *'098 Provisional*, p. 96-100; *Collinge*, [0133]. A POSITA would have found it obvious and would have been motivated to incorporate these disclosures into Collinge's payment system because implementing Collinge's payment system requires various display screens with user-selectable soft buttons and Collinge's Provisional provide details regarding layout and soft buttons functions that would assist a POSITA in implementing Collinge's teachings with a reasonable chance of success. *Dec.*, ¶206-211; 310.

As another example, Collinge teaches use of a "CAP token" (*Collinge,* [0144]) and the provisional applications provide examples of what controls on purchases may be represented by the token. *See '095 Provisional*, Claims 9-10 (day of week, time of day, etc.). A POSITA looking to implement a CAP token would have been motivated to implement the examples of a CAP token in Collinge's Provisional application, such as spending limits and expiration date limits which were well-known and would have increased security of Collinge's payment credentials. *See* Claim 6. *Dec.*, ¶236-237.

In addition, it would have been obvious and a POSITA would have been motivated to incorporate a time constraint when completing a payment transaction when Collinge's device is used for an NFC payment, as taught by Fig. 14 of the '248 Patent. A POSITA would have appreciated that using a timer would "limit the

potential exposure of sensitive data" as taught by Collinge. *'248 Provisional*, Fig. 14, [0197]; *Dec.*, ¶87.

In each case, a POSITA would have found a teaching, suggestion, or motivation in Collinge itself that would have led them to apply the additional details in Collinge's Provisionals to Collinge's payment system with a reasonable expectation of success. *Dec.*, ¶87.

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; Fig. 11B, 55:7-15; Fig. 14B, 70:8-27.

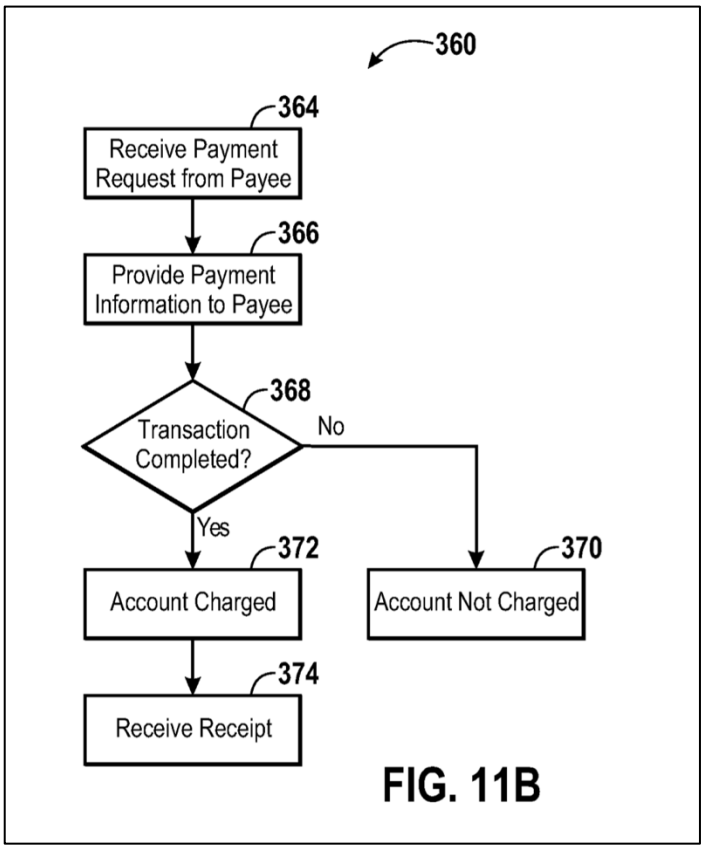
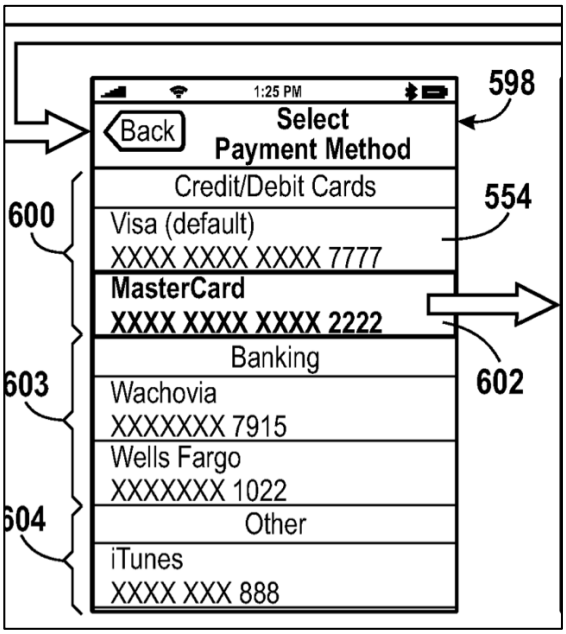


FIG. 11B

Lin, Fig. 11B.

Lin teaches a payment method selection page that displays only last 4-digit partial number of a card issuer supplied account number of a payment card.

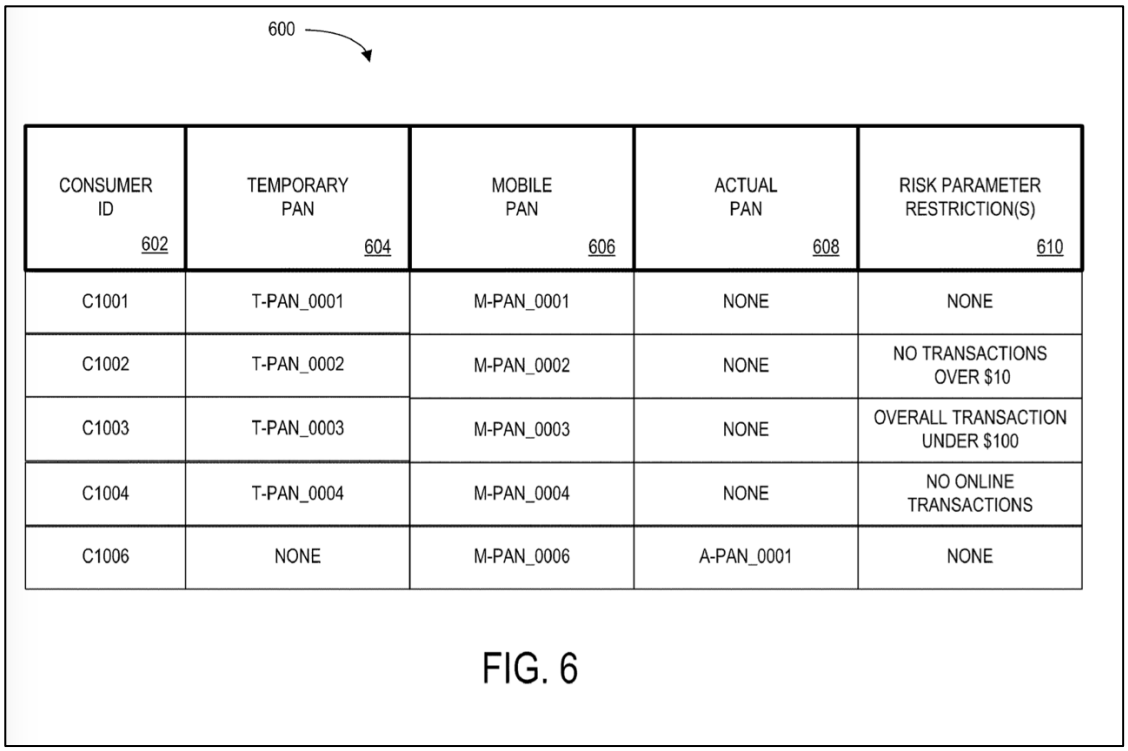


Lin, Fig. 14E. (excerpt).

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. Kranzley

Kranzley teaches that "[t]he payment application of the mobile device 12 converts the data (including the PAN, expiry, and dynamic data) into a bar code image 13." *Kranzley*, [0028]. Kranzley teaches displaying "the static VPAN…in plain text on a display device 14 of the mobile device 12 along with an expiry date and dynamic data[.]" *Kranzley*, [0035]; [0033]-[0036].

E. Phillips

Phillips teaches "a user interface that may facilitate use of mobile telephones for contactless payment transactions[.]" *Phillips,* [0006]. Phillips, like Collinge, is assigned to MasterCard, and the named inventor is also listed on several of Collinge's provisional applications. Phillips teaches a mobile phone with a "virtual wallet" application. *Phillips,* [0027]. The virtual wallet displays "small images of identification cards (e.g., payment cards such as debit or credit cards)" that a user may select from to map a payment using their mobile phone and a proximity reader. *Phillips,* [0012]. Phillips teaches displaying both the front and back of the payment card. *Phillips*, [0049].

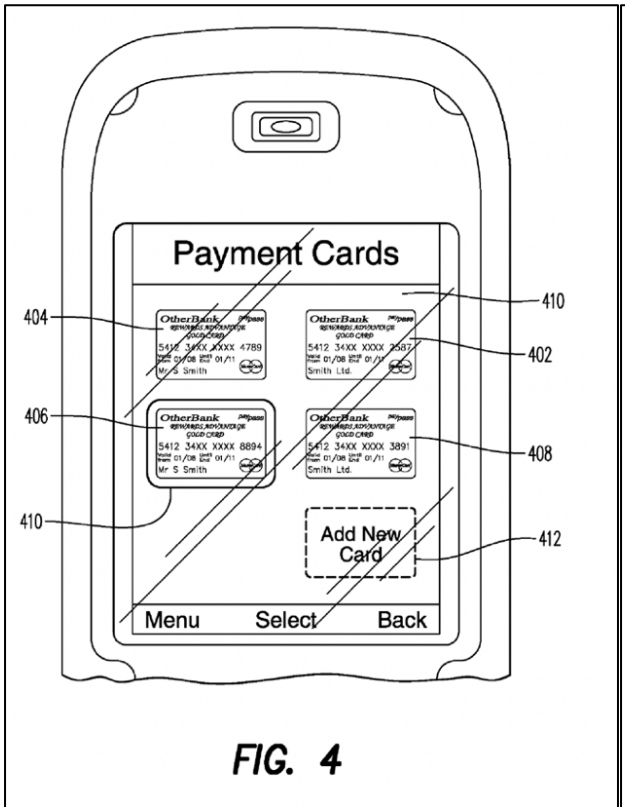


FIG. 4

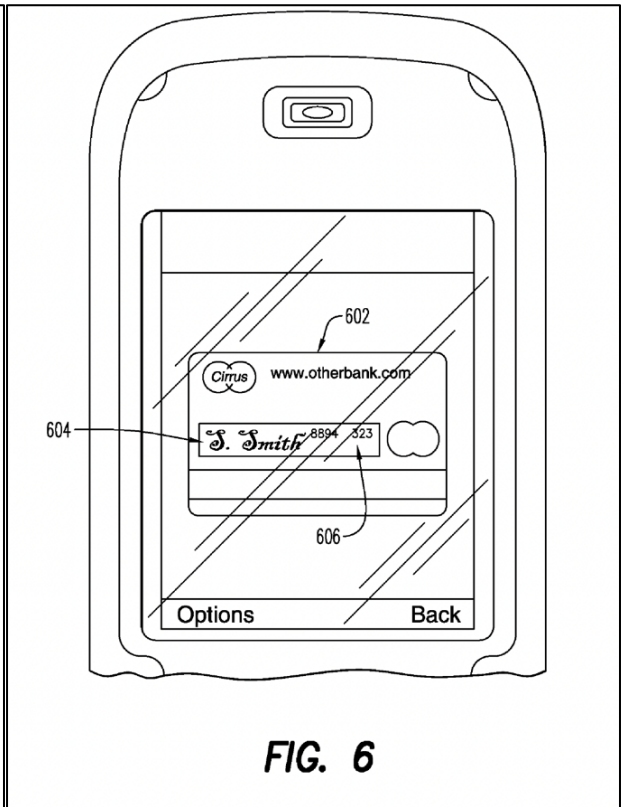


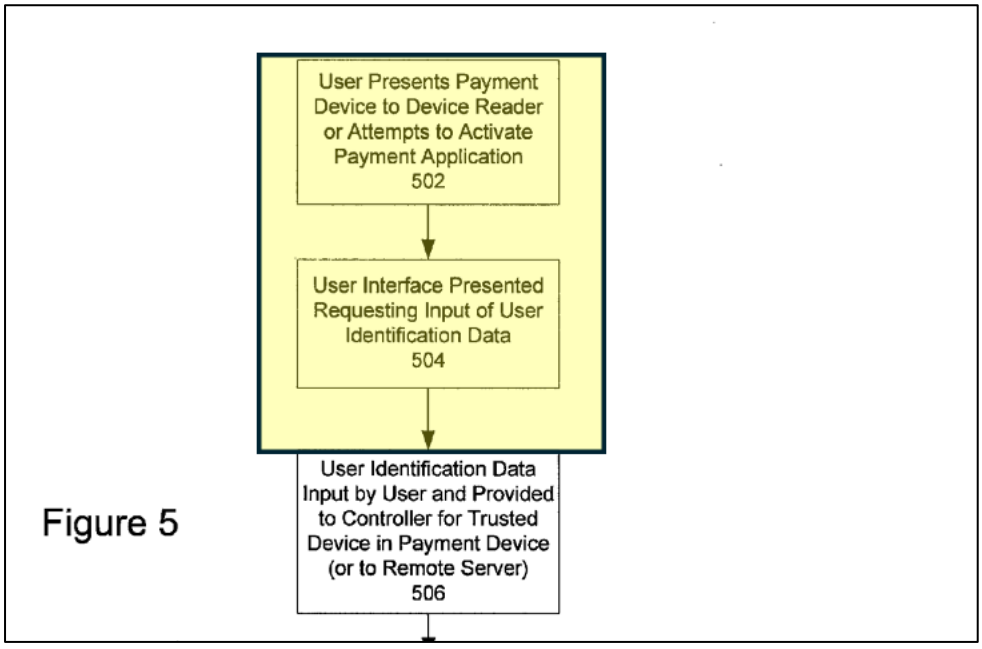
FIG. 6

Phillips, Figs. 4, 6.

F. Aabye

Aabye teaches the "the payment device may include a user data input element 402." *Aabye*, [0050]. This "input element 402" may be a "a fingerprint detector or sensor, a touchscreen, a biometric data sensor, etc." *Aabye*, [0050].

In response to the user presenting the "payment device to a device reader", "the user is presented with a user interface." *Aabye*, [0054]-[0055]. The mobile device's user interface "request[s] the user to input user identification data…into an appropriate data input device (e.g., element 402 of FIG. 4)." One example of identification is "a fingerprint reader for input of a user fingerprint[.]" *Aabye*, [0055].



Aabye, Fig. 5. (annotated excerpt).

The payment application compares "the received user identification data to a previously stored copy of the data)" and "[i]f the received data is verified as valid …then the user is provided access to the functionality of the payment application (stage 516, the payment application is 'activated' for the user; e.g., element 414 of FIG. 4)." *Aabye*, [0057].

G. Pisula

Pisula teaches determining "whether the detected interaction by the user with the first physical button corresponds to a second predefined action" which is "a double activation of the first physical button in a predefined time period (e.g., pressing the menu button 204 twice in succession in 0.3 seconds) (5018)." *Pisula*, 28:57-64. In response to "determining that the interaction by the user with the first physical button corresponds to the second predefined action, the device: turns on the touch screen display[.]" *Pisula*, 28:65-29:4. Pisula also teaches a "longer press of the push button (e.g., 206) may turn power to the device 100 on or off." *Pisula*, 14:23-25.

H. 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].

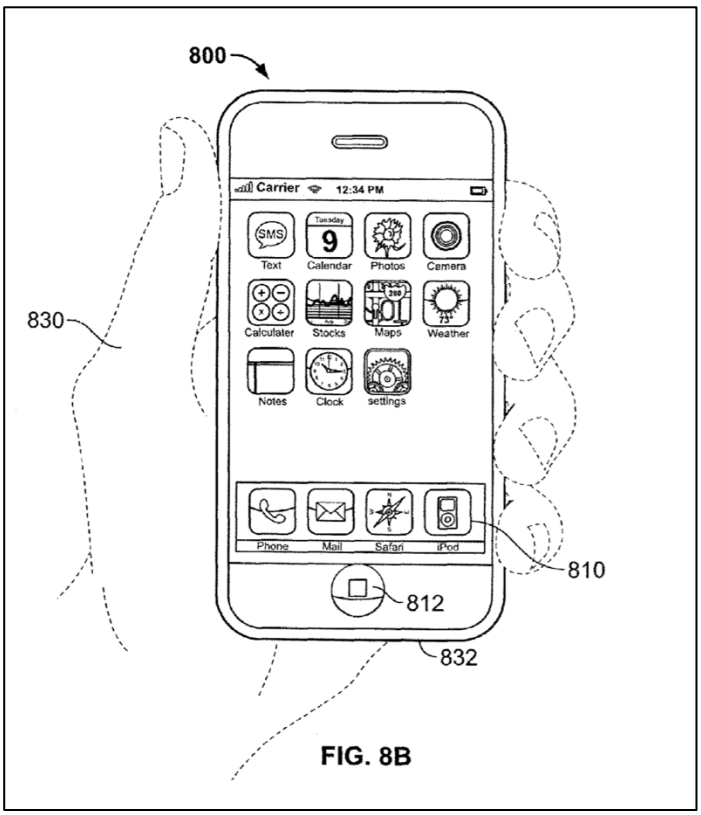


FIG. 8B

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].

I. Analogous Art

The applied prior art references disclose conducting secure payment transactions and are in the same field of endeavor as the '579 Patent. *Compare '579 Patent*, Abstract, 1:23-27, Fig. 1 *with Collinge,* Abstract, [0005], Fig. 1; *Phillips,* Abstract, [0006], [0012], [0014], Fig. 1; *Smith,* Abstract, [0021]-[0023]; *Lin,* Abstract, 68:13-25, Fig. 14C; *Kranzley,* Abstract, [0010], Fig. 1; *Aabye,* Abstract, [0010], [0054], Fig. 1, Fig. 5; *Fadell,* Abstract, [0031]; *Dec.* ¶¶78-80, 91-113.

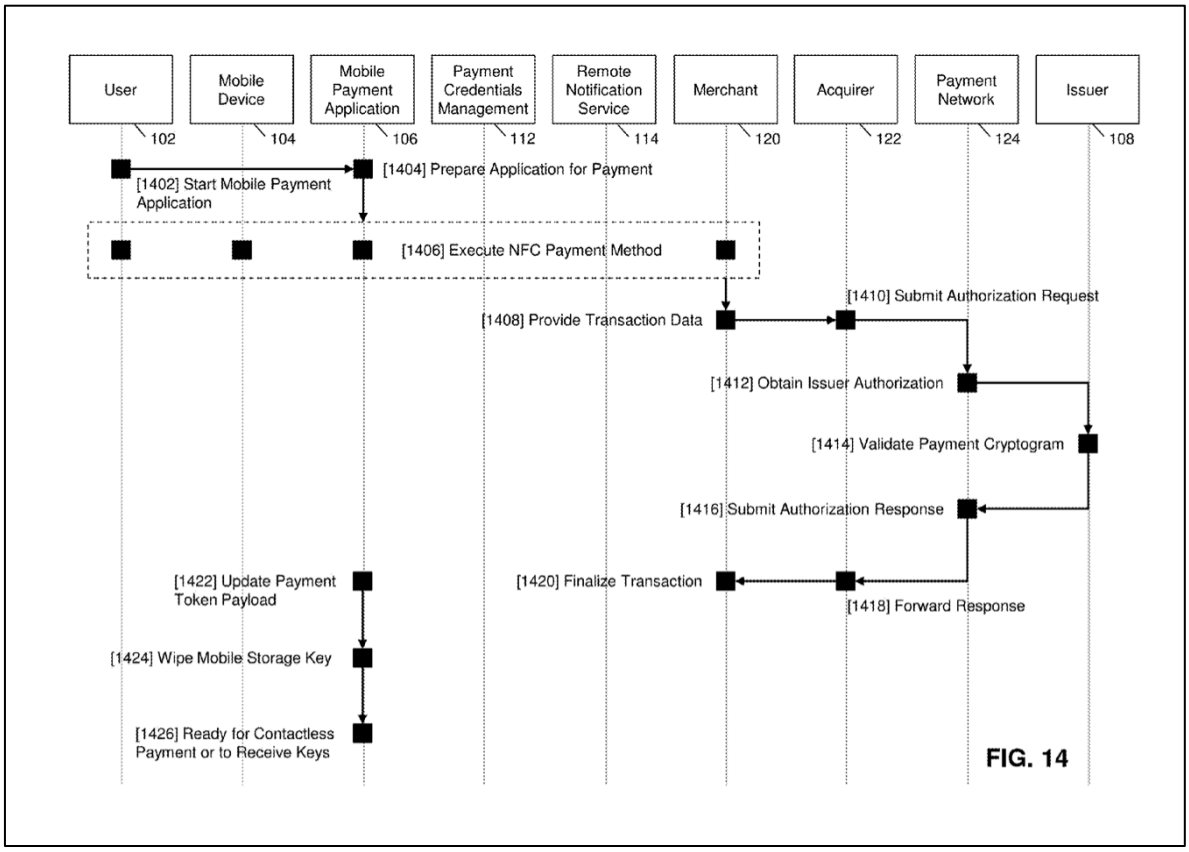
Further, each of the applied prior art references is reasonably pertinent to problems addressed by the '579 Patent such as increasing security of payment transactions or providing secure access to mobile applications through specific user interactions with a user interface. *Compare '579 Patent,* 1:23-27, 1:62-2:3, 9:9-9:15, 11:34-42, 15:14-24 *with Collinge*, [0003]-[0005]; *Dec.*, ¶¶78-80; *Phillips*, [0006], [0012]-[0014], [0027]-[0029]; *Dec.*, ¶¶101-102; *Smith*, [0002], [0015], [0020]; *Dec.*, ¶¶95-96; *Lin*, 27:26-28:15; *Dec.*, ¶¶91-92; *Dec.*, ¶¶105-106; *Kranzley*, [0003], [0065]; *Dec.*, ¶¶98-99; *Aabye*, Abstract, [0002]-[0010]; *Dec.*, ¶¶106-107; *Pisula*, 28:57-64; 14:23-25, Fig. 1A, Fig. 2; *Dec.*, ¶113; *Fadell*, [0004], [0054], [0064]; *Dec.*, ¶¶112-113. Therefore, each of the applied prior art references is analogous art to the '579 Patent.

V. GROUND 1: COLLINGE IN VIEW OF LIN AND PHILLIPS

1. 1(Pre): "A method of performing a transaction, the method comprising:"

To the extent the preamble is limiting, Collinge teaches "a *method*[6] for conducting a *payment transaction*" using a mobile device 104. *Collinge*, [0029] (emphasis added).

[6] Claim language identified with *italics* and underline.



Collinge, Fig. 14.

Collinge teaches "generating and provisioning payment credentials to a mobile device" for "use in mobile payment transactions." *Collinge*, [0006]-[0007].

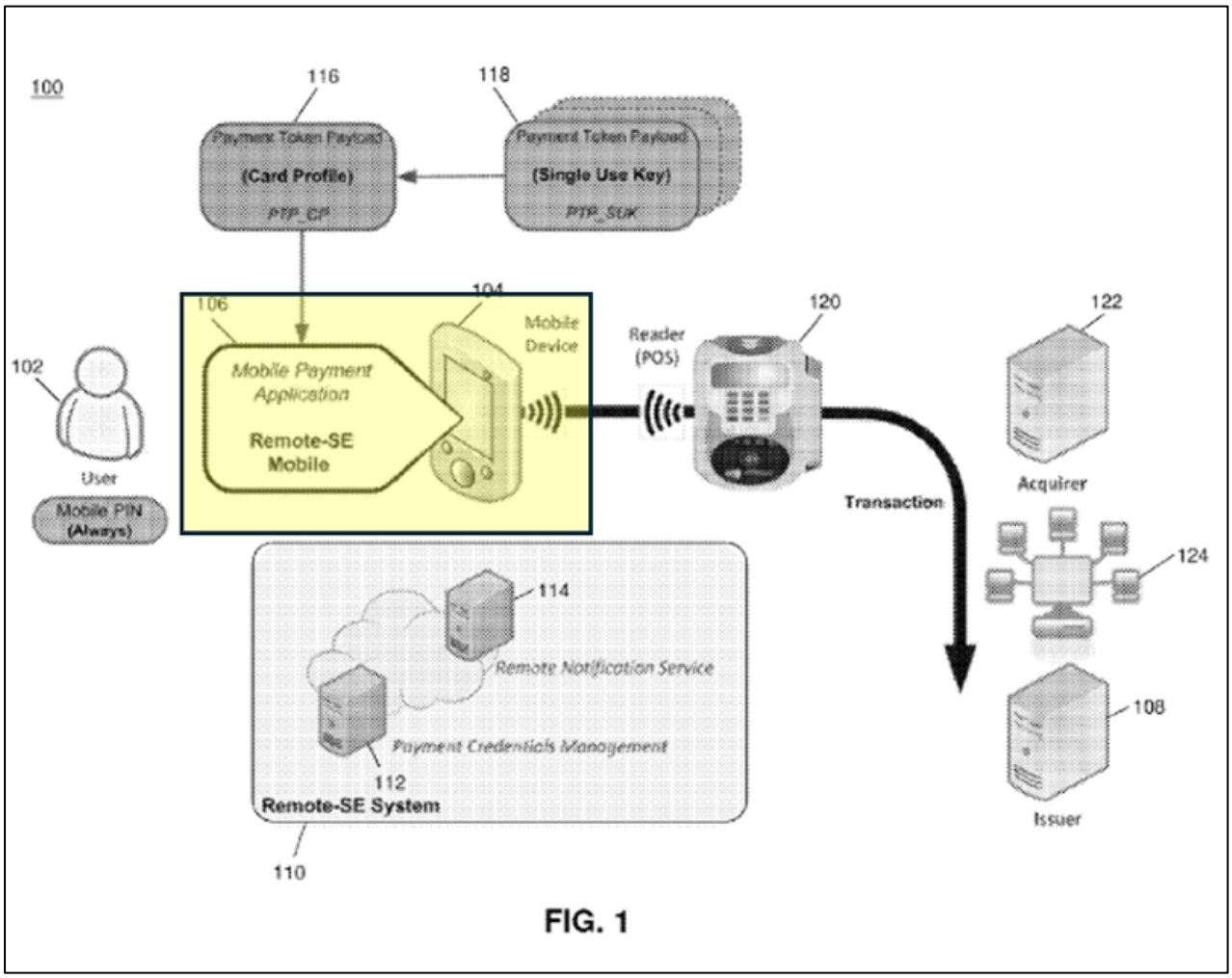


FIG. 1

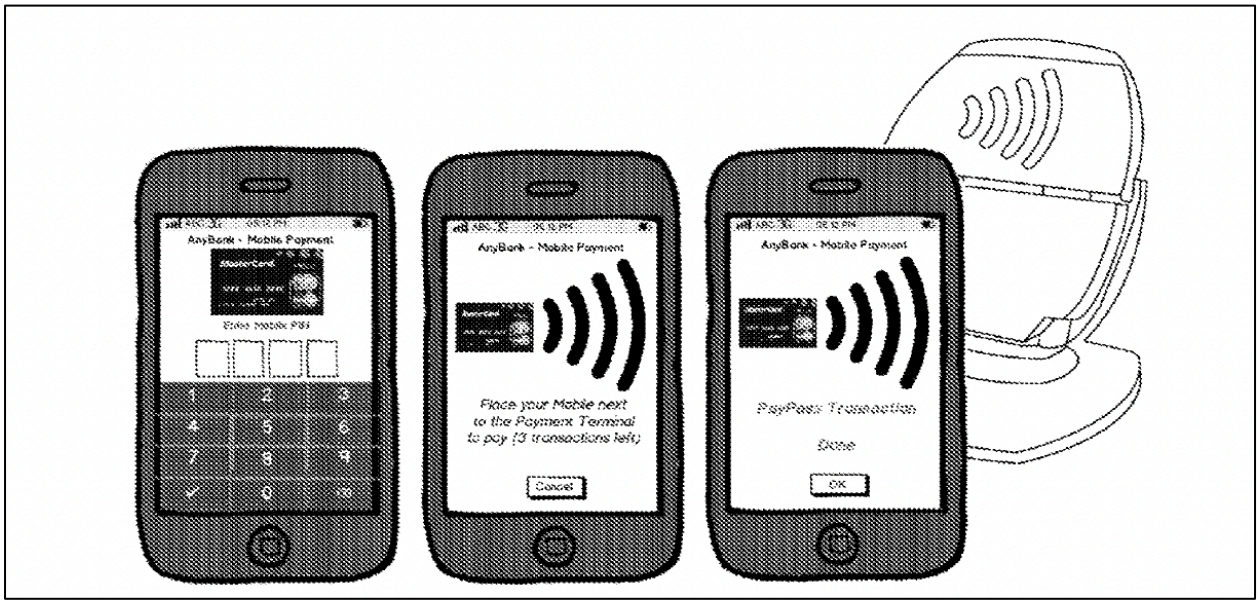
Collinge, Fig. 1. (annotated).

2. *1(a): "receiving an input at an electronic device, wherein the input corresponds to a priming operation of the electronic device by an identified user"*

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 the field of an NFC reader) of the electronic device by an *identified user* (an authenticated user). *Dec*., ¶¶120-128. The '579 Patent describes that "a user that has 'primed' the multi-

function electronic device 201b for a transaction has already performed a security authentication on the card…" Ex.1001, 11:34-36.

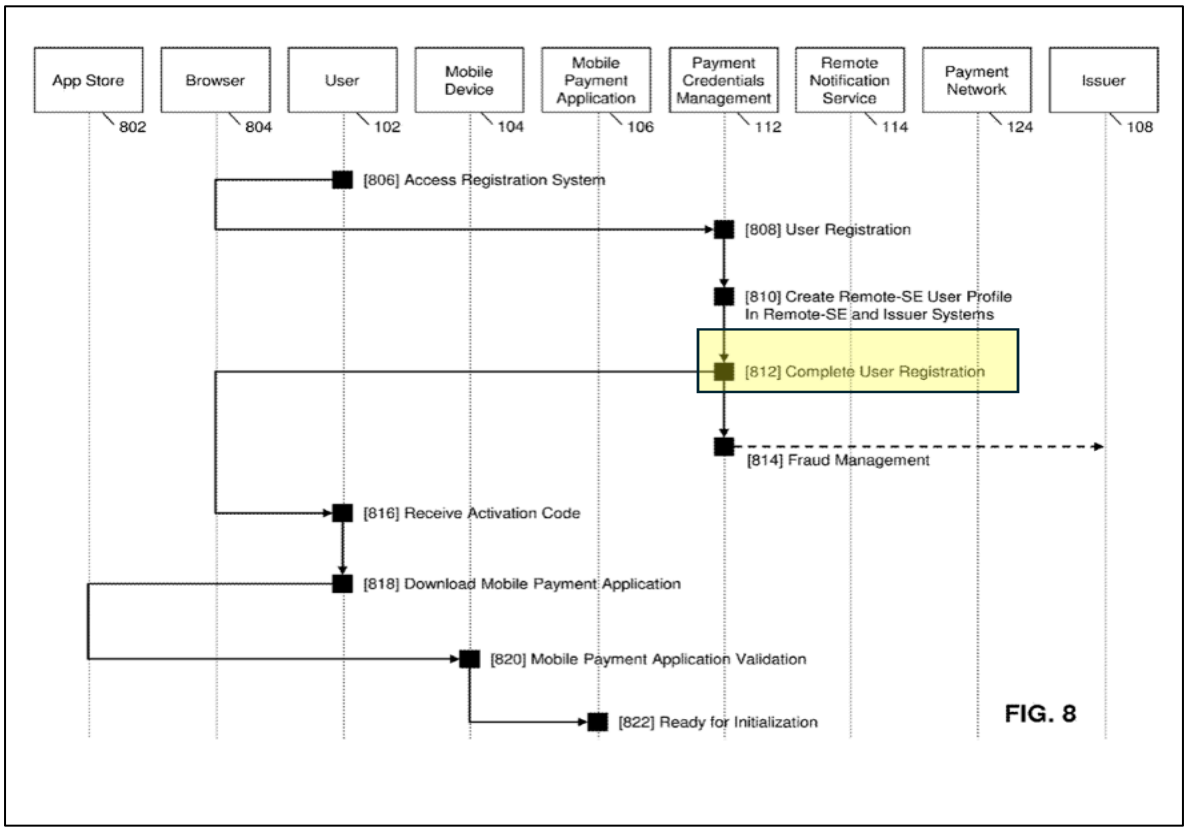
Collinge teaches that the touch screen of mobile device 104 receives a user's input of a "mobile personal identification number (PIN)" prior to generation of a payment cryptogram which is a *priming operation*. *Collinge*, [0094], [0128], [0133]. *Dec*., ¶¶126-128. Collinge teaches that user "must always provide the Mobile PIN for all PayPass transactions[.]" *'098 Provisional*, 99.



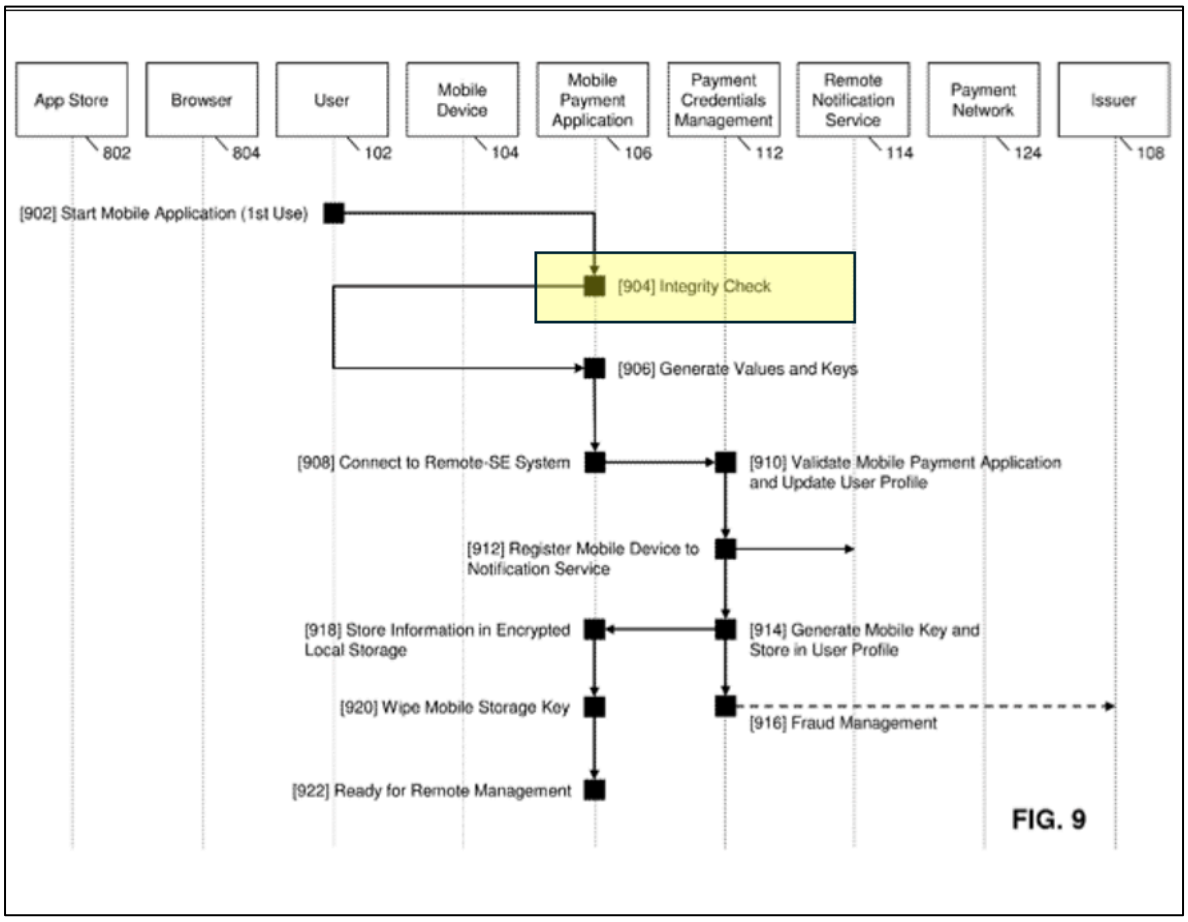
'098 Provisional, 99; *'248 Provisional*, Fig. 2B.

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").

As a further example of a priming operation, Collinge teaches that 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).

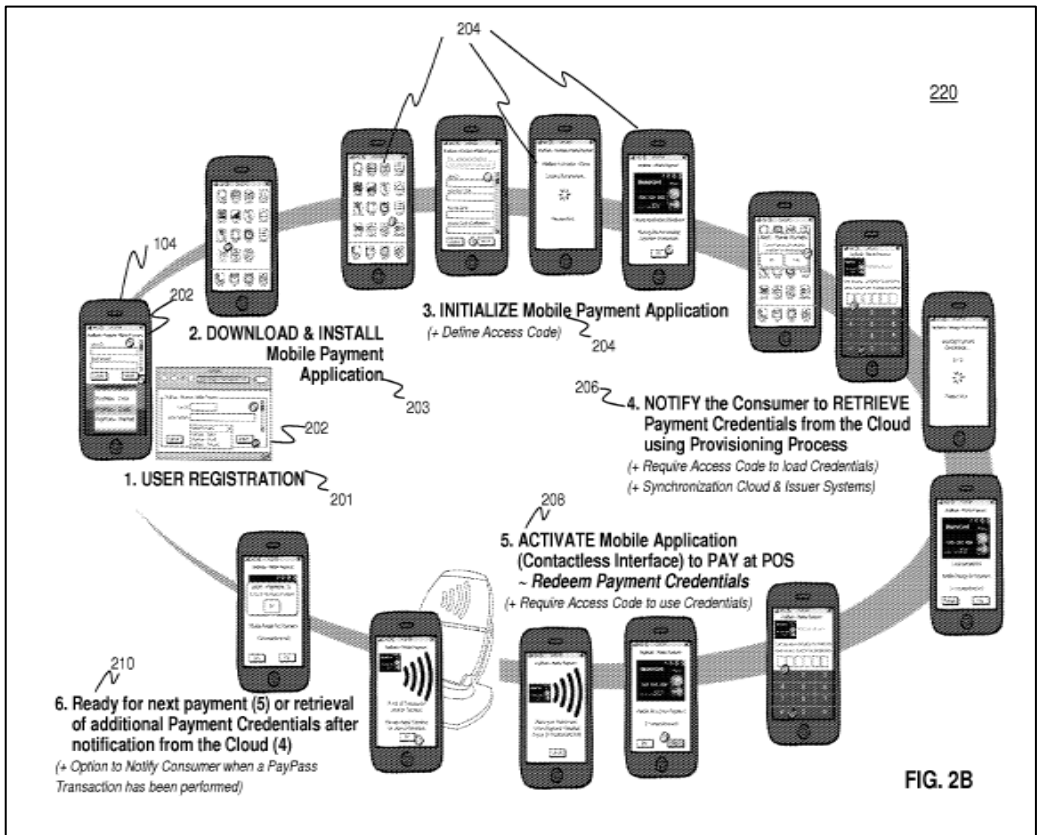


Collinge, Fig. 8. (annotated),



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*., ¶124.

Figure 2B (below) 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*. *Dec*., ¶125.



'248 Provisional, Fig. 2B.

3. 1(b): "and wherein the electronic device comprises a processor;"

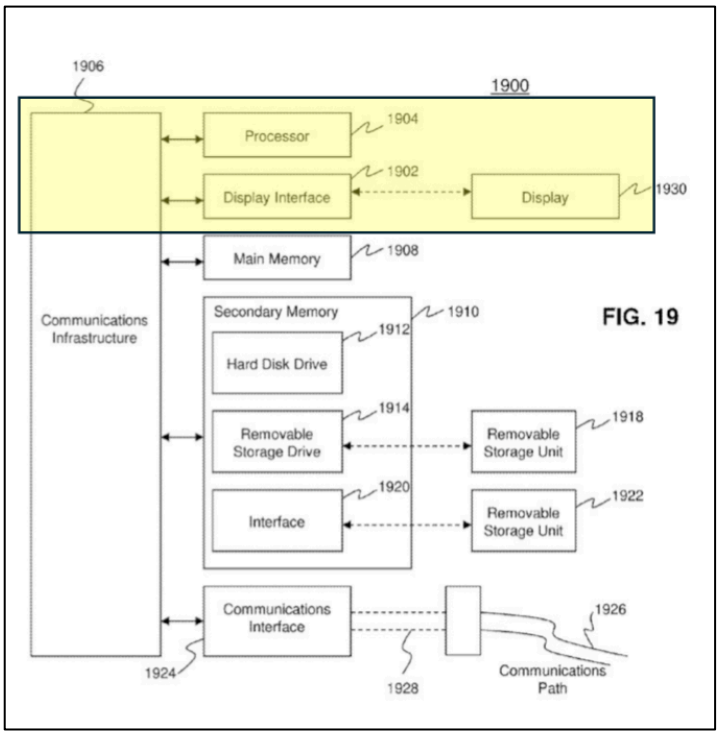
Collinge's mobile device includes "an application program stored in data storage of the mobile device" that is "executed by *a processor* included in the mobile device[.]" *Collinge*, [0041], [0147]. *Dec*., ¶129.

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

Collinge's mobile device 104 includes a "touch screen" display to receive user input. *Collinge*, [0133] (identifying the "touch screen" of "mobile device 104" as "an input device[.]").

Collinge teaches that "at least one processor device" is used to implement the payment system taught by Collinge. *Collinge,* [0147]. The touch screen of Collinge's mobile device 104 is *coupled to the processor* so that user input can be received and acted upon by mobile device 104. For example, the touch screen "receives a user's input of a "mobile personal identification number (PIN)" during generation of a payment cryptogram. *Collinge*, [0133]. 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 be coupled to a processor. *Collinge,* [0147], Fig. 16 (describing generation of a cryptogram by the processing device), *Dec.*, ¶¶130-139. It was well-known that touch screens of mobile devices allowed users to interact with the mobile device. *Dec.*, ¶138.

Collinge's display interface and display are "coupled" to the processor via the communication interface:



Collinge, Fig. 19 (annotated). Collinge teaches that the communications infrastructure may be a "bus, message queue, network, multi-core message-passing scheme, etc." Collinge, [0150]. Collinge teaches and a POSITA would have found it obvious that Collinge's mobile device 104 would be implemented as the computer system 1900. Dec., ¶¶133-139. 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]. Accordingly, Collinge teaches a display interface (the touchscreen) and display are coupled to a processor. Dec., ¶¶133-139.

5. 1(b)(2): "a near field communications (NFC) interface coupled to the processor;"

Collinge teaches a mobile device that include a *near field communications (NFC) interface*. *Collinge,* [0041] (Collinge's mobile device can "conduct payment transactions via *near field communication*[.]"). Per Collinge, a POSITA 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 '579 Patent, and a POSITA would have recognized that Collinge teaches that mobile device 104 has an NFC interface, and 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*., ¶¶140-143.

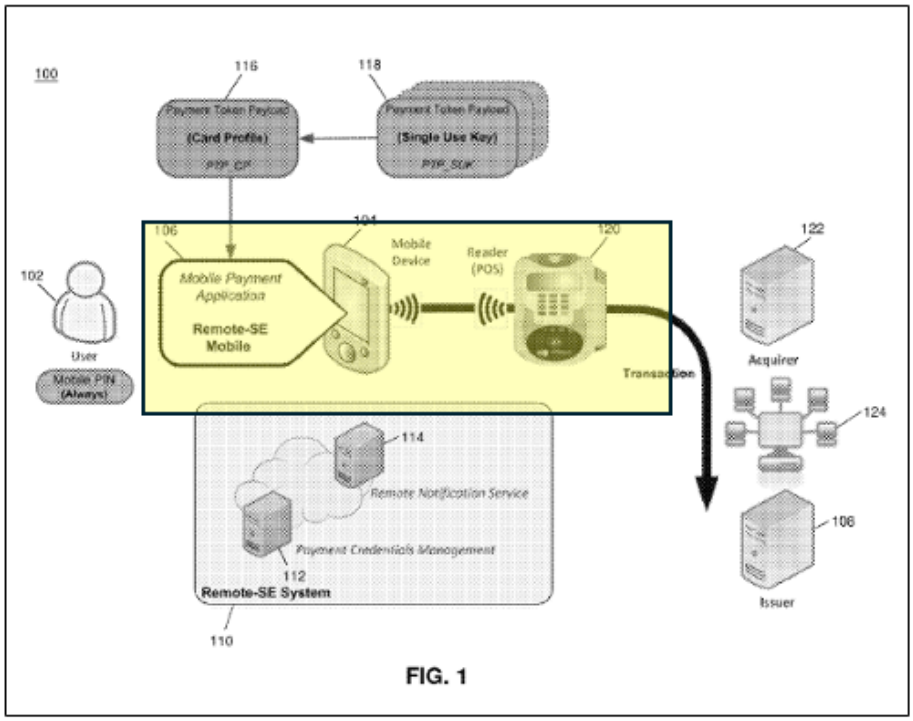
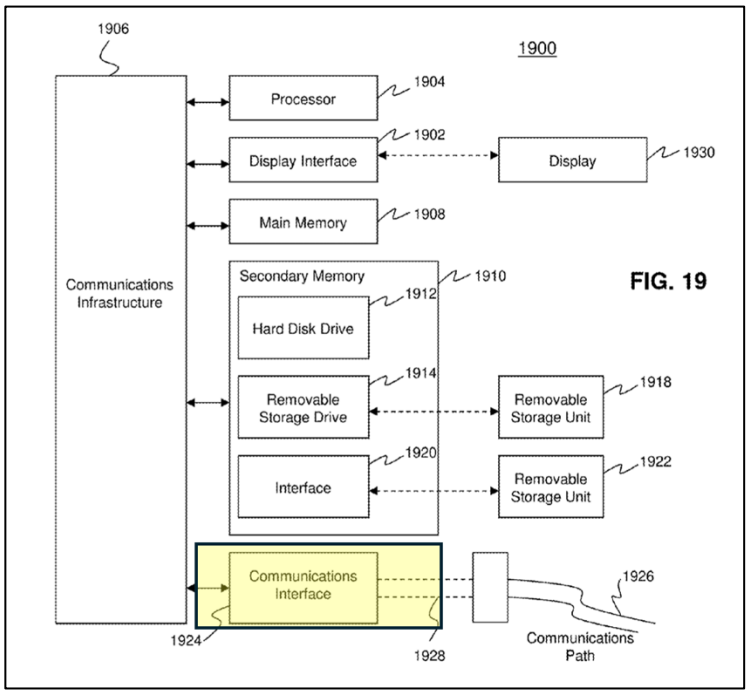


FIG. 1

Collinge, Fig. 1 (annotated excerpt).

Collinge further teaches that the near-field communication interface is *coupled to the processor*. Collinge teaches, and a POSITA would have understood, that to transmit payment information to a POS terminal via NFC in Collinge's mobile device, the NFC interface must be coupled to a processor of the mobile device. *Collinge,* [0135], [0147], Fig. 16, Fig. 19, *Dec.*, ¶144.

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



Collinge, Fig. 19 (annotated).

Further, a POSITA would have understood that Collinge's NFC interface (communications interface) is coupled to Collinge's processor through the communications infrastructure. *Dec.*, ¶145-147; *Collinge*, [0154] (a radio frequency link"). It was well known in the art that NFC uses electromagnetic signals, and specifically radio waves and magnetic fields to transmit data. *Dec.*, ¶147. Collinge teaches that the communications infrastructure may be a "bus, message queue, network, multi-core message-passing scheme, etc." *Collinge*, [0150].

6. 1(c): "receiving a request for a transaction payment at said electronic device via the NFC interface;"

Collinge, in view of Lin, teaches *receiving a request for a transaction payment* at Collinge's mobile device via Collinge's *NFC interface*.

(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 between the mobile device and a POS terminal. *Collinge,* [0135] ("payment credentials and the generated payment cryptogram may be transmitted, via near field communication, to a point-of-sale terminal…for use in a financial transaction.").

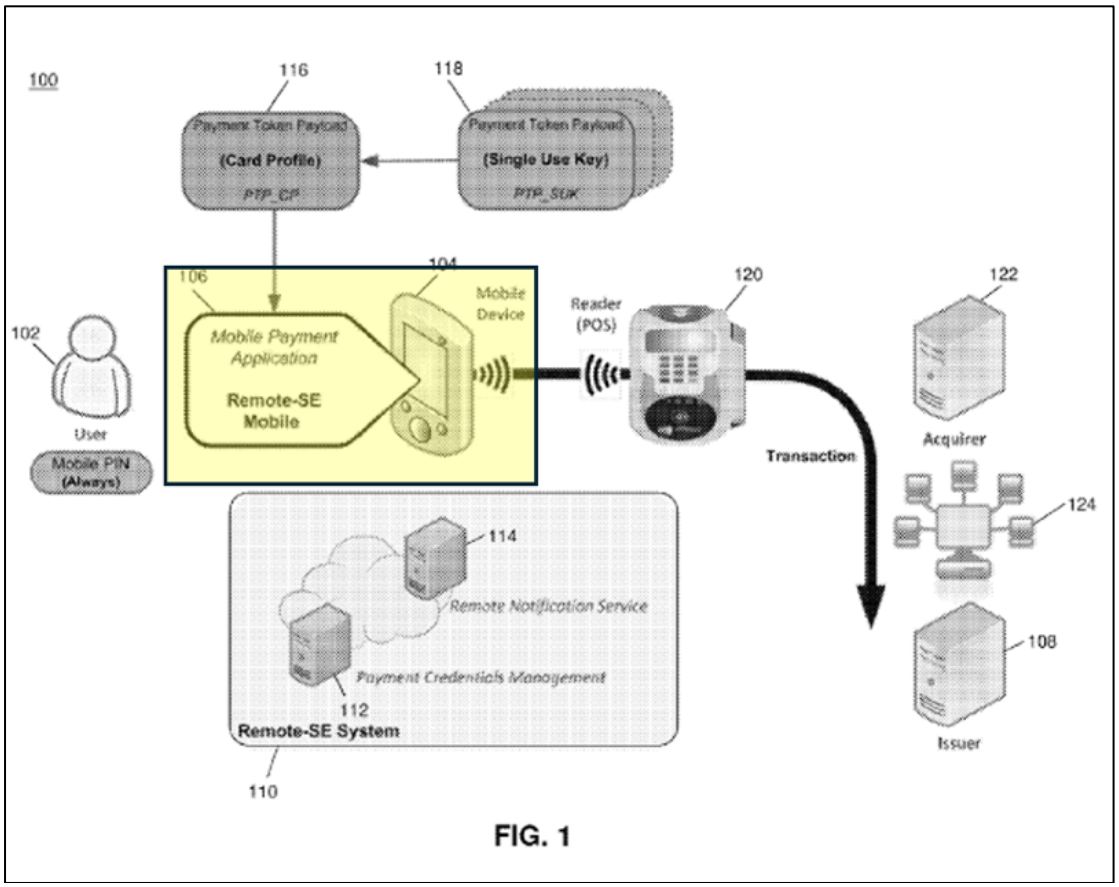
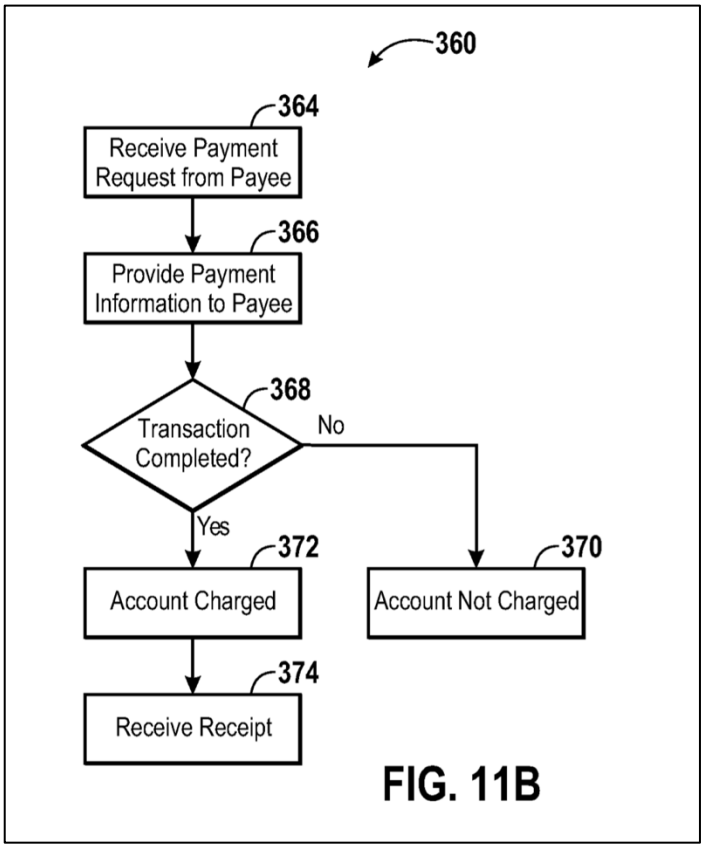


FIG. 1

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.* 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.*, ¶151. 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. *Id.* A POSITA would have recognized that this method allows the point of sale terminal greater control over the payment session, making it easier to enforce security measures, including session timeout. *Id.* A POSITA would have further recognized that 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. *Id., 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.*, ¶151.

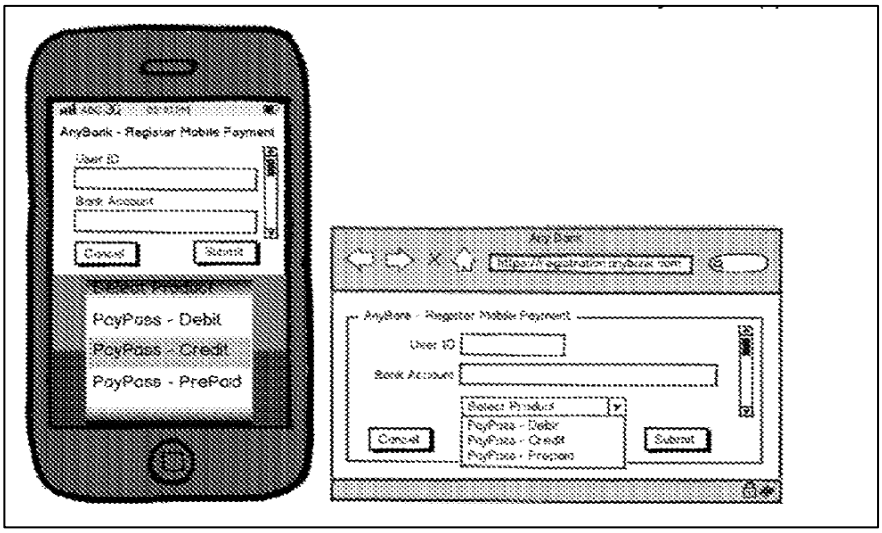
7. 1(d): "displaying, on the touch-screen display, images of: a card issuer payment method selection, including a last 4-digit partial

number of a card issuer supplied account number of a payment card; a card logo; and other iconography of the payment card;"

Collinge teaches a user may select from issuer-provided payment methods displayed on the *touch-screen display* of Collinge's mobile device to complete a payment transaction (a *card issuer payment method selection*). *Collinge*, [0038], *'098 Provisional*, 96, 100. In related art, Phillips provides further detail on what information to display to a user making a payment method selection.

(a) Collinge's Teachings

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-B.

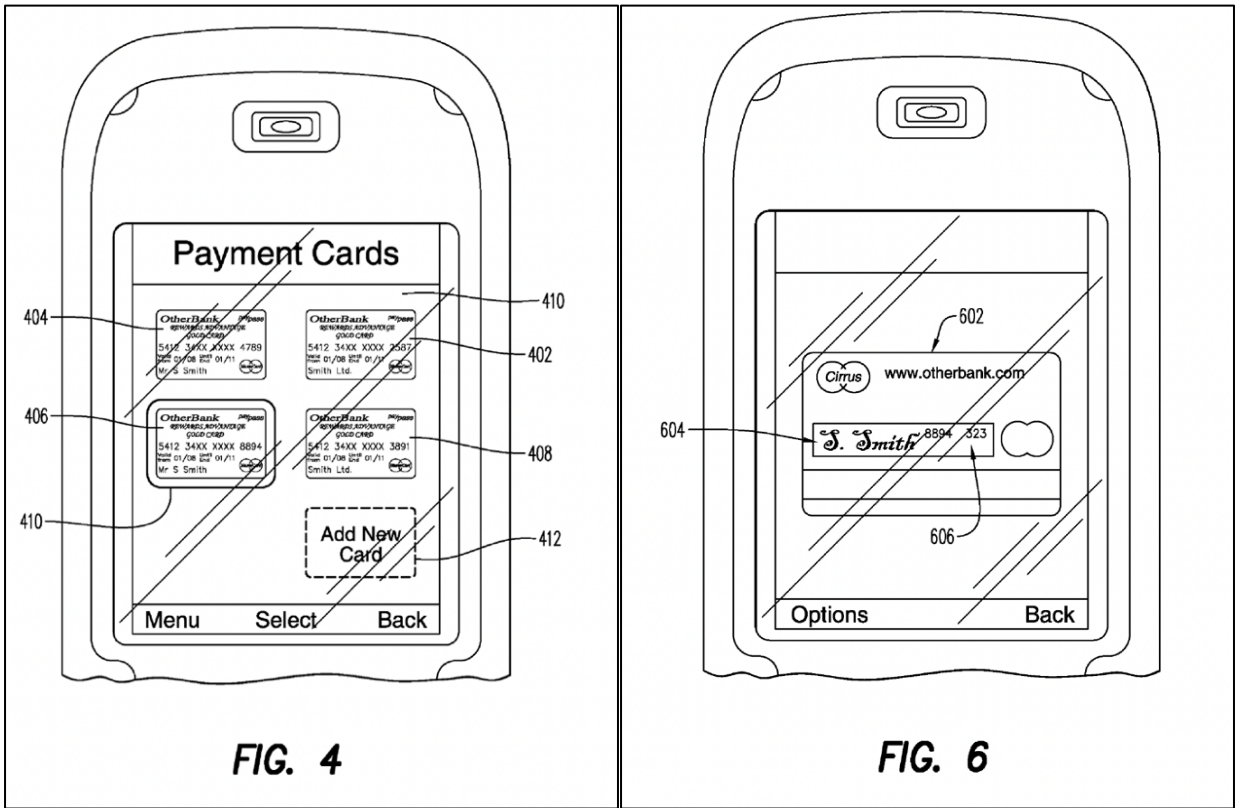
Collinge further teaches displaying on Collinge's mobile device touch screen a payment card image including a logo and other card iconography:



'098 Provisional, 100; *'248 Provisional*, Fig. 2B. Collinge teaches that the card logo (e.g., MasterCard) is displayed when the user chooses a payment method for the transaction, prior to the user selecting "pay" to complete the transaction. *Id.* Accordingly, Collinge teaches a *card issuer payment method selection* including a *card logo*. Collinge provides limited detail on how different payment methods are displayed to the user, including where the user has multiple credit and debit cards available for use. As also shown above Collinge teaches the user may select "pay" during a transaction (approval authorization). *Dec.,* ¶155.

(b) Phillips' Teachings

In related art, Phillips teaches a mobile phone, usable for contactless payment transactions, that includes a "virtual wallet" application. *Phillips,* [0027]. The virtual wallet displays "small images of identification cards (e.g., payment cards such as debit or credit cards)" that a user may select from to make a payment using their mobile phone and a proximity reader, as shown in Fig. 4. *Phillips,* [0012], [0029]. Phillips shows *a card logo* and *other iconography of the payment card* on the display:

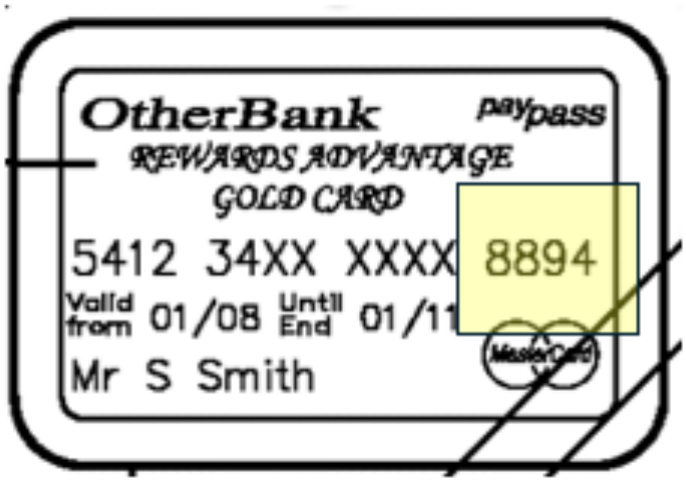


Phillips, Figs. 4, 6.

Phillips further teaches that the user interface includes a "flip card" function that causes the back of a payment card to be shown, as depicted in Fig. 6. *Phillips*,

[0047]. The back of the payment card includes "the user's signature 604 and a security code (CVC2) 606." *Phillips*, [0049].

In Fig. 4, Phillips shows that the last four digits of the payment card are shown, though other digits may be obscured:



Phillips, Fig. 4 (annotated excerpt). Phillips therefore teaches displaying card issuer supplied payment information including a *last 4-digit partial number,* an expiration date, and a CVC value in addition to a *card logo* and *other iconography* as part of a *card issuer payment method selection*. *Dec.,* ¶158. Notably, Phillips (like Collinge) is assigned to MasterCard, references MasterCard's PayPass system, and it shares an inventor with the Collinge Provisionals (Simon Phillips).

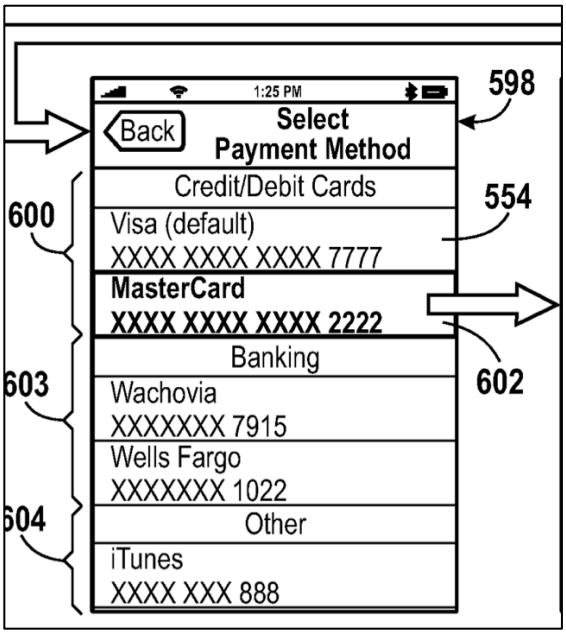
(c) Motivation to Combine

It would have been obvious, and a POSITA would have been motivated to configure Collinge's mobile payment application to display images of payment cards including the card logo, iconography, partial payment number, and other card issuer provided payment information (such as a CVC) as taught by Phillips. *Dec.*, ¶159. A POSITA would have understood that such a combination would have predictably allowed a user to easily select between multiple credit or debit card payment methods to compete a transaction and allowed the user to more easily distinguish between the payment methods available. *Id*. A POSITA would have understood the value of presenting the payment method options in a visual format that the user would already have been familiar with, i.e., akin to how the user already views an equivalent physical card in a physical wallet. *Dec.*, ¶159-161. A POSITA would have further understood, and Collinge already teaches, showing the user an image of the selected card, a "check" for the user that they are using the intended payment method, decreasing the risk of user error. *Dec.*, ¶160; *'098 Provisional, 100; '248 Provisional*, Fig. 2B. Collinge does not detail how the user interface of Collinge's mobile application would show multiple available cards. In deciding how to implement a user interface a POSITA would have considered other MasterCard PayPass art—including Phillips. A POSITA would have had a reasonable expectation of success in making such a modification, including because Collinge already teaches displaying an image of the payment method. *Dec*., ¶161.

(d) Lin's Teachings

To the extent that the limitation *including a last 4-digit partial number of a card issuer supplied account number* requires showing only the last 4-digits of the payment number, it would have been obvious to show only the last 4-digits of the payment account number on the payment selection screen of Collinge's modified mobile payment application as taught by Lin.

Lin teaches a payment method selection page that displays only last 4-digit partial number of a card issuer supplied account number of a payment card.



Lin, Fig. 14E (excerpt).

It would have been obvious, and a POSITA would have been motivated to configure Collinge's mobile payment application to display only the last 4-digit partial number of a card account number (as taught by Lin) for increased security.

Dec., ¶163. A POSITA would have understood that the last four digits of a credit card were commonly used to distinguish one payment card from another, including in mobile wallets. *Dec.*, ¶163. Accordingly, a POSITA would have been motivated, based on Lin's teachings and their understanding of the art to include the last four digits of each payment method on the payment selection screen of Collinge's touch screen display to achieve the predictable result of allowing a user to distinguish between multiple cards available for payment while maintaining the security of the complete account number. *Dec.*, ¶164. Collinge in view of Lin teaches displaying a plurality of payment options including debit, credit, or prepaid and receiving a user-selection of a payment method for a transaction via said touch-screen display user-interface. *Dec.*, ¶164.

A POSITA would have had a reasonable expectation of success in making such a modification based on Lin's teachings, Phillips' recognition that there is value in obscuring a portion of the payment number, and the POSITA's understanding of the last four digits of a payment method are typically used to distinguish between payment methods. Dec., ¶165. Accordingly, the proposed combination is an application of a known technique (using the last four digits to identify a payment card) to improve a similar product (Collinge's payment system) in the same way. *Dec.*, ¶165.

8. 1(e): "generating, by the processor, a limited-use payment information, and using said limited-use payment information in place of said card issuer supplied payment information;"

The processor of Collinge's mobile device dynamically *generat[es]* a payment cryptogram *(limited-use payment information)* which is used in place of said card issuer supplied payment information (i.e. the CVC associated with the card issuer payment method selected).

Collinge's mobile payment application is "stored in data storage of the mobile device 104 and **executed by a processor** included in the mobile device 104." *Collinge*, [0041]. *Dec.,* ¶¶166.;173 The processor executing the mobile payment application of Collinge's mobile device generates a **payment cryptogram** which "may be, for example, an application cryptogram or a dynamic card validation code (CVC3)." *Collinge,* [0077]; *Dec.,* ¶¶166-173. It was well-known at the time that an application cryptogram and CVC3 are dynamically generated alternatives to the static card issuer CVC found on the back of a traditional payment card. *Dec.,* ¶172; (discussing Bona and Kranzley).

Collinge's payment cryptogram is "valid for a single financial transaction[,]" therefore it is *limited-use payment information*. *Collinge*, [Abstract], [0128], Fig. 16. Collinge's payment cryptogram is dynamically generated by the processor of Collinge's mobile phone 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 payment cryptogram such as a CVC3 based on at least Collinge's processor cryptographically combining: "the supplied CVC3 value, the session key unpredictable number [(KS_{UN})], the application transaction counter, and the reader unpredictable number." *Collinge*, [0145].

Collinge teaches providing complete payment information (including payment credentials + the generated payment cryptogram) which is likewise *limited-use payment information* because it includes the limited use payment cryptogram. *Collinge,* Fig. 16, [0070] (recognizing that methods for transmitting payment credentials and a payment cryptogram to a point-of-sale terminal are apparent to POSITAs). Collinge's complete payment information is likewise used in place of the card issuer supplied payment information (e.g., complete payment credentials including a PAN+CVC). *Dec.,* ¶¶174-175.

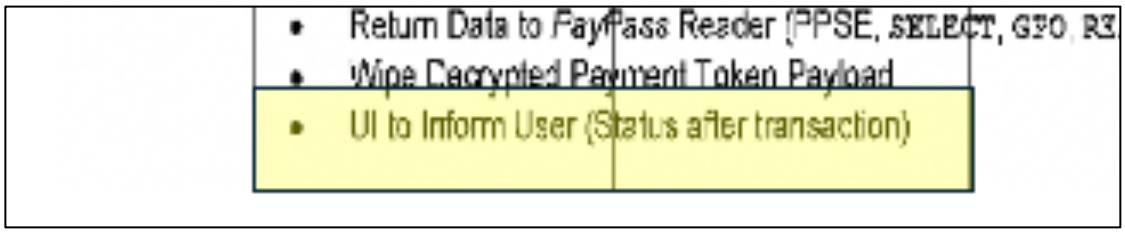
9. 1(f): "transmitting said limited-use payment information from said electronic device to an NFC recipient of the transaction via said NFC interface; and"

Collinge's mobile device transmits payment credentials and the generated payment cryptogram (*limited-use payment information*) via an *NFC interface* to a point of sale terminal (*NFC recipient*).

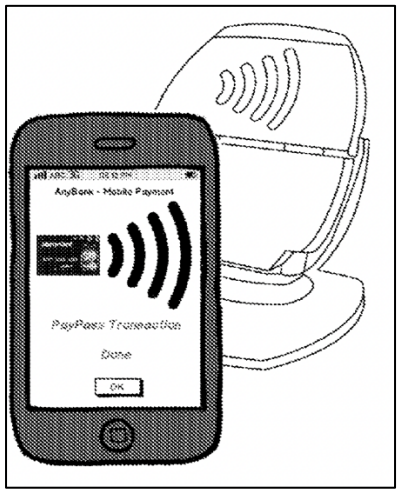
Collinge's "mobile device 104 may conduct a **contactless/NFC payment transaction** using the mobile payment application 106[.]" *Collinge,* [0070] (emphasis added). Collinge's mobile device transmits "the generated cryptogram and payment credentials to a point-of-sale terminal 120…via NFC." *Collinge,* [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.").

10. 1(g): "visually conveying a status of said transaction via a user-interface displayed on said touch-screen display."

Collinge teaches visually conveying a status of said transaction via a user-interface displayed on said touch-screen display by "notifying the user 113 when a PayPass® transaction has been performed." *'248 Provisional*, [0074], [0195] ("[a]s shown in Figure 14, a UI element of the GUI 202 can be used to inform the user 113 of the **status after the transaction**.") (emphasis added); *Collinge,* [0122]; [0010] ("mobile payment application 106 may also update a status to indicate…that the mobile payment application 106 is ready to conduct a payment transaction").. *Dec*., ¶¶177-180.



'248 Provisional, Fig. 14 (excerpt).



'098 Provisional, 99 (excerpt);*'248 Provisional*, Fig. 2B.

11. **Claim 2:**[7]

Collinge teaches wherein the generating the payment cryptogram (*limited-use payment information*) utilizes at least one information from a set of information comprising: ATC (a device transaction sequence counter)… and a PIN (*a user identification entry*).

[7] *See* Claim Listing Appendix.

Collinge's mobile device touch screen receives a user's input of a "mobile personal identification number (PIN)" during generation of a payment cryptogram. *Collinge*, [0133].

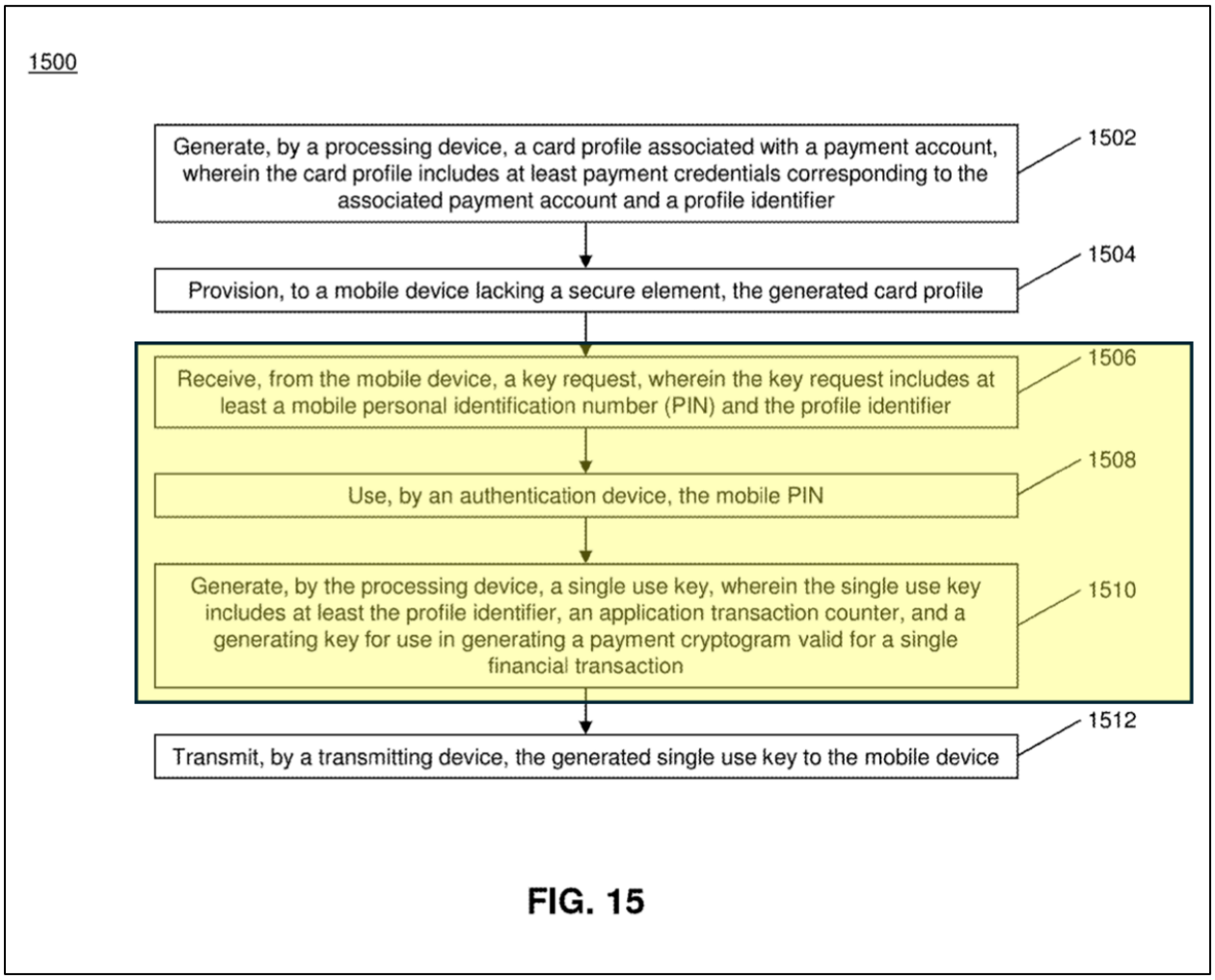


FIG. 15

Collinge, Fig. 15. (annotated). A single use key is generated in the cloud system and includes several elements used for "generating a payment cryptogram valid for a single financial transaction." *Collinge*, [0128]. The single use key "118 may be genuine if the mobile PIN is successfully authenticated in step 1508, and fake if the mobile PIN is unsuccessfully authenticated." *Collinge*, [0128]. The "mobile

payment application 106 may then generate a payment cryptogram using the generating key included in the single use key 118." *Collinge*, [0077].

Collinge teaches an application transaction counter (ATC) (*device transaction sequence count*) which is a "count of transactions used for fraud management and authentication[.]" *Collinge,* [0050]. A POSITA would have understood that Collinge's ATC corresponds to the claimed "*device transaction sequence counter*" and is updated each transaction. *Dec.,* ¶183.

Collinge's ATC is provisioned from the cloud system. The cloud system "identif[es] 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.,* ¶184.

12. Claim 3:

See Claim 1(e) and 2. Collinge further teaches *payment issuer secrets*. The issuer 108 validates the generated payment cryptogram. *Collinge,* [0141]. Specifically, the issuer received "at least the K_{SUN}, UN_{CLOUD}, and application transaction counter" (*secrets*) and the issuer 108 uses that information "in validating the generated CVC3 value used in the financial transaction." *Collinge*, [0141]. *Dec.,*

¶¶185-189. Collinge teaches generating a CVC3 based on the following values: "the supplied CVC3 value, the session key unpredictable number, the application transaction counter, and the reader unpredictable number." *Collinge*, [0145]. Additionally, Collinge teaches that the CVC3 payment cryptogram is generated using the single use key 118 that is "used one time to generate a payment cryptogram to be used in a payment transaction." *Collinge,* [0050]. The single use key in shared with issuer 108. *Collinge,* [0128] ("…method 1500 may further include transmitting the generated single use key 118 to an issuer associated with the payment account). Single use key 118 is *secret information* because a user must input a valid PIN in order for a genuine single use key 118 to be generated, indicating that secret use key 118 is secret to anyone who does not have the valid PIN. *Collinge*, [0128]. *Dec.,* ¶¶185-189.

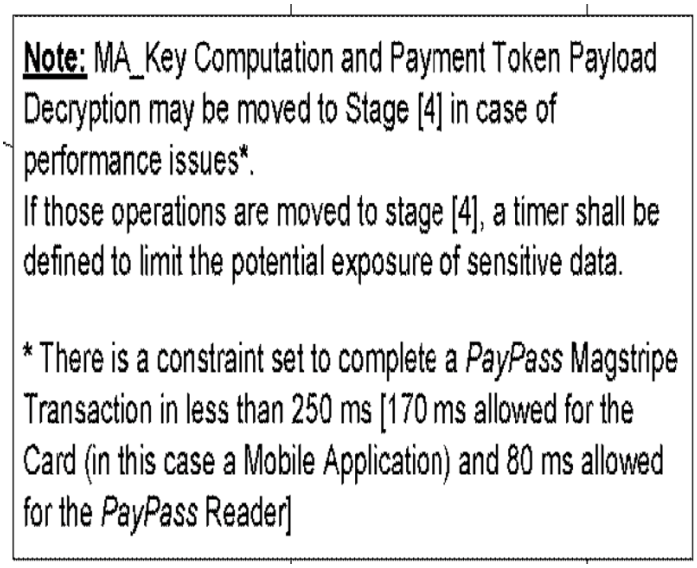
13. Claim 7:

Collinge's mobile *device touch screen* receives a user's input of a "mobile personal identification number (PIN)" that corresponds to a priming operation. *Collinge*, [0065], [0092]-[0093], [0133] ("an input device (e.g., of the mobile device 104, such as a **touch screen**) may receive a mobile personal identification number (PIN) input by a user…") (emphasis added). *See* Claim 1(a).

14. Claim 10:

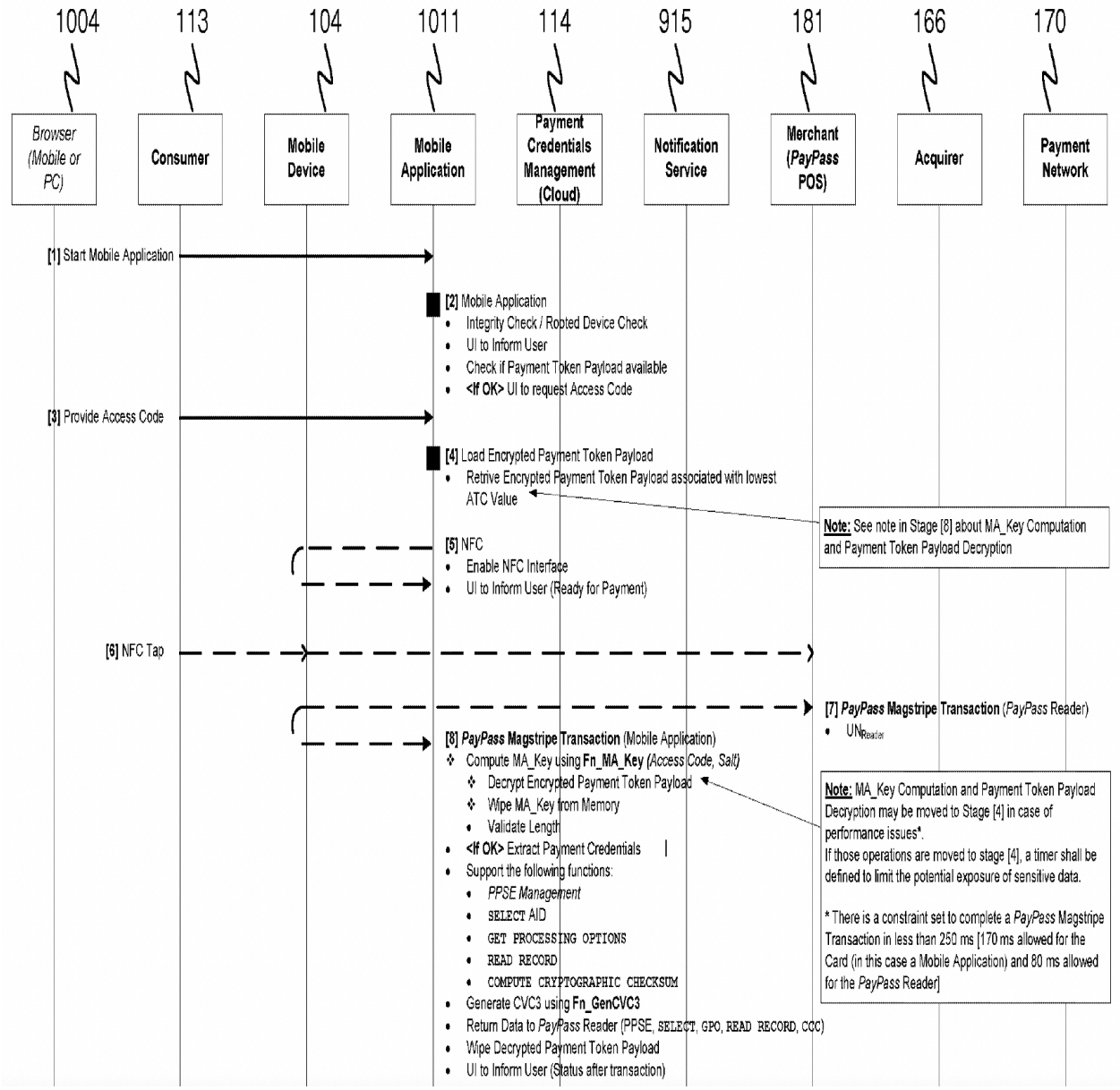
Collinge teaches activating an NFC communication *for a limited duration of time responsive to the electronic device priming* (e.g., providing an access code) and, *responsive to the preset duration being exceeded, terminating the NFC communications and aborting the transaction.*

Collinge teaches setting a time constraint for completing a PayPass transaction with the Mobile Application of "less than 250 ms [170 ms allowed for the Card (in this case a Mobile Application) and 80 ms allowed for the PayPass Reader]" *'248 Provisional*, Fig. 14.



Id., Fig. 14 (excerpt). Note while the cited figure refers to a "PayPass Magstripe Transaction" (Mobile Application), it describes a transaction that occurs via NFC, not a magnetic stripe. *'248 Provisional*, [0189], Fig. 14 (Stage [5] Enable "NFC interface"; Stage [6] "NFC Tap"). *Dec.*, ¶192.

Collinge additionally teaches if certain operations included in the [8] PayPass Magstripe Transaction are instead performed when the Payment Token Payload is loaded to the mobile application, then for that step, too, "a timer can be defined to limit the potential exposure of sensitive data." *'248 Provisional*, Fig. 14, [0197].



'248 Provisional, Fig. 14. (excerpt).

Accordingly, Collinge teaches a valid user inputting the activation code (*priming action*) enables Collinge's mobile device for imminent performance of a payment operation. *Dec*., ¶194.

15. Claim 11:

Collinge in view of Phillips teaches *completing the transaction on the electronic device*, including receiving an authorization input ("pay," PIN, passcode) and in response to *the transaction interval exceeding a pre-set time duration*, presenting the user with selectable options of *inputting an approval authorization* and *inputting a transaction denial*.

(a) Collinge's Teachings

Collinge teaches *completing a transaction* on the mobile device if the payment transaction is approved "based on funds or credits in the payment account[.]" *Collinge*, [0045].

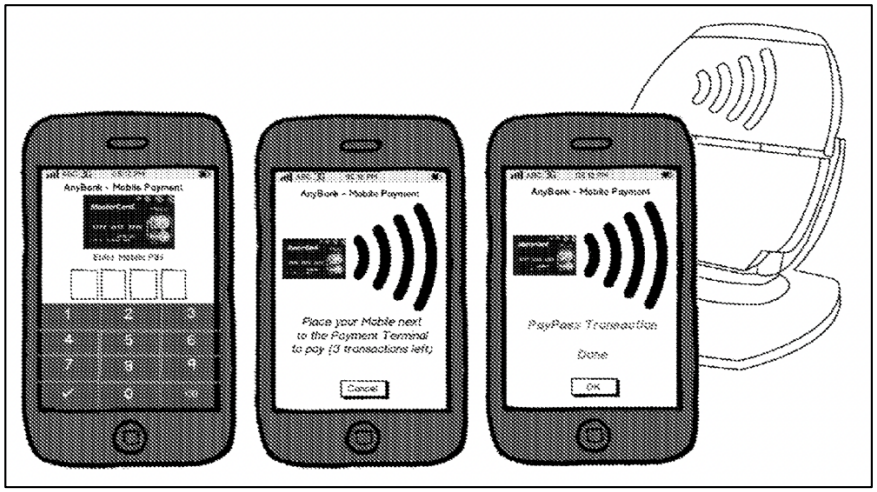
Collinge further teaches the user must input their PIN and then place the mobile device next to the payment terminal. Once the user places their mobile device next to the payment terminal, the NFC transaction must complete within 170ms. *'248 Provisional*, Fig. 14. *See* Claim 10. Collinge does not provide detail on what screen is shown next to the user in the event the transaction times out or exceeds the available funds. As discussed in Claim 10, Collinge teaches setting a time constrain

for completing a PayPass transaction with the Mobile Application of "less than 250 ms [170 ms allowed for the Card (in this case a Mobile Application) and 80 ms allowed for the PayPass Reader]" *'248 Provisional*, Fig. 14.

Note: MA_Key Computation and Payment Token Payload Decryption may be moved to Stage [4] in case of performance issues*.
If those operations are moved to stage [4], a timer shall be defined to limit the potential exposure of sensitive data.

* There is a constraint set to complete a *PayPass* Magstripe Transaction in less than 250 ms [170 ms allowed for the Card (in this case a Mobile Application) and 80 ms allowed for the *PayPass* Reader]

'248 Provisional, Fig. 14. (excerpt). Collinge does not provide detail on what screen is shown next to the user in the event the transaction times out or exceeds the available funds.



'098 Provisional, 99; *'248 Provisional*, Fig. 2B. Collinge also teaches the user may select the option to "pay."



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

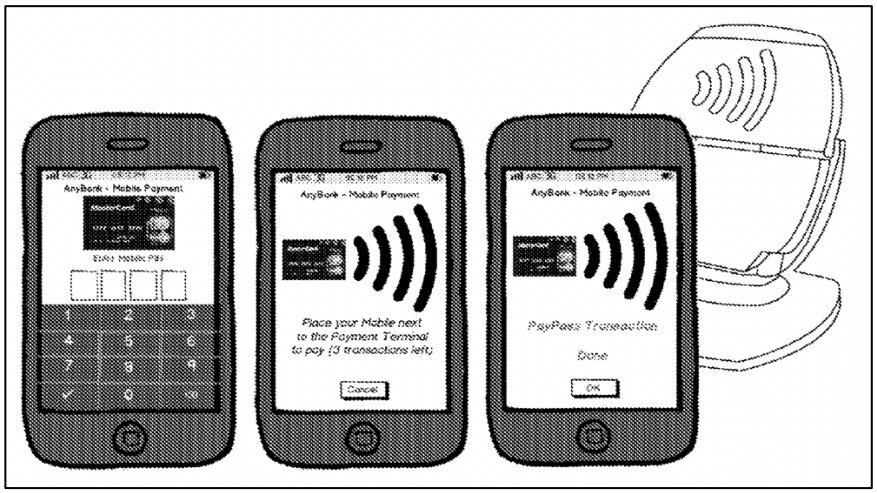
(b) Phillips' Teachings

Phillips teaches "the mobile phone 100 may be programmed such that entry of the user's PIN into the mobile phone is effective only for a limited period of time (say, a few minutes or less). Once the period times-out, the user may be required to enter the PIN into the phone again to enable the next transaction that is over the no-signature-required limit." *Phillips*, [0066].

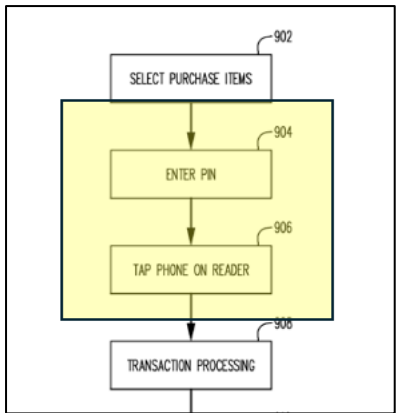
(c) Motivation to Combine

A POSITA would have been motivated to modify Collinge's mobile payment application to require a PIN to be re-input after a transaction is unable to complete

due to timing out or insufficient funds, as taught by Phillips. *Dec*., ¶198. After the PIN is entered, the user would be able to cancel the payment transaction or retry by placing the mobile device in the NFC field again. *Dec*., ¶198.



'098 Provisional, 99; *'248 Provisional*, Fig. 2B. A POSITA would have appreciated Phillips and Collinge both teach inputting a PIN just before the user taps the phone on the reader. *'098 Provisional*, 99; *Phillips*, Fig. 9.



Phillips, Fig. 9 (annotated excerpt).

It was well understood credit cards will decline when a credit limit is reached, but a user may still need to complete their payment, for example, because the service

being paid for has already been completed. Dec., ¶198. It was well known if a payment method fails the user may want to retry, decline, or go through with a transaction. Dec., ¶198. A POSITA would have appreciated such a modification would increase transaction speed instead of making the user go back to the first step one to complete a transaction, causing the user delay and potential embarrassment and a POSITA would have had a reasonable expectation of success in making this modification and would have appreciated that applying Phillips' known technique to improve a similar device (Collinge's mobile device and payment application) in the same way—allowing the user to retry or decline a transaction by re-entering their PIN after an initial failure—with predictable results including increased user convenience. Dec., ¶198.

16. Claim 12(a):

See Claims 1(a), (d).

17. Claim 12(b):

(a) Phillips' Teachings

Phillips teaches once "the user has previously selected a particular payment card account in the mobile phone 100" they have "established a default payment card account number to be used for purchase transactions except when another payment card account number has been selected." *Phillips*, [0060].

(b) Motivation to Combine

It would have been obvious and a POSITA would have been motivated to modify Collinge's mobile payment application to include a default payment method as taught by Phillips. *Dec*., ¶202. Providing a default payment method would have advantageously decreased the time it takes for a user to make a payment by allowing the user to skim payment selection steps, and a POSITA would have understood many users have one card they use considerably more often than other cards. Further, a POSITA would have appreciated in the combination, the user is still given a choice of payment methods, if they prefer not to use their default method. Accordingly, this modification of Collinge would have increased the speed with which a user of Collinge's mobile device can make a payment and a POSITA would have had a reasonable expectation of success in making such a modification to predictably increase user convenience. *Dec*., ¶202.

18. Claim 19(Pre):

See Claim 1(Pre).

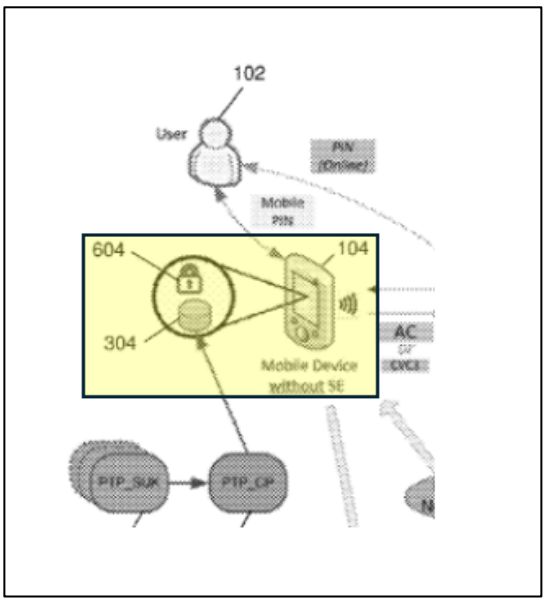
19. Claim 19(a):

See Claim 1(b).

20. Claim 19(b):

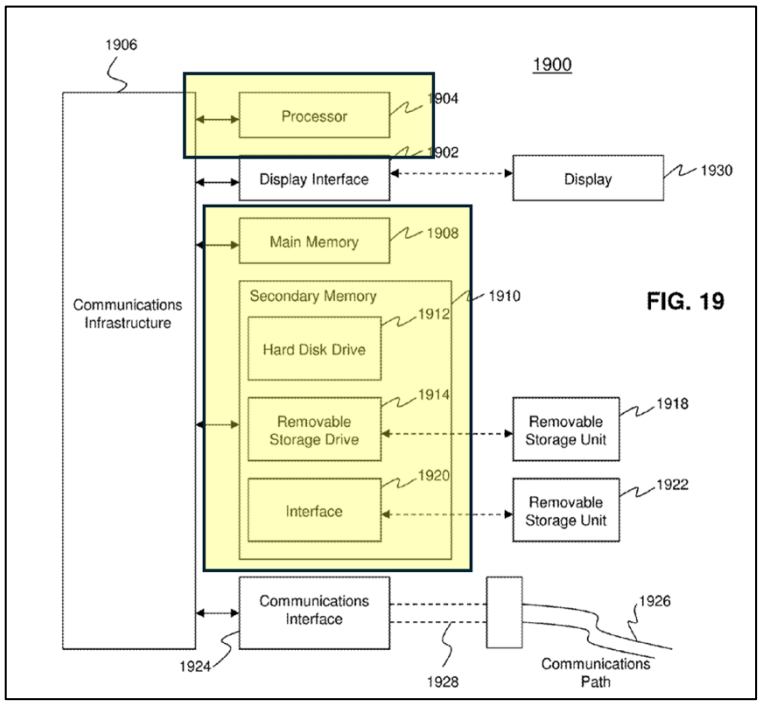
Collinge's mobile device includes *a memory*. Collinge teaches "an application program stored in **data storage** of the mobile device[.]" *Collinge*, [0041], [0147] ("at least one processor device and **a memory**") (emphasis added). Collinge's

memory includes storage 304, which may include a "local encrypted database." *Collinge*, [0067], [0147].



Collinge, Fig. 1 (annotated excerpt). Collinge further teaches the memory of mobile device 104 is *coupled to the processor*. Collinge teaches "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 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*., ¶¶205-207.

As shown below, Collinge teaches the payment system comprises a memory "coupled" to the processor:

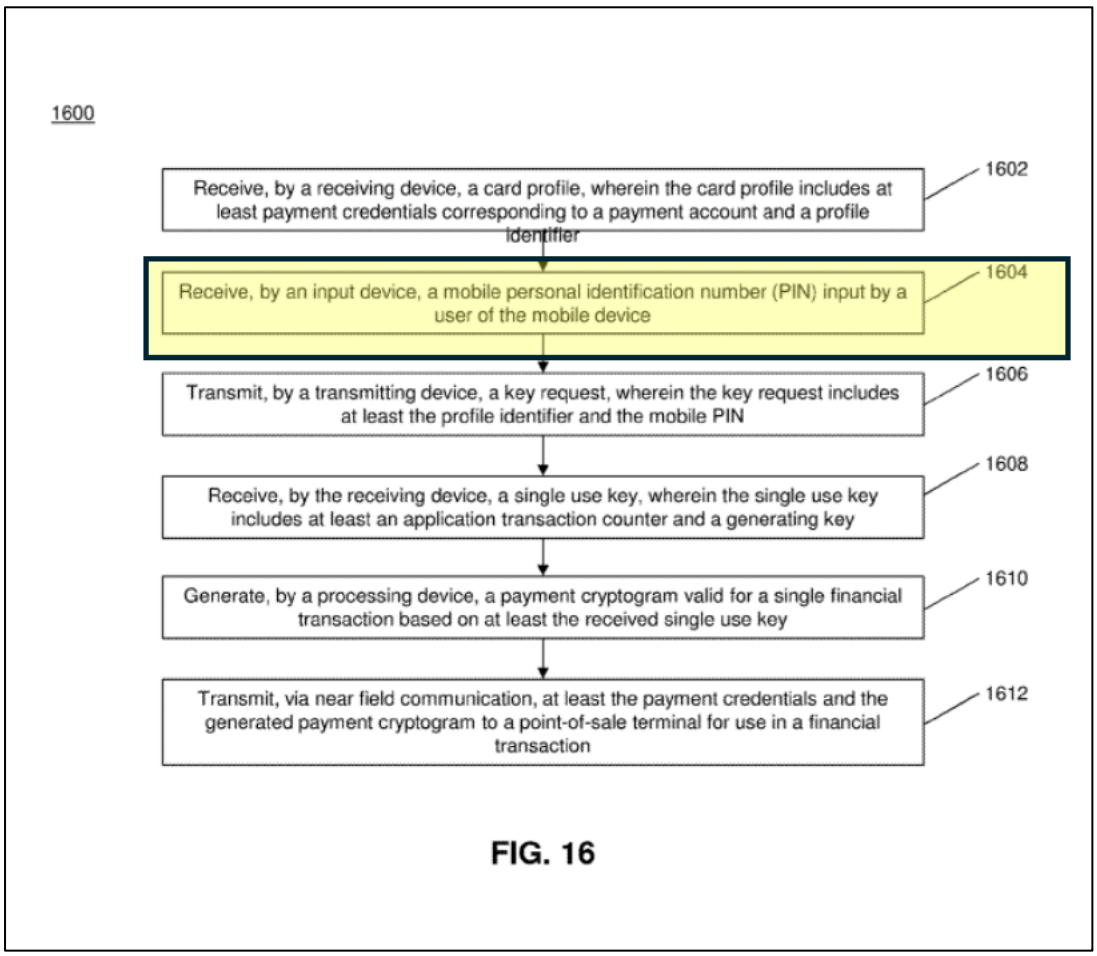


Collinge, Fig. 19 (annotated). Fig. 19 depicts a computer system including "memory that will configure associated processors to implement" Collinge's teachings and explains that Collinge's teachings can "be carried out, e.g., by processing capability on mobile device 104[.]" *'248 Provisional*, [0234]. Collinge teaches the communications infrastructure may be a "bus[.]" *Collinge*, [0150]. Collinge teaches that a memory is coupled to a processor. *Dec*., ¶¶205-207.

21. Claim 19(b):

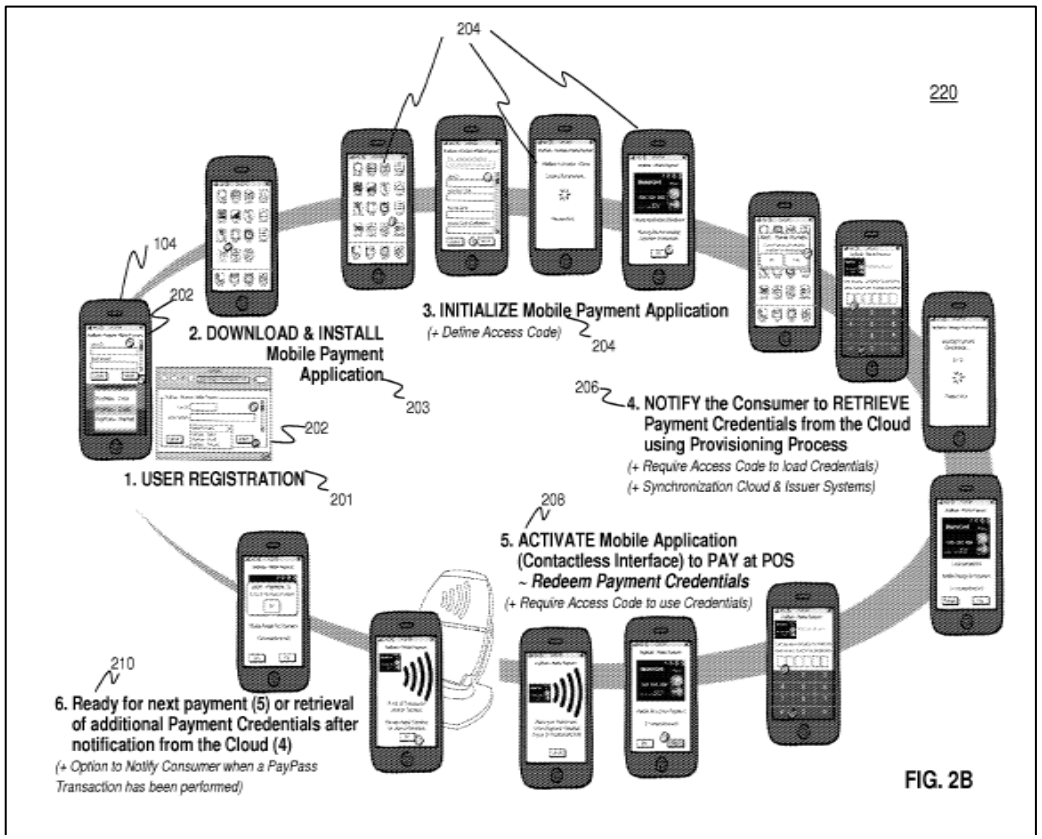
The touch screen *display* of Collinge's mobile device is an "input device" that includes user selectable soft buttons (*device inputs*) visually displayed to the user on a graphical visual user interface. *Collinge*, [0133]; *Dec*., ¶¶208-210. For example, Collinge teaches the touch screen of mobile device 104 receives a user's input of a

"mobile personal identification number (PIN)" prior to generation of a payment cryptogram. *Collinge*, [0133].



Collinge, Fig. 16. (annotated).

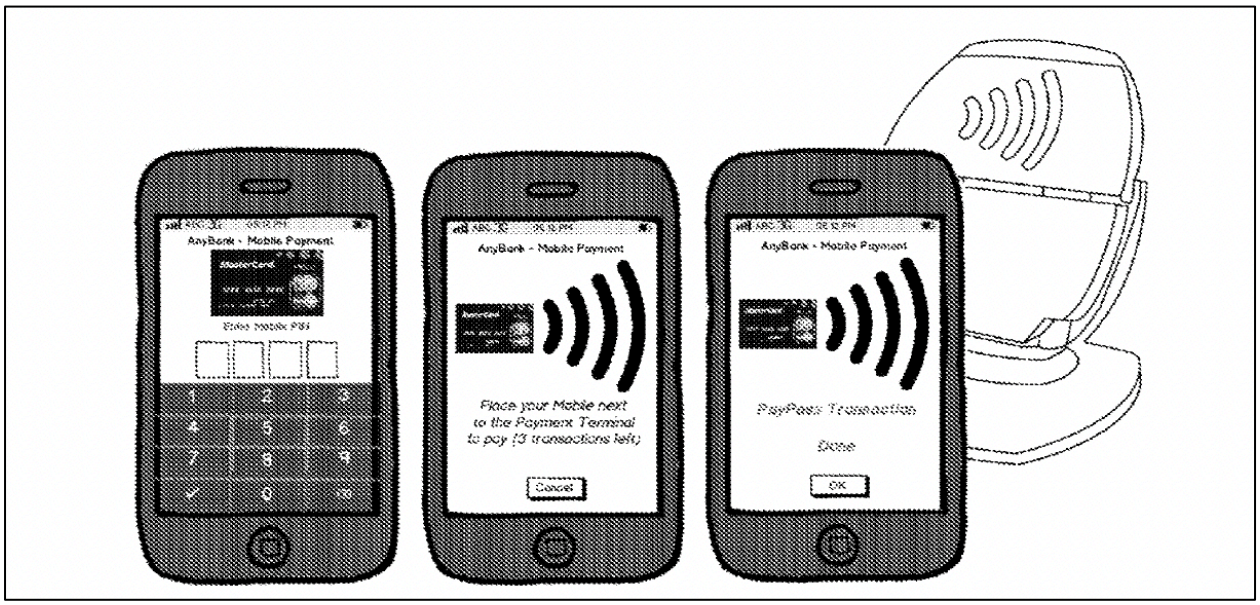
Collinge's '248 Provisional application, incorporated by reference (*see* Section IV.A.1., *supra*) provides further details of how the touch screen display of Collinge's mobile device provides a visual user-interface during the user registration and payment process. *Dec*., ¶¶211-213.



'248 Provisional, Fig. 2B.

22. 19(b)(1):

Collinge teaches a *display output*. Collinge teaches on Collinge's touch screen display, Collinge's display visually directs the user to input a PIN via the display output of the touchscreen, place the mobile device near a payment terminal, and provide an indication to the user when the payment transaction is complete. *Collinge,* [0133], Fig. 16.



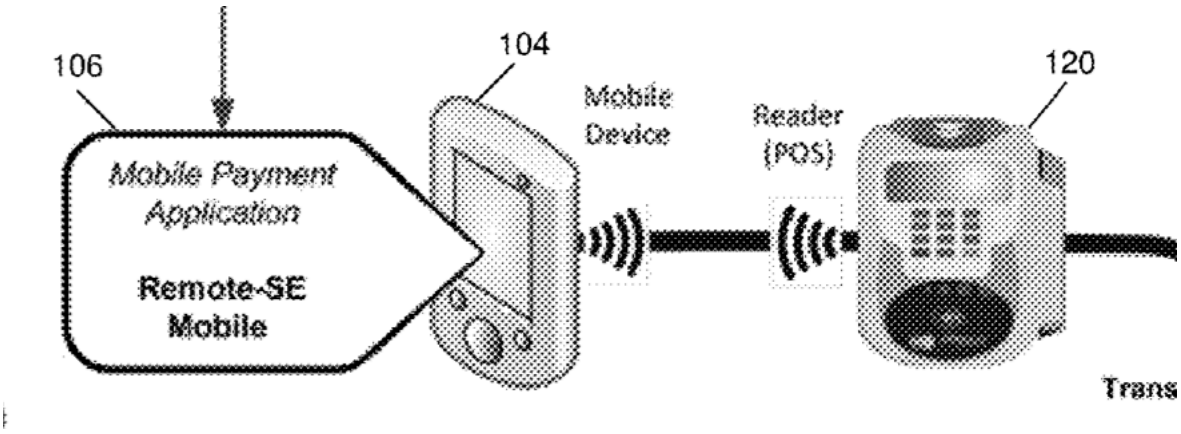
'098 Provisional, 99; *'248 Provisional*, Fig. 2B. The registration process steps can likewise "be accomplished using input supplied by a cardholder or user" "via a GUI" of the mobile device 104. *'098 Provisional,* [0063].

23. 19(b)(2):

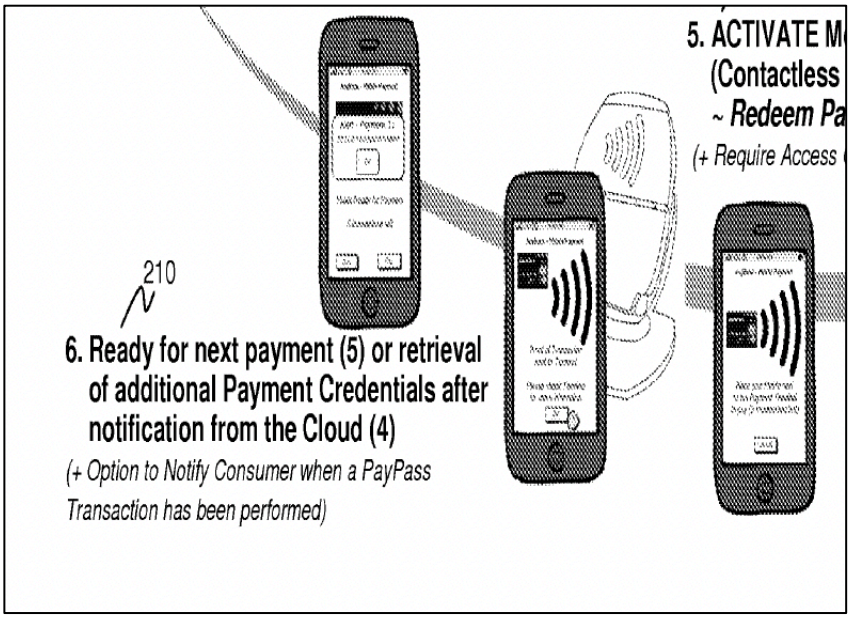
See Claim 19(b).

24. 19(b)(3):

As described above, Collinge, in view of Lin, renders obvious receiving a request for a transaction payment at Collinge's mobile device via Collinge's NFC interface. *See* Claim 1(c). A POSITA would have understood Collinge's mobile device in Figure 1 is within "proximity" to an NFC recipient. *See also '248 Provisional*, Fig. 2B. *Dec*., ¶¶216-219.



Collinge, Fig.1. (excerpt)



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

25. 19(c):

Collinge's mobile device processor executes a mobile payment application program. *Collinge*, [0044]. "The mobile device 104 may include a mobile payment application 106, which may be an application program stored in data storage of

the mobile device 104 and executed by a processor included in the mobile device 104.").

26. 19(d):

See Claim 1(a).

27. 19(e):

See Claim 1(a), 10.

28. Claim 19(f):

See Claim 1(d).

29. Claim 19(g):

See Claim 1(d).

30. Claim 19(h):

See Claim 1(c) and 1(e).

31. Claim 19(i):

See Claim 1(f).

32. Claim 19(j):

See Claim 1(g).

33. Claim 20:

Collinge teaches receiving the *priming action* (e.g., activation code, PIN) of a valid user via the touch screen of the mobile device and identifying a valid user through an accurate activation code/PIN input (*passcode entry sequence*). *See* Claim 1(a). Further, Collinge teaches multiple priming operations, including displaying to

user a request to input a PIN or a passcode (*security challenge question*) on the display of mobile device 104.

34. Claim 23:

Collinge teaches a processor that performs cryptographic functions, such as dynamically generate a single use payment cryptogram (*one-time limited-use cryptogram number*) by combining at least a ATC (*sequence counter*) and using the dynamically generated single use cryptogram number in place of the card issuer CVV/CVC (*in place of at least a portion of a card issuer payment information)* in a payment transaction. *Dec.*, ¶228. *See* Claim 1(e).

Collinge teaches the "[p]rocessor device 1904 may be a special purpose or a general purpose processor device." Collinge, [0150]. Collinge also teaches "payments from mobile devices are processed using an available Trusted Execution Environment (TEE) and the TEE hosts services used during the authentication and payment processing in conjunction with a Mobile Authentication Application (MAA), without requiring use of an SE." '*248 Provisional*, [0006]. A POSITA would have understood a TEE is a "secure area of a mobile device that is isolated from the main operating system and is designed to protect sensitive information and operations." *Dec.*, ¶229. It was well known a cryptographic processor performs cryptographic operations, such as generating a payment cryptogram. *Dec.*, ¶229.

VI. GROUND 2: COLLINGE IN VIEW OF PHILLIPS, LIN AND KRANZLEY

1. Claim 5(a):

Collinge teaches generating a *limited-use security number* (payment **cryptogram**) based on device secrets that are shared with the issuer. *See* Claim 3. Collinge teaches generating a CVC3 by *cryptographically combining* the following *device and issuer secrets*: "the session key unpredictable number, the application transaction counter, and the reader unpredictable number." *Collinge*, [0145].

2. Claim 5(b):

Collinge in view of Kranzley teaches *displaying the limited-use security number* (payment cryptogram) on Collinge's touch-screen display (*the user-interface of the display*).

Kranzley teaches a "**dynamic code** is a three or four digit code that may be used in place of a 'CVV', 'CVC' or other code (a code generally used in payment card systems and used to verify that a cardholder was in possession of a payment card during a transaction)." *Kranzley*, [0041] (emphasis added).

Kranzley teaches this "dynamic code is **displayed on the display device**." *Kranzley*, [0011] (emphasis added).

(a) Motivation to Combine

It would have been obvious and a POSITA would have been motivated to modify Collinge's mobile payment application to display Collinge's payment

cryptogram on Collinge's display as taught by Kranzley. A POSITA would have recognized consumers wanted flexibility to make payments in the most locations possible and this modification would have allowed Collinge's payment credentials to be used in more locations, such as where the point of sale requires a CVC-type value to be provided, as taught by Kranzley. *Kranzley,* [0011], [0040]. *Dec.,* ¶233. A POSITA would have had a reasonable chance of success in making the combination, including because (1) both Kranzley and Collinge teach compliance with PayPass standards when generating payment information (*Collinge,* Fig. 6; *'095 Provisional,* [0003]; *Kranzley,* [0020]) and (2) simply displaying payment information that Collinge's mobile device already has on Collinge's touchscreen display would have been well-within the skill level of a POSITA and a POSITA would have appreciated this would have been combining known elements to yield predicable results. *Dec*., ¶233.

3. Claim 6:

Collinge in view of Kranzley teaches a payment provider (*payment processing authority*) verifies a payment cryptogram (*limited-use number*) based on at least an ATC (*a transaction sequence count information*) and further comprising: authorizing said transaction, by the payment network (*payment processing authority*) where the payment cryptogram appears in place of *card issuer information* (CVC).

(a) Collinge's Teachings

When a user taps Collinge's device, "[t]he merchant point-of-sale terminal 120 may transmit the received payment information and any additional transaction information (e.g., transaction amount, merchant identifier, etc.) to the acquirer processing server 312 of the acquirer 122." *Collinge*, [0077]. "The acquirer processing server 312 may then generate and submit an authorization request for the financial transaction to the payment network 124." *Collinge*, [0077].

1. Collinge's payment network "process[es] the authorization request, such as by querying the issuer 108 for approval of the payment transaction (e.g., based on funds or credits in the payment account)." *Collinge*, [0045]. The "payment network 124 may transmit relevant transaction data, such as the payment information and transaction amount, to the issuer processing server 308." *Collinge*, [0077]. Specifically, as shown in Fig. 17, the issuer received "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 (Ex. 1004),* [0141].

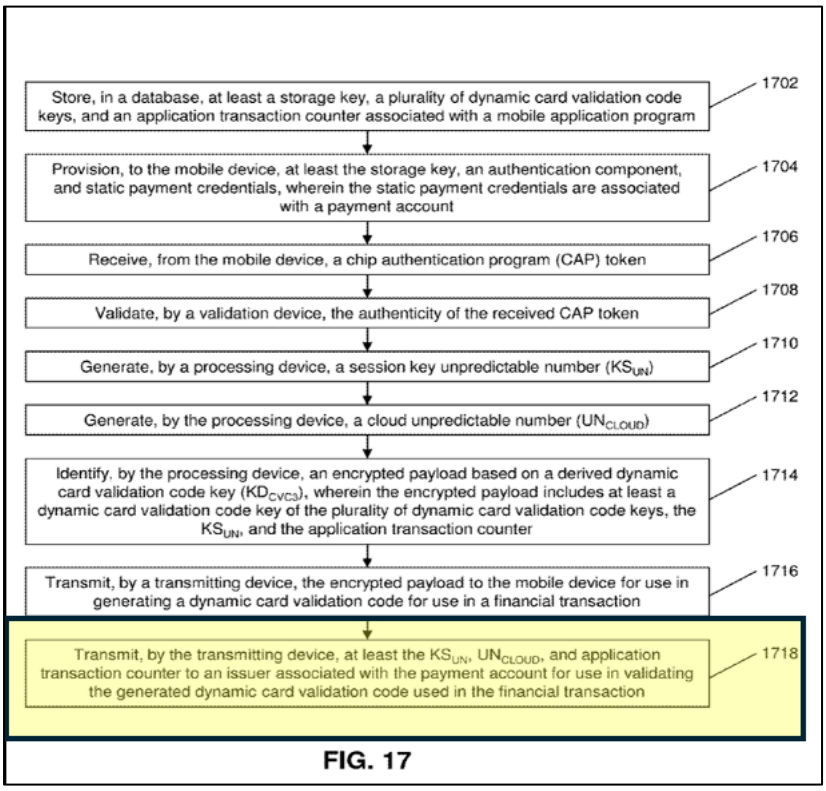


FIG. 17

Collinge (Ex. 1004), Fig. 17 (annotated). The issuer approves a transaction by "validat[ing] the application cryptogram." *Collinge*, [0077].

Collinge teaches issuer 108 will "deny the payment transaction" when the received CVC3 value is unable to be authenticated because, for example the single-use key is not genuine based on an unsuccessfully entered mobile PIN (*invalid number generation*). *Collinge,* [0076]-[0077], Abstract.; *Dec.,* ¶237.

Collinge further teaches issuer 108 may deny the payment transaction based on "control limits" (*use outside of a valid time limit*) synchronized between mobile payment application 106 and issuer 108. *'095 Provisional*, Claims 9-10. ("a day of week; a time of day; an expiration date associated with a CAP token; an expiration

date associated with a payment account; a merchant category corresponding to a point-of-sale (POS) terminal; a geographic location of a merchant; a spending limit for a payment account; a spending limit for a specified merchant category; and a spending limit for a duration."). *Dec.,* ¶238.

(b) Kranzley's Teachings

Kranzley teaches the "the payment provider 110 may generate a series of expected dynamic values based on the general range of counter values the payment provider expects from a particular mobile device." *Kranzley*, [0047]. "If the dynamic value received from the mobile device 102 is equal to one of the ten expected dynamic values, the transaction may continue. If the dynamic value received from the mobile device 102 is not equal to one of the ten expected dynamic values, then the transaction may be declined (e.g., by returning a denial response in message '5')." *Kranzley*, [0047]. Kranzley teaches this "dynamic code is a three or four digit code that may be used in place of a 'CVV', 'CVC' or other code (a code generally used in payment card systems and used to verify that a cardholder was in possession of a payment card during a transaction)." *Kranzley*, [0041].

(c) Motivation to Combine

It would have been obvious and a POSITA would have been motivated to modify Collinge's payment system so that Collinge's payment provider network (*payment processing authority*) as taught by Kranzley validates a payment

cryptogram instead of Collinge's issuer validating a. payment cryptogram. *Dec*., ¶241.

Collinge already teaches a payment network. *Collinge*, [0036] A POSITA would have understood one example of a payment processing authority would be Collinge's payment network. *Dec*., ¶241. The payment network has transaction data. *Collinge*, [0077]. ("payment network 124 may transmit relevant transaction data, such as the payment information and transaction amount, to the issuer processing server 308.") A POSITA would have appreciated one example of Kranzley's dynamic code would be Collinge's CVC3 payment cryptogram, since the CVC3 is used in place of a CVC/CVV. *Kranzley*, [0041]. *Dec*., ¶242.

A POSITA would have been motivated to have Collinge's payment network (payment provider) approve a payment transaction for a faster transaction. A POSITA would have had a reasonable expectation of success in making such a modification. *Dec*., ¶243. A POSITA would have been motivated to have the payment network validate Collinge's payment cryptogram based on the associated CAP token's limitations of use. *Dec*., ¶243. A POSITA would have been motivated to have Collinge's payment network approve a payment transaction and associated CAP token to monitor payment transactions on Collinge's mobile device and would have had a reasonable expectation of success in making such a modification. *Dec*., ¶243. Accordingly, implementing a CAP token is combining a well-known prior art

element according to known methods and would have yielded the predictable results, including a more secure payment system (with a CAP token as an additional authentication value), and greater flexibility in managing the use of payment credentials to limit fraud and manage spending habits. *Dec*., ¶243.

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

1. Claim 4(Pre):

The combination of Collinge and Smith teaches a *device account number*. As will be discussed in 4(c), Collinge uses Smith's PPAN (*device account number*) when generating Collinge's payment cryptogram (*limited-use number*). As will be shown in Claim 4, Collinge in view of Smith teaches Collinge's payment cryptogram is generated using a PPAN and Collinge's payment cryptogram is then combined with the PPAN when payment information is transmitted to a point of sale terminal. Therefore, Collinge's payment cryptogram comprises Smith's PPAN, based on CardWare's apparent interpretation of this claim. *See* Ex.1017, p.21-22 (explaining that one input to generating a cryptogram is a device account number therefore, the cryptogram value "'comprises' the device account number").

(a) Collinge's Teachings

Collinge teaches 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 the payment credentials include, for example, a primary account number (PAN). Collinge, [0049] ("payment account number"); *'098 Provisional*, 101. *Dec*., ¶¶250-253.

Collinge teaches using a virtual primary account number (VPAN) as an alternative to the card PAN. *'098 Provisional*, 159-160. Collinge teaches 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*., ¶¶250-253.

(b) Smith's Teachings

Smith (also assigned to MasterCard) teaches a "mobile device" that "may…be used…with a near field communications enabled purchasing transaction." *Smith*, Abstract. Whenever a user wishes to open a payment account, the issuer issues a "temporary PAN…and establishes any risk parameters (e.g., for use in controlling the authorization of transactions involving the temporary PAN)" so the user is able to make purchases while awaiting an actual PAN. *Smith*, [0026].

This "temporary PAN is mapped to a **mobile PAN (e.g., such as a PayPass® PAN, or PPAN)**." *Smith*, [0026] (emphasis added). The PPAN (*device account number*) is "assigned to the mobile device 104." *Smith*, [0016]. The PPAN is "stored in the mobile device 204." *Smith*, [0022]. The PPAN is, therefore, a *device* account number. *Dec*., ¶¶255-257.

Once an actual PAN is issued, the temporary PAN is swapped with the actual PAN. *Smith*, [0026], [0040]. The PPAN (*device account number*) is then associated with a "related PAN[.]" *Smith*, [0023]. The PPAN is "initially…mapped to the temporary PAN" but whenever the issuer issues the "actual PAN" the actual PAN "replace[s] the temporary PAN" so the PPAN is now an alternate number mapped to the actual PAN. *Smith*, [0040]. *Dec*., ¶256. The PPAN is a different number from the actual PAN. *Dec*., ¶¶256-257.

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].

The issuer can "implement dual account number structures" for "multiple NFC-enabled handsets may be managed for a single account." *Smith*, [0029]. It was well known a dual account number has separate and distinct numbers for each device the overall account is used on. *Dec*., ¶259. Accordingly, Smith's PPAN is a distinct *account number* for a payment account on a particular "mobile device." *Dec*., ¶259.

Even if the same user wants to register a new device, a user will get a different PPAN for that device to use because the PPAN is assigned immediately upon registering the device. *Smith*, [0026] ("an instantly-issued payment account that may be used by the customer almost immediately after submitting a request for a new payment account.") *Dec*., ¶260.

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 Smith's PPAN is static. *Dec*., ¶261. *See* '579 Patent, claim 21.

(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*., ¶¶262-263.

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*., ¶¶264-265. It was well known in the art that a device without a secure element (SE), such as Collinge's mobile device, could be vulnerable to malicious attacks and therefore storing Smith's PPAN instead of the PAN on Collinge's mobile device would have increased security for the user's account. *Dec*., ¶¶264-265

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*., ¶266. 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*., ¶266; *Smith,* [0023]. A POSITA would have understood using Smith's PPAN in place of Collinge's PAN would be combining prior art elements according to known methods to yield the predictable result of increased security. *Dec*., ¶266. A POSITA would have been motivated to apply Collinge and Smith's teachings and appreciated the compatibility of their teachings

because both discuss payment systems that rely on MasterCard PayPass functionalities. *Dec*., ¶266.

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]-[0049] ("The card profile 116 may include payment credentials… common payment credentials 202 may include all data elements…data elements may include payment account number"), 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."); *Dec*., ¶267.

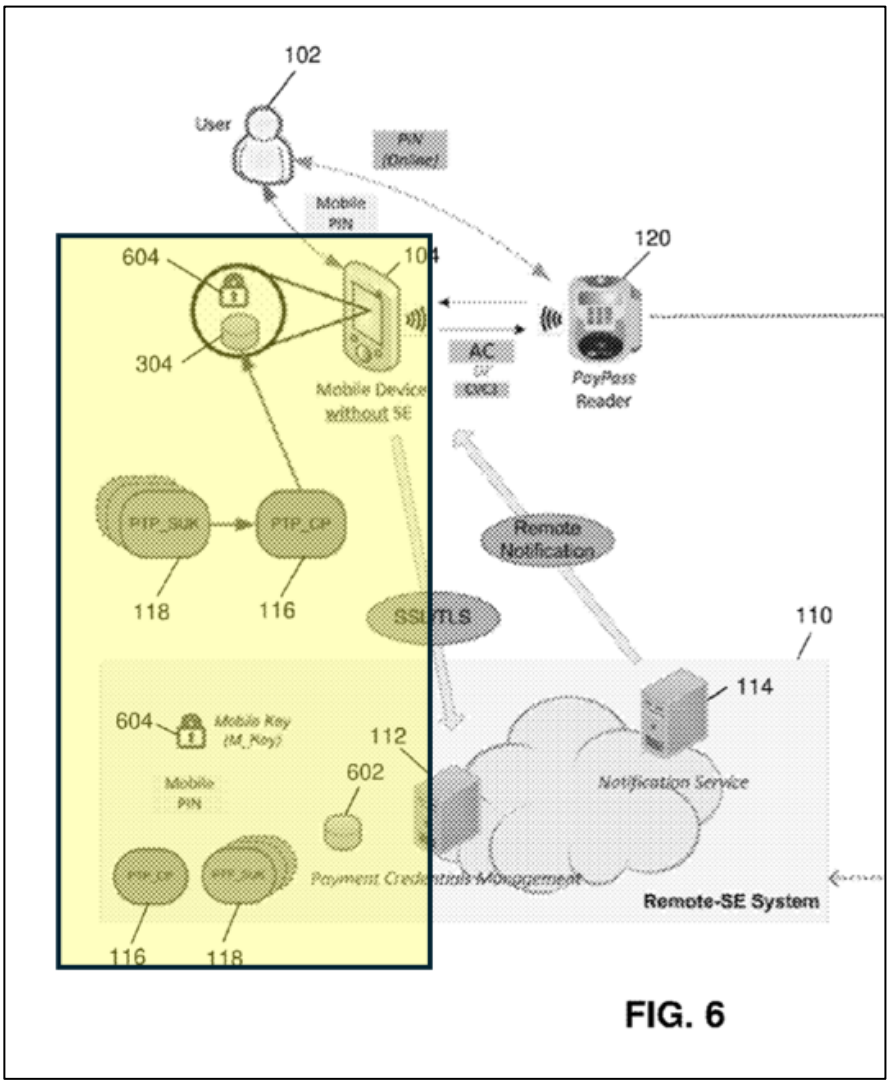


FIG. 6

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."). *Dec.,* ¶268.

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*., ¶¶268-269.

2. Claim 4(a):

As discussed in Claim 4(Pre), Collinge in view of Smith teaches wherein a card issuing authority provides said device account number for use only by the electronic device (device-specific), in place of the PAN (*card issuer information*) in performing payment transactions by Collinge's mobile device. *Dec*., ¶268. Smith teaches an expiration date but is not specific as to if that is assigned to the PPAN. *Collinge,* [0124], *Smith,* [0029] ("PPAN, an expiration date (e.g., an expiration month and year)").

In related art, 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].

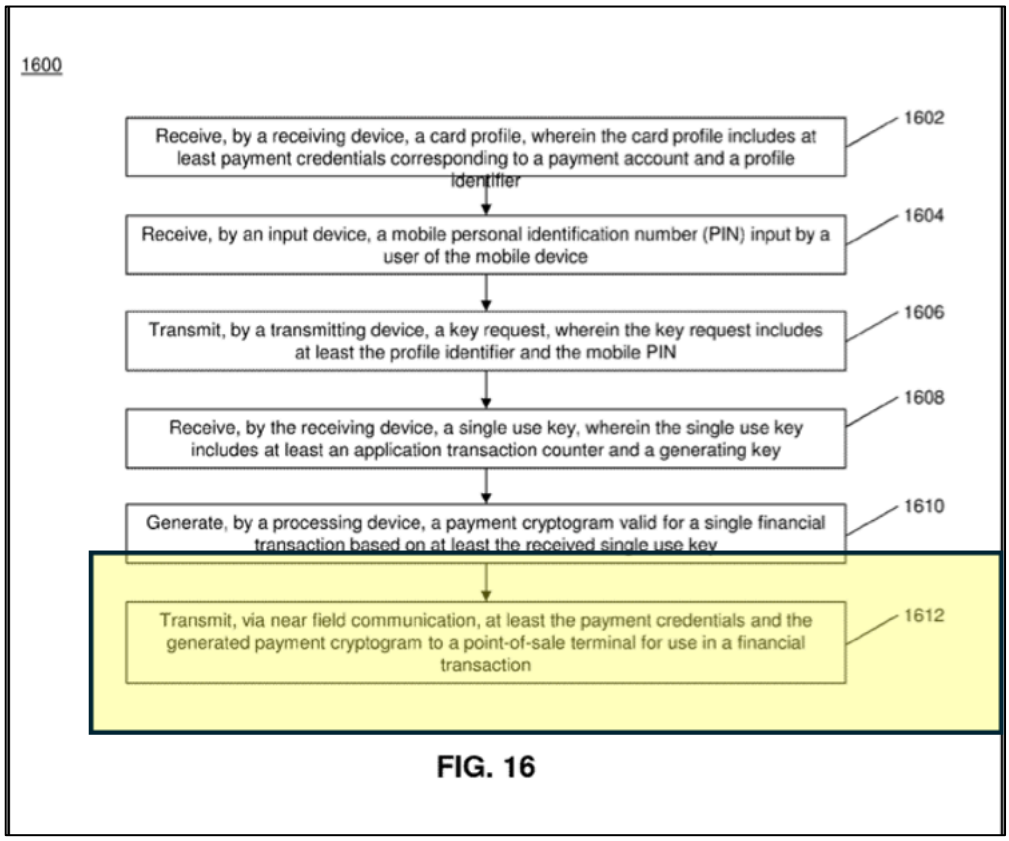
(a) Motivation to Combine

It would have been obvious and a POSITA would have been motivated to assign a virtual expiration date to the device account number, as taught by Kranzley. It was well known payment cards expire, and it would have been desirable for the device account number associated with the card to also expire to prevent the user from attempting to make a purchase after the payment credentials cease to be valid and to prevent fraud. *Dec*., ¶272. The modification is nothing more than the

application of a known technique (assigning an expiration date) to well-known device (mobile device) to yield predictable results of virtual wallet payment credentials with an expiration date, and a POSITA would have had a reasonable expectation of success in making this modification. *Dec*., ¶272,

3. Claim 4(b):

Collinge teaches sending the dynamically generated CVC3 and payment credentials (which in combination with Smith includes the PPAN, *see* Claim 4(a)) to a point-of-sale terminal. *Collinge*, [0070], [0077]; [0135].



Collinge, Fig. 16 (annotated), [0048]-[0049](" card profile 116 may include payment credentials…payment credentials 202 may include all data elements … data

elements may include payment account number"), Fig. 6, [0104] (card profile (PTP_CP)); *'098 Provisional*, 101 ("Payment Token Payload – Card Profile (PTP_CP_ contains the Payment Credentials required to perform a [MasterCard] *PayPass* transaction" including "data elements such as: **PAN,** PSN + Track Data.").

As shown above, Collinge's card profile includes the PAN. Collinge's card profile is included in the payment credentials. A POSITA would have been motivated to substitute Smith's PPAN for Collinge's PAN when making payment transactions, as taught by Smith. *Smith,* [0018]. *Dec.,* ¶274. A POSITA would again have recognized that substitution of a PayPass PAN would have increased security since sensitive information like a PAN would therefore not be transmitted. *Smith*, [0023]. *Dec.,* ¶274. It was well known in the art that an alternative to storing the PAN would reduce the risk of vulnerable sensitive information (such as the PAN) when performing a transaction. *Dec.,* ¶274. As discussed in Claim 4(Pre), a POSITA would have appreciated 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*., ¶¶268-269.

4. Claim 4(c):

Collinge in view of Smith teaches combining, by Collinge's mobile device, a *limited-use number* (payment cryptogram (CVC3)) and *device account number* (PPAN) to create *device generated payment information*. Collinge's mobile device transmits a combined payment credentials and the generated payment cryptogram (*limited-use payment information*) via an *NFC interface* to a point of sale terminal. *See* Claim 1(f).

Collinge teaches generating a payment cryptogram (CVC3) based, in part, on a PAN. Specifically, Collinge generates a payment cryptogram based on track data which includes a PAN.

12	Standard PayPass® Magstripe payment experience using a Mobile Device. The Mobile Payment Application use a specific process to generate the CVC3 using (KS_{UN}, $Cloud_CVC3_{TRACK1/2}$, ATC and UN_{READER})

'248 Provisional, Table 1;*'095 Provisional*, [0010]. ("some payment credentials …including track data…contain PAN information."); *'098 Provisional*, [0148] ("The generated encrypted payment token payload 112 contains sensitive data including Track Data, which in turn contains a PAN value[.]"); *Collinge*, [0048]-[0049] ("card profile 116 may include payment credentials… common payment credentials 202 may include all data elements…data elements may include payment account number")

It was well known in the art that a dynamic card verification value (CVC3) is generated in part based on the PAN. *Dec.,* ¶277. A POSITA would have understood that a CVC3 value is generated based on the PAN and PSN because it ensures that the dynamic card verification value is unique to the user's card used in the transaction. *Dec.,* ¶277.

(a) Smith's Teachings

Smith teaches using a PPAN in place of a traditional PAN. *See* Claim 4(a). A POSITA would have been motivated to use Smith's PPAN in place of a PAN in Collinge's mobile payment application on Collinge's mobile device. *Id.*

(a) Motivation to Combine

It would have been obvious to configure Collinge's mobile payment application on Collinge's mobile device to use Smith's PPAN instead of a PAN when generating a single use dynamic CVC3 value (payment cryptogram). *Dec.,* ¶279.

A POSITA would have appreciated that using Smith's PPAN instead of a PAN when generating a CVC3 would enhance security by obfuscating the real card number. *Dec.,* ¶279. A POSITA would have appreciated that Smith's PPAN is linked to the cardholder's account but differs from the actual PAN. *Dec.,* ¶278. By using Smith's PPAN when generating the dynamic CVC3 on Collinge's mobile device, the real PAN would not be exposed during the transmission of payment information,

reducing the risk of fraud. *Dec.,* ¶279. A POSITA would have appreciated that such a modification would help protect sensitive card information and a POSITA would have expected a reasonable expectation of success. *Dec.,* ¶279. Further, as emphasized in Claim 4(a) a POSITA would have been motivated to limit the possible exposure of sensitive information like the PAN on a mobile device without an SE (Collinge's mobile device). *Dec.,* ¶279.

5. Claim 4(d):

See Claims 1(e), 4(Pre), 4(b).

6. Claim 21:

See Claims 1(d), 4, and 19(b).

7. Claim 22:

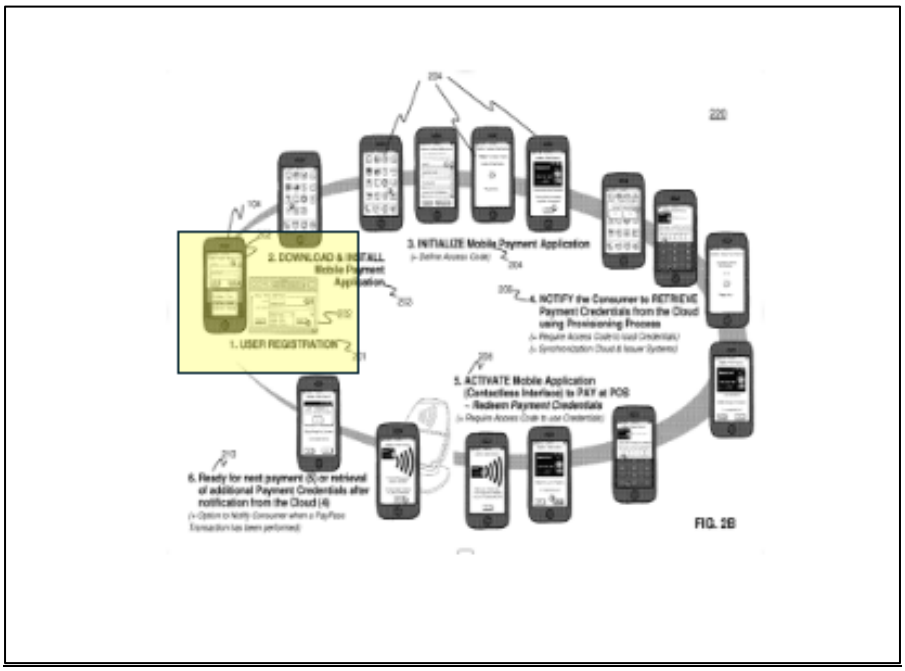
See Claims 1(d), 4, and 19(b).

VIII. GROUND 4: COLLINGE IN VIEW OF PHILLIPS, LIN, AND AABYE

1. Claim 8(a):

As described in Claim 1(a) Collinge teaches a *priming operation* performed using Collinge's touch screen (inputting an activation code). As described in Claim 1(d), Collinge teaches the user *selection of a payment method*.

Collinge further teaches selection of a payment method *initiating a payment-operation*.



'248 Provisional, Fig. 2B.(annotated) *Dec*., ¶281.

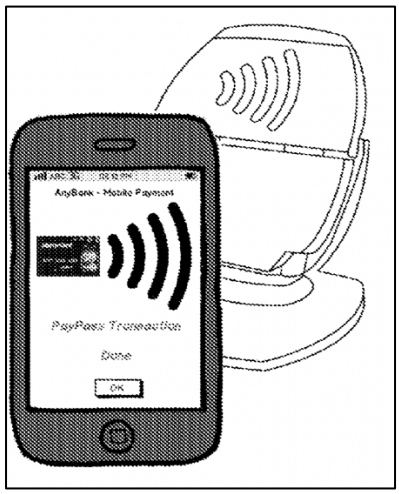
2. Claim 8(b):

Collinge teaches a priming operation performed on the touch screen by inputting an activation code (*a user entry of a valid passcode*) and that the user selects a payment method. *See* Claim 1(a).

Collinge in view of Aabye teaches *enabling the electronic device for payment* based on input from a device biometric sensor (e.g., a fingerprint sensor) detecting that the device is in the user's possession.

(a) Collinge's Teachings

Collinge teaches the user may supply "a biometric identifier." *Collinge*, [0143].

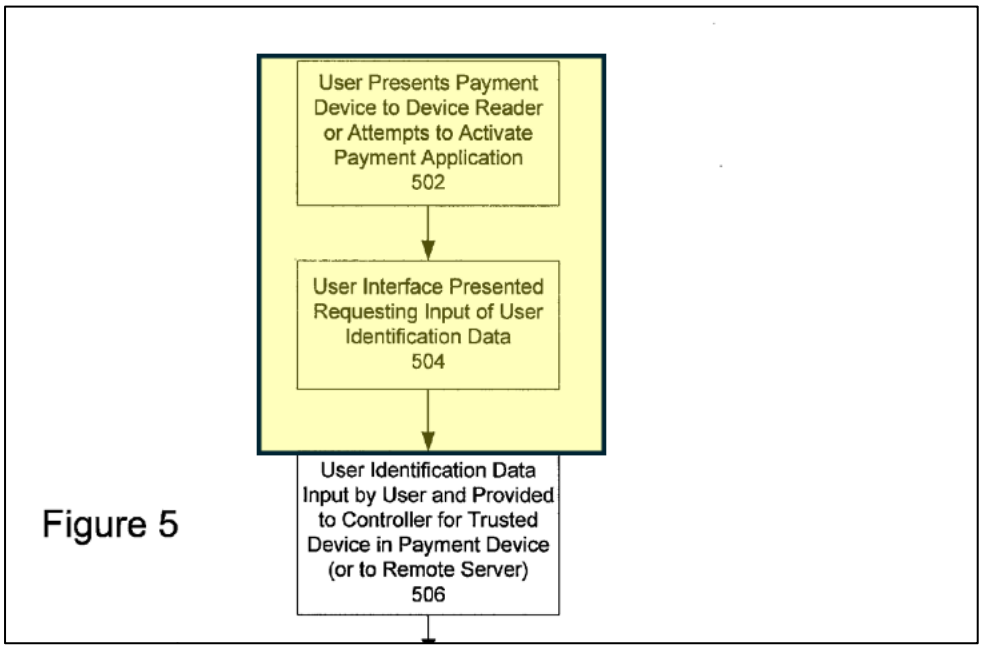


'098 Provisional, 99. (excerpt); *'248 Provisional*, Fig. 2B.

(b) Aabye's Teachings

Aabye teaches the "the payment device may include a user data input element 402." *Aabye*, [0050]. This "input element 402" may be a "a fingerprint detector or sensor, a touchscreen, a biometric data sensor, etc." *Aabye*, [0050].

In response to the user presenting the "payment device to a device reader", "the user is presented with a user interface." *Aabye*, [0054]-[0055]. The mobile device's user interface "request[s] the user to input user identification data…into an appropriate data input device (e.g., element 402 of FIG. 4). One example of identification is "a fingerprint reader for input of a user fingerprint[.]" *Aabye*, [0055].



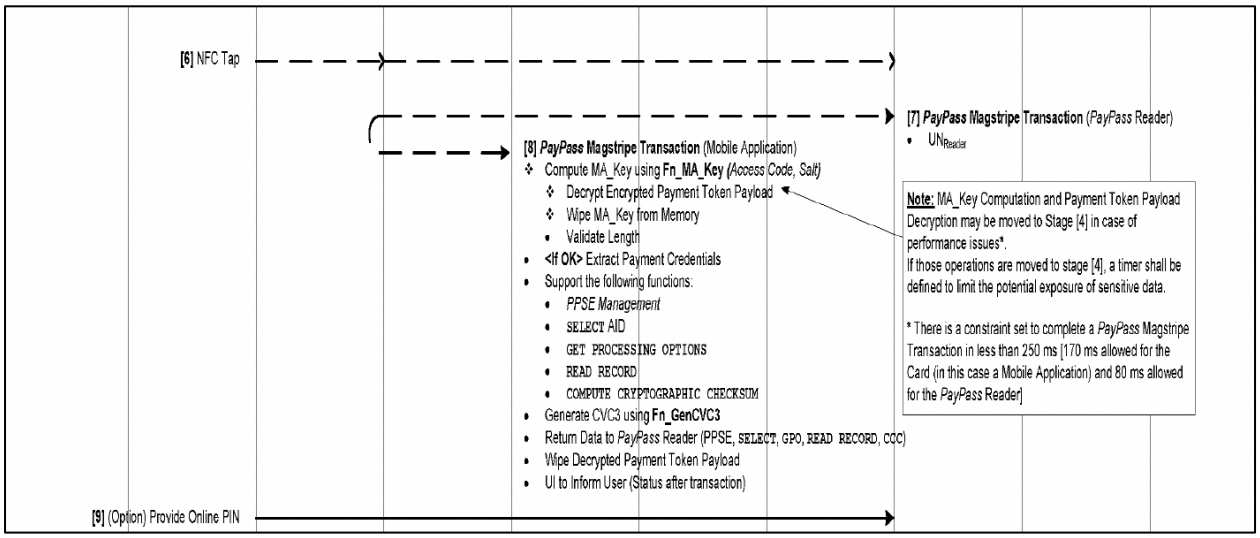
Aabye, Fig. 5. (annotated excerpt).

The payment application compares "the received user identification data to a previously stored copy of the data)" and "[i]f the received data is verified as valid …then the user is provided access to the functionality of the payment application" *Aabye*, [0057]. A POSITA would have appreciated that the user presenting the payment device to a POS reader and requesting a fingerprint of a user is device biometric sensing the electronic device is continuously remaining in the proximity possession of a valid user while Collinge's device maintains an NFC connection with the POS reader. *Dec*., ¶287. A POSITA would have understood that once the user's fingerprint is validated, the transaction is enabled the electronic device for payment. *Dec*., ¶287.

(c) Motivation to Combine

A POSITA would have been motivated to modify Collinge's mobile payment application to include user authentication via a fingerprint sensor while a user's device is at a point of sale reader to determine that the Collinge's mobile electronic device is continuously remaining in the proximity possession of a valid user while at the POS reader. *Dec*., ¶288.

Collinge already requires user authentication to use payment credentials when at a POS terminal. *Collinge*, [0093], [0123] (describing "authentication by the user 102 at both the mobile device 104 (e.g., entering of the mobile PIN) and the point-of-sale terminal 120 (e.g., entering of an online PIN or signature).").



'248 Provisional, Fig. 14 (excerpt). A POSITA would have been motivated to apply Aabye's teachings of authenticating a user via a fingerprint sensor at step 8 as shown above because a fingerprint provides additional security along with using Collinge's PIN. *Dec*., ¶288. Spoofing a fingerprint is significantly more difficult. *Id*.

Collinge already teaches that a user may supply a "biometric identifier" but contains little detail on how it would be implemented. *Collinge*, [0143]. A POSITA would have understood that using Aabye's teachings of authenticating a user via a fingerprint sensor while a user's device is at a point of sale reader 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. *Dec*., ¶289.

3. Claim 9(a):

Collinge and Aabye teach a device biometric sensor operable to determine the electronic device continuously remains in contact with a valid user. *See* Claim 8(b).

Collinge's *device touchscreen user interface* is operable to accept *a user approval* (selecting a pay option).



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

4. Claim 9(b):

See Claim 1(d).

5. Claim 9(c):

Collinge receives a *user input* of a payment method selection (*See* Claim 1(d)), *payment approval authorization*, and *payment denial*.

Collinge's *touchscreen user interface* is operable to accept *a user approval* (selecting a pay option) *and denial* (selecting "quit" or "cancel") a *payment transaction* at a merchant facility (point-of-sale terminal). *Dec.*, ¶293.



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

IX. GROUND 5: COLLINGE IN VIEW OF LIN AND AABYE

1. Claim 15(Pre):

See Claim 1(Pre).

2. Claim 15(a):

Collinge in view of Lin teaches receiving a request for a transaction payment at Collinge's electronic device via Collinge's NFC interface via a NFC communication link. *See* Claim 1(c). The Collinge-Lin combination teaches that this payment request is a recipient proximity communication request that is sent to Collinge's mobile device NFC interface. *Dec.*, ¶295. For example, Lin teaches the request is sent via NFC and that NFC communication must occur within "2 to 4 cm." *Lin*, 19:26-27. *See* Claim 1(c) (motivation to combine).

3. Claim 15(b):

See Claim 1(d).

4. Claim 15(c):

As described in Claim 1(a), Collinge teaches a *valid device user* and a *approval authorization input* on the electronic device. As described in Claim 1(d) Collinge teaches a card issuer *payment selection.*

5. Claim 15(d):

See Claim 1(e).

6. Claim 15(e):

See Claim 1(f).

7. Claim 15(f):

See Claim (1)(a) and 9(c).

8. Claim 15(h):

See Claim 8(b).

9. Claim 15(i):

See Claim 1(d).

10. Claim 15(j):

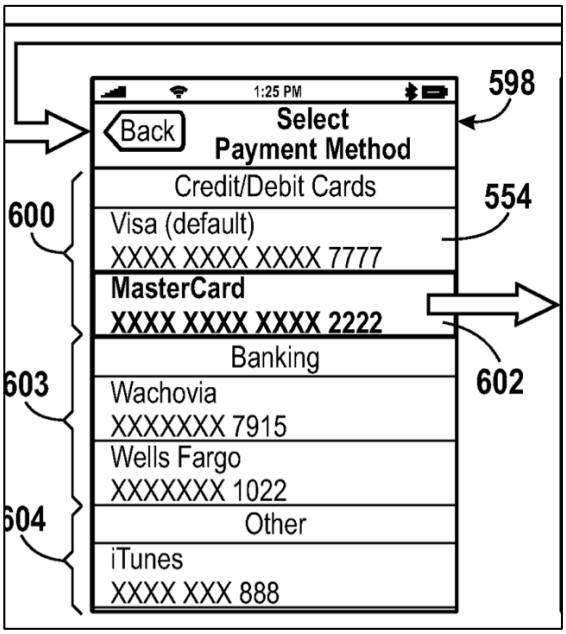
See Claim (1)(a) and 9(c).

11. Claim 16:

See Claim 1(g).

12. Claim 17:

Collinge in view of Lin teaches displaying a plurality of payment options including debit, credit, or prepaid (*a user's payment account information*) and receiving a user-selection of a payment method for a transaction via said touch-screen display user-interface. *See* Claim 1(d).



Lin, Fig. 14E. (excerpt).

13. Claim 18:

See Claims 1(a) and 8.

X. GROUND 6: COLLINGE IN VIEW OF LIN, PHILLIPS, AABYE AND PISULA

1. Claim 13(a):

As discussed in Claim 8, Collinge in view of Aabye teaches a biometric sense of the device continuously remaining in the proximity contact of a valid user, since a last validation.

Collinge in view of Pisula teaches a button double press.

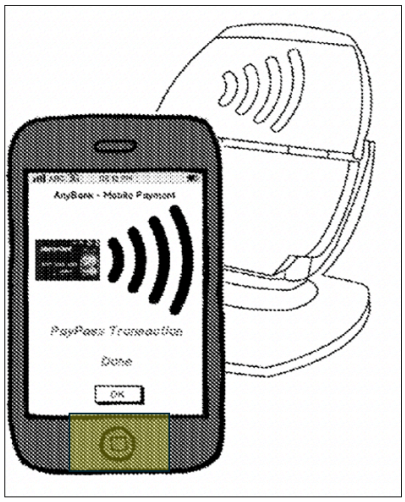
(a) Pisula's Teachings

Pisula teaches a *priming operation* of *a double button press*. Pisula teaches determining "whether the detected interaction by the user with the first physical

button corresponds to a second predefined action" where the "second predefined action is a double activation of the first physical button in a predefined time period (e.g., pressing the menu button 204 twice in succession in 0.3 seconds)" *Pisula*, 28:57-64. In response to "determining that the interaction by the user with the first physical button corresponds to the second predefined action, the device: turns on the touch screen display[.]" *Pisula*, 28:65-29:4. Pisula also teaches a "longer press of the push button (e.g., 206) may turn power to the device 100 on or off." *Pisula*, 14:23-25.

(b) Motivation to Combine

It would have been obvious and a POSITA would have been motivated to modify Collinge's mobile device to accept a double button press to turn on the display of Collinge's device and allow a user to access mobile applications based on the teachings of Pisula and because Collinge already teaches a button. *Dec.*, ¶¶309-313.



'098 Provisional, 99 (excerpt, annotated); *'248 Provisional,* Fig. 2A-B; *Collinge*, Fig. 1.

It was well-known that popular mobile devices at the time included one or more physical buttons that a user would interact with to lock or unlock a device screen. *Dec.*, ¶310. A POSITA further would have recognized that a button on a mobile device may be unintentionally pressed, such as by other objects in a user's pocket or purse, or if the mobile device is dropped, and that it is undesirable for a mobile device or its screen to unintentionally be activated for security and battery-life reasons. *Dec.*, ¶311; *Pisula,* 16:53-56 ("keep[] the screen off…to prevent unnecessary battery drainage").

A POSITA would further have been motivated to implement Pisula's teaching of a long button press to power the device on and off to Collinge's mobile device, and a POSITA would have recognized that the modification would have similarly

reduced the chances of a user inadvertently powering the device on (wasting battery). *Dec.*, ¶312.

A POSITA would have been motivated to apply the button press techniques implemented in Pisula's mobile device (including a double button press and a long button press) to improve Collinge's mobile device in the same way to achieve the predictable result of minimizing unintentional activation of the device, increasing security. *Dec.*, ¶313. A POSITA would have had a reasonable expectation of success, including because detecting a double button press or a long button press were already common ways for consumers to interact with electronics at the time and it would have been well-within the capabilities of a POSITA to implement such functions. *Dec.*, ¶313.

2. Claim 13(b):

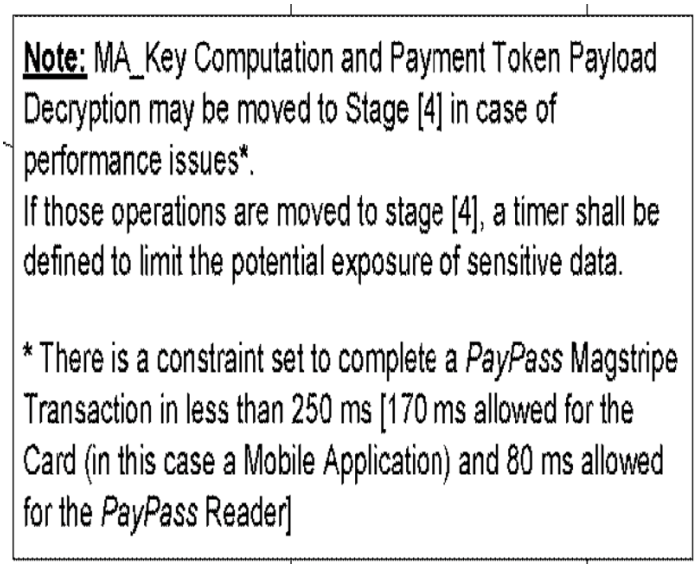
As the Collinge-Aabye combination teaches, if a user does not perform the fingerprint sensing (and the transaction) before the time limit elapses the transaction will not be allowed to complete. *See* Claim 8(b). A POSITA would have understood that if the transaction cannot complete, then a user would have to go through Collinge's authentication process again and re-enter the activation code as discussed in Claim 1(a). *Dec.*, ¶314.

3. Claim 13(c):

As the Collinge-Pisula combination teaches, if a user presses the button twice outside of the 0.3 second timeline, Collinge's device would not approve the button press. Collinge-Pisula also teaches a "longer press of the push button (e.g., 206) may turn power to the device 100 on or off." (disabling a device priming operation) *Dec.*, ¶313. *Pisula*, 14:23-25. *See* Claim 13(a).

4. Claim 13(d):

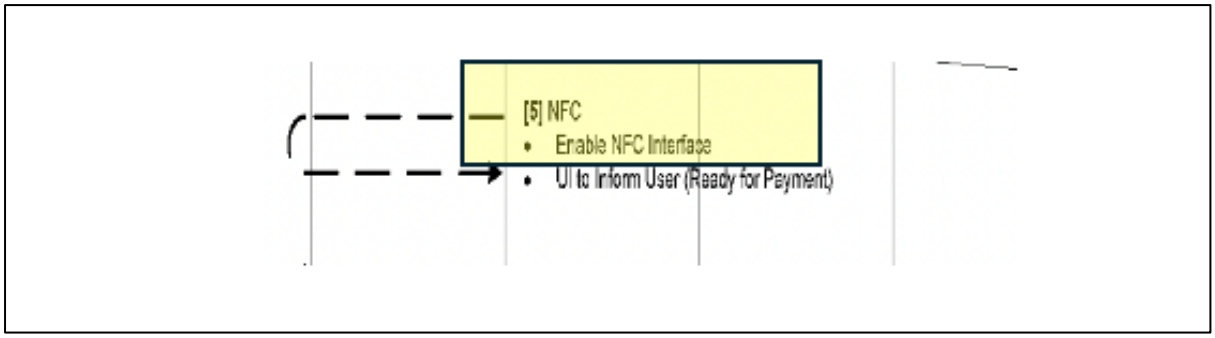
As modified by Aabye, Collinge teaches a pre-set time duration for the payment transaction to take place once the user has placed their device by the point of sale terminal with their finger on the biometric sensor (*successful priming action*). *Dec.*, ¶316. *See* Claim 8(b).



'248 Provisional, Fig. 14. (excerpt).

5. Claim 13(e):

Collinge teaches *disabling a device priming operation responsive to completing a transaction* since the NFC interface has to be enabled for a subsequent transaction. *Dec.*, ¶317.



'248 Provisional, Fig. 14 (excerpt).

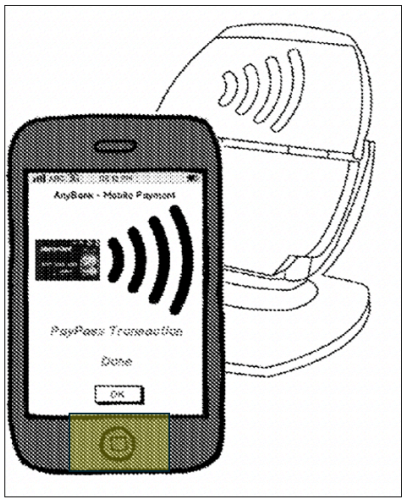
XI. GROUND 7: *COLLINGE* IN VIEW OF LIN, PHILLIPS, AABYE, PISULA AND FADELL

1. Claim 14(a):

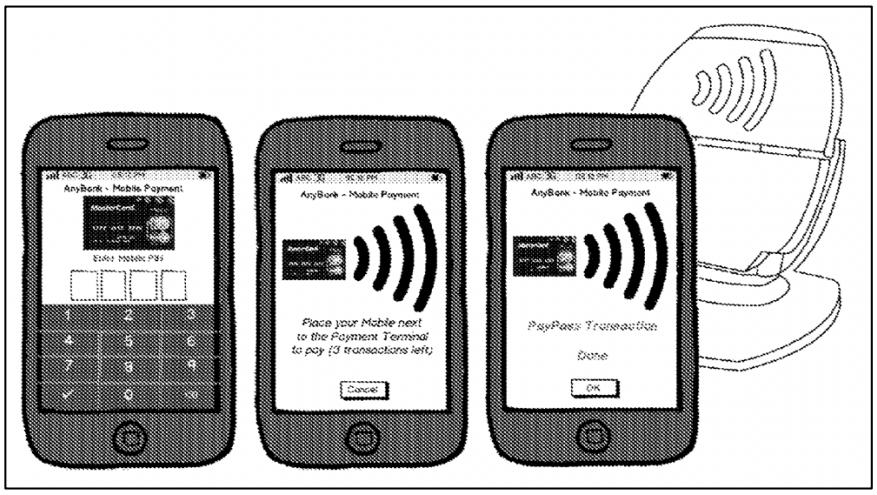
Collinge in view of Fadell teach a biometric sense of a touch contact of a valid user's skin on a touch ID button of the electronic device before Collinge would enter a PIN (priming operation) and bring Collinge's mobile device within proximity of an NFC recipient (which may form part of a priming operation).

(a) Collinge's Teachings

Collinge's mobile device already receives a "biometric identifier" to verify a user. *Collinge*, [0143]. As shown below Collinge's mobile device has a button. *Dec.*, ¶¶317-321.



'098 Provisional, 99 (excerpt); *'248 Provisional,* Fig. 2A-B; *Collinge*, Fig. 1. Collinge teaches the user of the mobile device inputs PIN into mobile device and then receives a notification on the display: "Place your Mobile next to the Payment Terminal to pay…"

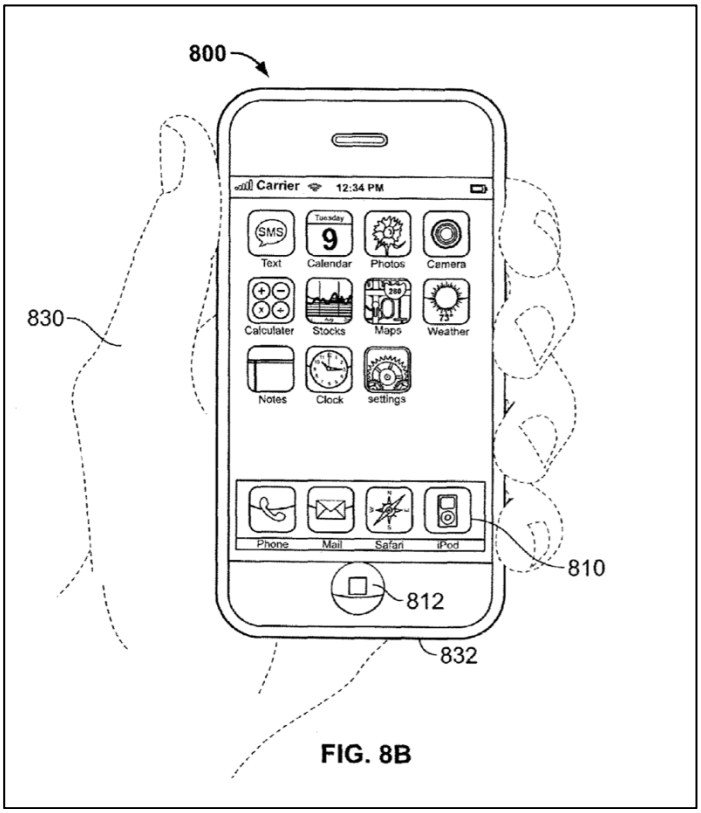


'098 Provisional, 99. A POSITA would have understood that input of "a mobile personal identification number (PIN)" is a *priming operation* because after the PIN

is input, the mobile device is primed to perform a payment transaction. *Collinge,* [0133]. *Dec.*, ¶321.

(b) Fadell's Teachings

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].

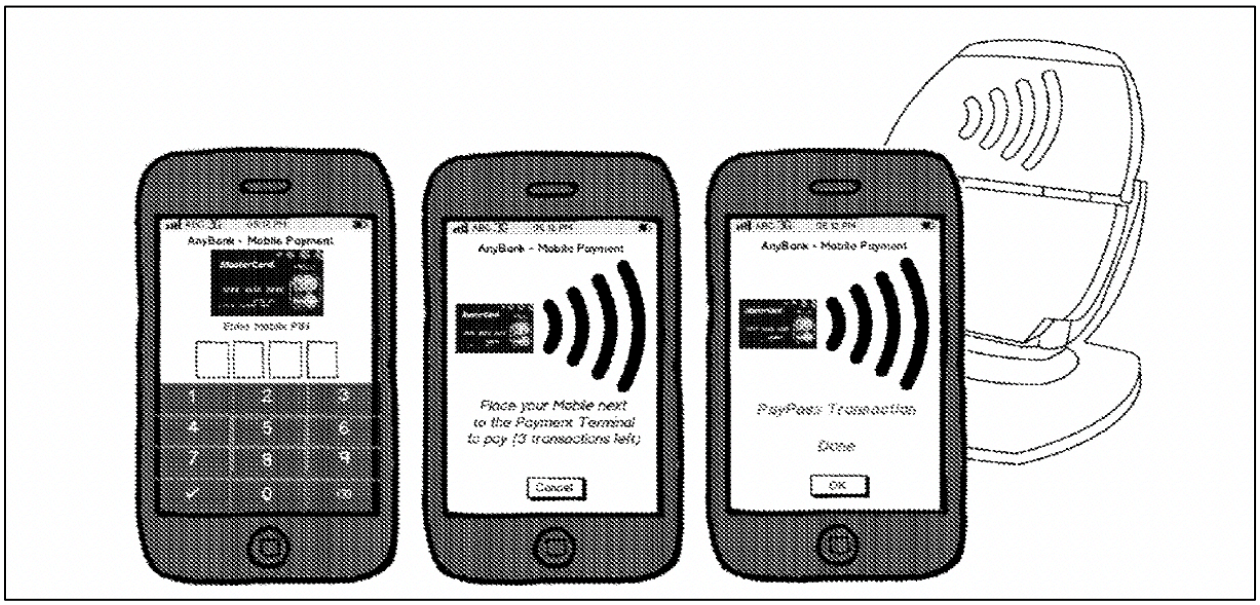


Fadell, Fig. 8B.

(c) Motivation to Combine

A POSITA would have been motivated to modify Collinge's button to be a fingerprint sensor used to authenticate a user based on the teachings of Fadell. *Dec*., ¶¶318-326.

Collinge already teaches a user supplying a "biometric identifier" for authentication purposes. *Collinge*, [0143]. A POSITA would have understood that the button on Collinge's mobile device 104 would be used to sense a user's fingerprint. *Dec*., ¶320. A POSITA would have understood that using Fadell's teachings of authenticating a user via a fingerprint sensor 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. *Dec*., ¶¶323-325. A POSITA would have been motivated to ask for a user's fingerprint before Collinge's process for prompting a user to "Place your Mobile next to the Payment Terminal to pay…" such as an initial step in Collinge's payment process.



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

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. *Dec*., ¶325. The modification is straightforward and would have merely required incorporating a fingerprint sensor behind the button on the bottom of Collinge's mobile device, since Collinge already discloses being able to accept a "biometric identifier." *Dec*., ¶326. Fingerprint sensors were a well-known feature of mobile devices prior to the time of the alleged invention, and a POSITA would have had the necessary skill set to incorporate a fingerprint sensor into Collinge's mobile device without any undue experimentation. *Dec*., ¶326.

2. Claim 14(b):

See Claim 1(a).

3. Claim 14(c):

See Claim 13(a)-(d).

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

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

XIII. 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

XIV. 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 '579 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.).

The '579 patent was previously the subject of an *Inter Partes* Review petition in *Samsung Electronics Co., Ltd., v. CardWare Inc.*, IPR2023-00196, which is no longer pending.

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

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

Lead Counsel	Back-Up Counsel
Adam Seitz (Reg. No. 52,206) Adam.seitz@eriseip.com PTAB@eriseip.com Postal and Hand-Delivery Address: 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 Postal and Hand-Delivery Address: ERISE IP, P.A. 7015 College Blvd., Suite 700 Overland Park, Kansas 66211 Telephone: (913) 777-5600 Fax: (913) 777-5601

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

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

APPENDIX OF EXHIBITS

Exhibit 1001	U.S Patent No. 10,810,579 ("*'579 Patent*")
Exhibit 1002	File History of the '579 Patent ("'579 *File History*")
Exhibit 1003	Declaration of Dr. Clifford Neuman ("*Dec.*")
Exhibit 1004	U.S. Patent Publication No. 2013/0262317 to Collinge et al. ("*Collinge*")
Exhibit 1005	U.S. Provisional Patent Application No 61/619,095 to Collinge et al. ("*'095 Provisional*")
Exhibit 1006	U.S. Provisional Patent Application No 61/635,248 to Collinge et al. ("*'248 Provisional*")
Exhibit 1007	U.S. Provisional Patent Application No 61/735,383 to Collinge et al. ("*'383 Provisional*")
Exhibit 1008	U.S. Provisional Patent Application No 61/762,098 to Collinge et al. ("*'098 Provisional*")
Exhibit 1009	U.S. Patent Appl. No. 2009/0307132 to Phillips ("Phillips")
Exhibit 1010	U.S. Patent Publication No. 2010/0125508 to Smith ("*Smith*")
Exhibit 1011	U.S. Patent Publication No. 2010/0217709 to Aabye, et al. ("*Aabye*")
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 No. 8,341,557 to Pisula ("*Pisula*")
Exhibit 1015	U.S. Patent Publication No. 2009/0083850 to Fadell ("*Fadell*")
Exhibit 1016	CardWare Inc.'s Preliminary Proposed Claim Constructions
Exhibit 1017	CardWare's Opening Markman Brief in Civil Action No. 2:22-cv-00141-JRG-RSP
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 ™ 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_Approved_Mobile_Devices.pdf, [https://web.archive.org/web/20120906234255/http://www.mastercard-mobilepartner.com:80/docs/MasterCard_Approved_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	U.S. Patent No. 7,740,168 to Hammad et al. ("Hammad")
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	Ashis K. Mahapatra, Touch Screen Systems, Orissa Review (2005), https://magazines.odisha.gov.in/orissareview/jun2005/engpdf/touch_screen_system.pdf ("Mahapatra")
Exhibit 1042	U.S. Patent Publication No. 2006/0097991 to Hotelling et al. ("Hotelling")
Exhibit 1043	iPhone User Guide, 2009, ("iPhone")
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")
Exhibit 1050	1747.09 Printing credit or debit card receipts; restrictions, CA CIVIL, January 2009 ("CA CIVIL")
Exhibit 1051	TPM MOBILE with Trusted Execution Environment for Comprehensive Mobile Device Security, June 2012, ("TPM")

CLAIM LISTING APPENDIX
U.S. Patent No. 10,810,579 for Claims 1-23

Claim Designation	Claim Language
Claim 1(Pre)	1. A method of performing a transaction, the method comprising:
Claim 1(a)	receiving an input at an electronic device, wherein the input corresponds to a priming operation of the electronic device by an identified user
Claim 1(b)	and wherein the electronic device comprises: a processor;
Claim 1(b)(1)	a touch screen display coupled to the processor; and;
Claim 1(b)(2)	a near field communications (NFC) interface coupled to the processor;
Claim 1(c)	receiving a request for a transaction payment at said electronic device via the NFC interface;
Claim 1(d)	displaying, on the touch-screen display, images of: a card issuer payment method selection, including a last 4-digit partial number of a card issuer supplied account number of a payment card; a card logo; and other iconography of the payment card;
Claim 1(e)	generating, by the processor, a limited-use payment information, and using said limited-use payment information in place of said card issuer supplied payment information;
Claim 1(f)	transmitting said limited-use payment information from said electronic device to an NFC recipient of the transaction via said NFC interface; and
Claim 1(g)	visually conveying a status of said transaction via a user-interface displayed on said touch-screen display.
Claim 2	2. The method of claim 1, wherein the generating the limited-use payment information utilizes at least one information from a set of information comprising: a device transaction sequence counter; a device account number; device secret keys; card issuer keys; merchant information; NFC recipient information; payment reader information; a time; a timestamp; an amount; a location; an online location; transaction information; payment information; device information; user information; an email address; and a user identification entry.
Claim 3	3. The method of claim 1, further comprising: dynamically generating a cryptogram number for use by the electronic device in place of a card validation value originated from the card issuer, and

Claim Designation	Claim Language
	wherein the dynamically generating the cryptogram number comprises cryptographically combining a device transaction sequence counter count and at least one information of a set of information comprising: a device account number; device identifiers; device secrets; device keys; payment issuer secrets; payment issuer keys; user information; a time; and transaction information; and wherein further, said dynamically generating the cryptogram number results in a one-time limited-use number via the device incrementing said device transaction sequence counter count on a transaction.
Claim 4(Pre)	4. The method of claim 1, wherein a limited-use number comprises a device account number,
Claim 4(a)	and wherein the device account number is of a limited time-duration of valid use, and wherein further a card issuing authority provides said device account number for use only by the electronic device, in place of card issuer information in performing payment transactions by the electronic device,
Claim 4(b)	and further comprising: performing payment transactions by the electronic device including the limited-use number;
Claim 4(c)	combining the limited-use number and said device account number within a device generated payment information; and
Claim 4(d)	conveying said device generated payment information, in place of card issuer information, when the device is performing payment transactions.
Claim 5(a)	5. The method of claim 1, further comprising: generating a limited-use security number for use in place of a card issuer card security code by cryptographically combining information from at least one of a set of information comprising: user information; an internet address; an email address; a device transaction sequence counter; a device account number; device identifiers; device secrets; device keys; issuer secrets; issuer keys; a payment card account number; a payment card security code; a time; an expiration date; an amount; a merchant locality; transaction information;
Claim 5(b)	and displaying the limited-use security number on the user-interface of the display.
Claim 6	6. The method of claim 1, wherein a payment processing authority verifies a limited-use number based on at least one information of

Claim Designation	Claim Language
	the set of information comprising: a transaction sequence count information; a device account number; user account information; issuer secrets; issuer keys; issuer-provided device keys; transaction information; and a time of use, and further comprising: authorizing said transaction, by the payment processing authority, responsive to verifying a valid limited-use number appearing in place of card issuer information; and rejecting a limited-use number, by the payment processing authority, on at least one unverifiable condition, of a set of unverifiable conditions comprising: an invalid number generation; an invalid device account number; a use outside of a valid time window; an invalid re-use of a limited-use number; and an invalid use of an expired limited-duration number.
Claim 7	7. The method of claim 1, wherein the receiving an input at an electronic device comprises receiving an input via a user interface from one of the set of user interfaces comprising: a device button; a device touch-screen interface; a device touch ID button interface; a device optical sensor array; a device skin touch sensor; a skin-contact sensor; a device motion detection interface; a device biometric sensor interface; and a device user-interface selection.
Claim 8(a)	8. The method of claim 1, wherein the priming operation comprises one operation of the set of operations comprising: a button press; a touch ID button press; a button double-press; a touch ID sensor touch; a touch-screen touch; a touch-input sequence; a gesture or swipe over a sensor-array; a skin-contact sense; an optical-sensor array sense; an optical-sensor array sense; an electronic device tap; a sequence of motions of the electronic device; a user-interface selection of a payment method; and a user-interface selection initiating a payment-operation;
Claim 8(b)	and, further comprising enabling the electronic device for payment via successfully completing at least one of a set of user-validations comprising: a touching from an identified valid user; a user entry of a valid passcode; a user entry of a valid PIN; swiping of a recognized user skin over a device sensor array; a correct user swiping or gesturing on the electronic device; a correct sequence of user taps on the electronic device; a correct user sequence of user motioning of the electronic device; a skin-contact sensing of an identified user; a device biometric sensing of a valid user identity;

Claim Designation	Claim Language
	and a device biometric sensing the electronic device is continuously remaining in the proximity possession of a valid user.
Claim 9(a)	9. The method of claim 1, further comprising: obtaining, by the electronic device, a user payment approval, through at least one device user interface of a set of interfaces comprising: a device display interface; a device touch-screen display interface; a device touch interface; device input buttons; device key-pad inputs, a device optical sensor array; a device motion detection unit; a device accelerometer; a device biometric user-sensor; and a device biometric sensing the electronic device is continuously remaining in the proximity contact of a valid user; and
Claim 9(b)	displaying, on the display, at least one information of a set of information comprising: a priming status of the electronic device for payment; a default payment method; a plurality of selectable payment accounts; a payment request; transaction information; a payment amount; a merchant identification; a time; an expiration date; a location; an account balance; a payment bank logo; a card image; a payment card issuer icon; a payment card network icon; the last 4-digits of the primary account number; the last 4-digits of the device account number; and other payment iconography; and
Claim 9(c)	receiving a user input of at least one user action, from a set of actions comprising: a payment method selection; a payment approval authorization; a payment denial; and an adjustment of a transaction payment.
Claim 10	10. The method of claim 1, further comprising: activating an NFC communication for a limited duration of time responsive to the electronic device priming; and responsive to the preset duration being exceeded, terminating the NFC communications and aborting the transaction.
Claim 11	11. The method of claim 1, further comprising completing the transaction on the electronic device, wherein the completing further comprises: receiving an authorization input on the electronic device from a valid device user, in response to at least one of a set of exceptional conditions comprising: the electronic device leaving the proximity of the NFC recipient; the incomplete identifying of a valid device user; the electronic device leaving the user's possession; the electronic device leaving the proximity contact of

Claim Designation	Claim Language
	the user; the electronic device leaving the grasp of the user; a biometric sensing the electronic device leaving the possession of a user since a last user validation; the transaction exceeding a pre-set amount limit; the transaction interval exceeding a pre-set time duration; a card issuing authority requesting a security check; and presenting the user with at least one of a set of selectable options comprising: requesting a transaction payment; continuing with the default payment method; selecting an alternate payment account; inputting an approval authorization; inputting a transaction denial; and inputting an adjustment of the transaction payment.
Claim 12(a)	12. The method of claim 1, further comprising: subsequent to the priming operation, offering a user selection of payment options for user input selection by presenting a selection of payment options in graphical format on said touch-screen display, including at least one of: a last four digits of a payment account number portion; a last four digits of a device account number portion; an expiration date; a card issuer icon; a bank logo; a card processing network logo; a card image; a card payment network icon; graphical images associated with the payment account; accepting a user input selection of a payment option, from said payment options, via said touch-screen display; and
Claim 12(b)	proceeding with a default payment option in said device payment transaction responsive to a user not selecting any of said payment options.
Claim 13(a)	13. A method of claim 1, wherein the priming operation comprises: a button double press; and a biometric sense of the device continuously remaining in the proximity contact of a valid user, since a last validation; and further comprising:
Claim 13(b)	denying the priming operation for payment when the electronic device is not sensed as being continuously within the proximity contact of a valid user, until after successfully re-validating a user; and wherein re-validating a user requires a correct user passcode re-entry;
Claim 13(c)	disabling a device priming operation on further button pressing;
Claim 13(d)	disabling a payment priming operation after the expiration of a pre-set time duration from a successful priming action; and

Claim Designation	Claim Language
Claim 13(e)	disabling a device priming operation responsive to completing a transaction.
Claim 14(a)	14. A method of claim 1, wherein the priming operation is input after at least one of: a biometric sense of a touch contact of a valid user's skin on a touch ID button of the electronic device,
Claim 14(b)	and validating a user passcode entry on the touch-screen display of the electronic device;
Claim 14(c)	disabling a device priming operation on further button pressing; disabling a payment priming operation after the expiration of a pre-set time duration from a successful priming action; and disabling a device priming operation responsive to completing a transaction.
Claim 15(Pre)	15. A method of performing a transaction, the method comprising:
Claim 15(a)	receiving an input signal at an electronic device, the input signal corresponding to a request for payment of a transaction at said electronic device, via a recipient proximity communication request to an NFC interface of the electronic device;
Claim 15(b)	displaying a summary of selectable payment account options at a touch-screen display user-interface of the electronic device;
Claim 15(c)	receiving, from a valid device user, a payment selection and approval authorization input on the electronic device;
Claim 15(d)	generating a limited-use number at said electronic device, and using said limited-use number in place of at least a portion of selected account issuer payment information; and
Claim 15(e)	transmitting said limited-use number from said electronic device to a transaction recipient via the NFC interface;
Claim 15(f)	obtaining a user payment approval through at least one user-interface of the electronic device, of a set of user-interfaces comprising: a touch-screen interface of the touch-screen display user-interface;
Claim 15(g)	a touch ID button; input buttons; a touch key-pad; an optical sensor array; a sensor array operable to recognize a swiping of a recognized user skin over the sensor array; a motion detection unit; an accelerometer;
Claim 15(h)	a device biometric sensor operable to determine the electronic device continuously remains in contact with a valid user while the electronic device is coming within proximity contact of an NFC recipient;

Claim Designation	Claim Language
Claim 15(i)	displaying on said display at least one of a set of information comprising: transaction information; merchant information; a time; a location of the transaction; a payment bank logo; a card issuer icon; a payment card image; an amount; and
Claim 15(j)	receiving a user input providing for at least one transaction action, from a set of actions comprising: approving a transaction; denying a transaction; and adjusting a transaction.
Claim 16(Pre)	16. The method of claim 15, further comprising: visually conveying on the touch-screen display user-interface, information regarding the transaction, including at least one of: a payment amount requested; an indication requesting an authorization input; an indication of an authorization success; an indication of an authorization failure; an option to retry a transaction; an option to retry a user authorization; an option to retry validating a user identity; an indication of a payment successfully completed; an indication of a payment failure; and an indication of a payment retry option.
Claim 17	17. The method of claim 15, further comprising: visually presenting on the touch-screen display user-interface, a plurality of payment options, including at least one of a set of payment method information for each payment option, the set comprising: a card image; a payment issuer logo; partial payment account numbers; a card payment network icon; a graphical image-encoding of a users payment account information; an amount of currency; an account balance; a credit limit; an amount of remaining credit; an amount of cryptocurrency; a cryptocurrency server network; and receiving a user-selection of a payment method for a transaction via said touch-screen display user-interface.
Claim 18	18. The method of claim 15, further comprising: receiving a priming operation at the electronic device for priming the electronic device for imminent payment, wherein the priming operation causes the electronic device to successfully identify the user through completing at least one user-validation, of a set of user validations comprising: a touching of the device by an identified user; a user entry of a valid passcode; a user entry of a valid PIN; a swiping of a recognized user skin over a sensor array of the electronic device; a correct user swiping or gesturing on a touch sensor array of the electronic device; a correct sequence of user taps on the electronic

Claim Designation	Claim Language
	device; a correct user sequence of user motions of the electronic device; a skin-contact sense of a valid user; and a device biometric recognition of a valid user.
Claim 19(Pre)	19. An electronic device comprising:
Claim 19(a)	at least one processor;
Claim 19(b)	a memory coupled to the at least one processor; a display operable to present a visual user-interface comprising device inputs;
Claim 19(b)(1)	display output;
Claim 19(b)(2)	a device input;
Claim 19(b)(3)	an NFC interface operable to receive a transaction request when in proximity to an NFC recipient;
Claim 19(c)	wherein the processor is operable to execute a program to implement a method comprising:
Claim 19(d)	accepting a priming action of the electronic device by an identified device user, from the device input;
Claim 19(e)	enabling the electronic device for imminent performance of a payment operation responsive to the priming action of a valid user;
Claim 19(f)	displaying a summary of selectable payment account options on the display;
Claim 19(g)	receiving a payment selection and approval authorization from a valid device user via the device input; and
Claim 19(h)	responsive to receiving an NFC transaction payment request, generating a limited-use payment information for use in place of card issuer payment information,
Claim 19(i)	wherein the NFC interface is operable to transmit said payment information from said electronic device to the NFC recipient of the transaction; and
Claim 19(j)	wherein further the processor is operable to cause the display to visually convey a status of the transaction.
Claim 20	20. The electronic device of claim 19, wherein the method further comprises: receiving the priming action of a valid user via the device input, wherein the device input comprises at least one of a set of device inputs comprising: a button; a touch ID button; a touch sensor array; a touch key-pad; a motion detection unit; an accelerometer; an optical sensor array; and identifying a valid

Claim Designation	Claim Language
	device user through an input detection, selected from at least one of a set comprising: a correct passcode entry sequence: a touch ID recognition of a known user; a biometric recognition of a valid user; a biometric sensing of a valid users skin; a biometric detection that the electronic device continuously remains in contact with a valid user; and receiving a correct user response input, from a security challenge presented on the display.
Claim 21	21. The electronic device of claim 19, wherein the memory is accessible to the processor, wherein said memory comprises a static device-specific device account number of limited-use that originates from a card issuing authority and is limited to use by the electronic device in place of a card issuer account information, wherein further said static device-specific device account number has an expiration date of limited duration of validity, and wherein the generating a limited-use payment information comprises the processor generating said limited-use payment information by combining said static device-specific device account number, said device account expiration date, when said issuer payment account method is selected.
Claim 22	22. The electronic device of claim 19, wherein the memory is accessible to the processor, and wherein said memory comprises: a static device-specific device account information including a device account number of limited-use; and keys, wherein said device-specific device account information originates from a card issuing authority and is for limited-use by the specific electronic device only; and wherein said static device-specific device account information is valid for a limited duration, and wherein the generating a limited-use payment information comprises the processor generating a one-time limited-use cryptogram number and combining said limited-use static device account information and said one-time use cryptogram number to produce the limited-use payment information.
Claim 23	23. The electronic device of claim 19 further comprising a cryptographic processor operable to dynamically generate a one-time limited-use cryptogram number by cryptographically combining of at least one information accessible on the electronic device, selected from a set comprising: a sequence counter; a device

Claim Designation	Claim Language
	account number; a device secret; device keys; card issuer keys; a time; an amount; an expiration date; a card security code; a location; merchant information; NFC recipient information; payment reader information; an online location; transaction information; payment information; device information; user information; an email address; a user identification entry; a hash of transaction information; and a hashed record of transactions, and wherein said cryptogram number is operable to be used in place of at least a portion of a card issuer payment information, in a payment transaction.

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 13,941 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 '579 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
(913) 777-5600 Telephone
(913) 777-5601 Facsimile

COUNSEL FOR PETITIONER