UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,

Petitioner

v.

CARDWARE INC.,

Patent Owner

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

DECLARATION OF DR. CLIFFORD NEUMAN

TABLE OF CONTENTS

I. INTRODUCTION ***24***
A. Educational Background and Professional Experience *24*
II. MATERIALS CONSIDERED ***27***
III. OVERVIEW AND LEGAL STANDARDS ***31***
A. Person of Ordinary Skill in the Art *31*
B. Obviousness *32*
C. Claim Construction *37*
D. Printed Subject Matter *38*
IV. LEVEL OF A PERSON OF ORDINARY SKILL ***38***
V. OVERVIEW OF THE '579 PATENT ***39***
A. Summary of the '579 Patent *39*
B. Field of Endeavor *40*
C. Problem Purportedly Solved by the Inventors of the '579 Patent *40*
D. File History of the '579 Patent *42*
VI. BACKGROUND OF TECHNOLOGY ***42***
A. The Evolution of Payment Cards *43*
1. Magnetic Stripe Cards 43
2. Smart/Chip Cards 46
3. Europay, MasterCard, and Visa (EMV) Standard 47
B. Contactless Payments *47*
1. Near Field Communications 47
2. Active Mode 49
3. Passive Mode 51
4. The Development of Near Field Communications 52
5. Contactless EMV Payment Cards 52
6. Mobile Devices and Mobile Wallets 53

7. Card Emulation Mode 56
C. Payment Credential Security Features *59*
1. Alternatives to a Payment Account Number (PAN) 59
2. Alternatives to Static Card Verification Values 62
VII. SUMMARY OF THE PRIOR ART REFERENCES....65
A. Collinge....*65*
1. Collinge is Analogous Art 68
2. Collinge is Prior Art 69
3. Support for Collinge in Collinge Provisionals 97
B. Lin *101*
1. Lin is Analogous....104
C. Smith *105*
1. Smith is Analogous....106
D. Kranzley *107*
1. Kranzley is Analogous....107
E. Phillips *109*
1. Phillips is Analogous 110
F. Aabye....*112*
1. Aabye is Analogous....113
G. Pisula *115*
1. Pisula is Analogous 116
H. Fadell *117*
1. Fadel is Analogous 118
VIII. SUMMARY OF UNPATENTABILITY....119
IX. OPINIONS REGARDING GROUND 1: COLLINGE, LIN, AND PHILLIPS....121
A. 1(Pre): "A method of performing a transaction, the method comprising:" *121*

B. 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" 124

C. 1(b): "and wherein the electronic device comprises a processor;" 132

D. 1(b)(1): "a touch screen display coupled to the processor; and;" 132

E. 1(b)(2): "a near field communications (NFC) interface coupled to the processor;" 138

F. 1(c): "receiving a request for a transaction payment at said electronic device via the NFC interface;" 144

1. Collinge's Teachings 144
2. Lin's Teachings 145
3. Motivation To Combine 146

G. 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;" 149

1. Collinge's Teachings 149
2. Phillips' Teachings 152
3. Motivation to Combine 154
4. Lin's Teachings 156
5. Motivation to Combine 157

H. 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;" 159

I. 1(f): "transmitting said limited-use payment information from said electronic device to an NFC recipient of the transaction via said NFC interface; and" 167

J. 1(g): "visually conveying a status of said transaction via a user-interface displayed on said touch-screen display." 168

K. *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… and a user identification entry."* 171

L. *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 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[…]: payment issuer secrets; 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.* 174

M. *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 touch-screen interface…:*.....178

N. *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."* 178

O. *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 transaction exceeding a pre-set amount limit; the transaction interval exceeding a pre-set time duration […] presenting the user with at least one of a set of selectable options comprising: […]requesting a transaction payment; selecting an alternate payment account; inputting a transaction denial"[…]* 182

1. Collinge's Teachings 182

2. Phillips' Teachings 184

3. Motivation to Combine....184

P. 12(a): "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: […]accepting a user input selection of a payment option, from said payment options, via said touch-screen display....186

Q. 12(b): "proceeding with a default payment option in said device payment transaction responsive to a user not selecting any of said payment options." 186

1. Motivation to Combine....186

R. 19(Pre): "An electronic device comprising:" 187

S. 19(a): "at least one processor;"....187

T. 19(b): "a memory coupled to the at least one processor;" 187

U. 19(b): "a display operable to present a visual user-interface comprising device inputs; 190

V. 19(b)(1): "display output;" 195

W. 19(b)(2): "a device input;"....196

X. 19(b)(3): "an NFC interface operable to receive a transaction request when in proximity to an NFC recipient;" 196

Y. 19(c): "wherein the processor is operable to execute a program to implement a method comprising:" 198

Z. 19(d): "accepting a priming action of the electronic device by an identified device user, from the device input;"....198

AA. 19(e): "enabling the electronic device for imminent performance of a payment operation responsive to the priming action of a valid user;"....199

BB. 19(f): "displaying a summary of selectable payment account options on the display;"....199

CC. 19(g): "receiving a payment selection and approval authorization from a valid device user via the device input; and" 199

DD. 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," *199*

EE. 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" *199*

FF. 19(j): "wherein further the processor is operable to cause the display to visually convey a status of the transaction." *199*

GG. 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 touch key-pad[…] and identifying a valid device user through an input detection, selected from at least one of a set comprising: a correct passcode entry sequence[…]: and receiving a correct user response input, from a security challenge presented on the display." *200*

HH. 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[…]; 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." *200*

X. OPINIONS REGARDING GROUND 2: COLLINGE IN VIEW OF LIN AND KRANZLEY ***202***

A. 5(a): "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: device secrets; issuer secrets;" *202*

B. 5(b): "and displaying the limited-use security number on the user-interface of the display." *202*

1. Motivation To Combine 203

C. 6: "The method of claim 1, wherein a payment processing authority verifies a limited-use number based on at least one information of the set of information comprising…a transaction sequence count information 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 and a use outside of a valid time window." 204

1. Collinge's Teachings 204

2. Kranzley's Teachings 206

3. Motivation to Combine.....207

XI. OPINOINS REGARDING GROUND 3: COLLINGE IN VIEW OF LIN, PHILLIPS, SMITH, AND KRANZLEY 209

A. 4(Pre): "The method of claim 1, wherein a limited-use number comprises a device account number," 209

1. Collinge's Teachings 210

2. Smith's Teachings 213

3. Motivation To Combine 216

B. 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," 223

1. Motivation to Combine.....223

C. 4(b): "and further comprising: performing payment transactions by the electronic device including the limited-use number;" 225

D. 4(c): "combining the limited-use number and said device account number within a device generated payment information; and" 227

1. Smith's Teachings 228

2. Motivation to Combine.....229

E. 4(d): "conveying said device generated payment information, in place of card issuer information, when the device is performing payment transactions.".....*230*

F. 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. *230*

G. 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.....*230*

XII. OPINIONS REGARDING GROUND 4: COLLINGE IN VIEW OF LIN PHILLIPS AND AABYE*.....*231

A. 8(a): "The method of claim 1, wherein the priming operation comprises one operation of the set of operations comprising…a touch-screen touch…a user-interface selection of a payment method; and a user-interface selection initiating a payment-operation;" *231*

1. '248 Provisional (Ex.1006), Fig. 2B. (annotated) 231

B. 8(b): "further comprising enabling the electronic device for payment via successfully completing at least one of a set of user-validations comprising: a user entry of a valid passcode; a device biometric sensing of a valid user identity; and a device biometric sensing the electronic device is continuously remaining in the proximity possession of a valid user.....232

1. Collinge's Teachings 232

2. Aabye's Teachings 232

3. Motivation to Combine.....234

C. 9(a): "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 touch-screen display interface....and a device biometric sensing the electronic device is continuously remaining in the proximity contact of a valid user; and".....237

D. 9(b): "displaying, on the display, at least one information of a set of information comprising… a card image; and other payment iconography".....237

E. 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".....238

XIII. OPINIONS REGARDING GROUND 5: COLLINGE IN VIEW OF LIN AND AABYE 239

A. 15(Pre):" A method of performing a transaction, the method comprising:".....239

B. 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;".....239

C. 15(b): "displaying a summary of selectable payment account options at a touch-screen display user-interface of the electronic device;".....240

D. *15(c): "receiving, from a valid device user, a payment selection and approval authorization input on the electronic device;".....240*

E. *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".....240*

F. *15(e): "transmitting said limited-use number from said electronic device to a transaction recipient via the NFC interface;".....240*

G. *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…" 240*

H. *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;" 240*

I. *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" 241*

J. *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." 241*

K. *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: an indication of a payment successfully completed." 241*

L. *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 users payment account information;…and receiving a user-selection of a payment method for a transaction via said touch-screen display user-interface."…….241*

M. 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 user entry of a valid passcode; and a device biometric recognition of a valid user." 241

XIV. OPINIONS REGARDING GROUND 6: COLLINGE IN VIEW OF LIN, PHILLIPS, AABYE AND PISULA 242

A. 13(a): " 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:.....242

1. Pisula's Teachings 242

2. Motivation to Combine.....242

B. 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;" 246

C. 13(c): "disabling a device priming operation on further button pressing;" 247

D. 13(d): "disabling a payment priming operation after the expiration of a pre-set time duration from a successful priming action; and" 247

E. 13(e): "disabling a device priming operation responsive to completing a transaction." 248

XV. OPINIONS REGARDING GROUND 7: COLLINGE IN VIEW OF LIN, PHILLIPS, AABYE, PISULA AND FADELL 249

A. 14(a): "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, ...249

1. Collinge's Teachings 249

2. Fadell's Teachings.....252

3. Motivation to Combine.....254

B. 14(b): "and validating a user passcode entry on the touch-screen display of the electronic device;".....257

C. 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." 257

XVI. CONCLUSION.....257

CLAIM LISTING

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 wherein the dynamically generating the cryptogram number

Claim Designation	Claim Language
	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

Claim Designation	Claim Language
	information of 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

Claim Designation	Claim Language
	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; 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

Claim Designation	Claim Language
	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 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

Claim Designation	Claim Language
	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 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 Designation	Claim Language
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 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 Designation	Claim Language
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 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 Designation	Claim Language
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 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

Claim Designation	Claim Language
	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 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.

I, Dr. Clifford Neuman declare the following:

I. INTRODUCTION

1. I have been retained by counsel for Petitioners as a technical expert in the above-captioned case. Specifically, I have been asked to render certain options regarding the IPR petition with respect to U.S. Patent No. 10,810,579 (the "'579 Patent"). I understand that the Challenged Claims are 1-22, and my opinions herein are limited to those claims. A true and correct copy of my Curriculum Vitae, which provides further details about my background and experience, is appended to this Declaration.

Educational Background and Professional Experience

2. My complete qualifications and professional experience are described in my *Curriculum Vitae*, a copy of which can be found in Appendix A. The following is a brief summary of my relevant qualifications and professional experience. I received a Ph. D. in Computer Science in 1992 and an M.S. in Computer Science in 1988 from the University of Washington, and an S.B. (Bachelor's) in Computer Science and Engineering in 1985 from the Massachusetts Institute of Technology.

3. Since receiving my doctorate, I have devoted my career to the field of distributed computer systems development and research with a significant portion of my experience in the area of electronic commerce and internet payments. I have

studied, taught, practiced, and researched in the field of computer science for over forty years.

4. I am currently an Associate Professor of Computer Science Practice in the Department of Computer Science at the University of Southern California (USC), where I have taught since 1992. I am also the Director of the Center for Computer Systems Security, an affiliated Scientist at USC's Information Sciences Institute, and I direct the Computer Security Curricula within the Data Science Program at USC. I teach and have taught numerous courses at USC, including advanced courses in computer science for upper-level undergraduates and graduate students, on topics such as distributed systems and computer and network security.

5. As part of my research at USC, I have worked in a number of areas, including research in distributed computer systems with emphasis on scalability and computer security, especially in the areas of authentication, authorization, policy, electronic commerce, and protection of cyber-physical systems and critical infrastructure such as the power grid. I have worked on the design and development of scalable information, security, and computing infrastructure for the Internet. I am also the principal designer of the Kerberos system, an encryption-based authentication system used among other things as the primary authentication method for most versions of Microsoft's Windows and for many other enterprise computer systems. I have also developed systems that used Kerberos as a base for more

comprehensive computer security services supporting authorization, audit, and electronic payments.

6. In addition to my academic experience, I have many years of practical experience designing computer security systems. For example, from 1985-1986, I worked on Project Athena at MIT, to produce a campus-wide distributed computing environment. I also served as Chief Scientist at CyberSafe Corporation from 1992-2001. I have designed systems for network payment which build upon security infrastructure to provide a secure means to pay for services provided over the Internet. For example, I designed the NetCheque and NetCash systems, which are suitable for micropayments (payments on the order of pennies where the cost of clearing a credit card payment would be prohibitive). In 2000 and 2001, I was on the advisory board for NetResearch Inc, d/b/a BayBuilder, which was a company developing online auction platforms.

7. As part of my research on improving authentication and the security of electronic commerce in the late 1990s, I was involved with the integration of smart cards and PCMCIA cryptographic processors into security services used by end-point computing devices such as personal computers. Also in the late 1990's I worked with the Financial Services Technology Consortium on their electronic check project.

8. I have authored or co-authored over 50 academic publications in the fields of computer science and engineering. In addition, I have been a referee or editor for the following academic journals: ACM Transaction on Information and Systems Security and International Journal of Electronic Commerce. My curriculum vitae includes a list of publications on which I am a named author. I am also a member of the IEEE, Association for Computer Machinery (ACM), and the Internet Society (ISOC), among others. I have also served as program and/or general chair of the following conferences: The Internet Society Symposium on Network and Distributed System Security and the ACM Conference on Computer and Communications Security.

II. MATERIALS CONSIDERED

9. I have relied upon my education, knowledge, and experience with payment systems, including mobile payment systems, as well as the other materials discussed in this declaration in forming my opinions.

10. In developing my opinions, I have considered the following materials:

Exhibit	Description
1001	U.S. Patent No. 10, 810, 579 (the "'579 Patent")
1002	File History of the '579 ("the '579 File History")
1004	U.S. Patent Publication No. 2013/0262317 to Collinge et al. ("*Collinge*")
1005	U.S. Provisional Patent Application No 61/619,095 to Collinge et al. ("*'095 Provisional*")
1006	U.S. Provisional Patent Application No 61/635,248 to Collinge et al. ("*'248 Provisional*")

1007	U.S. Provisional Patent Application No 61/735,383 to Collinge et al. ("*'383 Provisional*")
1008	U.S. Provisional Patent Application No 61/762,098 to Collinge et al. ("*'098 Provisional")*
1009	U.S. Patent Appl. No. 2009/0307132 to Phillips ("Phillips")
1010	U.S. Patent Publication No. 2010/0125508 to Smith ("*Smith)*")
1011	U.S. Patent Publication No. 2010/0217709 to Aabye et al. ("*Aabye*")
1012	WIPO International Publication No. WO 2010/039337 to Lin et al. ("*Lin*")
1013	U.S. Patent Publication No. 2010/0125509 to Kranzley et al. ("*Kranzley*")
1014	U.S. Patent No. 8,341,557 to Pisula et al. ("*Pisula*")
1015	U.S. Patent Publication No. 2009/0083850 to Fadell et al. ("*Fadell*")
1016	CardWare Inc.'s Preliminary Proposed Claim Constructions
1017	CardWare's Opening Markman Brief in Civil Action No. 2:22-cv-00141-JRG-RSP
1020	IBM, *The Magnetic Stripe*, IBM, https://www.ibm.com/history/magnetic-stripe. ("*IBM*")
1021	VEDAT COSKUN, NEAR FIELD COMMUNICATION: THEORY TO PRACTICE (John Wiley & Sons, 1st ed. 2012) ("*Coskun*")
1022	MAGTEK, MAGNETIC STRIPE CARD STANDARDS, (MagTek Inc. eds., 2011) ("*MagTek*")
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*")
1024	KLAUS FINKENZELLER, RFID HANDBOOK (John Wiley & Sons, 3rd ed. 2010) ("*Finkenzeller*")
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*")
1026	SMART CARD ALLIANCE, EMV AND NFC: COMPLEMENTARY TECHNOLOGIES THAT DELIVER SECURE PAYMENTS AND VALUE-ADDED FUNCTIONALITY (Smart Card Alliance, Inc. eds., 2012) ("*Smart*")

1027	U.S. Patent Publication No. 2012/0011058 to Pitroda et al. ("*Pitroda*")
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*")
1029	U.S. Patent Publication No. 2013/0054474 to Yeager ("*Yeager*")
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*")
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*")
1032	ALESSANDRO VIZZARRI ET AL., SECURITY IN MOBILE PAYMENTS (2013) ("*Vizzarri*")
1033	U.S. Patent Publication No. 2008/00110983 to Ashfield ("*Ashfield*")
1034	U.S. Patent Publication No. 2014/0310113 to Sengupta et al. ("Sengupta")
1035	U.S. Patent Appl. No. 2012/0169593 to Mak et al. ("Mak")
1036	U.S. Patent Appl. No. 2012/0148115 to Birdwell et al. ("Birdwell")
1037	U.S. Patent Appl. No. 2007/0076923 to Chiu et al. ("Chiu")
1038	U.S. Patent No. 7,740,168 to Hammad et al. ("Hammad")
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*")
1040	ANNIKA PAUS, NEAR FIELD COMMUNICATION IN CELL PHONES (2017) ("*Paus*")
1041	Ashis K. Mahapatra, *Touch Screen Systems*, ORISSA REVIEW

	(2005), https://magazines.odisha.gov.in/orissareview/jun2005/engpdf/touch_screen_system.pdf ("*Mahapatra*")
1042	U.S. Patent Publication No. 2006/0097991 to Hotelling et al. ("*Hotelling*")
1043	iPhone User Guide, 2009, ("iPhone")
1044	U.S. Patent No. 10,181,121 ("*Roberts*")
1045	U.S. Patent Publication No. 2013/0151292 to Van Deloo et al. ("*Deloo*")
1046	U.S. Patent Publication No. 2006/0186195 to Gray ("*Gray*")
1047	U.S. Patent Publication No. 2014/0006276 to Grigg et al. ("*Grigg*")
1048	Anup K. Ghosh & Tara M. Swaminatha, *Software Security and Privacy Risks in Mobile E-Commerce*, 44 CACM 51 (2001) ("*Ghosh*")
1049	U.S. Patent Appl. No. 2011/0140841 to Bona et al. ("Bona")
1050	1747.09 Printing credit or debit card receipts; restrictions, CA CIVIL, January 2009 ("CA CIVIL")
1051	TPM MOBILE with Trusted Execution Environment for Comprehensive Mobile Device Security, June 2012, ("TPM")

11. I have considered these materials from the viewpoint of a POSITA as of the priority date of the '579 Patent. For the purposes of this declaration, I have been asked to assume that the earliest priority date of the '579 Patent is March 15, 2013. I note that my opinions provided in this Declaration are made from the perspective of a POSITA as of this priority date of the '579 Patent unless expressly stated otherwise. To the extent that I use any verb tense in this Declaration that is present tense (e.g., "a POSITA would understand" instead of "a POSITA would have understood"), such verb tense should be understood to be my opinion as of the '579

Patent's priority date (again, unless expressly stated otherwise). I merely use the present verb tense for ease of reading.

III. OVERVIEW AND LEGAL STANDARDS

12. In formulating my opinions, I have been instructed to apply certain legal standards. I am not a lawyer. I do not offer any testimony regarding what the law is. Instead, the following sections summarize the law as I have been instructed to apply it in formulating and rendering my opinions found later in this declaration. I understand that, in an *inter partes* review ("IPR") proceeding, patent claims may be deemed unpatentable if it is shown that they are anticipated or rendered obvious in view of the prior art. I understand that prior art in an IPR review is limited to patents or printed publications that predate the priority date of the patent at issue. I understand that questions of claim clarity (definiteness) and enablement cannot be considered as a ground for considering the patentability of a claim in these proceedings.

Person of Ordinary Skill in the Art

13. I understand that the '579 Patent, the record of the proceedings at the Patent Office (which I understand is called the "File History" or "Prosecution History"), and the teachings of the prior art are evaluated from the perspective of a person of ordinary skill in the art ("POSITA"). I understand that the factors considered in determining the ordinary level of skill in the art may include: (i) the

levels of education of the inventor; (ii) the types of problems encountered in the art; (iii) prior art solutions to those problems; (iv) the rapidity with which innovations are made; (v) the sophistication of the technology; and (vi) the educational level of persons working in the field.

14. I understand that a person of ordinary skill in the art is not a specific real individual, but rather a hypothetical individual having the qualities reflected by the factors above. The hypothetical person is presumed to have the same level of skill as the typical practitioner of the art and is presumed to have knowledge of all prior art in the relevant field. I understand that the inventor's actual knowledge or lack of knowledge of prior art reference is irrelevant to the obviousness determination.

Obviousness

15. I understand that a claim may be invalid under 35 U.S.C. § 103(a) if the subject matter described by the claim as a whole would have been "obvious" to a POSITA in view of a single or combination of prior art references at the time the claimed invention was made. I further understand that a POSITA is assumed to know and to have all relevant prior art in the field of endeavor covered by the patent-in-suit and all analogous prior art. I understand that obviousness in an IPR review proceeding is evaluated using a preponderance of the evidence standard, which means that the claims must be more likely obvious than nonobvious.

16. I also understand that an obviousness determination includes the consideration of various factors including: (1) the scope and content of the prior art, (2) the differences between the prior art and the claim at issue, and (3) the level of ordinary skill in the pertinent art. I understand that secondary considerations of non-obviousness such as commercial success, long-felt but unresolved needs, failure of others, and so forth may be assessed as well. I have been informed that an obviousness analysis must focus on the state of the art at the time of the invention to avoid impermissibly using hindsight to invalidate a patent.

17. In considering whether certain prior art renders a particular patent claim obvious, I have been informed that I can consider the scope and content of the prior art, including the fact that a POSITA would regularly look to the disclosures in patents, trade publications, journal articles, conference papers, industry standards, product literature and documentation, texts describing competitive technologies, requests for comment published by standard setting organizations, and materials from industry conferences, as examples.

18. I have been informed that for a prior art reference to be proper for use in an obviousness analysis, the reference must be "analogous art" to the claimed invention. A reference is analogous art if: (1) the reference is from the same field of endeavor as the claimed invention (even if it addresses a different problem); or (2) the reference is reasonably pertinent to the problem faced by the inventor (even if it

is not in the same field of endeavor as the claimed invention). For a reference to be "reasonably pertinent" to the problem, it must logically have commended itself to an inventor's attention in considering the problem. In determining whether a reference is reasonably pertinent, one should consider the problem faced by the inventor, as reflected either explicitly or implicitly, in the specification. I believe that the documents I considered in forming my opinions in this IPR are well within the range of documents a POSITA would have consulted to address the type of problems described in the Challenged Claims.

19. I have been informed that to establish that a claimed invention was obvious based on a combination of prior art elements, an articulation of the reason(s) why a claimed invention would have been obvious must be provided. Specifically, I have been informed that the prior art, either as a single reference or a combination of multiple items of prior art, renders a patent claim obvious when there was an apparent reason for a POSITA, at the time of the invention, to combine or modify the prior art. Rationales for combining or modifying the prior art include, but are not limited to, any of the following: (A) combining prior art methods according to known methods to yield predictable results; (B) substituting one known element for another to obtain predictable results; (C) using a known technique to improve a similar device in the same way; (D) applying a known technique to a known device ready for improvement to yield predictable results; (E) trying a finite number of

identified, predictable potential solutions, with a reasonable expectation of success; (F) identifying that known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations are predictable to one of ordinary skill in the art; or (G) identifying an explicit teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine the prior art references to arrive at the claimed invention.

20. I have also been informed that where there is a motivation to combine, claims may be rejected as obvious provided a POSITA would have had a reasonable expectation of success regarding the proposed combination. I have also been informed that common sense may be considered. Common sense teaches that familiar items may have obvious uses beyond their primary purposes. I have been informed that if the combination was obvious to try (regardless of whether it was actually tried) or leads to anticipated success, then it is likely the result of ordinary skill and common sense rather than non-obvious innovation.

21. I have been informed that the existence of an explicit teaching, suggestion, or motivation to combine known elements of the prior art is a sufficient, but not a necessary, condition to a finding of obviousness. In determining whether the subject matter of a patent claim is obvious, neither the particular motivation nor the avowed purpose described in the patent-in-suit controls. I have been further

informed that the obviousness analysis may consider the effects of demands known to the technological community or present in the marketplace and the background knowledge possessed by a POSITA. These issues may be considered to determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent.

22. I have been informed that it is improper to combine references where the references teach away from their combination. A reference may be said to teach away when a POSITA, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the patent applicant. I have also been informed that a reference does not teach away if it merely expresses a general preference for an alternative invention but does not criticize, discredit, or otherwise discourage investigation into the invention claimed.

23. I am informed that even if a case of obviousness is established, the final determination of obviousness must also consider "secondary considerations" if presented. Secondary considerations include: (a) commercial success of a product due to the merits of the claimed invention; (b) a long-felt, but unsatisfied need for the invention; (c) failure of others to find the solution provided by the claimed invention; (d) deliberate copying of the invention by others; (e) unexpected results achieved by the invention; (f) praise of the invention by others skilled in the art; (g)

lack of independent simultaneous invention within a comparatively short space of time; and (h) teaching away from the invention in the prior art.

24. I have been further informed that secondary considerations evidence is only relevant if the offering party establishes a connection, or nexus, between the evidence and the claimed invention. The nexus cannot be based on prior art features. The establishment of a nexus is a question of fact. While I understand that Patent Owner here has not offered any secondary considerations at this time, I will supplement my opinions should Patent Owner raise secondary considerations during the course of this proceeding.

Claim Construction

25. I understand that the claim terms in an IPR proceeding are construed according to their plain and ordinary meaning as understood in light of the claim language, the patent's description, and the prosecution history viewed from the perspective of a POSITA. I further understand that where a patent defines claim language, the definition of the patent controls, even if there are other definitions that might be understood by those working in the art. I have applied these principles when interpreting the Challenged Claims and in rendering the opinions provided in this declaration.

26. I understand that Petitioner does not assert that any claim terms require express construction for purposes of this IPR.

Printed Subject Matter

27. I have been informed and understand that limitations that are directed to the presence or absence of printed matter are not entitled to patentable weight if the printed matter has no functional or structural relationship to the associated physical substrate.

IV. LEVEL OF A PERSON OF ORDINARY SKILL

28. Based on my review and analysis of the '579 Patent, the cited prior art, and the ordinary skill factors described in this section, a POSITA in the field of the '579 Patent at the time of the earliest possible priority date (March 15, 2013) would have been knowledgeable regarding the field of payment processing and digital authentication. In my experience in this field, most workers of ordinary skill in the art as of the earliest possible priority date of March 15, 2013 would have had at least 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 such as NFC. Additional industry experience or technical training may offset less formal education, while advanced degrees or additional formal education may offset lesser levels of industry experience. When I refer to the understanding of a POSITA, I am referring to the understanding of such a person as of March 15, 2013.

29. As of March 15, 2013, I had more than ordinary skill in the art. I am, however, familiar with the skills and knowledge possessed by those I would have considered to be of ordinary skill in the art as of that date.

30. My opinions provided in this declaration would not change in view of minor modifications to this level of ordinary skill.

V. OVERVIEW OF THE '579 PATENT

Summary of the '579 Patent

31. 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), 2:13-17. The '579 Patent also describes "generating a limited-duration credit card number…which is limited in scope to a predetermined number of authorized transactions." *'579 Patent* (Ex. 1001) at 2:24-28. The '579 describes "a user that has "primed" the credit card device 201 b for a transaction has already performed a security authentication on the card, and therefore a subsequent card transaction is able to be pre-authorized to perform the transaction without further user authentication steps." *'579 Patent* (Ex. 1001), 11:34-42. The '579 describes a "priming action can be a tap of the credit card device 201 b detected by accelerometers 235, or a gesture, swipe, or a key input received by touch sensor array 245." *'579 Patent* (Ex. 1001), 11:34-42.

Field of Endeavor

32. I have been informed that the field of endeavor of the claimed invention can be determined by reference to explanations of the invention's subject matter in the patent application, including the embodiments, function, and structure of the claimed invention.

33. The '579 Patent defines the "Field of the Invention" as relating to "electronic or smart multi-function electronic devices and, more specifically, to more secure, smart multi-function electronic payment card and device systems and transaction processing thereof." *'579 Patent* at 1:23-27. After reviewing the '579 Patent, it is my option that a POSITA would understand that the field of endeavor of the '579Patent includes more secure payment cards, devices and systems.

34. The '579 Patent's specification criticizes existing systems due to being "susceptible to theft and/or compromise" *'579 Patent* at 1:66-2:3 For these reasons, a POSITA would have understood that the '579 Patent is trying to solve the problem of providing payment solutions that limit opportunities for theft or compromise of payment credentials.

Problem Purportedly Solved by the Inventors of the '579 Patent

35. I have been informed that a prior art reference is "reasonably pertinent" if a POSITA would have consulted it and applied its teachings when faced with the

problem that the inventor was trying to solve. As such, I have been asked to analyze the ’579 Patent and determine the problem that the inventors were trying to solve.

36. The ’579 Patent notes that a concern with “credit cards presently available in the marketplace is that they can all be, in various ways, susceptible to theft and/or compromise” and therefore they “have security limitations.” *’579 Patent* at 1:62-64. The ’579 Patent also noted that “cards employing smart integrated circuit chips and RF technology are not in wide use at present because they are incompatible with existing credit card infrastructure, which still predominantly supports conventional plastic credit cards.” *’579 Patent* at 1:66-2:3. To solve these problems, the “Summary of the Invention” describes “multi-function electronic device capable of generating a programmed magnetic field of alternating polarity based on a speed of a card swipe” for the “purpose of emulating a standard credit card.” *’579 Patent* at 2:13-17. The “Summary of the Invention” further describes a method of performing a transaction that includes “generating…a limited duration credit card number.” *’579 Patent* at 2:23-28. Thus, a POSITA would understand that the ’579 Patent is directed to solving the problem of providing payment solutions that limit opportunities for theft or compromise of payment credentials.

File History of the ’579 Patent

37. I have reviewed the prosecution history for the ’579 Patent. The ’579 Patent claims priority to Provisional Application No. 61/794,891, filed March 15, 2013. The ’579 Patent faced one non-final rejection. *’579 File History* (Ex. 1002).

VI. BACKGROUND OF TECHNOLOGY

38. I was asked to briefly summarize the background of the prior art from the standpoint of a person having ordinary skill in the art prior to March 15, 2013. As explained below, a POSITA would have understood that the payment system features described in the ’579 Patent (including, for example, limited-use payment information, transaction sequence counts, device account numbers, and secrets) had long been a feature of payment systems that were developed by leading payment processors (including Mastercard and Visa) years before the earliest filing date of the ’579 Patent.

39. As described below, all of the hardware components and functionalities encompassed by the Challenged Claims were well-known to a POSITA in the industry prior to the invention of the ’579 patent.

40. The evolution of electronic payment systems can be traced back several decades, marked by key technological milestones that have transformed how financial transactions are processed. Early developments in this field centered on introducing magnetic stripe technology for payment card transactions. Before the

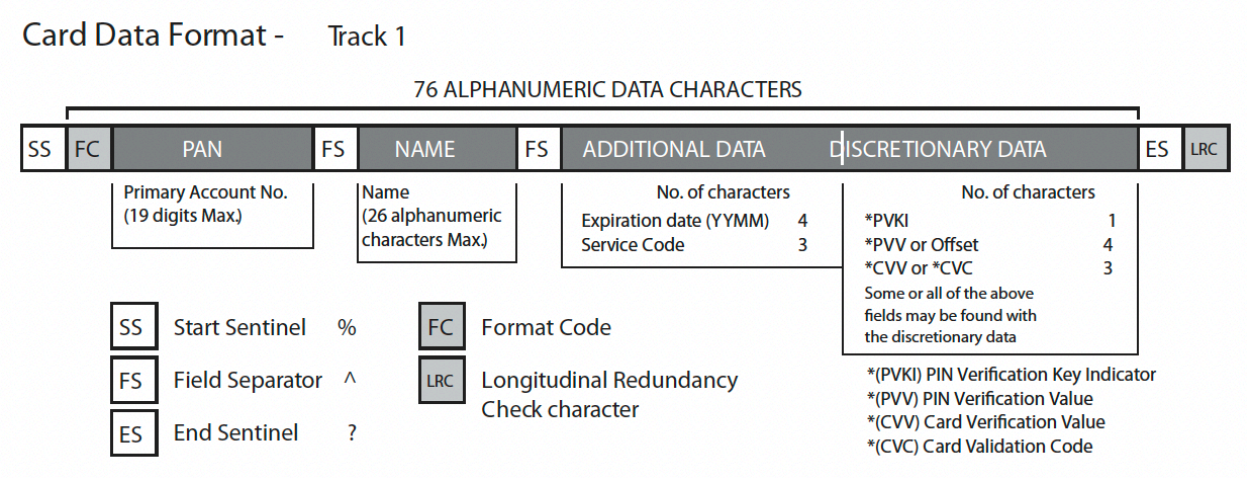
late 1960s, credit card transactions primarily consisted of "a tiny printing press to record raised letters and numbers from a card onto a form made of pressure-sensitive paper with carbon copies." *IBM (EX.1020)*, 1. However, this process was "insecure, slow, and prone to errors" therefore a need for magnetic stripe cards arose. *IBM (EX.1020)*, 1.

The Evolution of Payment Cards

1. *Magnetic Stripe Cards*

41. In the 1960s, "[t]he process of attaching a magnetic stripe to a plastic card was invented by IBM [.]" *Coskun (Ex.1021)*, 59. "A magnetic stripe card is one that contains a digital storage space where the data are loaded during the manufacturing phase. The stripe is made up of tiny magnetic particles in a resin. It is traditionally a read-only item. It is read by physical contact by swiping the card past a device with a magnetic reading head." *Coskun (Ex.1021)*, 6.

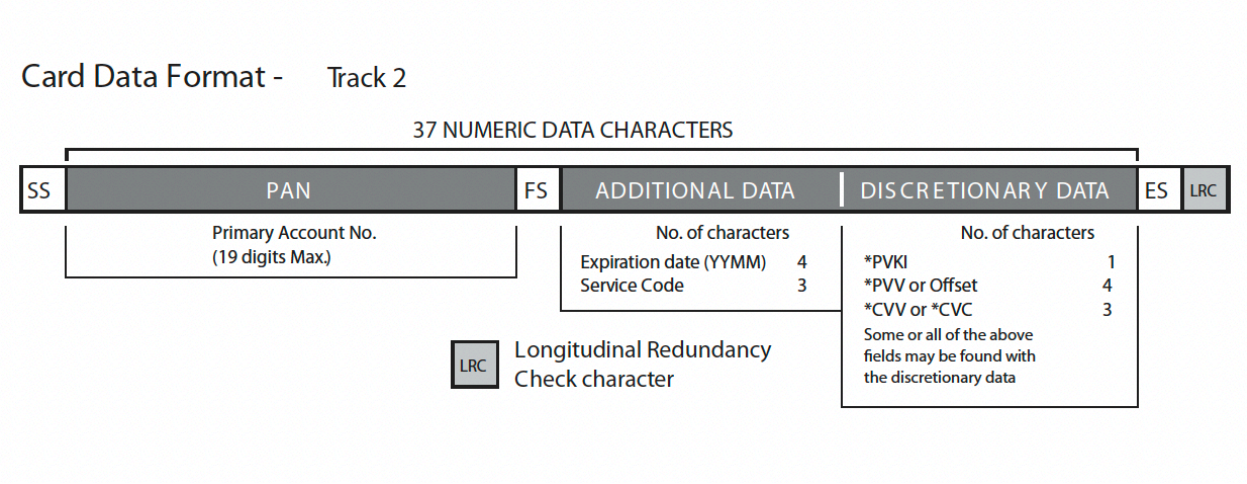
42. Data encoded on the back of the magnetic stripe is called track data such as what is defined in the with ISO/IEC 7813, 7810, and 7811. *Magtek (Ex.1022)*, 1. For example, track 1 data includes the following:



Magtek (Ex.1022), 1. On a card's track:

> "there is a Discretionary Data (DD) segment that allows for the issuer to include some relevant information to use in the transaction authorization process. The typical DD segment includes the static CVV (VISA) or CVC (MASTERCARD) values, which are allotted three characters. Replacing the three character CVV or CVC data with a three digit dynamic code (dCVV in Visa, Inc. terms, or CVC3 in MasterCard, Inc. terms), including the dCVV of CVC3 indicator character (e.g., a status flag indicating that dynamic data is present), and including a four character Application Transaction Counter value allows the card issuer to use a set of data unique to each transaction to authorize a transaction."

Bona, [0102]. Track 2 data includes the following data:



Magtek (Ex.1022), 1.

43. The mag stripe "approach that IBM had helped develop was adopted as a US standard in 1969 and as an international standard two years later, enabling mag stripe cards to be used anywhere in the world." *IBM (EX.1020), 1*. The global standardization of magnetic stripe cards paved the way for global adoption.

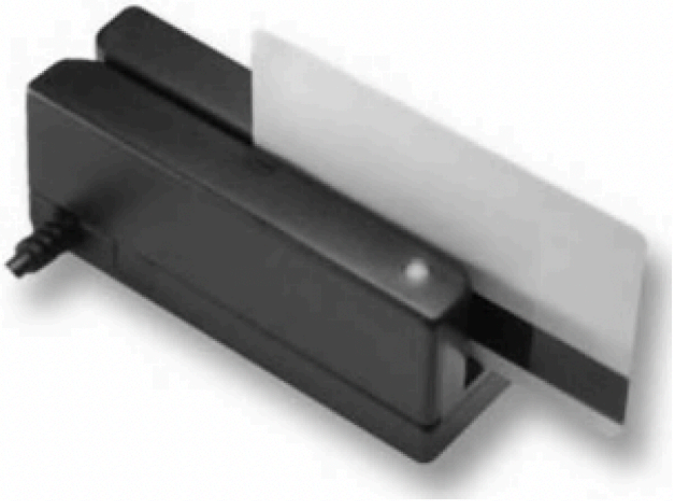


Figure 2.15 Magnetic stripe card.

Coskun (Ex.1021), Figure 2.15.

44. "In recent years, chip-enabled cards that encrypt cardholder data have begun to replace mag stripe cards, which carry static data directly in the magnetic stripe. However, demand for magnetic stripe cards remains strong because of their low cost, reliability and the huge, global installed base of card readers. And even though the job performed by magnetic stripes can now be done with chip cards and mobile phones, the global financial and transaction systems that thrive today are a legacy of the unassuming magnetic stripe." *IBM (EX.1020)*, 2.

2. Smart/Chip Cards

45. Smart cards were well known in the art all the way back to the "1970s." *Coskun (Ex.1021)*, 60. "The first mass use of the cards was for telephone payments in the 1980s. In the meantime, microprocessor smart cards were introduced. Microchips were integrated into debit cards in the 1990s. Smart card based electronic purse systems which store values on a card and do not need network connectivity, began to be used in Europe from the mid 1990s." *Coskun (Ex.1021)*, 60.

46. One major improvement "in smart card technology occurred in the 1990s; smart card based SIMs were introduced and started to be used in GSM based mobile phone environments in Europe. The use of smart cards increased with the ubiquity of mobile phones in Europe. In 1993, the international payment brands

Europay, MasterCard, and Visa (EMV) collaborated to develop new specifications for smart cards in order to use them in payments both as a debit and a credit card." *Coskun (Ex.1021)*, 60.

3. Europay, MasterCard, and Visa (EMV) Standard

47. The EMV standard established a global framework for secure, chip-based payment card transactions. It introduced dynamic data generation, such as cryptograms to prevent replay attacks and authenticate transactions securely. *EMV (EX.1023)*, 71-74 ("generation of the combined dynamic signature and Application Cryptogram"); *EMV (EX.1023)*, 74-77 ("Dynamic Signature Verification"); *EMV (EX.1023)*, 87-91 "generation of the Application Cryptograms (TC, ARQC, or AAC) generated by the ICC and the Authorisation Response Cryptogram (ARPC) generated by the issuer and verified by the ICC.") The EMV standard defined clear steps in the transaction process, including cardholder verification (e.g., PIN or signature). *See EMV (EX.1023)*, 81-86. The EMV standard laid the foundation for modern secure payments, including contactless and mobile EMV solutions.

Contactless Payments

4. Near Field Communications

48. Near Field Communication (NFC) "enables communication between an NFC enabled mobile phone at one end, and another NFC-enabled mobile phone, an NFC reader, or an NFC tag at the other end." *Coskun (Ex.1021)*, 1. In terms of

distance, "NFC is restricted to within very close proximity." *Coskun (Ex.1021)*, 1. This proximity is often "within 4 cm[.]" *Coskun (Ex.1021)*, 32.

49. Around 2006-2007, several companies began testing contactless NFC payments. For example, in April 2006, Visa conducted "the world's first mobile Visa payWave payment pilot" involving about "2000 merchants and 200 participants." *Coskun (Ex.1021)*, 341-342. As another example, HSBC partnered with MasterCard "tested the use of NFC enabled mobile handsets in payment." *Coskun (Ex.1021)*, 342. This "payment service was used where payment by contactless credit card and MasterCard PayPass was accepted. About 36 000 merchants accepted the MasterCard PayPass payment option at that time." *Coskun (Ex.1021)*, 342.

50. NFC has been used to facilitate contactless transactions in payment cards and mobile devices, enabling consumers to make payments simply by tapping their cards. *Smart (Ex.1026),* 7. NFC "technology is defined by the NFC Forum founded by Nokia, Philips, and Sony which allow communication based on RFID technology and ISO/IEC 14443 infrastructures." *Coskun (Ex.1021)*, 71.

51. For communication "between two NFC interfaces, the individual NFC interface can take on different functions, i.e. that of an NFC initiator (master device) or an NFC target (slave device). Communication is always started by the NFC initiator. In addition, NFC communication distinguishes between two different operational modes, the active and the passive mode." *Finkenzellller*, 57.

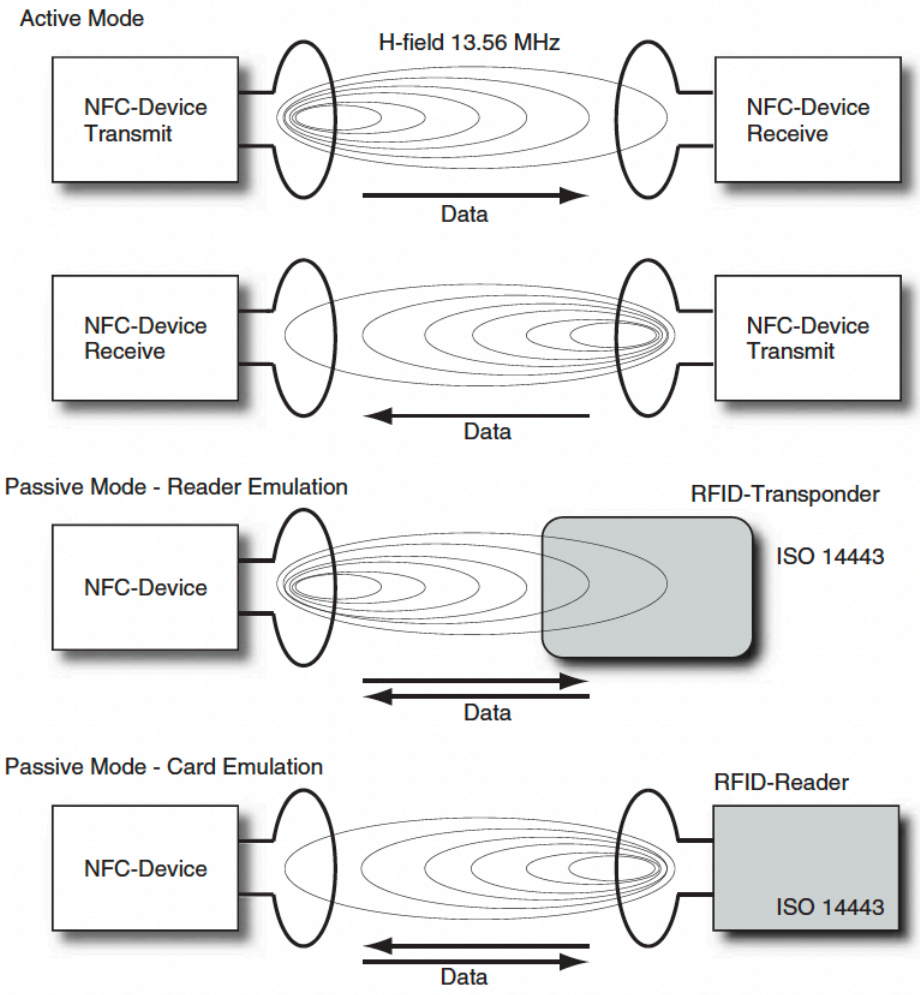


Figure 3.33 NFC distinguishes between three different operating modes: active mode (i); and passive mode in the operating modes reader emulation (ii); and card emulation (iii)

Finkenzelller, 58.

5. Active Mode

52. An NFC device, for example a mobile phone or payment card, can send information via NFC to another NFC interface. For example, "to transmit data between two NFC interfaces in active mode, at first one of the NFC interfaces activates its transmitter and thus works as the NFC initiator. The high-frequency

current that flows in the antenna induces an alternating magnetic field *H* which spreads around the antenna loop. Part of the induced magnetic field moves through the antenna loop of the other NFC interface which is located close by. Then a voltage *U* is induced in the antenna loop and can be detected by the receiver of the other NFC interface. If the NFC interface receives signals and the corresponding commands of an NFC initiator, this NFC interface automatically adopts the roll of an NFC target." *Finkenzelller*, 57.

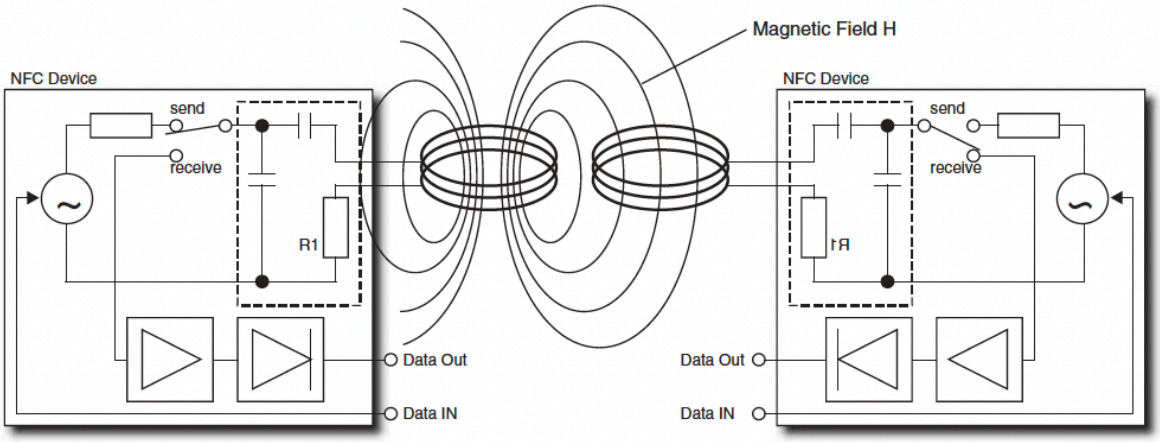


Figure 3.32 In active mode, the NFC interfaces alternately emit magnetic fields for data transmission

Finkenzelller, 58.

53. A mobile device or card is also able to receive an NFC request. For example, "[t]he transmission direction is reversed in order to send data from the NFC target to the NFC initiator. This means that the NFC target activates the transmitter and the NFC initiator switches to receiving mode. Both NFC interfaces

alternately induce magnetic fields where data is transmitted from transmitter to receiver only." *Finkenzelller*, 59.

6. Passive Mode

54. In passive mode "the NFC initiator induces a magnetic alternating field for transmitting data to the NFC target. The field's amplitude is modulated in line with the pulse of the data to be transmitted (ASK modulation). However, after having transmitted a data block, the field is not interrupted, but continues to be emitted in an unmodulated way. The NFC target now is able to transmit data to the NFC initiator by generating a *load modulation*. The load modulation method is also known from RFID systems." *Finkenzelller*, 59.

55. The NFC interface "that is the target is also able to establish, in addition to other NFC interfaces, the communication to compatible passive transponders (e.g. according to ISO/IEC 14443) that the NFC target supplies with power and that, via load modulation, can transmit data to the NFC interface. This option enables electronic devices equipped with NFC interfaces, such as NFC mobile phones, to read and write on different transponders such as smart labels or e-tickets. As the NFC interface in this case behaves similar to an RFID reader, this option is also called 'reader mode' or '*reader-emulation mode*'." *Finkenzelller*, 59.

56. If an NFC interface "is located close to a compatible RFID reader (e.g. according to ISO/IEC 14443), the NFC reader is also able to communicate with a reader. Here, the NFC interface adopts the roll of an NFC target and can transmit data to the reader using load modulation. This option enables RFID readers to exchange data with an electronic device with NFC interface, such as NFC mobile phones. From the reader's perspective, the electronic device behaves like a contactless smart card; this option is also called 'card mode' or '*card-emulation mode*'." *Finkenzelller*, 59.

7. The Development of Near Field Communications

57. Around 2006-2007, several companies began tested contactless NFC payments. For example, in April 2006, Visa conducted "the world's first mobile Visa payWave payment pilot" involving about "2000 merchants and 200 participants." *Coskun (Ex.1021)*, 341-342. As another example, HSBC partnered with MasterCard "tested the use of NFC enabled mobile handsets in payment." *Coskun (Ex.1021)*, 342. This "payment service was used where payment by contactless credit card and MasterCard PayPass was accepted. About 36 000 merchants accepted the MasterCard PayPass payment option at that time." *Coskun (Ex.1021)*, 342.

8. *Contactless EMV Payment Cards*

58. "From a contactless smart card technology perspective, the major progress was the agreement of Visa and MasterCard in 2004–2006 to implement

contactless payment and ticketing applications such as mass transit and highway tolls in the USA. With the introduction of contactless smart cards such as the MIFARE proximity smart card by Philips, contactless smart card applications started to have a considerable market share in Europe and the US." *Coskun (Ex.1021)*, 60. As an example, in 2006, Mastercard "worked with the Ohio Turnpike Commission to bring a consumer trail of *PayPass* payments" using "payment cards for self-service toll transactions." *PayPass (Ex.1025),* 1.

59. As of 2012, the typical contactless payment card working in the US were not EMV-compliant but instead utilized a NFC-enabled chip that transmitted the magnetic stripe data (MSD) included on the associated payment card along with a dynamic value or cryptogram to facilitate transactions. *Smart (Ex.1026),* 6.

9. *Mobile Devices and Mobile Wallets*

60. Mobile devices performing contactless payments were well known before the '579 Patent.

61. Around 2006-2008, several companies began testing mobile contactless NFC payments. As an example, HSBC partnered with MasterCard to test "the use of NFC enabled mobile handsets in payment." *Coskun (Ex.1021)*, 342. This "payment service was used where payment by contactless credit card and MasterCard PayPass was accepted. About 36 000 merchants accepted the MasterCard PayPass payment option at that time." *Coskun (Ex.1021)*, 342. In 2008

the ING Bank also tested the "viability of NFC technology in mobile payment systems for low value purchases in Romania" using" MasterCard (PayPass)" *Coskun (Ex.1021)*, 344.

62. A mobile phone can perform these contactless payments via the use of a mobile wallet. A mobile or electronic wallet is similar to "a person's leather, physical wallet[.]" *Pitroda (Ex.1027),* [0025]. An "electronic wallet contains one or more identification cards, credit cards, or the like. The electronic wallet is an electronic collection of one or more of these types of physical materials that can be reviewed, viewed and used electronically to achieve similar results to the physical analogs." *Pitroda (Ex.1027),* [0025].

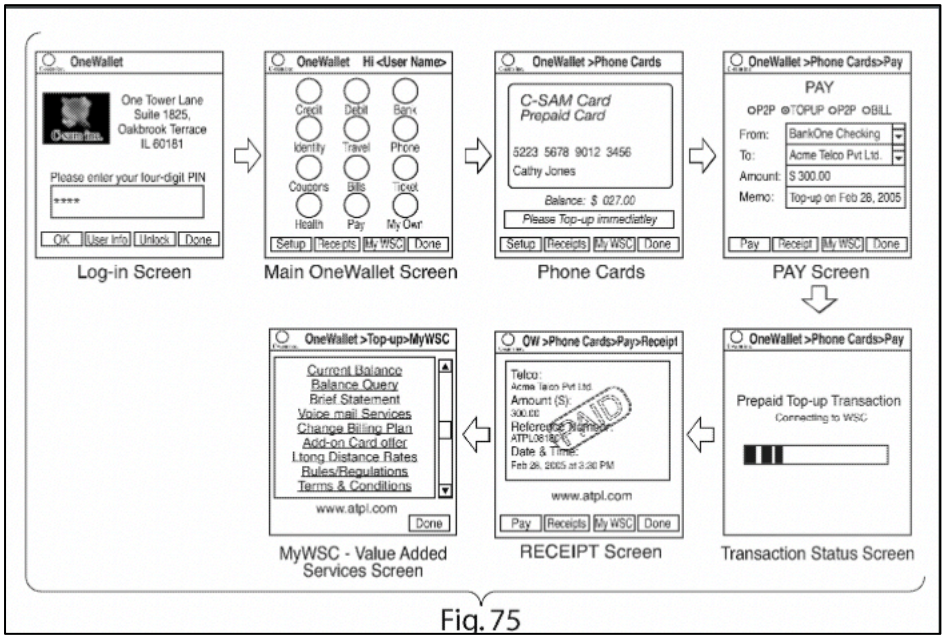


Fig. 75

Pitroda (Ex.1027), Fig. 75. A user can "view and manage mobile payment cards and other applications…through the mobile wallet graphical user interface." *Smart (Ex.1026),* 11.

63. In 2007, a Q2 Wallet trial was run. The Q2 Wallet "eliminates the need for users to carry Oyster smart cards in their wallets. Users can pay for their travel expenses through the Oyster application by simply touching their mobile phones to the Oyster NFC readers at London underground tube stations, on buses, and on trams." *Coskun (Ex.1021)*, 35. *See* also *Coskun (Ex.1021)*, 346. Nokia 6131, one of the first NFC enabled phones was the piolet test phone for the Q2 Wallet. *Coskun (Ex.1021)*, 346. ("About 500 O2 mobile network subscribers participated in the pilot and they were equipped with Nokia 6131 NFC enabled mobile phones.")



Figure 9.8 O2 Wallet [1]. Photographed by Juha Sarkkinen, The City of Oulu, Smart Touch Project.

Coskun (Ex.1021), 347.

64. As another example, "Yapı Kredi Bank and the MNO Turkcell collaborated in the NFC enabled mobile-wallet service. The service is launched commercially in 2011 [7]." Turkcell's mobile wallet software is preloaded and "supports more than one bank-issued application." *Coskun (Ex.1021)*, 345.

65. By 2012 the use of mobile phones with mobile wallets was well known. For example, MasterCard PayPass Wallet was released. *PayPass (Ex.1025),* 1. ("integrate PayPass Wallet into its mobile application.") MasterCard also released a list of 42 "Approved Mobile Devices"—including phones from Google, Intel, LG, Asus, HTC, Nokia, BlackBerry, Samsung, Zony, and ZTE—all of which supported at least one mobile payment wallet. *Mastercard Mobile Partner (Ex.1028),* 1.

10. Card Emulation Mode

66. A mobile phone can perform transactions via the mobile wallet using card-emulation mode. *Finkenzeller (Ex.1024)*, 59. ("the electronic device behaves like a contactless smart card; this option is also called 'card mode' or '*card-emulation mode*'."); *See also Coskun (Ex.1021)*, 78. ("card emulation mode provides smart card capability for mobile phones.") Card emulation mode allows mobile phones to perform payments using either magnetic stripe payment information or IC chip payment information. For example, U.S. Patent Publication No. 2014/0310113 to Sengupta et al. ("Sengupta") discusses how the "electronic device 110 formats the payment information in accordance with a specified format, for example an EMV-

CL or MSD Emulation…user enters an input into the point of sale device 320 to select a contactless payment transaction as a source of payment." *Sengupta (Ex.1034)* at [0035].



Figure 3.2 NFC mobile and NFC reader.

Coskun (Ex.1021), Fig. 3.2.

67. In "card emulation mode, the RF interface is based on the ISO/IEC 14443 (Type A, Type B) standard and FeliCa." *Coskun (Ex.1021)*, 96. "Either an NFC enabled mobile phone emulates an ISO 14443 smart card or a smart card chip integrated in a mobile phone is connected to the antenna of the NFC module." *Coskun (Ex.1021)*, 111. A NFC application needs a Graphical User Interface (GUI) and Secure Element (SE) application. *Coskun (Ex.1021)*, 152. ("GUI (Graphical

User Interface) application which must be present for all operating mode applications and provides both a GUI for the user and the capability to read NFC components…Secure Element (SE) application which is needed in order to provide a secure and trusted environment for applications") The SE may be within the mobile phone or a remote-SE.

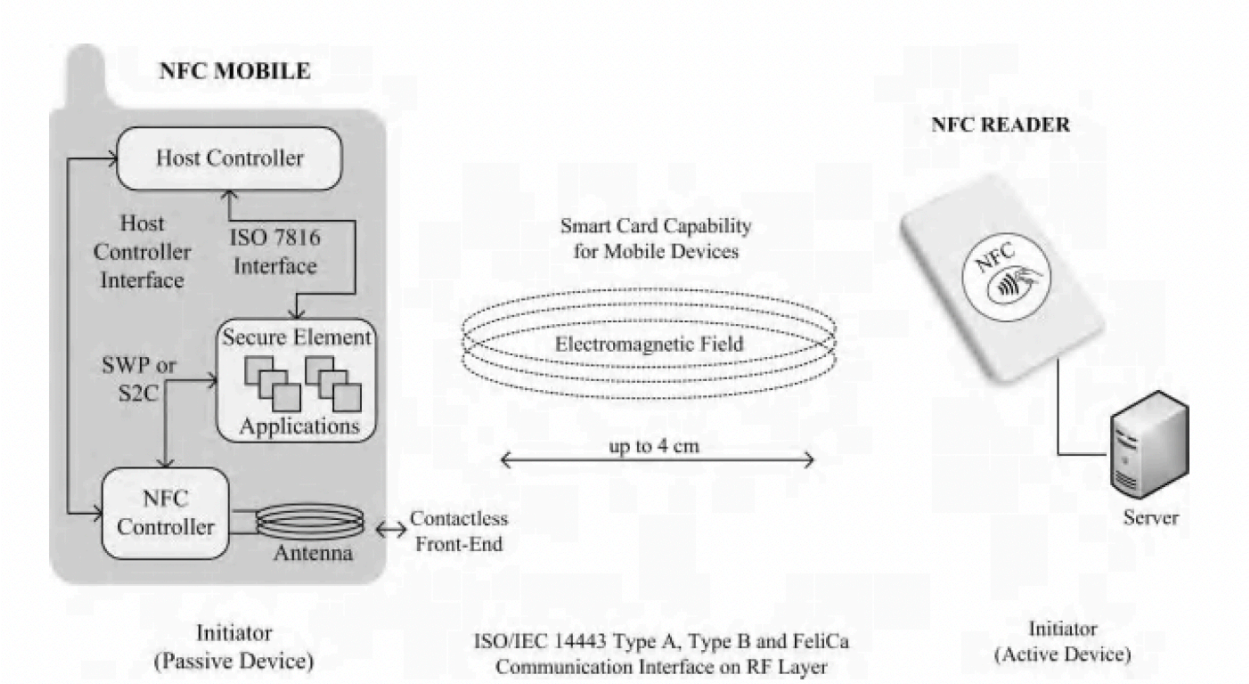


Figure 3.32 Communication architecture of card emulation operating mode.

Coskun (Ex.1021), Figure 3.32. It is worth noting that the above phone includes a secure element.

68. In the instance where a phone does not include a secure element, the mobile phone still needs a way to provide a secure and trusted environment for applications. Often, the mobile phone will have a remote-SE located outside of the

mobile phone's hardware. As an example, "the NFC mobile device has the ability to use a SE for the transaction that is not physically located in the mobile device. This may be done be creating a data connection to a remote SE for which is used for the payment transaction. In step 757, while the phone is being placed into card emulation mode, the connection to the remote SE that will be used for emulation is attempting to connect. As illustrated in step 758 there is a chance that the connection is already open in which case the flow in FIG. 14 will simply allow the ISO/IEC 7816-4 APDU data to pass directly through the connection to the remote SE and back 763successfully completing the transaction 764. There is also a chance that the connection to the remote SE does not exist and needs to be created, as described subsequently in step 762." *Yeager (Ex.1029)*, [0089].

Payment Credential Security Features

69. With the increase in contactless payment transactions came additional opportunities for malicious individuals to gain unauthorized access to a user's payment information. Below, I describe an exemplary group of prior art attempts to prevent fraud and protect sensitive information.

11. Alternatives to a Payment Account Number (PAN)

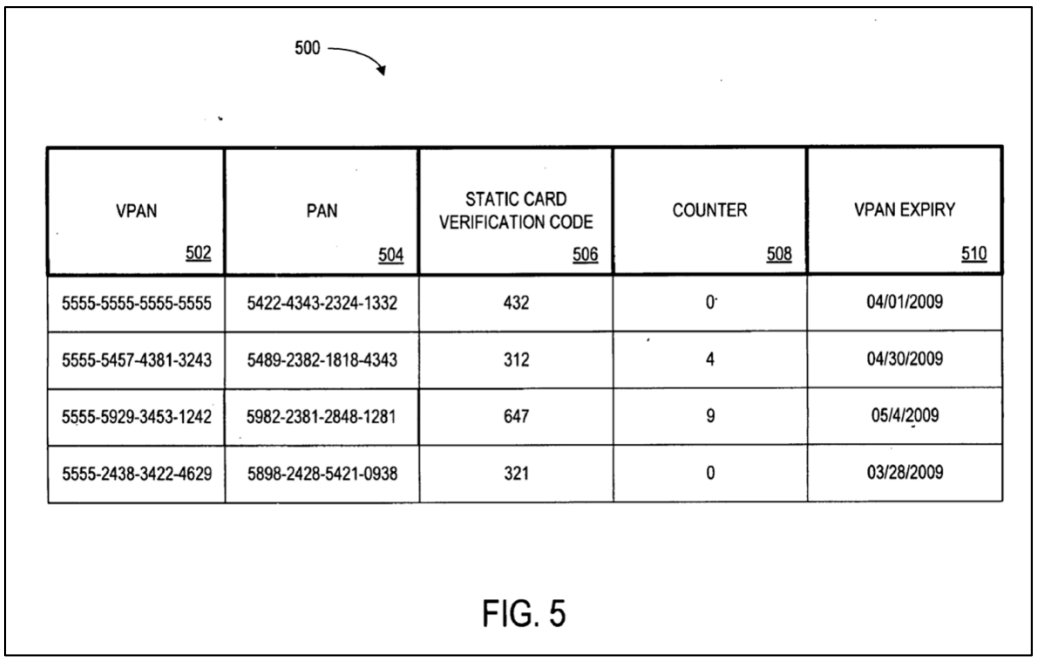
70. Early payment cards (e.g., magnetic stripe cards) lacked significant security protocols and architecture to protect customer's payment account numbers (PAN). However, the integration of tokenization—replacing a PAN with a

cryptographically created replacement called a token—into the payment card industry allowed for substantially more secure payment transactions. *EMVCo (Ex.1030)*, 6, 9.

71. Using these limited-use numbers or tokens in place of the PAN was well-known long before the Critical Date. In fact, in August of 2011, PCI SSC (EX.1031) adopted tokenization guidelines. *PCI SSC (EX.1031)*, 5. Tokenization replaces "sensitive PAN values with non-sensitive token values." *PCI SSC (EX.1031)*, 5. Non-sensitive means that the number does "not require any security or protection" because "the token has no value to an attacker." PCI SSC (EX.1031), 5. These limited-use tokens are either "single-use or multi-use." *PCI SSC (EX.1031)*, 5. Using tokens "instead of PANs is one alternative that can help to reduce the amount of cardholder data in the environment[.]" *PCI SSC (EX.1031)*, 3. PCI SSC also teaches that "[o]ne of the primary goals of tokenization solution should be to replace sensitive PAN values with non-sensitive token values." *PCI SSC (EX.1031)*, 5.

72. Another alternative to the PAN is called a virtual PAN (VPAN). As an example, Kranzley teaches that each "VPAN 502 is associated with a PAN 504. That is, each VPAN 502 is associated with an actual payment account number that has been issued to a cardholders" *Kranzley*, [0066]. Each VPAN is also "associated with the static card verification code 506 from the payment account." *Kranzley*,

[0066]. In Figure 5 "[t]he table includes entries identifying VPANs that have been issued or assigned by the payment provider 110."



VPAN 502	PAN 504	STATIC CARD VERIFICATION CODE 506	COUNTER 508	VPAN EXPIRY 510
5555-5555-5555-5555	5422-4343-2324-1332	432	0	04/01/2009
5555-5457-4381-3243	5489-2382-1818-4343	312	4	04/30/2009
5555-5929-3453-1242	5982-2381-2848-1281	647	9	05/4/2009
5555-2438-3422-4629	5898-2428-5421-0938	321	0	03/28/2009

FIG. 5

Kranzley, Fig. 5. The "VPANs processed over the payment network operated by MasterCard International Incorporated, VPANs are 16 digit numeric codes in which the first 6 digits are used to identify the VPAN as a VPAN to be routed to a payment provider 110 for processing." *Kranzley*, [0065].

73. It was well known in the art that replacing a PAN with a different number increases security. For example, an article titled "Security in Mobile Payments" by Vizzarri et al. "Vizzarri" teaches different techniques to guarantee security in m-payment systems. Classical methods are end-to-end encryption and tokenization. With tokenization an encrypted or random value, called token, replaces the card number (PAN) or the magnetic stripe track data in an electronic transaction.

The token then becomes the reference number representing the card number, so all tokens can be referenced back to the original card number." Vizzarri (Ex.1032), 5. As an additional example, Grigg teaches a "mobile wallet account number" that "is a distinct number that is different from any traditional financial institution account number or any other account number associated with a payment device...[that] may be utilized for a transaction for a product." *Grigg*, [0011]. Grigg teaches that the mobile wallet on the user device 204 will be assigned a "mobile wallet account number" to be used by the user device 204 in place of a traditional account number such as a credit card number (PAN). *Grigg,* [0006], [0047], [0051]. Grigg notes that the payment device or devices are for example, "credit cards" or a "payment device account number (such as a traditional bank account number) [.]" *Grigg*, [0002], [0006]. Grigg notes that each payment device has a "different mobile wallet account number[.]" *Grigg*, [0011], [0003] ("[A] mobile wallet is typically associated with the individual's mobile device[.]"). In Grigg, the financial institution application "provide[s] the user 202 via the user device 204 the assigned mobile wallet account number." *Grigg*, [0053]. This mobile wallet number "may be permanently associated with the mobile wallet" *Grigg*, [0051]. "[A] user 202 may use his/her user device 204 as a mobile wallet" to make payments at a point-of-transaction (POT) or online. *Grigg,* [0043].

12. Alternatives to Static Card Verification Values

74. Another method to increase security int transactions comes in the form of the card verification value (CVV- Visa) or card verification code (CVC - MasterCard). The banking industry "developed a type of "password" for use with credit and debit cards. This password takes the form of an authentication code and is commonly referred to in the industry as a "card verification value" or "CVV." *Ashfield (Ex.1033)*, [0002]. A CVV is "a "3-digit security code[.]" *Ashfield (Ex.1033)*, [0002].

75. To increase security in transactions, a one-time use dynamic CVV/CVC code may be generated. For example, this "dynamic CVV can be compared to at least a portion of a one-time password generated for the specific credit/debit card, and a transaction authorization can be sent to the merchant or vendor when the dynamic CVV matches all or a portion of the one-time password. A transaction denial can be sent when the dynamic CVV does not match." *Ashfield (Ex.1033)*, [0005]. The bank "can separate the dynamic CVV from credit/debit card data, validate the credit/debit card data, and then merge the CVV with the credit/debit card data once the dynamic CVV is authenticated to produce the transaction authorization." *Ashfield (Ex.1033)*, [0005].

76. Mastercard uses a CVC3 value and Visa uses a dCVV value to replace the static CVV. For example, Bona teaches "the static CVV value with the dynamic dCVV or CVC3 codes (in the embodiments where the data is formatted for VISA®

and MASTERCARD® transactions, respectively) [.]" *Bona*, [0037]. Kranzley teaches "in the case of a MasterCard payment card, the static card verification code 506 may be the MasterCard CVC number printed on the back face of a MasterCard credit or debit card." *Kranzley,* [0066]. Bona notes that "[t]hese one-time (i.e., dynamic) codes are generated by the smart card chip and are unique to each transaction." *Bona*, [0037]. Dynamic data such as a CVC3 "would provide sufficient information in the payment authorization process to eliminate both 'card present' and 'card not present' fraud." *Bona*, [0037]. Yeager teaches that "[e]xamples of cryptograms at the time of this filing are defined by the following card specification in table 4." *Yeager (Ex.1029),* [0162].

TABLE 4

Card specification	Cryptogram Designator or Name
MasterCard PayPass MSD	CVC3
Visa Contactless MSD	dCVV
Discover ZIP MSD	dCVV
EMV, Visa QVSDC, VISA VSDC, MasterCard MCHIP	AC, TC, AAC, ARQC

Yeager (Ex.1029), Table 4. Yeager teaches "[a] "cryptogram" as used herein may be classified as "dynamic" meaning that it is always changing from one interrogation (transaction) to the next[.]" *Yeager (Ex.1029)*, [0162].

VII. SUMMARY OF THE PRIOR ART REFERENCES

Collinge

77. Collinge was filed on March 14, 2013, and claims priority to the following provisional applications: Ex. 1005 (U.S. Provisional Appl. No. 61/619,095, filed April 2, 2012 ("'095 Provisional")); Ex. 1006 (U.S. Provisional Appl. No. 61/635,248, filed April 18, 2012 ("'248 Provisional"), Ex.1007 Appl. No. 61/745,383, filed December 10, 2012 ("'383 Provisional"), Ex.1008 Appl. No. 61/762,098, filed February 7, 2023 ("'098 Provisional"). It is my understanding it is entitled to a priority date of April 18, 2012 for the reasons discussed below. 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.

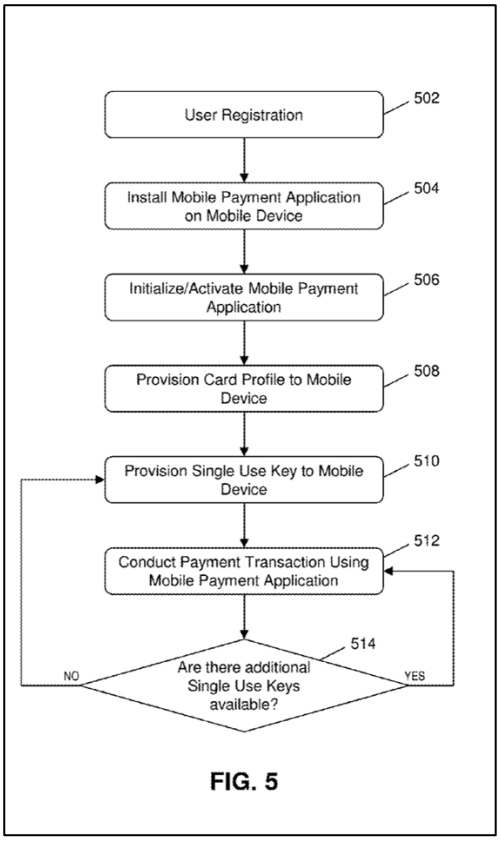


FIG. 5

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].

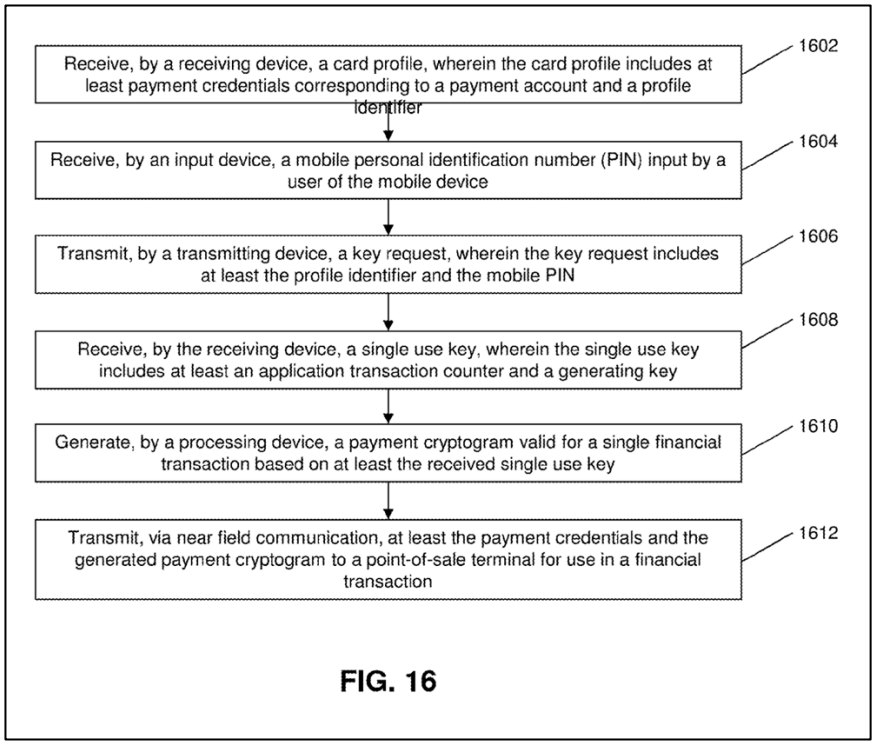


FIG. 16

Collinge, Fig. 16. As I produced below, a table of key terminology used throughout Collinge.

Abbreviation in Collinge	***Meaning in Collinge***	***Mapping in Petition***
KS_{UN} *Collinge*, Fig. 17, [0141], [0145].	session key unpredictable number	Secret used to generate and validate a payment cryptogram. Shared with issuer.
UN_{CLOUD} *Collinge*, Fig. 17, [0141].	cloud unpredictable number	Issuer secret used to validate a payment cryptogram.
single use key Collinge, [0128]	single use key	Secret used to generate and validate a payment cryptogram. Shared with issuer.
PAN Collinge, [0048]-[0049].	Primary/payment account number	For example, a traditional 16-digit credit card number is a PAN.
ATC	Application transaction counter	Transaction counter, also shared with issuer

Collinge, Fig. 18, [0141], [0145].		
CVC3 *Collinge*, Fig. 18, [0145].	A type of payment cryptogram used in contactless magstripe transactions (AC is the other payment cryptogram used in chip transactions)	Limited-use payment information used in place of the static CVC.
UN_{READER} *Collinge*, Fig. 18, [0145].	Reader unpredictable number	Device secret used to generate a payment cryptogram.

1. Collinge is Analogous Art

78. I have been informed that for a prior art reference to be proper for use in an obviousness analysis, the reference must be "analogous art" to the claimed invention. I have been informed that a prior art reference is analogous to the claimed invention if the reference is from the same field of endeavor as the claimed invention or if it is reasonably pertinent to the particular problem that the inventor was trying to solve.

79. A POSITA would have classified Collinge within the same field of endeavor as the '579 Patent because both Collinge and the '579 Patent relate to the generation and use of credentials for smart payment devices. For example, Collinge describes provisioning and storage of payment credentials for use in conducting near field financial transactions. *Collinge*, [0002]. Collinge further describes a remote system that generates and provides to a mobile device payment credentials that

include a payment token payload, where the payload includes a card profile and single use key. *Collinge*, [0043]. The mobile device can then use the single use key to generate a payment cryptogram for use in a financial transaction. *Collinge*, [0070]. The '579 Patent similarly describes payment devices and transaction processing that can be utilized with near field communications. Ex. 1001 ('579 Patent) at 1:23-27. Similar to Collinge, the '579 Patent describes a credit card device that generates a limited duration payment credential using the user's payment information for use in a financial transaction. '579 Patent at 11:46-49.

80. Additionally, a POSITA would have found Collinge reasonably pertinent to the problem faced by the inventors of the '579 Patent because both Collinge and the '579 Patent describe the need for increased security in financial transactions using smart card or mobile devices to prevent fraudulent or unauthorized transactions. For example, Collinge describes a device and process for securely generating and transmitting payment credentials from a mobile device to a payment terminal (e.g., NFC point-of-sale terminal). *Collinge*, [0003]-[0007]. Likewise, the '579 Patent describes that its invention "address security concerns of a credit card owner" for use in RFID transactions. '579 Patent at 2:4-12, 9:63-10:2. Accordingly, a POSITA would have considered Collinge analogous art to the '579 Patent.

2. Collinge is Prior Art

81. Collinge was filed on March 14, 2013, and is therefore prior art because it was filed earlier than the priority date of '579 Patent's provisional application, filed on March 15, 2013.

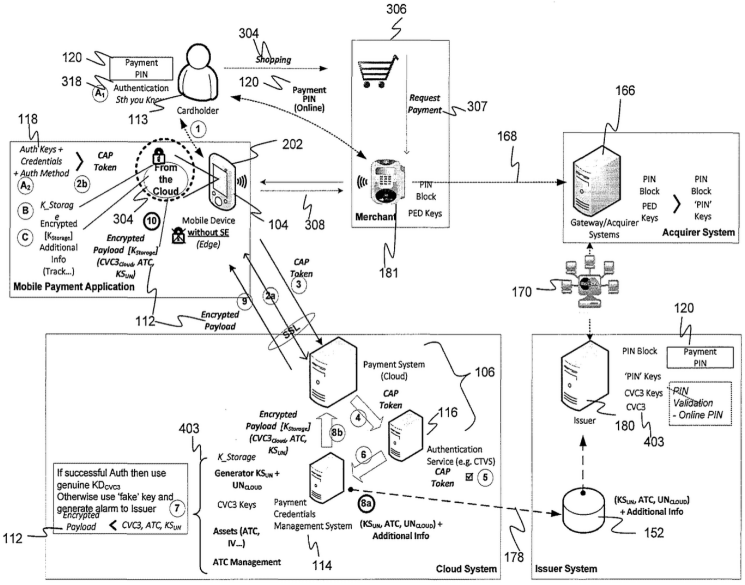
82. In the event that Cardware attempts to demonstrate that it is entitled to a date earlier than March 15, 2013 based on a showing of earlier conception and reduction to practice, it is additionally my understanding that Collinge is entitled to a prior date at least as early as April 18, 2012 based on Collinge's provisional application filed on and before that date (Provisional Nos. 61/619,095 (Ex.1005), filed April 2, 2012 ("*'095 Provisional*"), and 61/635,248 (Ex.1006) filed April 18, 2012 ("*'248 Provisional*") (collectively, "Collinge's April 2012 Provisionals").

83. I understand that for Collinge to be entitled to the April 18, 2012 filing date of the '248 Provisional, Collinge's April 2012 Provisionals must contain a written description of the invention to have enabled a POSITA to practice the invention claimed in the non-provisional application. I have reviewed the Collinge Provisionals and it is my opinion that Collinge's April 2012 Provisionals provides a detailed disclosure of the provisioning, storage and use of payment credentials for use in an NFC financial transaction disclosed and claimed in Collinge, including storing a storage key, a plurality of dynamic card validation codes ("DCV3"), and an application transaction counter ("ATC"); providing the storage key, an authentication component, and static payment credentials to a mobile device;

validating a mobile device using a CAP token; generating a session key and cloud unpredictable number; identifying an encrypted payload, that includes a DCV3, the session key unpredictable number and ATC, based on a derived dynamic card validation code; transmitting the encrypted payload to the mobile device to generate a DCV3 for use in a financial transaction; and, transmitting the session key and cloud unpredictable number and ATC to an issuer for use in validating the DCV3 generated by the mobile device, which is similar to the level of disclosure in Collinge itself. In my opinion, Collinge's April 2012 Provisionals provide sufficient written description to enable a POSITA to practice the inventions claimed in at least claim 20 of Collinge.

84. The table below identifies where, for example, written description support can be found in Collinge's April 2012 Provisionals for claim 20 of Collinge. The disclosure of Collinge's April 2012 Provisionals provide similar detail to Collinge itself, and enables a POSITA to practice claim 20 of Collinge.

Collinge (Ex. 1004)	**Supporting Disclosure from Collinge's April 2012 Provisionals – the** *'095 Provisional*" (Ex.1005) and the *'248 Provisional* (Ex. 1006).
20. A method for generating and provisioning payment credentials to a mobile device lacking a secure	The Collinge Provisionals disclose methods for provisioning payment credentials to a mobile device lacking a secured element. "The present disclosure is directed to a method and system providing technical solutions for processing electronic payments initiated from a mobile device without requiring a secure element (SE) in the mobile device using in part a

element, comprising:	financial transaction card processing system or network as a part thereof."[1] '095 Provisional (Ex. 1005), ¶0001 "According to an embodiment, a set of processes deliver solutions for contactless payments, such as online transactions at a Point-of-Sale (POS), when using a mobile device but not requiring use or presence of an SE. One embodiment uses a combination of remote authentication and the provisioning of payment credentials to the mobile device for one transaction. In an alternative embodiment, remote authentication is performed and payment credentials are provisioned to a mobile device without an SE for a limited number of transactions." '095 Provisional(Ex. 1005), ¶0005  '095 Provisional(Ex. 1005), Fig. 5
storing, in a database, at least a storage key, a	The Collinge Provisionals disclose storing in a database of the payment credentials management a storage key ($K_{Storage}$), a plurality of dynamic card validation code keys (CVC3), and

[1] Unless otherwise noted, all emphasis is added.

plurality of dynamic card validation code keys, and an application transaction counter associated with a mobile application program;	an application counter (ATC) associated with a mobile application program. "As shown in Figure 1, the cloud-based transaction data generation system 106 further comprises key storage 110 for storing keys and encrypted information 113. In the exemplary embodiment of Figure 1, the encrypted information 113 has been encrypted using $K_{storage}$ and includes Track 1 data, and/or Track 2 data. As shown in Figure 1 the encrypted payload 112 is provisioned to the mobile device 104 from the cloud-based transaction data generation system 106. The cloud-based transaction data generation system 106 also includes a payment credentials management system 114 and an authentication service 116." '095 Provisional (Ex. 1005), ¶0038 "The payment credentials management system 114 may manage the CVC3 keys 403." '095 Provisional (Ex. 1005), ¶0066 "Exemplary solutions and embodiments disclosed herein can incorporate several core principles outlined below: ▸ Storage Key ($K_{storage}$) defined at time of authentication profile and static Payment credentials provisioning." '095 Provisional (Ex. 1005), ¶0068

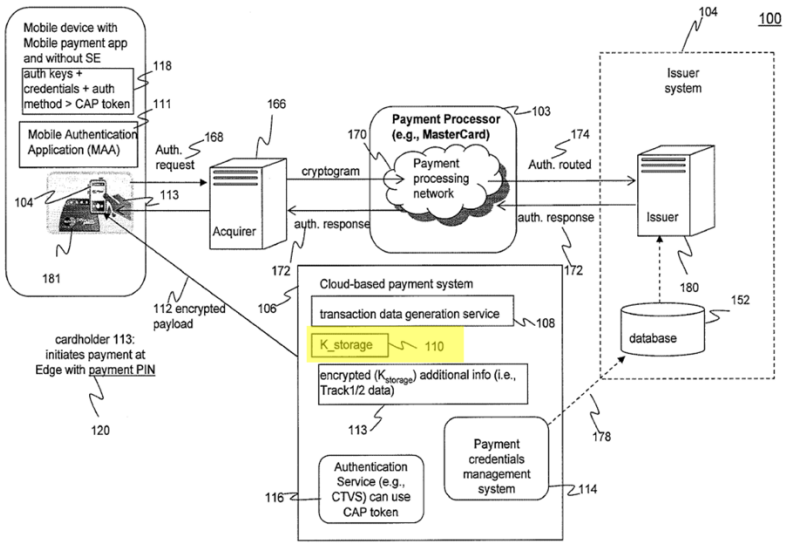
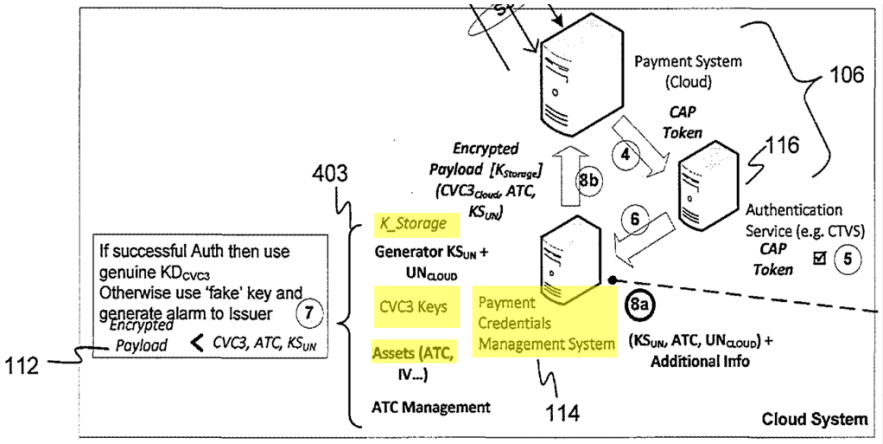


FIG. 1

’095 Provisional (Ex. 1005), Fig. 1.

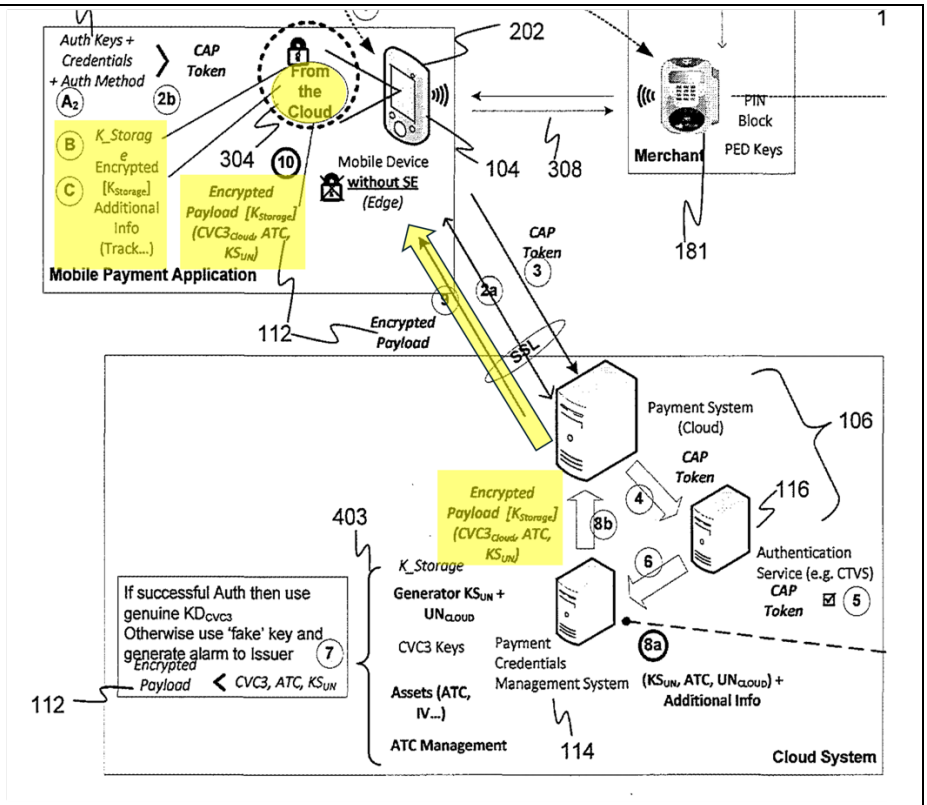


’095 Provisional, Fig. 5 (annotated excerpt);
’095 Provisional (Ex. 1005), Figs. 4, 6-8

provisioning, to the mobile device, at least the storage key, an authentication component, and static payment	The Collinge Provisionals disclose providing the mobile device a storage key, an authentication component, and static payment credentials associated with a payment account. “In step 205, authentication credentials associated with a payment card are provisioned to the mobile device 104.” ’095 Provisional (Ex. 1005), ¶0051

credentials, wherein the static payment credentials are associated with a payment account;	<table><tr><td>**B**</td><td>At time of the authentication credentials provisioning, a storage key is also stored in the Mobile Payment Application. This key is used to protect the static payment credentials and the transport of the payload from the Cloud to the Mobile Payment Application</td></tr><tr><td>**C**</td><td>At time of the authentication credentials provisioning, static payment credentials are also provisioned</td></tr></table> '095 Provisional (Ex. 1005), Table 1 (p. 15) "System 100 can obtain authentication keys 118, CVC3 keys 403, and payment credentials 174 from a cloud-based transaction data generation system 106 and provisioning the retrieved payment credentials 174 to the MAA 111." '095 Provisional (Ex. 1005), ¶0062 "Exemplary solutions and embodiments disclosed herein can incorporate several core principles outlined below: ► Storage Key ($K_{storage}$) defined at time of authentication profile and static Payment credentials provisioning. ► Authentication credentials protected using MAA rules (e.g. Key Camouflage) (Not using $K_{storage}$) *** ► The values KD_{CVC3} and $IVCVC3_{Trackl/2}$ are static (if one considers a given PAN (and PSN) value, the values KD_{CVC3} and $IVCVC3_{Trackl/2}$ remain the same during the entire lifespan of the card. Those values are static. It also means that once the value is disclosed, you can reuse it.) for a given PAN (and PSN). The PSN (if available) can be part of the KD_{CVC3} derivation process. This avoids mandating any change regarding the management of this value at issuer level even if the PSN may be used to identify a SE-less 'virtual card' defined for a given PAN. ***

	► Delivery of Encrypted Payload [using $K_{storage}$] (KS_{UN}, Cloud_$CVC3_{TRACK1/2}$ and ATC) to Mobile Payment Application" '095 Provisional (Ex. 1005), ¶0068 "(Static) Information known by the Mobile Payment Application ◊ FCI (PPSE) ◊ AID (Application Identifier) ◊ FCI (File Control Information) ◊ AFL (Application File Locator) ◊ AIP (Application Interchange Profile) ◊ AVN (Application Version Number) ◊ Encrypted (using $K_{storage}$) Payment Credentials provisioned at time of authentication credentials provisioning." '095 Provisional (Ex. 1005), ¶0071 (p. 22) "provisioning a storage key ($K_{storage}$), authentication credentials and static payment credentials associated with a payment account to the mobile device, wherein the $K_{storage}$ key is used to protect static payment credentials stored on the mobile device and the transport of a payload from the Cloud to the mobile payment application" '248 Provisional (Ex. 1006), Claim 1



'095 Provisional (Ex. 1005), Fig. 5 (annotated excerpt)

"As shown in Figure 9A, once these operations have been completed, the pull environment is ready, and the next phase can take place using the following processes: a process to send authentication credentials and Keys 918 and any needed static payment credentials 928 to a user (cardholder 113) of the mobile device 104, a remote authentication 824, a process to retrieve dynamic payment credentials 938 (i.e., using an encrypted payment token payload 112); and a process to synchronize 978 the cloud-based transaction data generation system 106 and issuer 180 systems."

'248 Provisional (Ex.1006), ¶0091

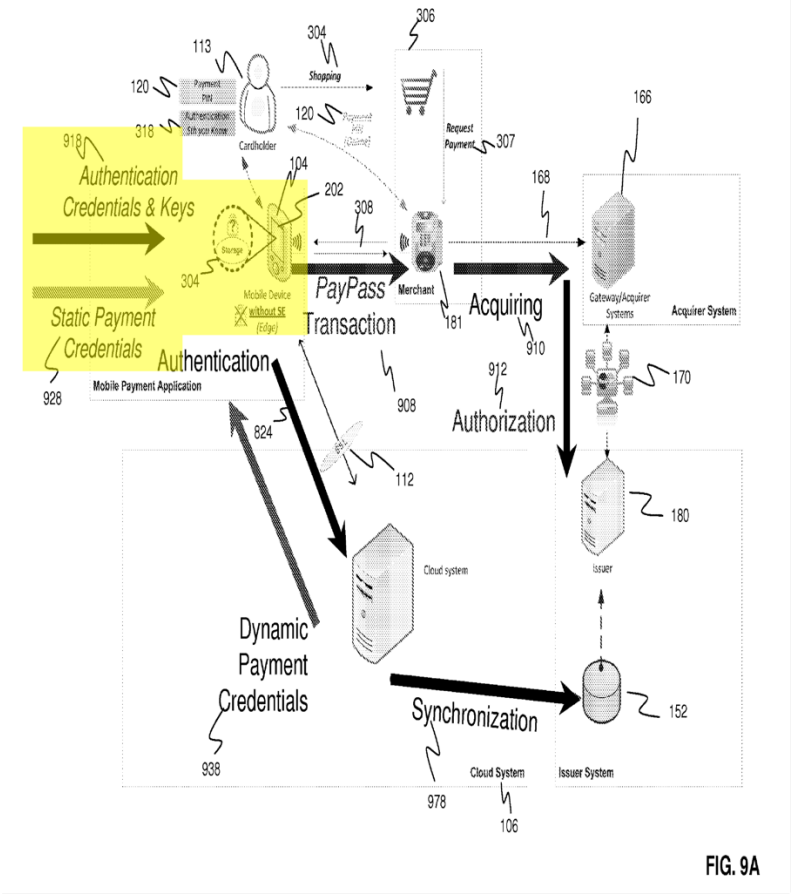


FIG. 9A

’248 Provisional (Ex.1006), Fig. 9A

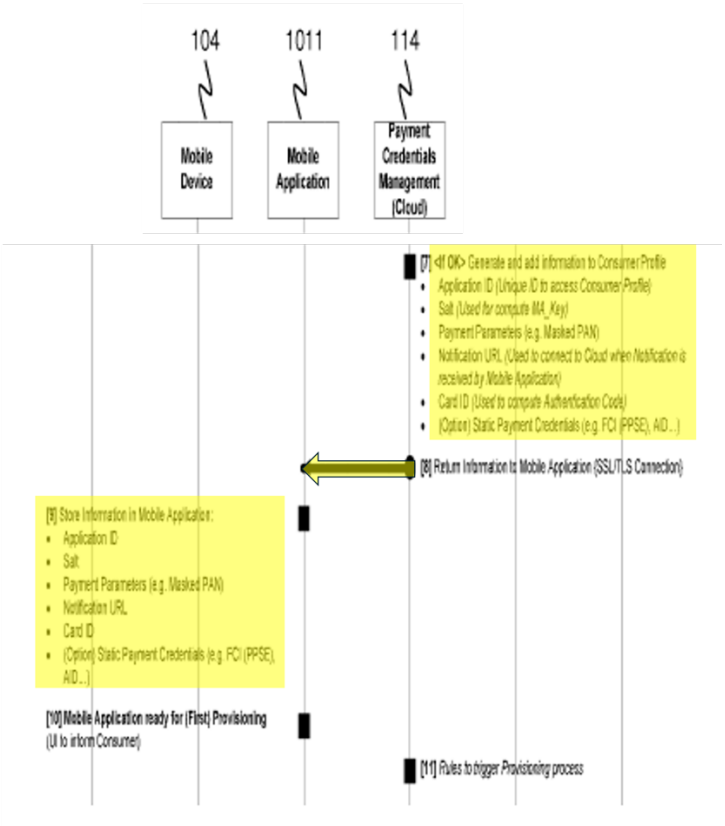
“The communications sequence depicted in Figure 11 encompasses pushing the following parameters/data to the mobile application 1011 as part of stage [7]: an application ID, which is a unique ID used to access the consumer profile (i.e., the profile for the user 113); a salt, which is a value used (in combination with the access code) in the cryptographic process (Fn_MA_Key) to generate the key used for transport and storage of the payment token payload; payment parameters including the required payment card artwork with a masked PAN value (e.g., XXXX XXXX XXXX 4321); a notification URL used to connect to the cloud-based transaction data generation system 106 to retrieve the encrypted payment token payload; and a card ID, which is a unique ID used in the generation (Fn_Auth_Code) of an authentication code. In an embodiment, the parameters

optionally further comprise some additional non-sensitive static payment credentials.

In stage [8], this information is returned to the mobile application 1011 via an SSL/TLS connection before proceeding to stage [9] where the information is stored in the mobile application 1011.

As shown in Figure 11, the information stored in stage [9], can include: an application ID, the salt, payment parameters (e.g. the Masked PAN), the notification URL, and the card ID. Optional information stored can include static payment credentials (e.g. FCI (PPSE), AID shown in Figure 11)."

'248 Provisional (Ex.1006), ¶¶0135-0137



'248 Provisional (Ex.1006), Fig. 11 (annotated excerpt)

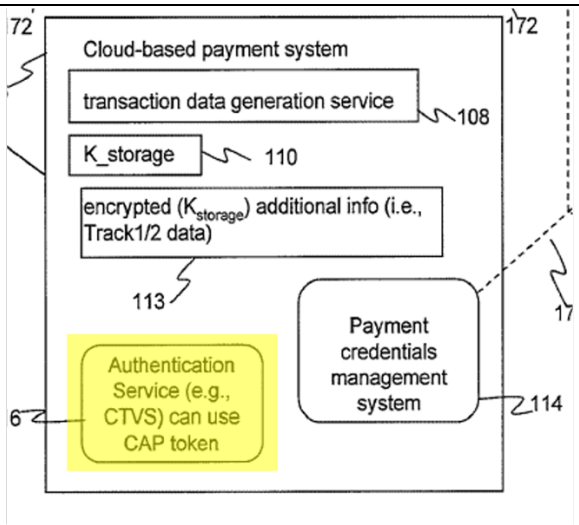
"The following section provides further details for exemplary embodiments of the parameters, data elements and fields

	depicted in Figures 9-15 and described above with reference to those Figures. **Payment Token Payload** According to an embodiment, the Payment Token Payload contains four parts: ♦ Length ♦ Proof Information ♦ Payment Data (Static - Non Sensitive, Static - Sensitive, Dynamic) ♦ [End Tag] The Payment Token Payload is transported and stored in encrypted form using a Mobile Application Key (MA_Key). The process to derive this key is defined in *Fn_MA_Key*. *** The Payment Data contains all the data elements required to perform a Pay Pass Magstripe Transaction. In an embodiment, the detailed content of the Payment Token Payload is: ♦ *Length* ♦ *Proof Information* o Proof (Random - 5 bytes) ♦ *Static Payment Data* o FCI (PPSE) o AID o FCI (PayPass App) o AIP o APL ♦ *Static Payment Data (PayPass Transaction)* o PUNATC Track 1 o PUNATC Track 2 o PCVC3 Track 1 o PCVC3 Track 2 o NATC Track 1 o NATC Track 2 o UDOL ♦ *Static Payment Data (Sensitive Data)* o Track 1 Data

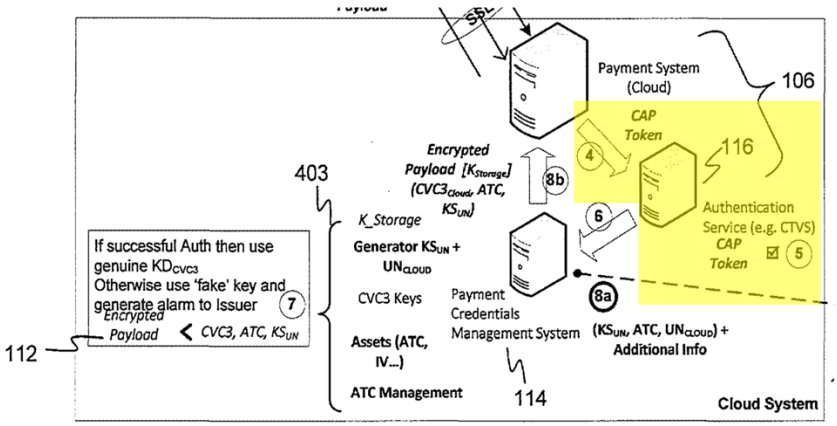
	o Track 2 Data ♦ *Dynamic Payment Data (Sensitive Data)* o IVS_CVC3 (Track 1 and Track 2) o ATC o KS_CVC3 ♦ *Control Data* o [End Tag]" '248 Provisional (Ex.1006), ¶¶0211-0213 "♦ The Mobile Payment Application can be: o A single "card". The PPSE has to be set with the AID of the "card". o Embedded in a Wallet. The AID must be added to the list of AID managed by the PPSE." '248 Provisional (Ex.1006), p. 155
receiving, from the mobile device, a chip authentication program (CAP) token;	The Collinge Provisionals disclose the mobile device sending a chip authentication program (CAP) to the cloud-based payment system. "A method for providing technical solutions for processing electronic payments initiated from a mobile device without requiring a secure element (SE) in a mobile device, comprising: …sending a token from a mobile authentication application (MAA) component of the mobile payment application to the Cloud; validating the token based on upon authentication credentials; …." '095 Provisional (Ex.1005), Abstract (p. 38) "The system 100 performs authentication using the MAA 111. According to an embodiment, the MAA 111 is a software implementation of MasterCard Authentication Solutions (two-factor authentication using a CAP Token). A CAP Token Generation Service (CTGS) can be integrated in a mobile application to build a MasterCard Authentication Solution for mobile device 104 where the cardholder 113 uses the Mobile

	Authentication Application (MAA) to generate a CAP Token." '095 Provisional (Ex.1005), ¶0031 "The cloud-based transaction data generation system 106 also includes a payment credentials management system 114 and an authentication service 116. In the exemplary embodiment of Figure 1, the authentication service 116 is configured to perform CVTS CAP Token validation (CTVS) and can use a Chip Authentication Program (CAP) token for authentication." '095 Provisional (Ex.1005), ¶0038 **2b** The Cardholder uses the MAA component of the Mobile Payment Application to generate a CAP Token for the authentication transaction. The Cardholder has to supply some credentials (e.g. A gesture, a password…) **3** Mobile Payment Application sends a CAP Token to the Cloud '095 Provisional (Ex.1005), Table 1 (p. 15) "forwarding payment credentials comprising at least one token from the Cloud to the mobile device; receiving, at the Cloud, a token from a mobile authentication application (MAA) component of the mobile payment application; validating the token based upon the authentication credentials and at least one additional credential received from the mobile device;" '095 Provisional (Ex.1005), Claim 1 "9. The method of claim 1, wherein the token is a Chip Authentication Program (CAP) token indicating one or more controls on purchases." '095 Provisional (Ex.1005), Claim 9

validating, by a validation device, the authenticity of the received CAP token;	The Collinge Provisionals disclose an authentication service validating the authenticity of the CAP token sent by the mobile device. "A method for providing technical solutions for processing electronic payments initiated from a mobile device without requiring a secure element (SE) in a mobile device, comprising: …sending a token from a mobile authentication application (MAA) component of the mobile payment application to the Cloud; validating the token based on upon authentication credentials; …." '095 Provisional (Ex.1005), Abstract "In accordance with another exemplary embodiment, mobile authentication and mobile payment services arc implemented as an online-only solution wherein a CAP token is verified online by a CAP Token Validation Service (CTVS)." '095 Provisional (Ex.1005), ¶0010 "In the exemplary embodiment of Figure 1, the authentication service 116 is configured to perform CVTS CAP Token validation (CTVS) and can use a Chip Authentication Program (CAP) token for authentication." '095 Provisional (Ex.1005), ¶0038 "As shown in Figure 5, the authentication service 512 in system 100 may be a CAP Token Validation Service (CTVS)." '095 Provisional (Ex.1005), ¶0066 **4** The Payment System (in the Cloud) validates the CAP Token using a CAP Token Validation Service (CTVS). The Payment System can be operated by MasterCard or by the Issuer. **5** The CTVS validates the CAP Token. The CTVS can be operated by MasterCard or by the Issuer. '095 Provisional (Ex.1005), Table 1 (p. 24)



'095 Provisional (Ex.1005), Fig. 1 (annotated excerpt)



'095 Provisional (Ex.1005), Fig. 5 (annotated excerpt);
'095 Provisional (Ex.1005), Figs. 4, 6-8

"validating the token based upon the authentication credentials and at least one additional credential received from the mobile device;"

'095 Provisional (Ex.1005), Claim 1

"9. The method of claim 1, wherein the token is a Chip Authentication Program (CAP) token indicating one or more controls on purchases."

'095 Provisional (Ex.1005), Claim 9

generating, by a processing device, a session key unpredictable number (KS_{UN});	The Collinge Provisionals disclose a cloud-based payment system generating a session key unpredictable number (KS_{UN}). "Exemplary data flow stages depicted in Figures 5-7 are described in Table 1 below. *** 7 Upon successful authentication, a genuine KD_{CVC3} is used and (KS_{UN}, Cloud_$CVC3_{TRACK1/2}$, ATC) is returned. " '095 Provisional (Ex.1005), Table 1 (p. 16) "Exemplary solutions and embodiments disclosed herein can incorporate several core principles outlined below: *** ► Session key generation (KS_{UN}) in the Cloud to bind (ATC, UN_{CLOUD}, PAN and PSN) at the Edge (Mobile Payment Application)" '095 Provisional (Ex.1005), ¶0068 "A Glossary of terms and acronyms described above and depicted in Figures 3-8 is provided in Table 2 below: **Table 2** **Stage** **Description** *** UN Unpredictable Number '095 Provisional (Ex.1005), Table 2 (p. 26) "According to an embodiment, the principles for the synchronization process (between the Cloud-based transaction data generation system 106 to issuer 180) are as follows: 1. The Cloud_$CVC3_{TRACK1/2}$ generation is managed in the Cloud-based transaction data generation system 106 ("the

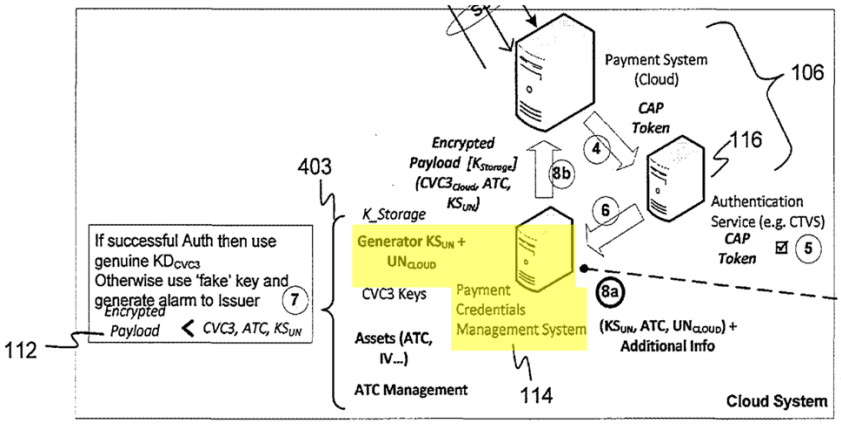
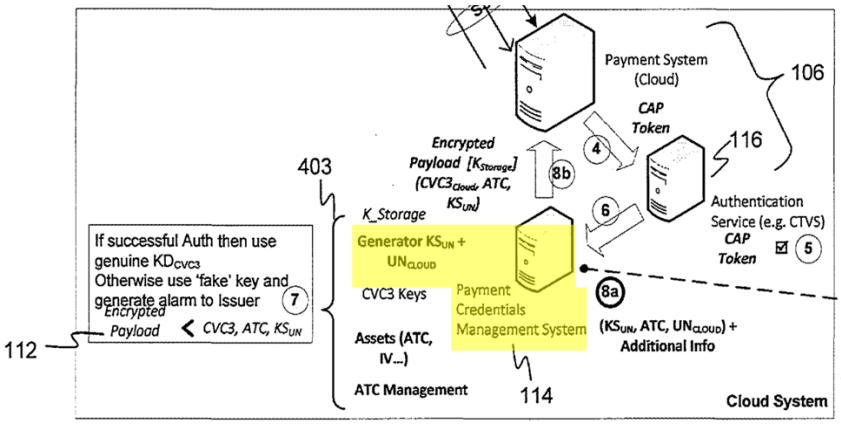
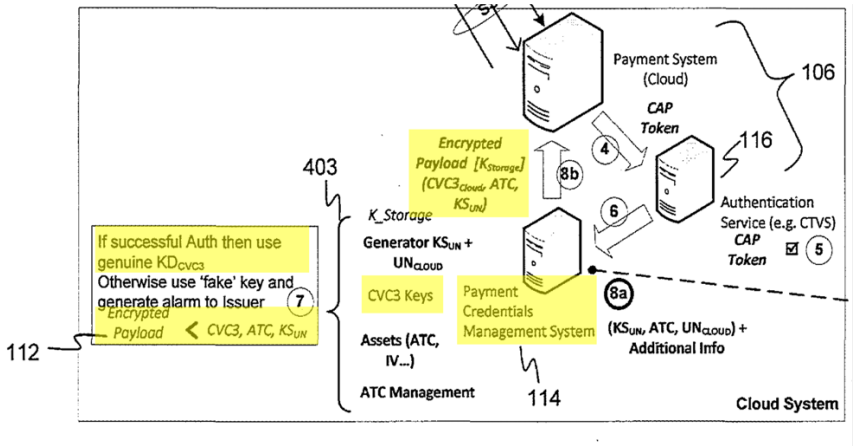
	Cloud). This encompasses the generation of KS_{UN} and UN_{CLOUD}, and the application transaction counter (ATC) management." '248 Provisional (Ex.1006), ¶0077; '095 Provisional (Ex.1005), ¶0056 (p.13)  '095 Provisional (Ex.1005), Fig. 1 (annotated excerpt); '095 Provisional (Ex.1005), Fig. 7
generating, by the processing device, a cloud unpredictable number (UN_{CLOUD});	The Collinge Provisionals disclose a cloud-based payment system generating a cloud unpredictable number (UN_{CLOUD}). "According to an embodiment, the principles for the synchronization process (between the Cloud-based transaction data generation system 106 to issuer 180) are as follows: 1. The Cloud_$CVC3_{TRACK1/2}$ generation is managed in the Cloud-based transaction data generation system 106 ("the Cloud). This encompasses the generation of KS_{UN} and UN_{CLOUD}, and the application transaction counter (ATC) management." '248 Provisional (Ex.1006), ¶0077; '095 Provisional (Ex.1005), ¶0056 (p.13) "A Glossary of terms and acronyms described above and depicted in Figures 3-8 is provided in Table 2 below:

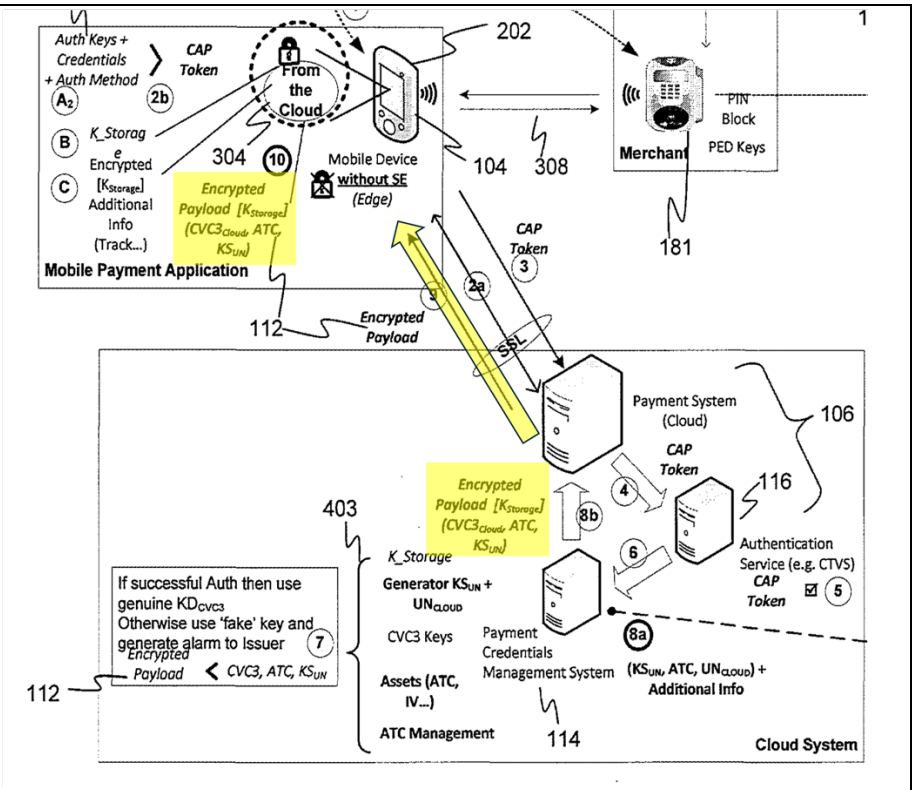
	Table 2 **Stage** **Description** *** **UN** Unpredictable Number '095 Provisional (Ex.1005), Table 2 (p. 25)  '095 Provisional (Ex.1005), Fig. 5 (annotated excerpt); '095 Provisional (Ex.1005), Fig. 4, 6-7
identifying, by the processing device, an encrypted payload based on a derived dynamic card validation code key (KD_{CVC3}), wherein the encrypted payload includes at least a dynamic card validation code key of the plurality of	The Collinge Provisionals disclose the cloud-based transaction data generation system identifying an encrypted payload, including a dynamic card validation code (CVC3), KS_{UN}, and an application transaction counter (ATC), based on a dynamic card validation code key (KD_{CVC3}). "4. If the validation of the CAP Token is successful, the cloud-based transaction data generation system 106 generates the CVC3 value using a genuine KD_{CVC3} and returns an encrypted payload to the Mobile Payment Application." '095 Provisional (Ex.1005), ¶0056 (p.13) **7** Upon successful authentication, a genuine KD_{CVC3} is used and (KS_{UN}, $Cloud\_CVC3_{TRACK1/2}$, ATC) is returned. '248 Provisional (Ex.1006), Table 1 (p. 16)

dynamic card validation code keys, the KS_{UN}, and the application transaction counter;	"Exemplary solutions and embodiments disclosed herein can incorporate several core principles outlined below: *** ▸ Key derivation process in the Cloud (KD_{CVC3} + KD_{UN})" '095 Provisional (Ex.1005), ¶0068 (p.20)  '095 Provisional (Ex.1005), Fig. 5 (annotated excerpt); '095 Provisional (Ex.1005), Figs. 4, 6-8 "in response to determining that the authenticating was successful, including a genuine CVC3 derived key (KDcvc3) in the payment credentials and returning an encrypted payload to the mobile device including at least one of the KSUN, the Cloud_ CVC3TRACK1/o2r, the ATC" '095 Provisional (Ex.1005), Claim 1
transmitting, by a transmitting device, the encrypted payload to the mobile device for use in generating a dynamic card validation code for use in a financial transaction; and	The Collinge Provisionals disclose the cloud-based transaction data generation system transmitting the encrypted payload the mobile device for use in generating a dynamic card validation code for use in a financial transaction "The present disclosure is directed to a method and system providing technical solutions for processing electronic payments initiated from a mobile device without requiring a secure element (SE) in the mobile device using in part a financial transaction card processing system or network as a part thereof." '095 Provisional (Ex.1005), ¶0001

	"As shown in Figure 1 the encrypted payload 112 is provisioned to the mobile device 104 from the cloud-based transaction data generation system 106." '095 Provisional (Ex.1005), ¶0038 "The mobile payment application may generate a cryptogram. This cryptogram may be forwarded with the authorization request 168 to the acquirer 166. As shown in Figure 1, this can be further sent to the payment processing network 170. In an embodiment, the cryptogram 178 may be generated using key management services (i.e., through CVC3 validation, including dynamic CVC3 validation). The payment processor 103 then routes an authorization request 168 based on the payment credentials 174 and the cryptogram 178 to the issuer 180 and the issuer 180 responds to the authorization request 168 with the authorization response 172. In one embodiment, system 100 includes a connection 178 between the issuer 180 and a payment credentials management system 114. After receiving the authorization response 172, the payment processor 103 forwards the authorization response 172 to the acquirer 166, which in tum routes the authorization response 172 back to the POS terminal 181." '095 Provisional (Ex.1005), ¶¶0044-0047; '248 Provisional (Ex.1006), ¶¶0053-0055 **"Payment Process** The principles for the payment process (Mobile to Cloud) are: 1. The Mobile Payment Application must have retrieved at least one (KS_{UN}, Cloud_$CVC3_{TRACK1/2}$, ATC) before the Tap. 2. The dynamic values (CVC3 and ATC) are used as a first form factor to authenticate the payment transaction. The Online PIN can be used as a second form factor." '095 Provisional (Ex.1005), ¶0056.

	"► Delivery of Encrypted Payload [using $K_{Storage}$] (KS_{UN}, Cloud_$CVC3_{TRACK1/2}$ and ATC) to Mobile Payment Application" '095 Provisional (Ex.1005), ¶0068. "4. If the validation of the CAP Token is successful, the cloud-based transaction data generation system 106 generates the CVC3 value using a genuine KD_{CVC3} and returns an encrypted payload to the Mobile Payment Application." '095 Provisional (Ex.1005), ¶0056. "Encrypted (using $K_{Storage}$) Payload sent to the Mobile Payment Application (Valid for one contactless payment transaction) ◊ Cloud_$CVC3_{TRACKI/2}$ ◊ ATC ◊ KSUN '095 Provisional (Ex.1005), p. 23 "Payload sent to the Issuer ◊ Identifier (PAN ...) ◊ UNCLOUD ◊ ATC ◊ Authentication Status Info+ Additional Generation Information (e.g. Validity) **$CVC3_{TRACKI/2}$** Mobile Payment Application to perform CVC3 generation using: ◊ Information from the Reader ◊ Stored Information ◊ Credentials previously retrieved from the Cloud CVC3 value to be included in Payment Authorization message (Track 2 (and Track 1) information). '095 Provisional (Ex.1005), p. 23

	"Issuer Validation Process An exemplary validation process is described below wherein the Issuer 180 uses the information provided in the payment transaction: • Identifier - e.g. PAN Information • UN_{READER} (4 bytes) - Partial Information retrieved from Track data (Discretionary Information) • ATC (2 bytes)-Partial Information retrieved from Track data (Discretionary Information) • $CVC3_{TRACK1/2}$ Partial Information retrieved from Track data (Discretionary Information) *** The Issuer can validate the **$CVC3_{TRACK1/2}$**." '095 Provisional (Ex.1005),¶¶0072-0074 "The dynamic values (CVC3 and ATC) are used as a first form factor to authenticate the payment transaction. The Online PIN can be used as a second form factor. This dynamic CVC3 value is generated by the mobile payment application using information from the payload provided by the cloud-based transaction data generation system 106 ('the Cloud')." '095 Provisional (Ex.1005), ¶0112



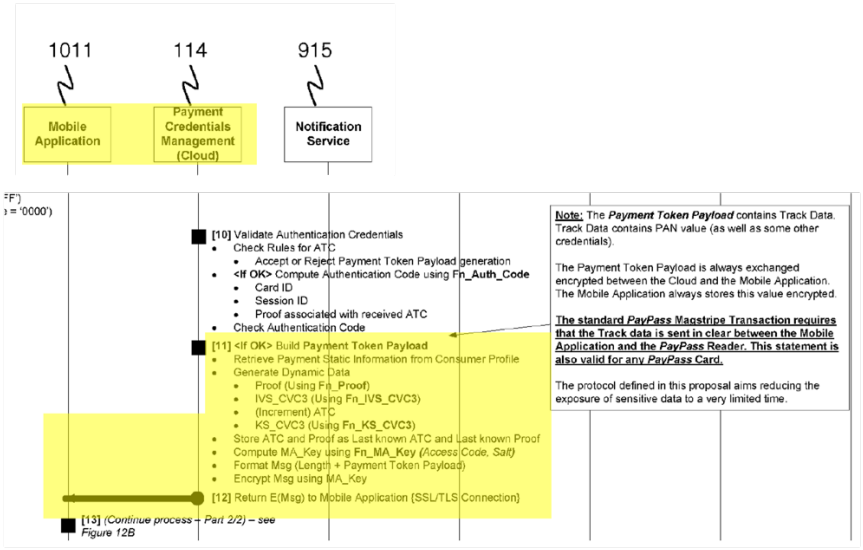
'095 Provisional (Ex.1005), Fig. 5 (annotated excerpt);
'095 Provisional (Ex.1005), Figs. 1, 6-8

"In stage [11], the payment token payload is built. In the exemplary embodiment of Figure 12A this stage includes retrieving payment static information from the consumer profile and generating dynamic data. Such dynamic data generation includes: the proof (using Fn_Proof), the IVS_CVC3 (using Fn_IVS_CVC3), incrementing the ATC, and the KS_CVC3 (Using Fn_KS_CVC3)."

'248 Provisional (Ex.1006), ¶0161

"Stage [11] continues with the computation of the MA_Key using Fn_MA_Key (Access Code, Salt), formatting of the message Msg (Length+ Payment Token Payload) and encryption of Msg using MA_Key before proceeding to stage [12] where the E(Msg) is returned to the mobile application 1011 over the SSL/TLS Connection."

'248 Provisional (Ex.1006), ¶0166



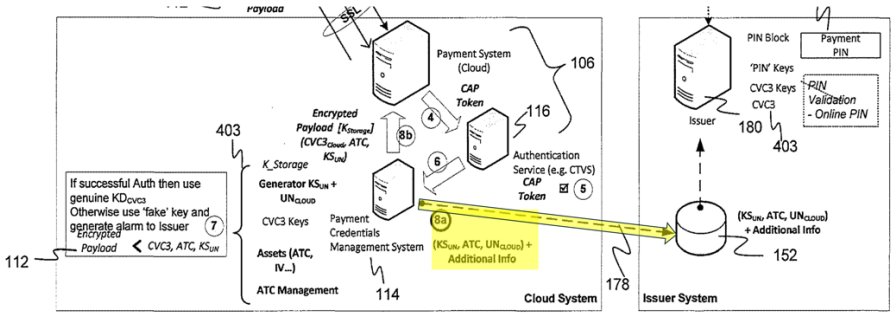
'248 Provisional (Ex.1006), Fig. 12A (annotated excerpt)

transmitting, by the transmitting device, at least the KS_{UN}, UN_{CLOUD}, and application transaction counter to an issuer associated with the payment account for use in validating the generated dynamic card validation code used in the financial transaction.

The Collinge Provisionals disclose the cloud-based transaction data generation system transmitting KS_{UN}, UN_{CLOUD}, and application transaction counter to an issuer associated with the account for use in validating the generated dynamic card validation code used in the financial transaction.

8a	There is synchronization process between the Cloud and the Issuer. The synchronization process may include the definition of rules for the validity of the generated CVC3 values.

'095 Provisional (Ex.1005),Table 1 (p. 16)



'095 Provisional, Fig. 5 (annotated excerpt);
'095 Provisional (Ex.1005), Figs. 6-7

19a	The Issuer has a mean to identify transaction that requires additional processing for CVC3 validation when an embodiment using SE-less Mobile Contactless Payment is used. Using the ATC provided in the Payment Transaction, the Issuer is able to retrieve the UN_{CLOUD} and KS_{UN} values that were used by the Payment Credential Management System to generate the CVC3 value. Detection of unsuccessful authentication can also take place at this stage.
19b	A standard process applies for the CVC3 validation using the UN_{CLOUD} and KS_{UN} values.
20	The completion of the Payment transaction process remains unchanged.

'095 Provisional (Ex.1005), Table 1 (p. 17)

"Payload sent to the Issuer
◊ Identifier (PAN ...)
◊ UN_{CLOUD}
◊ ATC
◊ Authentication Status Info+ Additional Generation Information (e.g. Validity)"

'095 Provisional (Ex.1005), p. 23

"Issuer Validation Process
An exemplary validation process is described below wherein the Issuer 180 uses the information provided in the payment transaction:

- Identifier - e.g. PAN Information
- UN_{READER} (4 bytes) - Partial Information retrieved from Track data (Discretionary Information)
- ATC (2 bytes)-Partial Information retrieved from Track data (Discretionary Information)
- $CVC3_{TRACK1/2}$ Partial Information retrieved from Track data (Discretionary Information)

The Issuer system is able to compute Cloud_$CVC3_{TRACK1/2}$ using:

- $IVCVC3_{TRACK1/2}$ (2 bytes)
- UN_{CLOUD} (4 bytes)
- ATC (2 bytes)

The Issuer system is able to compute $CVC3_{TRACK1/2}$ using:

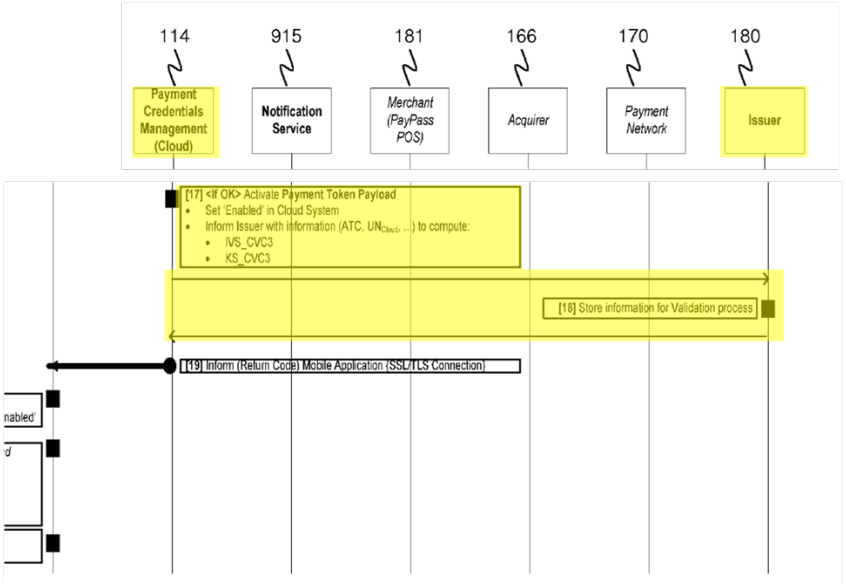
- $Cloud\_CVC3_{TRACK1/2}$ (2 bytes)
- UN_{READER} (4 bytes)
- ATC (2 bytes)

The Issuer can validate the $CVC3_{TRACK1/2}$"

'095 Provisional (Ex.1005), ¶¶0072-0074;
'248 Provisional (Ex.1006), ¶0226 (p. 54)

"In stage [17], the payment token payload is activated by setting 'Enabled' in the cloud-based transaction data generation system 106. Then, the issuer 180 is provided (informed) with information (ATC, UN_{CLOUD}, ...) needed to compute the IVS_CVC3 and KS_CVC3. In stage [18], this information is stored for a subsequent validation process."

'248 Provisional, ¶0172



'248 Provisional (Ex.1006), Fig. 12A (annotated excerpt)

	"CVC3 Validation process (*Fn_ValCVC3*) by the Issuer using information provided by the Cloud at time of the synchronization process;" '248 Provisional (Ex.1006), ¶0184 Next, in stage [14], CVC3 validation is done using Fn_ValCVC3 before proceeding to stage [15], where the standard process for PayPass Magstripe Transaction is completed between the issuer 180, the payment processing network 170, the Acquirer 166, and the Merchant 181 (see reference number 14 in Figure 15). '248 Provisional (Ex.1006), ¶¶0203 "*UN_{CLOUD} is part of the payload exchanged between the Cloud and the Issuer during the Synchronization process*." '248 Provisional (Ex.1006), ¶0224. "**Fn ValCVC3** This function validates CVC3 values (Track 1 and Track 2) generated by the Mobile Payment Application using UN_{Reader} and the content of the Payment Token Payload. For the validation process, the Issuer uses the information provided in the payment transaction: ♦ Identifier - e.g. PAN Information retrieved from Track Data ♦ UN_{READER}(4 bytes) - Partial Information retrieved from Track data (Discretionary Information) ♦ ATC (2 bytes) - Partial Information retrieved from Track data (Discretionary Information) ♦ $CVC3_{TRACK1/2}$ - Partial Information retrieved from Track data (Discretionary Information) The Identifier and ATC values are used to retrieve the information provided by the cloud-based transaction data generation system 106 ("the Cloud system"): ◊ Identifier (PAN, ...) ◊ UN_{CLOUD} ◊ ATC

	◊ (Option) Additional Generation Information The issuer 180 system is able to compute IVS_CVC3 using: ◊ $IVCVC3_{TRACK112}$(2 bytes) ◊ UN_{CLOUD} (4 bytes) ◊ ATC (2 bytes) ◊ KD_{CVC3} The Issuer system is able to compute $CVC3_{TRACK1/2}$ using: ◊ IVS_CVC3 (2 bytes) ◊ UN_{READER}(4 bytes) ◊ ATC (2 bytes) ◊ KS_CVC3 The issuer 180 can validate the $CVC3_{TRACK1/2}$ value." '248 Provisional, ¶¶0226 (p. 54) "Generate KS_{UN} using: UL:= DES3(KD_{UN})[(ATC II 'FO' II '00' II UN_{CLOUD})] UR:= DES3(KD_{UN})[(ATC II 'OF' II '00' II UN_{CLOUD})] KS_{UN} := (UL II UR) **KS_CVC3 := KS_{UN} generated in the Cloud**" '248 Provisional (Ex.1006), ¶¶0226 (p. 53)

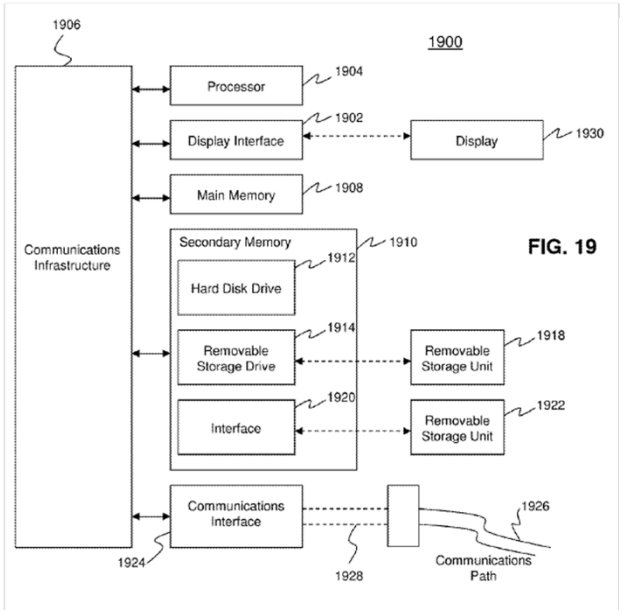
3. Support for Collinge in Collinge Provisionals

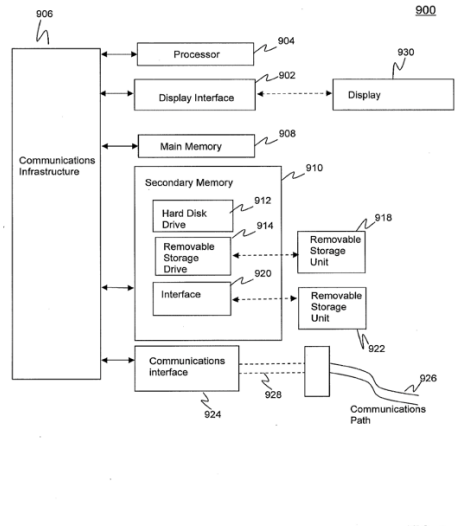
85. I have been informed that for Collinge to be §102(e) prior art as of the filing date of the Collinge Provisionals, the Collinge Provisionals must provide written description support for the subject matter relied upon in the petition. *See In re Giacomini*, 612 F.3d 1380, 1383 (Fed. Cir. 2010). "To satisfy the written description requirement, the claimed subject matter need not be described "in haec

verba" in the original disclosure. *See In re Wright*, 866 F.2d 422, 425 (Fed. Cir. 1989). Rather, the test for determining compliance with the written description requirement is whether the original disclosure of the patent application reasonably conveys to a person of ordinary skill in the art that the inventor had possession of the claimed subject matter as of the filing date. *Ariad Pharms., Inc. v. Eli Lilly & Co.*, 598 F.3d 1336, 1351 (Fed. Cir. 2010) (*en banc*)."

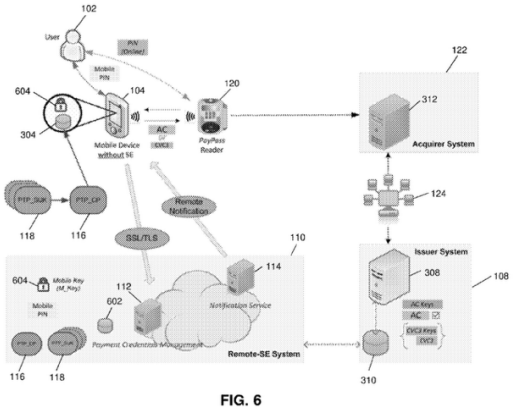
86. My opinion relies on many disclosures from Collinge, each of which a POSITA would have understood to be disclosed by the Collinge Provisionals.

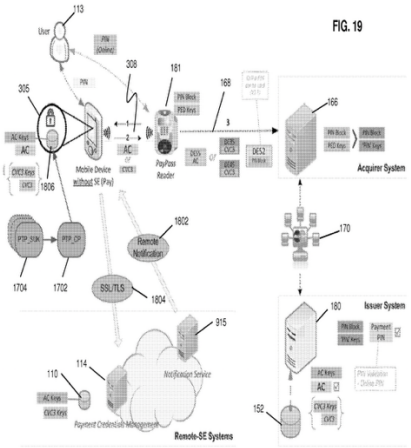
87. All portions of Collinge cited in the proposed ground below appear substantially identically in Collinge Provisionals. I have endeavored to include citations to corresponding disclosures in the Collinge Provisionals in the charts above. Accordingly, the disclosure relied on to meet challenged claim limitations is entitled to Collinge Provisionals' filing date. Further, Collinge's provisional applications are directed to the same invention. Figures, invention elements numbering, and invention descriptions substantially overlap, and a POSITA would recognize that the Provisionals provide additional implementation details relevant to Collinge's payment system. *Compare '098 Provisional (Ex. 1008)*, Fig. 19 *with Collinge (Ex. 1004),* Fig. 6; *'095 Provisional (Ex. 1005),* Fig. 9 *with Collinge (Ex. 1004),* Fig. 19 and *'248 Provisional (Ex.1006),* Fig. 16.





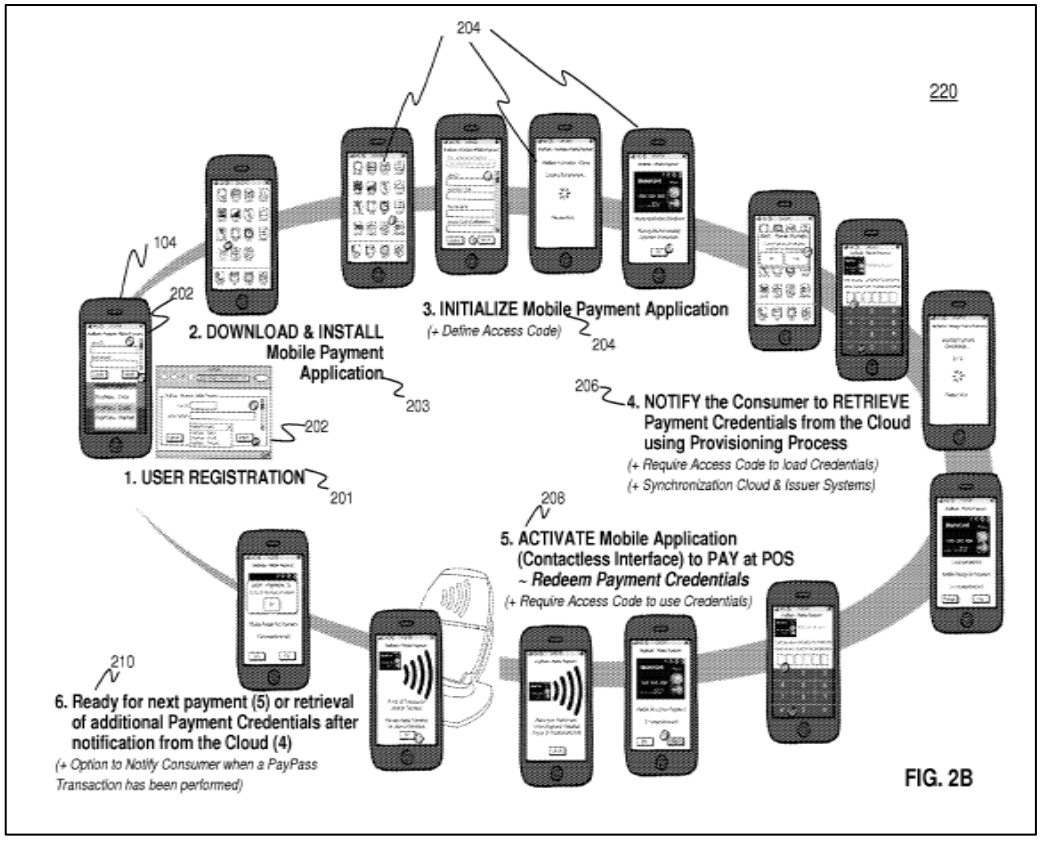
Collinge at Figure 19 (left); *'095 Provisional (Ex. 1005),* Figure 9 (right).





Collinge at Figure 6 (left); *'095 Provisional (Ex. 1005),* Figure 19 (right). 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. 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 (Ex. 1006),* Fig. 2A, 2B; *'098 Provisional (Ex. 1008)*, p. 96-100; *Collinge (Ex. 1004),* [0133].



'248 Provisional (Ex. 1006), Fig. 2B. A POSITA would have found it obvious and would have been motivated to incorporate these disclosures into Collinge's payment system, As another example, Collinge teaches use of a "CAP token" (*Collinge (Ex. 1004),* [0144]) and the provisional applications provide examples of what controls on purchases may be represented by the token. *See '095 Provisional (Ex. 1005),* Claims 9-10 (day of week, time of day, etc.). 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 Provisional. A POSITA would have appreciated that using a timer would "limit the potential exposure of sensitive data" as taught by Collinge. *Id.* A POSITA looking to implement a CAP token would have been motivated to implement one or more of the examples of a CAP token in Collinge's Provisional application. In each case, a POSITA would have found a teaching, suggestion, or motivation in Collinge since the provisional was directed to the same mobile device used in Collinge, that would have led them to apply the additional details in Collinge's Provisionals to Collinge's payment system and would have had a reasonable expectation of success.

Lin

88. Lin was filed August 11, 2009, and published on April 8, 2010. Lin describes "various techniques…for carrying out peer-to-peer financial transactions using one or more electronic devices 10, 92. *Lin* at Abstract. Lin teaches techniques for "carrying out peer-to-peer financial transactions using one or more electronic devices 10, 92[.]" *Lin* at Abstract. "As shown in FIG. 4, the device 10 acts as the payee device of the transaction, and the second device 92 acts as the payor device." *Lin* at 30:18-19. "Payee" refers to "one party in a transaction that is receiving a payment" and "payor" refers to "another party in the transaction that is making the

payment." *Lin* at 30:11-15. "Initially, the payee device 10 may transmit a payment request, illustrated herein by reference numeral 94, to the payor device 92." *Lin* at 30:19-21.

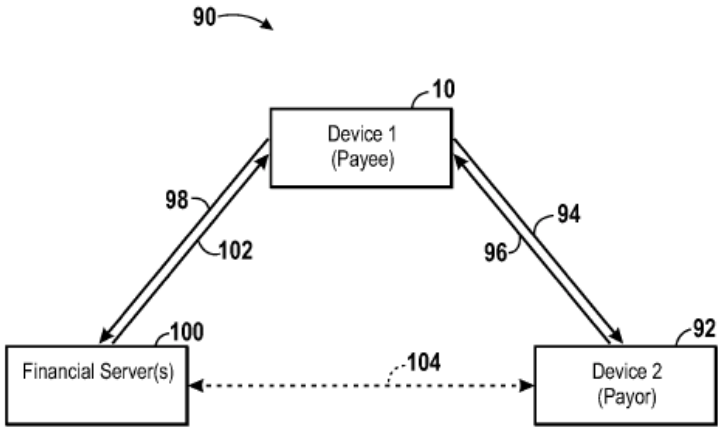


FIG. 4

Lin at Figure 4.

89. Figures 11B depicts a flowchart that illustrates the method of operating the payor device of Figure 4. *Lin* at 7:11-15. Specifically, figure 11B "illustrates a method 360 describing the receipt of a transaction request…from the viewpoint of a payor" *Lin* at 52:20-23 (emphasis added). The "transmission of the payment request…may be accomplished by way of an NFC connection between a payee device 10 and a payor device 92." *Lin* at 55:20-22. Lin further teaches that "receipt of the payment request at step 364 may correspond to the transmission of the invoice statement at step 334 of the method 328." *Lin* at 55:10-12. "Transmission of the invoice statement" is a step of method 328, which teaches a method for "initiating

and subsequently processing a transaction from the viewpoint of a payee[.]" *Lin* at 52:17-20. Lin states "the term 'invoice' may refer to the general terms of a payment request, which may include the amount of the requested payment, the identity of the requesting payee, as well as additional information describing the nature or reasons as to why the payment is being requested." *Lin* at 52:27-30.

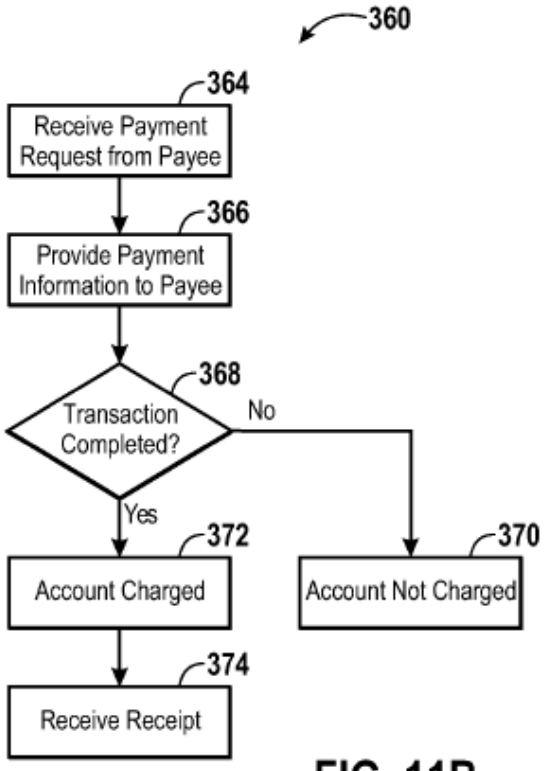


FIG. 11B

Lin at Figure 11B.

90. Lin further teaches that "once the payment request has been received by the payor device, the screen 516 may be updated to display the details 540 of the payment request[.]" *Lin* at 71:7-9, Figure 14. The screen "may further display the

presently selected payment account 554." *Lin* at 71:24-25. As depicted below 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.

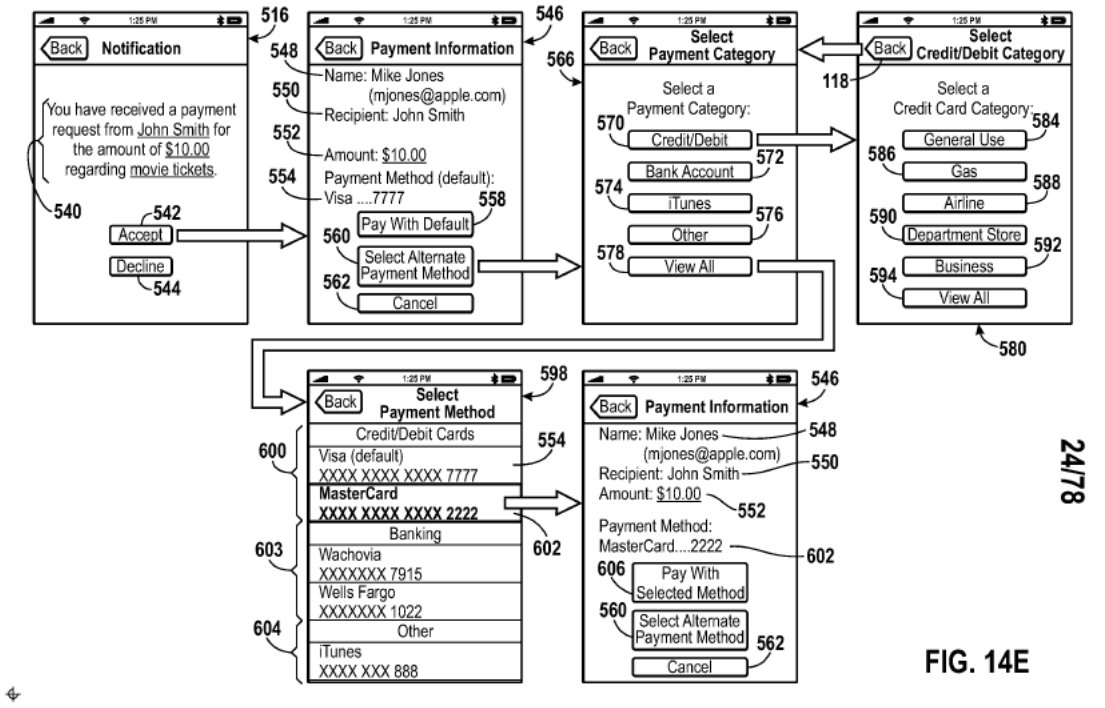


FIG. 14E

Lin at Figure 14E.

4. Lin is Analogous

91. Lin is analogous art to the '579 Patent because it is from the same field of endeavor. Like the '579 Patent, Lin is concerned with conducting secure payment transactions. *See, e.g., Lin* at Abstract ("…one or more external financial servers 100 configured to process and determine whether the payment may be authorized."), 33:2-7 ("Regardless of the type of connection established between the device 10 and the financial servers 100, it should be understood that one or more of the data

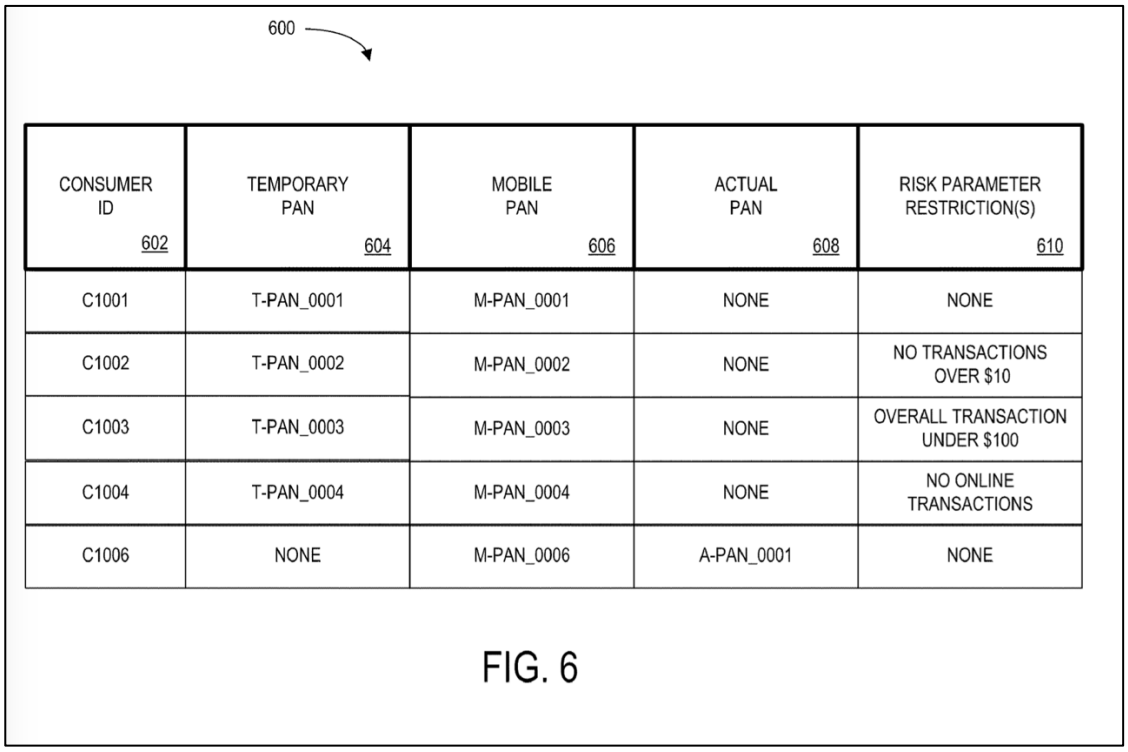
encryption techniques and security protocols…may be further utilized in order to facilitate the secure transmission of the transaction data 98 to the financial servers 100."), 98:7-10 (The smart card server 874 may perform a one or more verification and/or authorization processes…wherein the payor's smart card account 872 is verified for validity and sufficiency of funds, for example."). *Compare '579 Patent*, Abstract, 1:23-27, *with Lin,* Abstract, 68:13-25, Fig. 14C.

92. Lin is also reasonably pertinent to at least one problem addressed by the '579 Patent. Like the '579 Patent, Lin is concerned with increasing security of payment transactions. *See, e.g., Lin* at 26:26–27:7 ("The security features 74 may be stored in the storage device 54 and may include one or more cryptographic protocols, such as a secure sockets layer (SSL) protocol or a transport layer security (TLS) protocol, for establishing secure communications between the device 10 and an external device. The security features 74 may also include one or more encryption applications for encrypting information sent from the device 10."), *see also Lin* at 27:8–28:15. *Compare '579 Patent,* 1:23-27, 2:4-12, 9:63-10:2 *with Lin*, 26:26-28-15.

Smith

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

94. I understand Smith teaches a "mobile PAN" is used in place of the actual PAN. *Smith* at [0023] (the PPAN is associated with a "related PAN[.]"). *See also Smith* at [0026].



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 at Fig. 6. The mobile PAN is "stored in the mobile device 204." *Smith* at [0022].

5. Smith is Analogous

95. Smith is analogous art to the '579 Patent because it is from the same field of endeavor. Like the '579 Patent, Smith is concerned with conducting secure payment transactions. *See, e.g., Smith* at Abstract ("The mobile device may then be used, for example, in connection with a near field communications enabled purchasing transaction."), [0021] ("System 200 includes a number of components or

entities which interact to allow a mobile device 2104 to be used to conduct a payment transaction using a payment application stored in the mobile device 204[.]"), *see also* Smith at [0022]-0023], [0029].

96. Smith is also reasonably pertinent to at least one problem addressed by the '579 Patent. Like the '579 Patent, Smith is concerned with increasing security of payment transactions. *See, e.g., Smith* at [0002] ("One approach…is to securely install a payment application in mobile phones that are Near Field Communications (NFC)-enabled[.]"), [0015] ("The issuer 106 may also provide one or more risk data elements which the issuer may use to define transaction parameters in which transactions may be authorized."), [0020] ("The over-the-air personalization may provide a secure transfer of the cardholder's payment account information[.]"), *see also* Smith at [0029], [0032]. *Compare '579 Patent,* 1:23-27, 2:4-12, 9:63-10:2 *with Smith*, [0002], [0015], [0020].

Kranzley

97. I understand 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].

6. Kranzley is Analogous

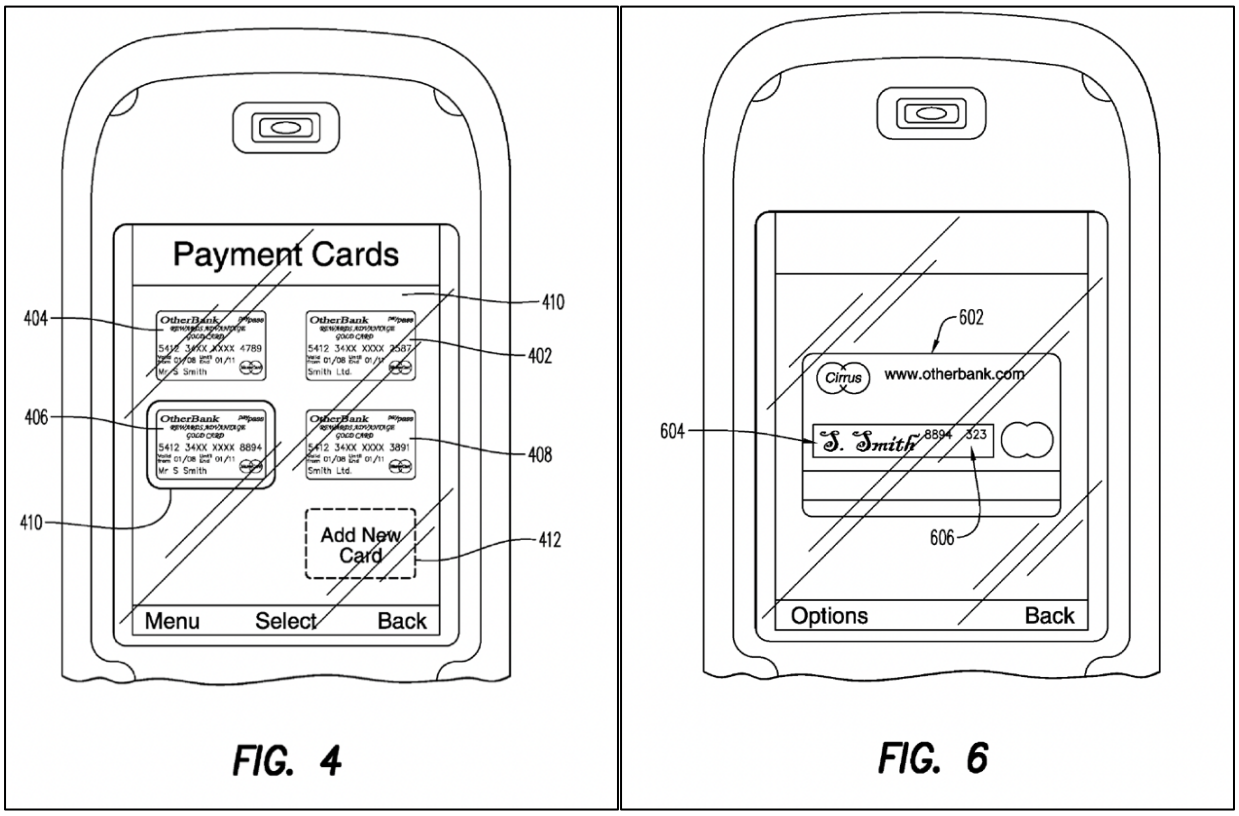
98. Kranzley is analogous art to the '579 Patent because it is from the same field of endeavor. Like the '579 Patent, Kranzley is concerned with conducting secure payment transactions. *See, e.g., Kranzley* at Abstract ("Systems, methods processes, computer program code and means for conducting a payment transaction which include…a dynamic verification code generated by the payment application[.]"), [0003] ("It would further be desirable to provide mobile payment transactions which are secure and in which the cardholder's presence may be confirmed."), [0010] ("…and means for conducting a payment transaction include…at least one of a payment account number, an expiry date of said payment account number, and a dynamic verification code generated by said payment application[.]").*Compare '579 Patent*, Abstract, 1:23-27 *with Kranzley* Abstract, [0010], Fig. 1.

99. Kranzley is also reasonably pertinent to at least one problem addressed by the '579 Patent. Like the '579 Patent, Kranzley is concerned with increasing security of payment transactions. *See, e.g., Kranzley* at [0003] ("It would further be desirable to provide mobile payment transactions which are secure and in which the cardholder's presence may be confirmed."), [0065] ("As a specific example, for VPANs processed over the payment network operated by MasterCard International Incorporated, VPANs are 16 digit numeric codes in which the first 6 digits are used to identify the VPAN as a VPAN to be routed to a payment provider 110 for

processing."), [0067] ("The shared secret key may be used to encrypt a dynamic value transmitted from the mobile device. The payment provider 110 may use the shared secret key, in conjunction with the counter 508, to decrypt the dynamic value from the mobile device 102 to ascertain the authenticity of the transaction request."). *Compare '579 Patent*, 1:23-27, 2:4-12, 9:63-10:2 *with Kranzley*, [0003], [0065].

Phillips

100. I understand Phillips teaches "a user interface that may facilitate use of mobile telephones for contactless payment transactions[.]" *Phillips* at [0006]. Phillips, similar to 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* at [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* at [0012]. As shown below Phillips teaches displaying both the front and back of the payment card. *Phillips* at [0049].



Phillips at Figs. 4, 6.

7. Phillips is Analogous

101. Phillips is analogous art to the '579 Patent because it is from the same field of endeavor. Like the '579 Patent, Phillips discloses a mobile device with a mobile payment application used to conduct secure payment transactions. *See, e.g., Phillips* at Abstract ("A payment card account number is downloaded to a contactless payment application program stored in a mobile telephone. In association with the payment card account number, at least one image that represents a payment card is also downloaded to the contactless payment application program stored in the mobile telephone. The at least one card payment card image displays the

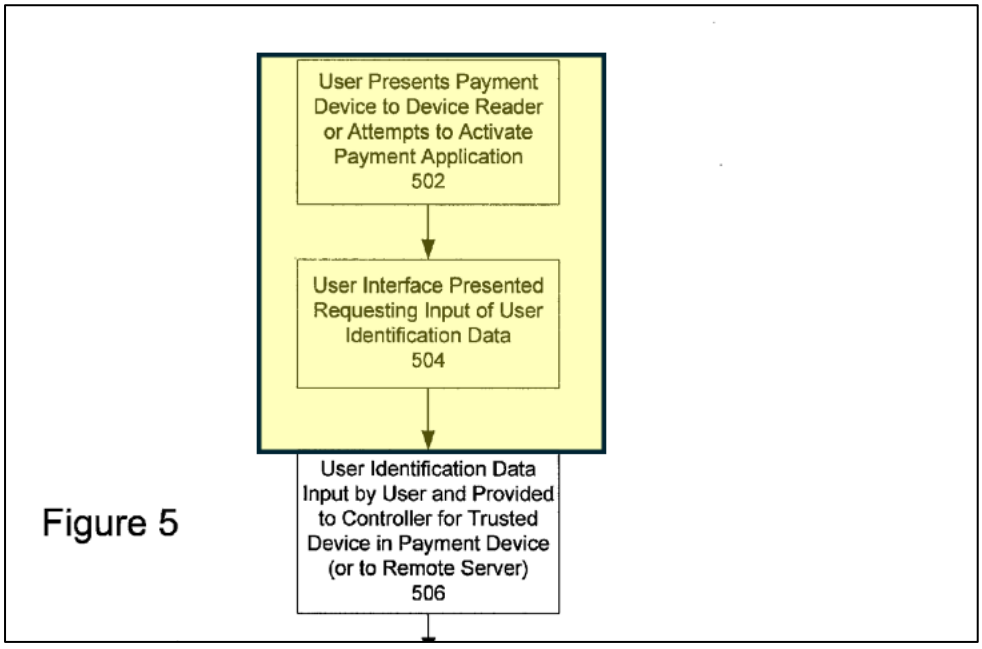
downloaded payment card account number."); [0006] ("The present disclosure addresses issues related to a user interface that may facilitate use of mobile telephones for contactless payment transactions and other types of transactions."); [0012] ("In this way, for example, the user may select among a number of payment card accounts for use in a current purchase transaction."); [0014] (" Since the mobile phone 100 is also operable for contactless payment transactions, in addition to conventional mobile phone functions") *Compare '579 Patent*, Abstract, 1:23-27, Fig. 1 *with Phillips,* Abstract, [0006], [0012], [0014], Fig. 1.

102. Phillips is also reasonably pertinent to at least one problem addressed by the '579 Patent. Like the '579 Patent, Phillips is concerned with providing a mobile application and related user interface on a mobile device that allows for contactless payments. *See, e.g., Phillips* at [0006] ("The present disclosure addresses issues related to a user interface that may facilitate use of mobile telephones for contactless payment transactions and other types of transactions."); [0012] ("At that point, if the user positions the mobile phone for reading by a proximity reader, then the mobile phone uploads to the proximity reader an identification number which corresponds to the selected and displayed card image."); [0027] ("Selection of the wallet icon may provide the path by which the user may access functions such as a contactless payment function.") *Compare '579 Patent,* 1:23-27, 2:4-12, 9:63-10:2 *with Phillips*, [0006], [0012]-[0014], [0027]-[0029].

Aabye

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

104. In response to the user presenting the "payment device to device reader", "the user is presented with a user interface." *Aabye* at [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). An example of identification is "a fingerprint reader for input of a user fingerprint[.]" *Aabye* at [0055].



Aabye at Fig. 5. (annotated excerpt)

105. Aabye's 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* at [0057].

8. Aabye is Analogous

106. Aabye is analogous art to the '579 Patent because it is from the same field of endeavor. Like the '579 Patent, Aabye is concerned with conducting secure payment transactions. *See, e.g., Aabye* at Abstract, ("A system, apparatus, and method for preventing the unauthorized access to a payment application installed on a mobile payment device, or to transaction data stored in the device. The mobile payment device may be a mobile phone that includes a contactless element (such as a contactless smart chip) and that is capable of communication and data transfer using a wireless communications network and a near field communications capability."); [0054] ("As shown in the figure, in an exemplary case, at stage 502 a user presents their payment device to a device reader or point of sale terminal (POS), or otherwise attempts to activate a payment application installed on the payment device. For example, the user may "swipe", "wave", or otherwise present their payment device to the device reader in an attempt to initiate a payment transaction using a near field or short range communications capability of the device.")

Compare '579 Patent, Abstract, 1:23-27 *with Aabye* Abstract, [0010], [0054], Fig. 1, Fig. 5.

107. Aabye is also reasonably pertinent to at least one problem addressed by the '579 Patent. Like the '579 Patent, Aabye is concerned with increasing security of payment transactions. *See, e.g., Aabye* at Abstract, ("A system, apparatus, and method for preventing the unauthorized access to a payment application installed on a mobile payment device, or to transaction data stored in the device…. Unauthorized access to the payment application is prevented by requiring that access control data be received from a trusted source, such as a controller or application in charge of managing inputs from a phone keypad, in order to activate the payment application or to access stored data."); [0009] ("What is desired is a system, apparatus and method for preventing unauthorized access to a payment application installed on a mobile payment device or to transaction data stored in the device, particularly for the case of a payment device that is capable of communications using a wireless network."); [0010] ("The security code and passcode are verified by the payment application, and if both are valid, then the payment application and/or secure transaction data is made available to the user.") *Compare '579 Patent,* 1:23-27, 2:4-12, 9:63-10:2 *with Aabye*, Abstract, [0002]-[0010].

Pisula

108. Pisula teaches determining "whether the detected interaction by the user with the first physical button corresponds to a second predefined action, the second predefined action being different from the first predefined action" via "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* at 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* at 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* at 14:23-25.

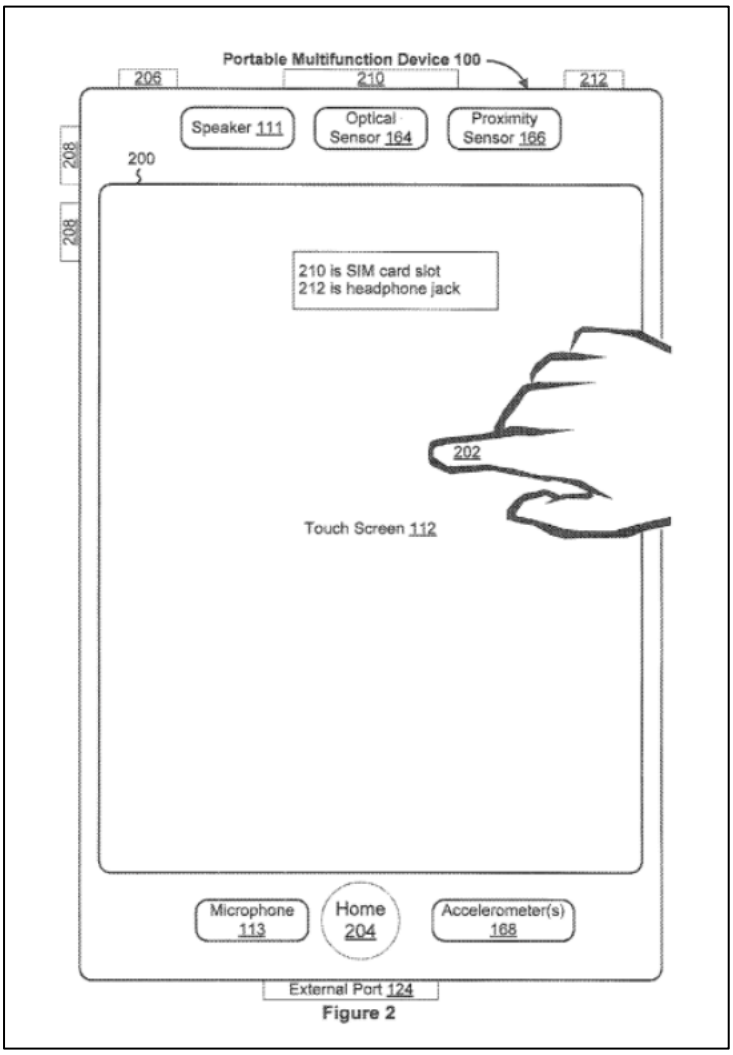


Figure 2

Pisula, Fig. 2.

9. Pisula is Analogous

109. Pisula is reasonably pertinent to at least one problem addressed by the '579 Patent such as providing access to functions of mobile applications on a mobile device through specific user interactions with the device's user interface. *See, e.g., Pisula* at 14:23-25 ("longer press of the push button (e.g., 206) may turn power to the device 100 on or off."); 28:57-64 ("whether the detected interaction by the user

with the first physical button corresponds to a second predefined action, the second predefined action being different from the first predefined action" via "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).") *Compare '579 Patent,* 1:23-27, 2:4-12, 9:63-10:2,11:34-42, 15:14-24; with *Pisula*, 28:57-64; 14:23-25, Fig. 1A, Fig. 2.

Fadell

110. 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* at [0065]-[0066].

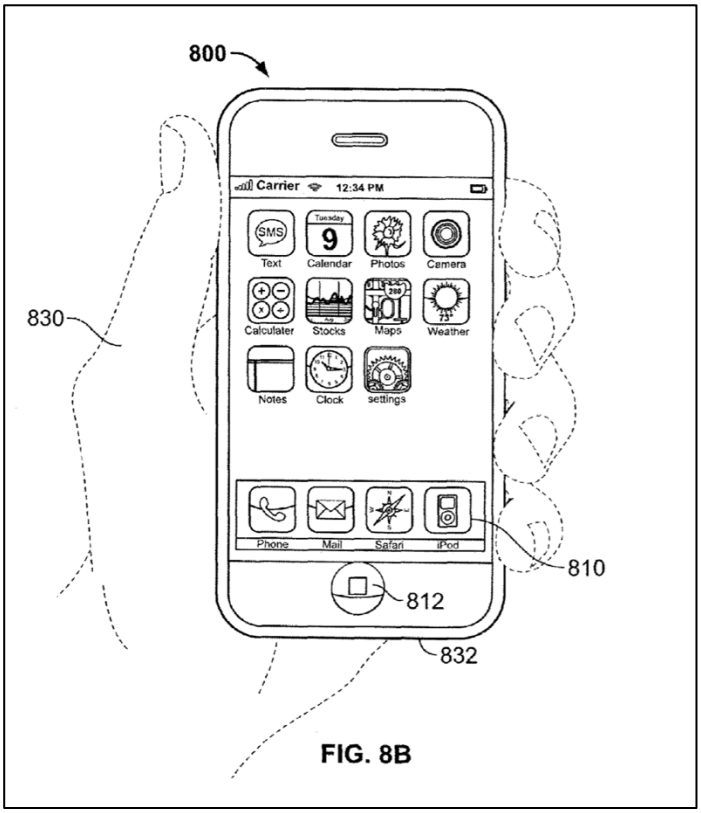


FIG. 8B

Fadell at Figure 8B.

111. 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* at [0006].

10. Fadel is Analogous

112. Fadell is analogous art to the '579 Patent because it is from the same field of endeavor. Like the '579 Patent, Fadell is concerned with authentication systems for an electronic device such as a mobile phone, including authenticating a user for accessing restricted information such as "transaction information data (e.g., information such as credit card information).". *See, e.g., Fadell* at Abstract ("This

invention is directed to an electronic device with an embedded authentication system for restricting access to device resources."), [0031] ("Storage 104 may store…transaction information data (e.g., information such as credit card information)[.]"). *Compare '579 Patent*, Abstract,1:23-27, 2:4-12, 9:63-10:2, *with Fadell,* Abstract, [0031].

113. Fadell is also reasonably pertinent to at least one problem addressed by the '579 Patent. Like the '579 Patent, Fadell is concerned with increasing security of access to sensitive payment information. *See, e.g., Fadell* at [0004] ("It would be desirable, therefore, to provide an electronic device by which biometric and other authentication mechanisms are implement in the device such that the device authenticates the user quickly and seamlessly[.]"), [0054] ("The electronic device may use any suitable type of authentication system to prevent unauthorized access of device resources."), [0064] ("To provide for secure access to resources, electronic device 700 may include at least one sensor 720 operative to detect features of a user's fingerprint to identify the user.") *Compare '579 Patent,* 1:23-27, 2:4-12, 9:63-10:2 *with Fadell*, [0004], [0054], [0064].

VIII. SUMMARY OF UNPATENTABILITY

114. I have reproduced the Proposed Grounds of Unpatentability from the Petition for ease of reference:

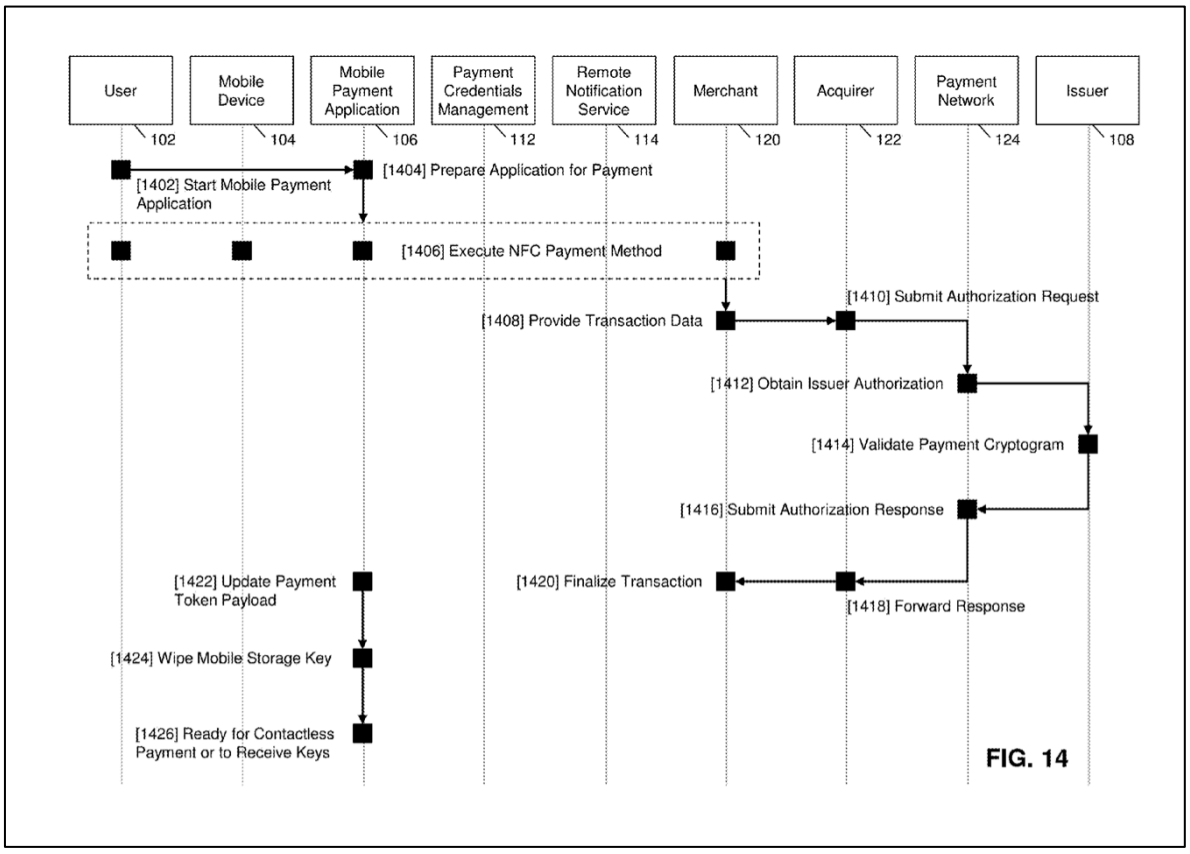
Ground	Claim(s)	References

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)

IX. OPINIONS REGARDING GROUND 1: COLLINGE, LIN, AND PHILLIPS.

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

115. Illustrated in Figure 14 below, Collinge teaches a method of performing a payment transaction. Specifically, Collinge at Figure 14 teaches "a flow diagram illustrating a method for conducting a contactless payment transaction using the mobile payment application 106 on the mobile device 104[.]" *Collinge* at [0118]. I note that the method of Figure 14 is related to the system of Figure 1. *Collinge* at [0029].



Collinge at Figure 14.

116. Collinge explains that in "step 1402, the user 102 may start the mobile payment application 106 on the mobile device 104" then the mobile payment application 106 "may prepare for payment." *Collinge* at [0119]. "To prepare for payment, the mobile payment application may regenerate the mobile storage key and may retrieve the payment credentials and generating key from the card profile 116 and the single use key 118 in the encrypted local storage 304." *Collinge* at [0119].

117. The "generating key" referenced by Collinge with respect to the method of Figure 14 is first introduced regarding the system of Figure 1. *Collinge* at [0050].

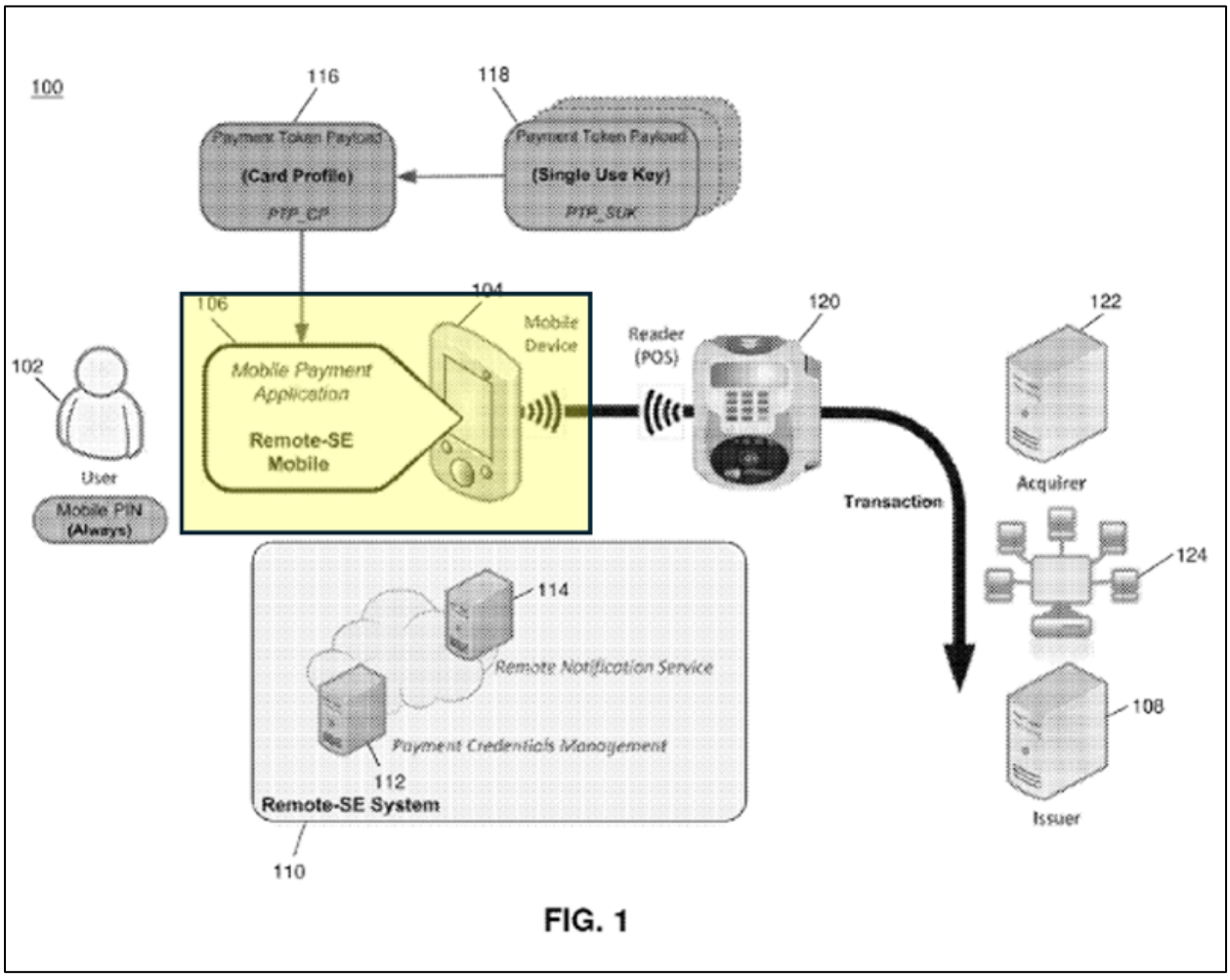


FIG. 1

Collinge, Fig. 1. (annotated)

118. The "generating key" may be included alongside an application transaction count (ATC) as part of single use key 118. *Collinge* at [0050]. "In one embodiment, the generating key 208 may generate a dynamic card validation code (CVC3) or an application cryptogram (AC)." *Collinge* at [0050].

119. Returning to the method of Figure 14, Collinge expressly teaches that the "generating key may be used by the mobile payment application 106 to **generate a payment cryptogram** for use in the payment transaction." *Collinge* at [0119] (emphasis added). In step 1406, "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." *Collinge* at [0120]. To execute the NFC payment, the point-of-sale terminal 120 provides "transaction data to the acquirer 122 including the payment credentials and payment cryptogram[,]" then the acquirer "may submit an authorization request including the transaction data" (i.e., including the payment cryptogram) to the payment network 124." *Collinge* at [0121]. The payment network 124 "may seek authorization from the issuer 108 for the payment transaction[,]" then in step 1414, the "issuer 108 may validate the payment cryptogram." *Collinge* at [0121]. "The issuer 108 may, once the payment cryptogram is validated, approve or deny the payment transaction[.]" *Collinge* at [0121].

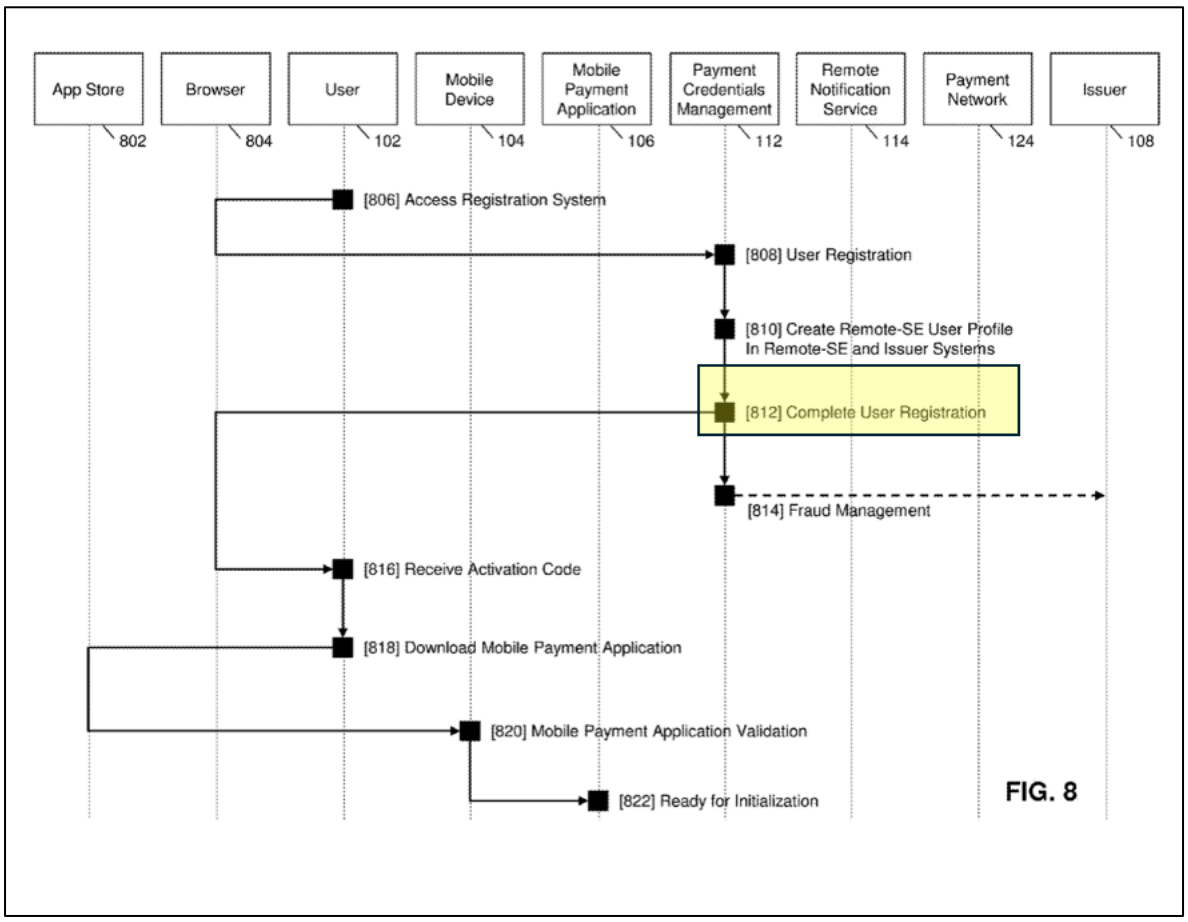
1(a): "receiving an input at an electronic device, wherein the input corresponds to a priming operation of the electronic device by an identified user"

120. Collinge teaches a method "for the user 102 to register with the remote-SE system 110 to enable a payment account for remote payment transactions using a mobile device 104" (e.g., *an electronic device*). Regarding Figure 8, Collinge teaches at "step 806, the user 102 may access the registration system of the remote-SE system 110" via a "web browser 804, which may be executed on a computing device. In one embodiment, the computing device may be the mobile device 104." *Collinge* at [0089].

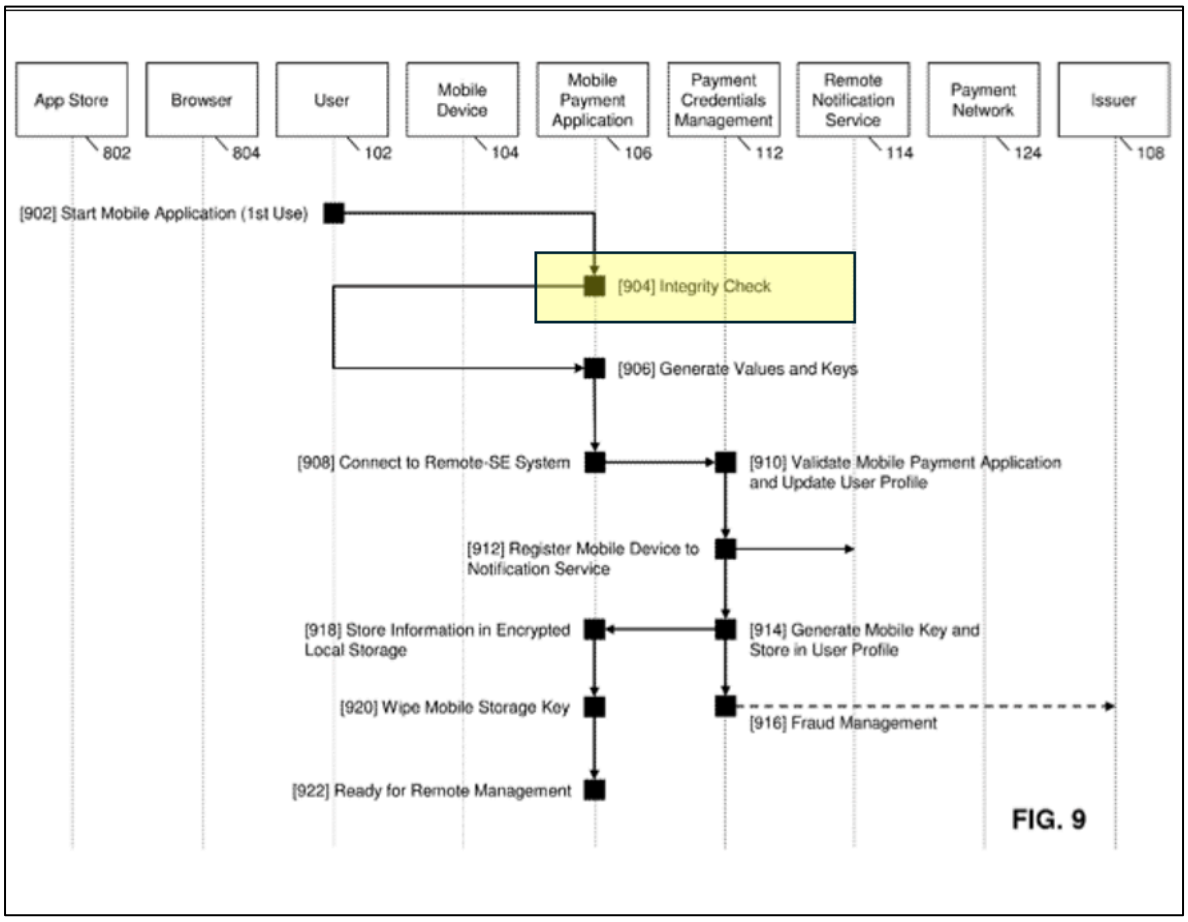
121. At step 808 "the user 102 may register with the payment credentials management service 112" then the payment credentials management service 112 "may create a user profile for the user 102[.]" *Collinge* at [0090]. "As part of the creation of the user profile, the payment credentials management service 112 may generate and/or identify an activation code" that may be transmitted back to the user 102. *Collinge* at [0090], Figure 8.

122. After user registration, Collinge teaches a "method for initialization of the mobile payment application 106 on the mobile device 104 for use in contactless payment transactions." *Collinge* at [0092], Figure 9. "At step 902, the mobile payment application may perform an integrity check. As part of the integrity check, the mobile payment application 106 may authenticate user 102 and request the

activation code provided to the user during the registration process (e.g., at step 812 in FIG. 8). *Collinge* at [0093], Figure 9.



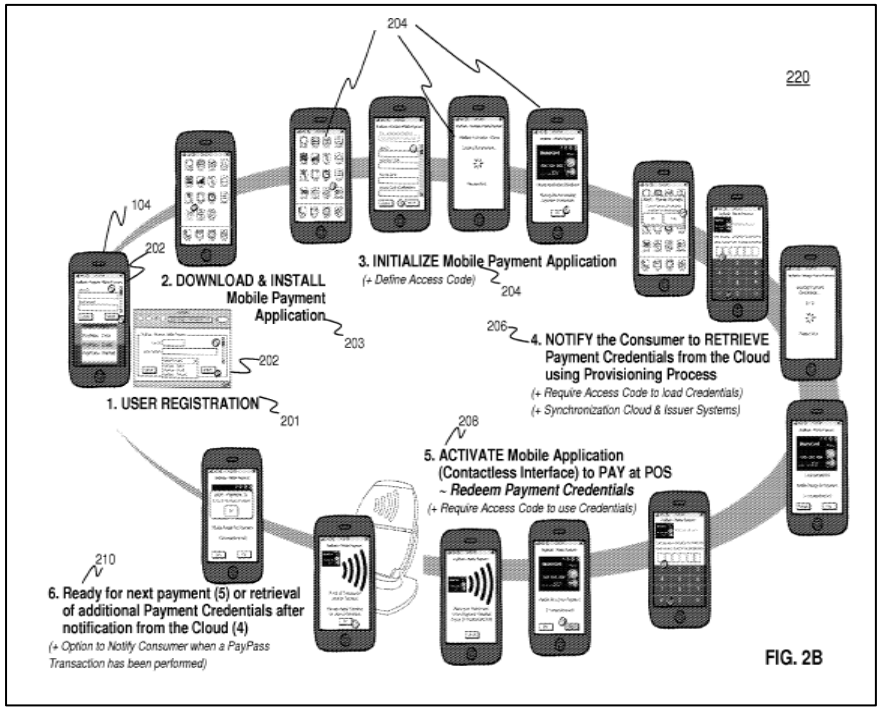
Collinge, Fig. 8. (annotated)



Collinge, Fig. 9.

123. A POSITA would have understood that user 102 inputs the activation code into the mobile payment application 106 during the integrity check using a touch screen of the mobile device for two reasons. First, Collinge expressly teaches that "an input device (e.g., of the mobile device 104, such as a touch screen) may receive a mobile person identification (PIN) input by a user…of the mobile device 104." *Collinge* at [0133]. Though Collinge is referring to a PIN and not an activation code, a POSITA would have understood that the user of the mobile device 104 would similarly input the activation code using a touch screen of the mobile device 104

during the integrity check described above. Second, the '248 Provisional (Ex.1006) application of Collinge expressly shows a mobile device 104 having a "GUI 202" though which "input" is "supplied by a cardholder or user 113[.]" *'248 Provisional (Ex.1006)* at [0068], Figure 2B. Thus, Collinge teaches <u>*receiving an input at an electronic device*</u>.



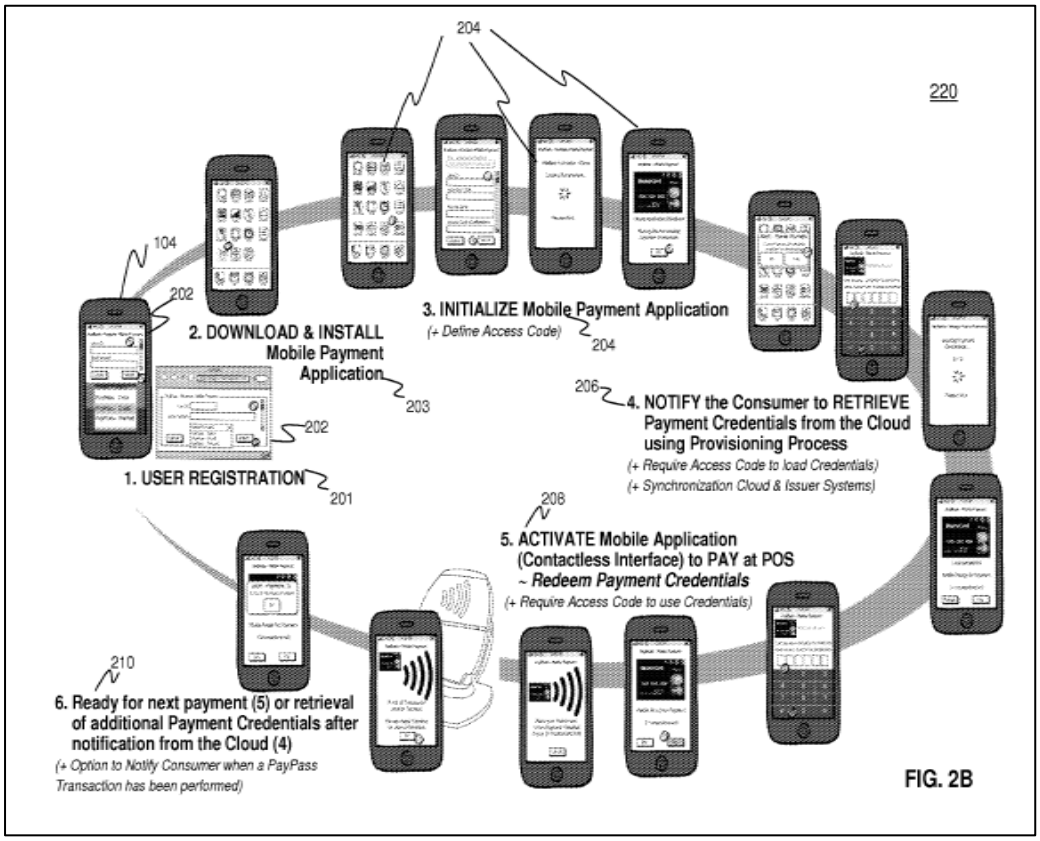
'248 Provisional (Ex.1006) at Figure 2B.

124. As discussed above in the overview section, the'579 Patent discloses a priming operation may have several different examples. *See '579 Patent* (Ex. 1001), 11:34-42 Collinge teaches receiving an activation code (i.e., <u>*input*</u>) at the mobile device 104 (<u>*electronic device*</u>). A POSITA would have further understood that receiving an activation code of the user is one example of a <u>*priming operation*</u>. 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…" *'579 Patent* at 11:34-36. Regarding the activation code, Collinge expressly teaches that "the mobile payment application 106 may transmit the activation code …as a method of authentication." *Collinge* at [0094]. A POSITA would have understood that this method of authenticating the user of the mobile payment application 106 using the activation code on mobile device 104 is an example of a *priming operation* because the activation code authenticates the user. In other words, a POSITA would have understood that when the user inputs the correct activation code during the initialization process taught with respect to Figure 9, the mobile device 104 with mobile payment application 106 is primed for use in conducting a payment transaction using the mobile payment application. As such, Collinge teaches *receiving an input at an electronic device, wherein the input comprises a priming operation*.

125. In the '248 Provisional (Ex.1006) Collinge further teaches, in steps 4 and 5 of Fig. 2B, that a user must input an "access code" in order to both load payment credentials and use the payment credentials during a payment transaction. *'248 Provisional (Ex.1006)* at Figure 2B. Each of step 4 and step 5 are an example of a *priming operation* because they prepare (i.e., prime) mobile device 104 to complete a payment transaction. That is, if in step 4 the payment credentials were

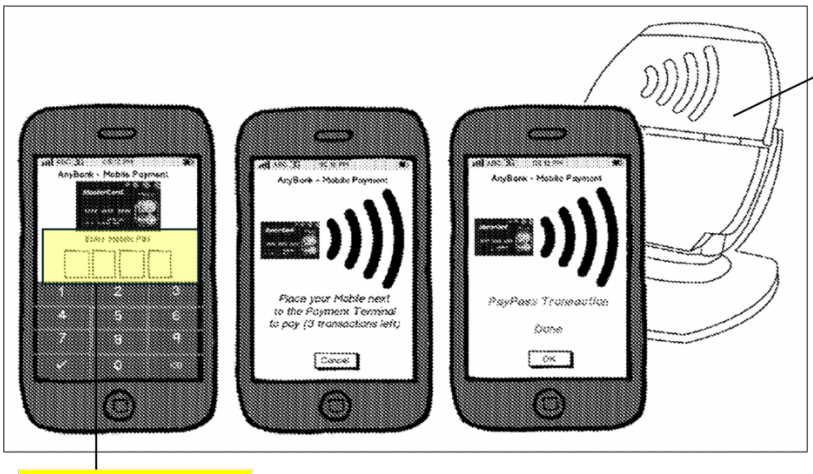
not loaded, mobile device 104 would not be able to conduct a payment transaction because the payment credentials are needed for the payment transition. Similarly, if in step 5 the payment credentials were not able to be used, then the payment transaction would not be completed. Thus, inputting the access code in both step 4 and step 5 are examples of a *priming operation* because they prepare mobile device 104 to successfully conduct a payment transaction.

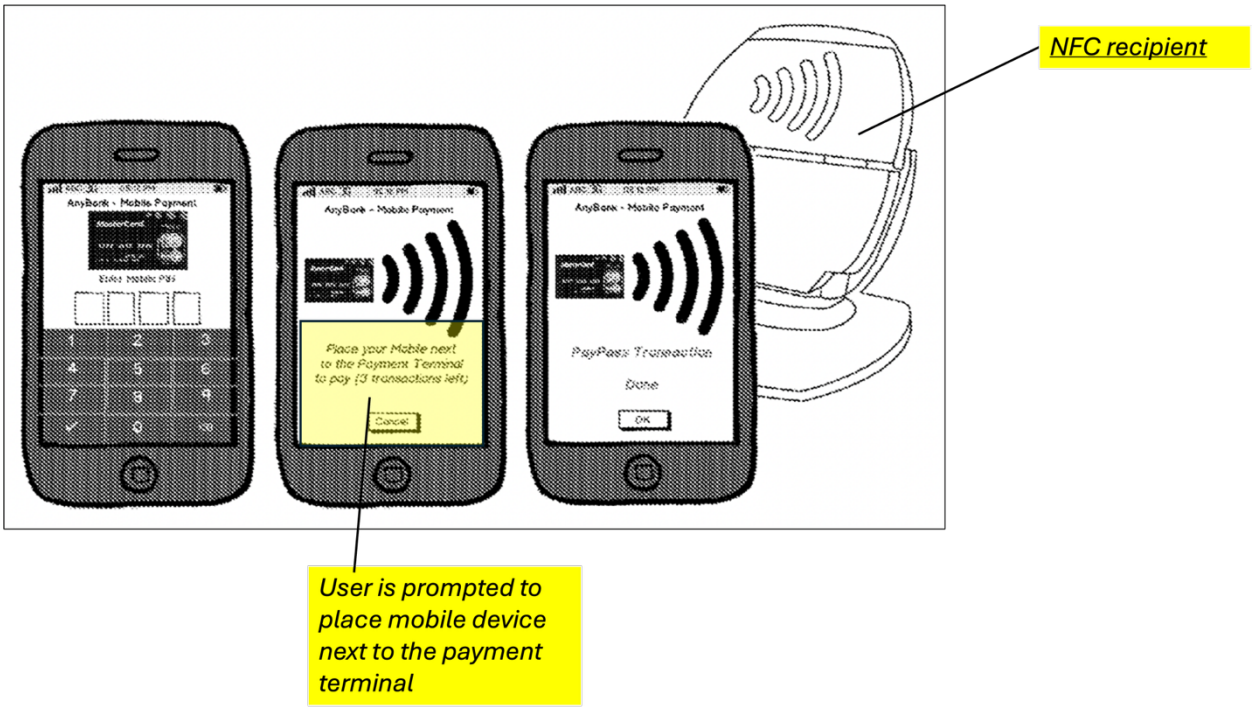


'248 Provisional (Ex.1006), Fig. 2B.

126. Collinge teaches an additional priming operation where a user inputs a PIN into mobile device 104 (*the electronic device*) then places mobile device 104 in proximity to an NFC recipient, as illustrated in the below figure from the '098

Provisional (Ex.1008), which I understand is incorporated by reference into Collinge.





'098 Provisional (Ex.1008) at page 99*; '248 Provisional (Ex.1006),* Figs. 2A-B.

127. As can be seen in the above figure, the user of the mobile device inputs a PIN into mobile device and then receives a notification on the display that says "Place your Mobile next to the Payment Terminal to pay (3 transactions left)[.]" *'098 Provisional (Ex.1008)* at p. 99. A POSITA would have understood that input of "a mobile personal identification number (PIN)" before a payment cryptogram is generated is another example of a *priming operation* because after the PIN is input, the mobile device is primed to perform a payment transaction. *Collinge* at [0133]. Using mobile device 104, the user "must always provide the Mobile PIN for all PayPass transactions[.]" *'098 Provisional (Ex.1008)* at p. 99.

128. A POSITA would have further understood that bringing mobile device 104 in proximity to point-of-sale terminal 120 (NFC recipient) may form part of another *priming operation* because it is a step in preparing mobile device 104 to complete a payment transaction. As illustrated above, the user is prompted to place mobile device 104 in proximity to the payment terminal so that an NFC payment transaction may be performed. *'098 Provisional (Ex.1008)* at p. 99. Collinge, in the '248 Provisional (Ex.1006), which I understand is incorporated by reference into Collinge, additionally teaches that an "**NFC tap** is detected and the process proceeds to stage [7][,]" where a PayPass transaction is initiated. *'248 Provisional (Ex.1006)* at [0189]-[0190], Figure 14 (emphasis added). Thus, an NFC tap/positioning the mobile device near an NFC payment terminal may form part of a *priming operation*

because in response to detecting an NFC tap, a PayPass transaction is initiated, thereby indicating that the NFC tap has primed the mobile device to perform a payment transaction. In sum, Collinge teaches multiple examples of priming operations similar to the '579 patent, which may include NFC tap/positioning of Collinge's mobile device, input of an access code, input of a PIN/passcode, and/or input of an activation code.

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

129. Collinge teaches that the mobile device 104 (*electronic device*) includes *a processor*. Specifically, Collinge teaches that 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**." *Collinge* at [0041] (emphasis added). *See also Collinge* at [0147] ("at least one processor device… may be used to implement the above described embodiments").

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

130. As I discussed above, Collinge teaches the mobile device 104 (*electronic device*) having "an input device (e.g., of the mobile device, **such as a touch screen**)" is used to receive a PIN input by a user. *Collinge* at [0133]. Thus, Collinge teaches the *electronic device* having a *touch-screen display*. Additionally

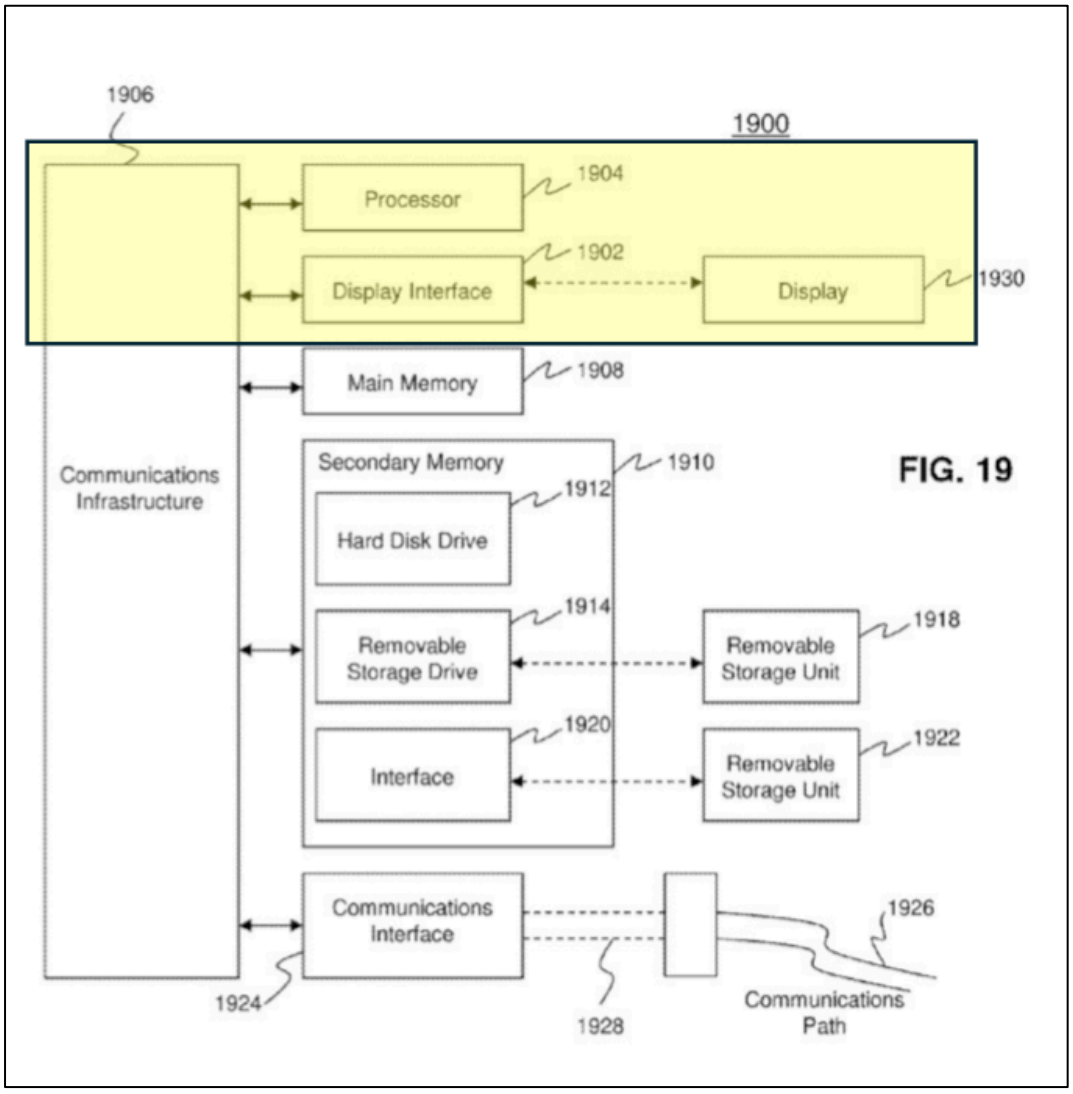
discussed above, Collinge expressly teaches that the mobile device has a processor that executes mobile payment application 106.

131. A POSITA would have understood that the touch screen of Collinge's mobile device 104 is *coupled to the processor*. Collinge teaches that the user of mobile device 104 inputs information, such as a PIN, using the touch screen. *Collinge* at [0133]. The PIN input by the user is used by the mobile payment application 106 to authenticate the user. *Collinge* at [0051]. The mobile payment application 106 is expressly taught as being executed by the processor. *Collinge* at [0041]. Because the user inputs information such as the PIN using the touch screen of Collinge's mobile device 104, and because the PIN is used by the mobile payment application 106, which is executed by the processor, the touch screen (*touch-screen display*) is necessarily *coupled to the processor*.

132. In other words, for the touch screen of mobile device 104 to receive input relevant to mobile payment application 106, the touch screen must be coupled to the processor by which mobile payment application 106 is executed. It was well known that displays and processors are coupled in mobile devices. As one example, U.S. Patent Appl. No. 2006/0097991 to Hotelling et. al. ("Hotelling") teaches that "[t]he computer system 50 also includes a touch screen70 that is operatively coupled to the processor 56." Hotelling (Ex.1042), [0052]. Thus, in Collinge's mobile device 104, the touch screen must be coupled to the processor, otherwise the

mobile payment application 106 would not be able to act on any user input received via the touch screen.

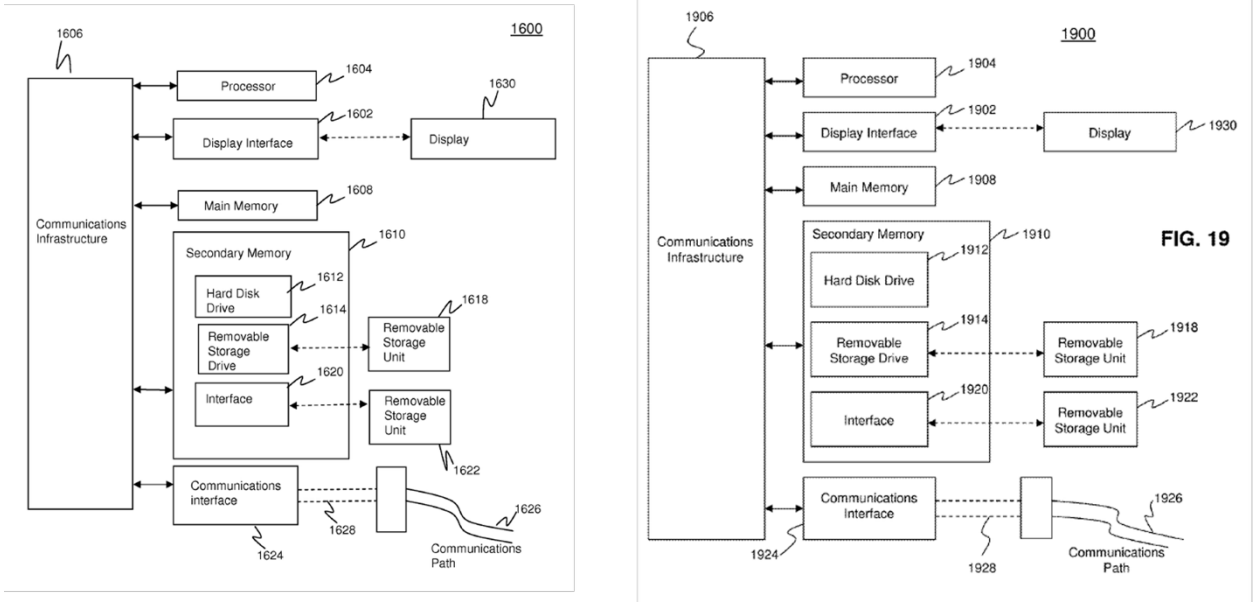
133. Additionally, Collinge teaches that "at least one processor device" is used to implement Collinge's payment system. *Collinge* at [0147]. System 1900, shown in Figure 19 below, further confirms that the mobile device 104's touch screen is "coupled" to the processor by the communications infrastructure 1906.



Collinge at Figure 19. (annotated).

134. The "processor device 1904 may be connected to a communication infrastructure 1906, such as a bus, message queue, network, multi-core message-passing scheme, etc." *Collinge* at [0150].

135. A POSITA would have understood or found obvious that Collinge's mobile device 104 would be implemented as the computer system 1900. For example, in the '248 Provisional (Ex.1006), which I understand is incorporated by reference into Collinge, the computer system of Figure 16 (which corresponds to Figure 19 in Collinge) is taught as corresponding to the mobile device.



'248 Provisional (Ex.1006) at Figure 16 (left); *Collinge* at Figure 19 (right).

136. Specifically, the '248 Provisional (Ex.1006), regarding Figure 16, teaches "the computer programs, when executed, enable the **processor 1604** to implement the processes of the present disclosure, such as the methods illustrated by

Figures 2A and 2B[.]" *'248 Provisional (Ex.1006)* at [0246] (emphasis added). Figures 2A and 2B are "storyboards depicting provisioning processes for downloading, installing, provisioning, activation and using a mobile payment application with a mobile computing device[.]" *'248 Provisional (Ex.1006)* at [0017]. Further, Figures 2A and 2B are expressly taught as being carried out by "mobile device 104[.]" *'248 Provisional (Ex.1006)* at [0048].

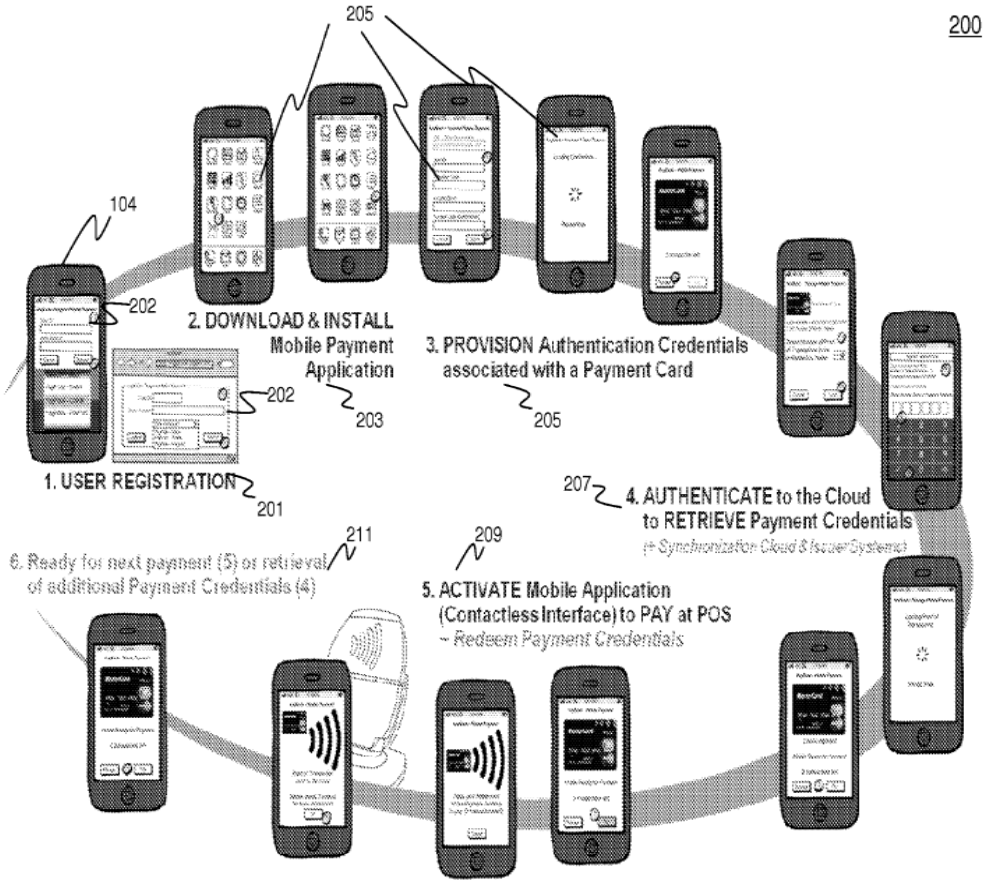


FIG. 2A

'248 Provisional (Ex.1006) at Figure 2A.

137. Because Figure 16 of the '248 Provisional (Ex.1006) corresponds to Figure 19 of Collinge, and because the processor 1604 is taught as implementing the methods of Figures 2A and 2B, which are done by mobile device 104, a POSITA would have understood that processor 1904 in Figure 19 of Collinge is that of mobile device 104. In other words, because processor 1604/1904 in the '248 Provisional (Ex.1006) implements computer programs on mobile device 104, a POSITA would understand that Figure 19 of Collinge represents mobile device 104 (the *electronic device*).

138. Additionally, a POSITA would have understood that in Figure 19, display interface 1902 is Collinge's touchscreen. It was well-known that a touch screen of a mobile device allowed a user to interact with the mobile device. *See, e.g., Mak (Ex.1035)* at [0004] ("An increasing number of mobile devices are now provided with touchscreen interfaces, which integrate the device's display with a touch-based input mechanism allowing the user to interact with displayed content…") As such, a POSITA would understand that display interface 1902 represents the touch screen of mobile device 104.

139. For these reasons, Collinge teaches that the touch screen (*touch-screen display*) is coupled to processor 1904 (*coupled to the processor*) because processor 1904 and display interface 1902 are coupled through communications interface 1906, as shown in Figure 19.

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

140. Collinge teaches that "system 100 and the use…enable the user 102 to use the mobile device to conduct NFC payment transactions[.]" *Collinge* at [0046]. Particularly, with respect to Figure 5, Collinge teaches a "method 500 for the initialization and use of the mobile payment application in the mobile device 104" where in "step 512, the mobile device 104 may conduct a contactless/**NFC payment** transaction using the mobile payment application 106 and the single use key 118[.]" *Collinge* at [0064], [0070]. Because Collinge teaches the mobile device 104 (*the electronic device*) conducts near field communication (NFC) payment transactions, Collinge teaches *a near field communications (NFC) interface*. A POSITA would understand that an NFC interface is required for the mobile device 104 to conduct NFC payments, because without an NFC interface, the mobile device 104 would not have the ability to conduct NFC payments. Collinge was familiar with how NFC payments work, stating "[s]uitable methods and protocols for the secure transmission of information via NFC will be apparent to persons having skill the art[.]" *Collinge* at [0044]. Collinge references the use of NFC several times. *Collinge* at [0003]-[0004], [0044], [0046], [0070], [0085]-[0086], [0120].

141. A POSITA would have understood that "Near Field Communications (NFC) is a short-range wireless technology that allows mobile devices to actively

interact with passive physical objects and other active mobile devices, connecting the physical world to mobile services in ways that empower and benefit users." *Cavoukian (Ex.1039)*, 1. NFC is an open platform technology. Ex. 1040 ("*Paus*"*),* 3. A POSITA at the time would have been familiar with NFC communication and methods of executing standard NFC payment transactions, including those set out in ISO/IEC 18092:2013 and ECMA-340 (Near Field Communication – Interface and Protocol (NFCIP-1), 2nd Edition, December 2004. *Id.* These standards specify capabilities such as transfer speeds, bit encoding schemes, modulation, frame architecture, and transport protocol, as well as operating modes, and provide the information necessary for a POSITA to implement NFC communication on a mobile device. *Id.*

142. A POSITA would have understood that Collinge teaches that mobile phone 104 has an NFC interface that allows Collinge's mobile phone 104 to "conduct payment transactions via near field communication[.]" *Collinge*, [0041]. It was well known that an NFC interface is the combination of hardware and software that enables an NFC-enabled device to communicate with another NFC-enabled device over a short distance (typically less than 4 cm). For example, Lin teaches "In certain embodiments, the communication using the NFC device 46 may occur within a range of approximately 2 to 4 cm." *Lin*, 19: 26-27.

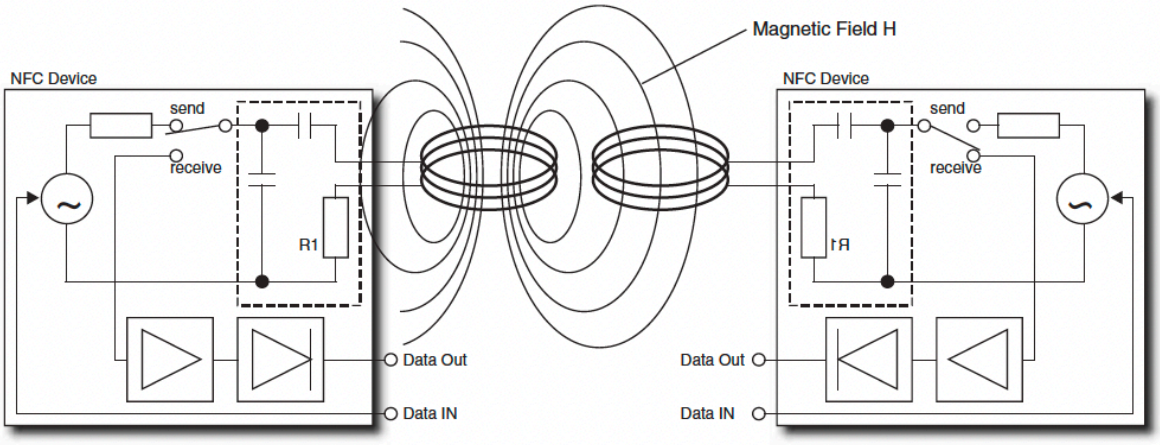
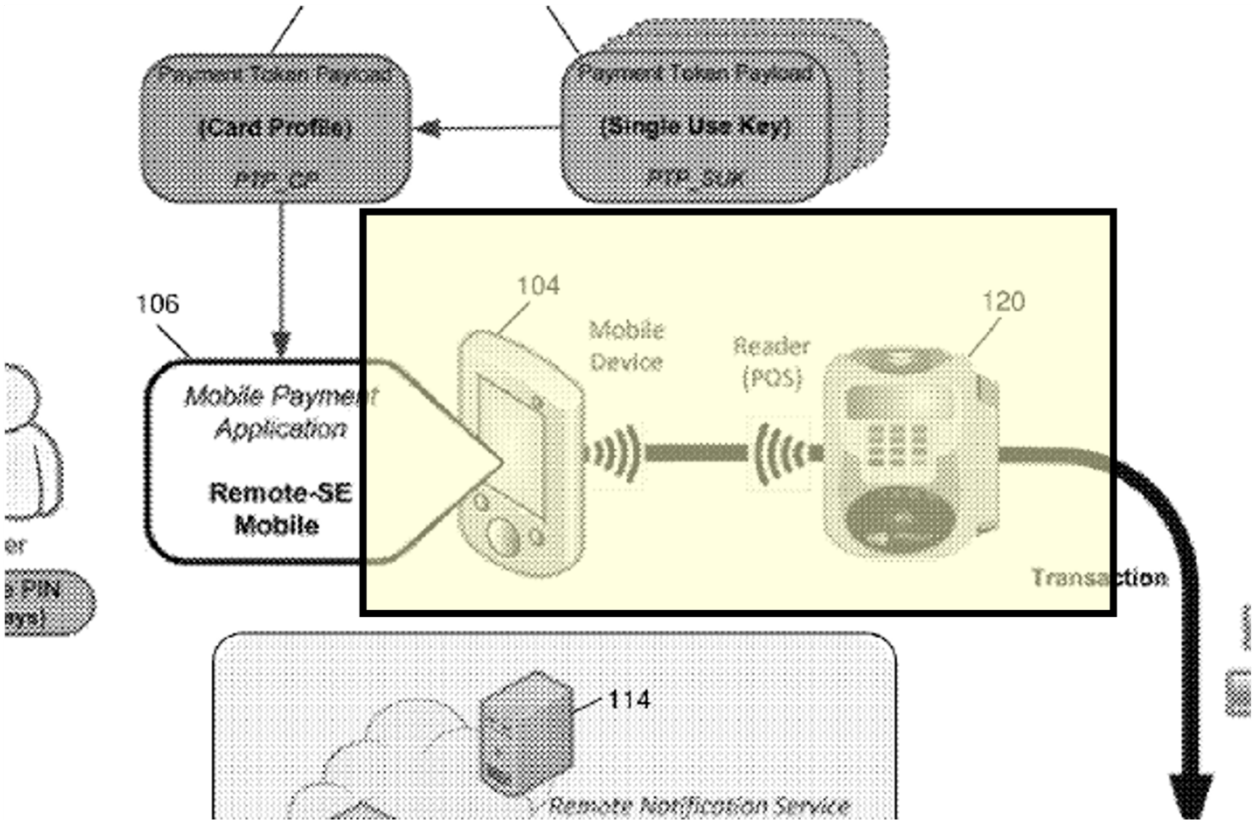


Figure 3.32 In active mode, the NFC interfaces alternately emit magnetic fields for data transmission

Finkenzelller, 58. In addition, a POSITA would have understood that an NFC interface is a wireless interface. Near-field communication is "short-range wireless technology[.]" *Cavoukian (Ex.1039)*, 1. NFC-enabled devices are able to communicate with other NFC-enabled devices over a short distance (typically less than 10 cm). *Paus,* 5.

143. Additionally, the '248 Provisional (Ex.1006), which I understand is incorporated by reference into Collinge, expressly teaches the mobile device 104 having an NFC interface. "In accordance with an embodiment, the process 220 provides access from the mobile payment application to an **NFC interface of the mobile device 104**…" *'248 Provisional (Ex.1006)* at [0067], [0184]. For this additional reason, Collinge teaches the mobile device 104 (*the electronic device*) having *a near field communications (NFC) interface*.



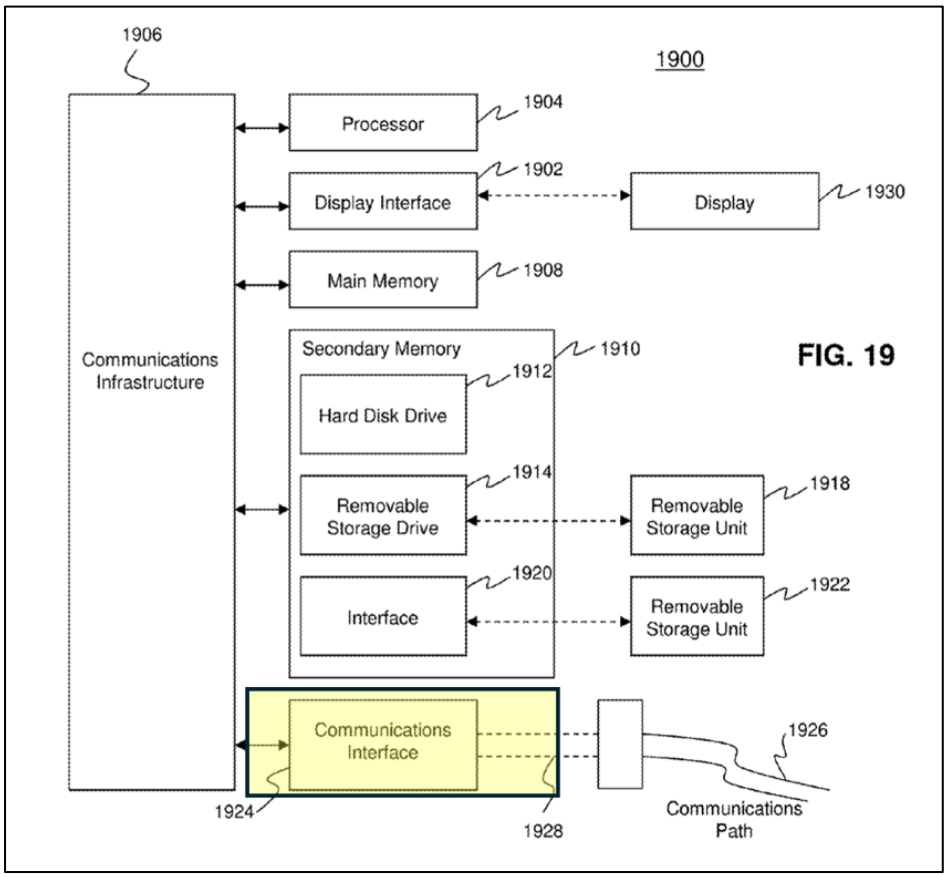
Collinge at Figure 1 (illustrating mobile device 104 communicating with a merchant point-of-sale terminal 120) (annotated excerpt).

144. A POSITA would understand that Collinge's NFC interface is coupled to the processor of mobile device 104. Collinge expressly teaches that "mobile device 104 may include a mobile payment application 105" that is "executed by a processor included in the mobile device 104" (i.e., the *processor*). *Collinge* at [0041]. Regarding the mobile device 104 conducting a "contactless/NFC payment transaction[,]" Collinge expressly teaches that "the mobile device 104 may conduct a contactless/NFC payment transaction using the mobile payment application 106…" *Collinge* at [0070]. Because the mobile payment application 106 is used to

conduct NFC transactions, and because the mobile payment application 106 is executed by the *processor*, the NFC interface used to conduct the NFC transaction is necessarily *coupled to the processor*. That is, the mobile payment application 106 would not be able to successfully complete an NFC transaction because if the NFC interface were not coupled to the processor, then the mobile payment application 106 (executed by the processor) would not have the ability to utilize the NFC interface. Thus, Collinge teaches, and POSITA would have understood that the NFC interface of mobile device 104 is coupled to the processor.

145. Additionally, a POSITA would have understood that Collinge's mobile device 104 comprises an NFC interface coupled to the processor based on the teachings of Figure 19. A POSITA would have also understood and/or found obvious that Collinge's mobile device 104 would be implemented as the computer system 1900 based on the teachings of the '248 Provisional (Ex.1006) that teaches processor 1604 of Figure 16 (corresponding to processor 1904 in Figure 19 of Collinge) as carrying out the methods of Figures 2A-B, which are done on mobile device 104.

146. I have reproduced Figure 19 of Collinge below, which illustrates "communications interface 1924" as being coupled to processor 1904 through communications infrastructure 1906. *Collinge* at Figure 19.



Collinge at Figure 19 (annotated).

147. "The communications interface 1924 may be configured to allow software and data to be transferred between the computer system 1900 and external devices[.]" *Collinge* at [0154]. Collinge further teaches that "[s]oftware and data may in the form of signals, which may be…electromagnetic" and that such signals may "travel via a communications path 1926" that may be implemented using a "radio frequency link." *Collinge* at [0154]. A POSITA would have understood that communications interface 1924 would be implemented as an NFC interface in Collinge's mobile device 104 (*electronic device*). An NFC interface was well-known

to work by sending electromagnetic signals over a radio frequency link. *See*, *e.g., Finkenzeller (Ex.1024)* at p. 57 ("Data transmission between two NFC interfaces uses high-frequency magnetic alternating fields in the frequency range of 13.56 MHz). Thus, a POSITA would have understood and/or found obvious that communications interface 1924 is an NFC interface. Accordingly, because Figure 19 illustrates communications interface 1924 as being coupled to processor 1904 by communications infrastructure 1906, for this additional reason, Collinge teaches *a near field communications (NFC) interface coupled to the processor*.

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

1. Collinge's Teachings

148. As I described above, Collinge teaches mobile device 104 having a "touch screen" (*touch-screen display*) that a user of mobile device 104 may use to input information. *See* Claim 1(a).

149. Collinge's mobile device receives data from a POS terminal during a payment transaction such as "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 that conducting a payment transaction involves NFC between the mobile device and a POS terminal. *Collinge,* [0145] ("the application transaction counter may be transmitted, via near field communication, to

the point-of-sale terminal 120 for including in an authorization request in a financial transaction."); [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.").

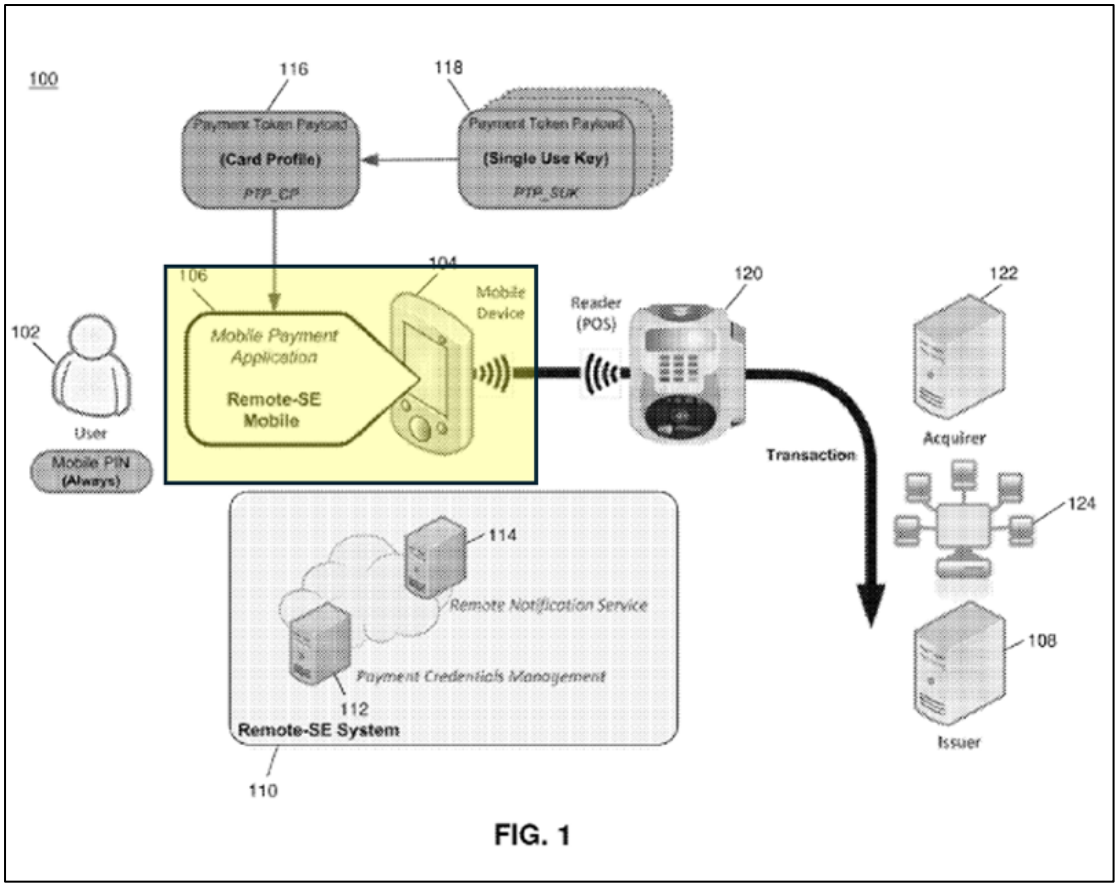


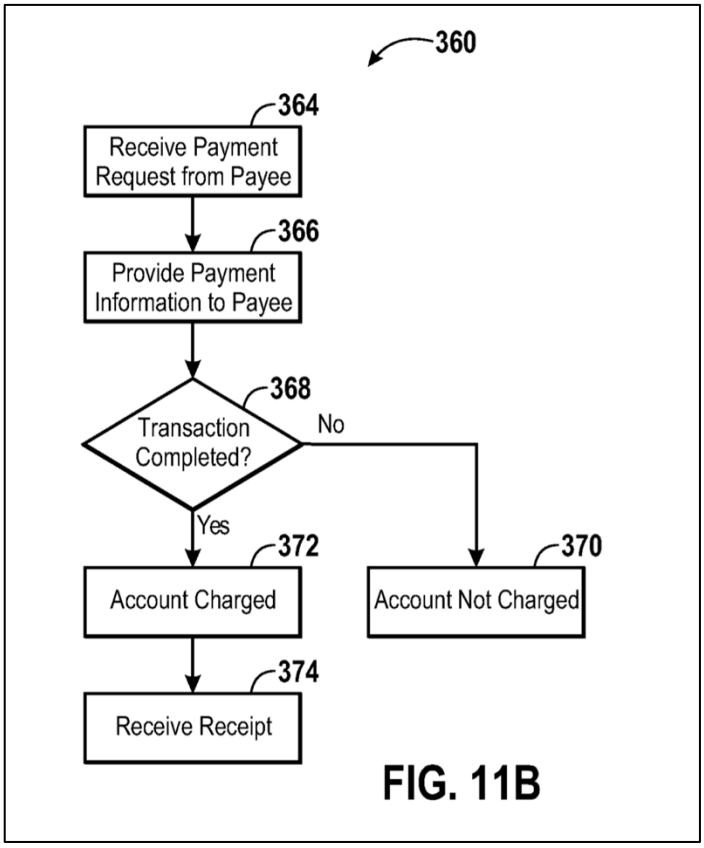
FIG. 1

Collinge, Fig. 1 (annotated).

2. Lin's Teachings

150. Lin teaches sending a payment request to a payor device and that "the 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* at 56:25-28. As shown in Figure 14E below, the screen of Lin's payor device "may be updated to display the details 540 of the payment request." *Lin* at 71:7-10. Specifically, in method step 364, payor electronic device receives a request for payment via its wireless NFC interface from a payee device. *Id.*, Fig. 11B, 55:7-15; *see also, id.* at Fig. 14B, 70:8-27.



Lin, Fig. 11B.

3. Motivation To Combine

151. As I discussed above, Lin teaches sending a payment request to a payor device, and a POSITA would have been motivated to modify Collinge per Lin such that a payment request is sent to mobile device 104 so Collinge's mobile device

receives a request for payment via Collinge's mobile device NFC interface, as taught by Lin. *Lin* at 56:25-28. A POSITA would have found it obvious and been motivated to modify Collinge such that mobile device 104 would receive a request for a transaction payment, as taught by Lin. 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. As an example, when a mobile device performs payments in card emulation mode (as discussed in the background of technology section) it was common for the POS terminal to generate the RF field and send a request to a mobile device. *Coskun (Ex.1021)*, 132. ("In this operating mode an NFC enabled mobile phone does not generate its own RF field; the NFC reader creates this field instead.")

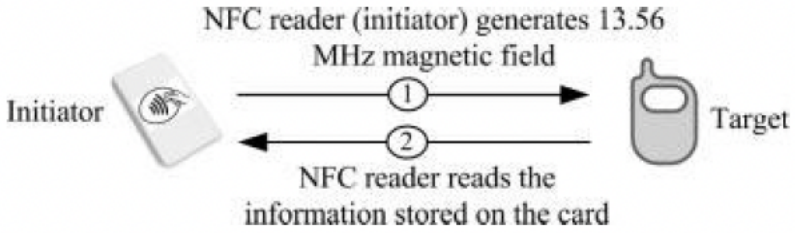


Figure 4.17 Card emulation mode.

Coskun (Ex.1021), Fig. 4.17. As another example, Kranzley teaches "the merchant tallying up a total purchase price and requesting payment from the consumer." *Kranzley*, [0032]. 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. 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. For example, Collinge teaches "a reader unpredictable number may be received, via near field communication, from a point-of-sale terminal (e.g., the point-of-sale terminal 120)." *Collinge,* [0145]. As discussed above, the reader unpredictable number is used when generating a payment cryptogram. *Collinge,* [0145]. ("generate a payment CVC3 value based on at least the supplied CVC3 value, the session key unpredictable number, the application transaction counter, and the reader unpredictable number.") 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.

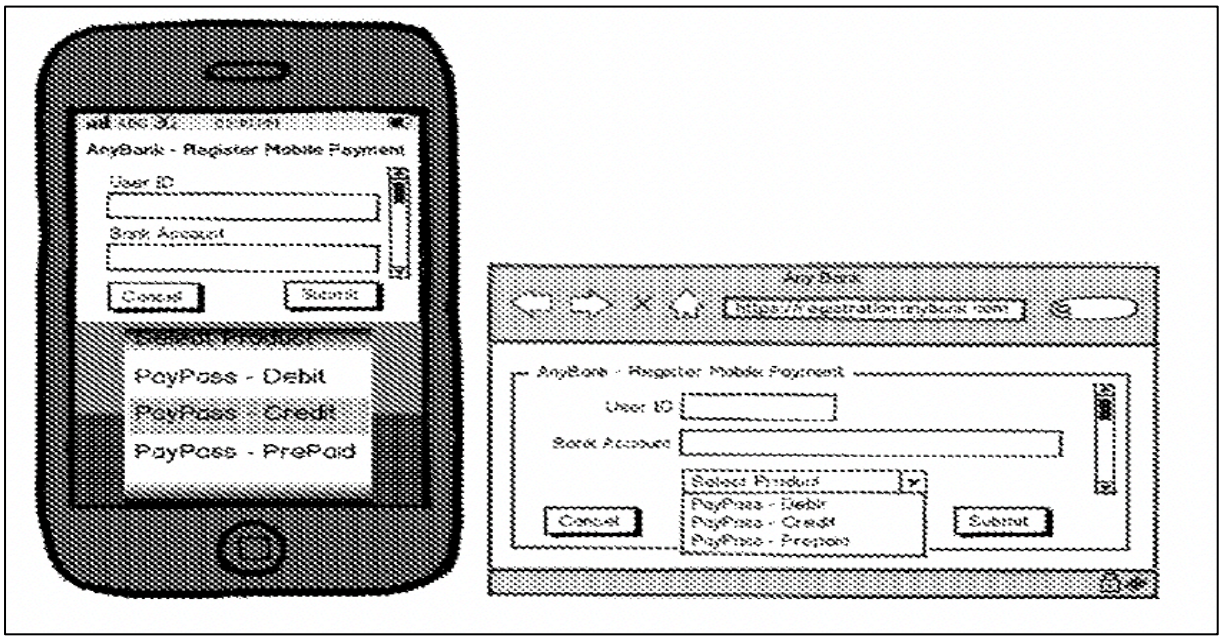
1(d): "displaying, on the touch-screen display, images of: a card issuer payment method selection, including a last 4-digit partial number of a card issuer supplied account number of a payment card; a card logo; and other iconography of the payment card;"

152. 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 (Ex.1008)*, 96, 100. In related art, Phillips provides further detail on what information to display to a user making a payment method selection, rendering this limitation obvious.

4. Collinge's Teachings

153. 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].

154. Collinge further teaches in the '098 Provisional (Ex.1008), which I understand is incorporated in by reference to Collinge, teaches that the user of mobile device 104 may use the user interface of the mobile device to select a payment method for use in a payment transaction. A POSITA would have understood that each of the listed payment methods (Debit, Credit or Prepaid) are a *card issuer payment* account because they correspond to a user's issued payment method such as a credit card and a debit card.



'098 Provisional (Ex.1008) at p. 96; *'248 Provisional (Ex.1006),* Figs. 2A-B..

155. Additionally, the '098 Provisional (Ex.1008) teaches that mobile device 104 displays information corresponding to selected a payment account on the screen of the mobile device, such as the MasterCard account displayed on the user interface of the mobile device (an *card image including a logo and other card iconography* representing a selected issued payment account), illustrated below.



'098 Provisional (Ex.1008) at p. 100; *'248 Provisional (Ex.1006)*, Fig. 2B. (annotated) *See also '248 Provisional (Ex.1006),* Figs. 2A-B. As shown above the mobile device displays a MasterCard payment account on the touch screen of Collinge's mobile device. As also shown above Colling teaches the user may select "pay" during a transaction (approval authorization).

156. Collinge teaches that the card logo (MasterCard) is displayed when the user is choosing the payment method to be used in the transaction, prior to the user selecting "pay" to complete the transaction. '098 Provisional (Ex.1008) at p. 100. Accordingly, Collinge teaches a *card issuer payment method selection* which includes of a *card logo*.

5. Phillips' Teachings

157. 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]. 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].

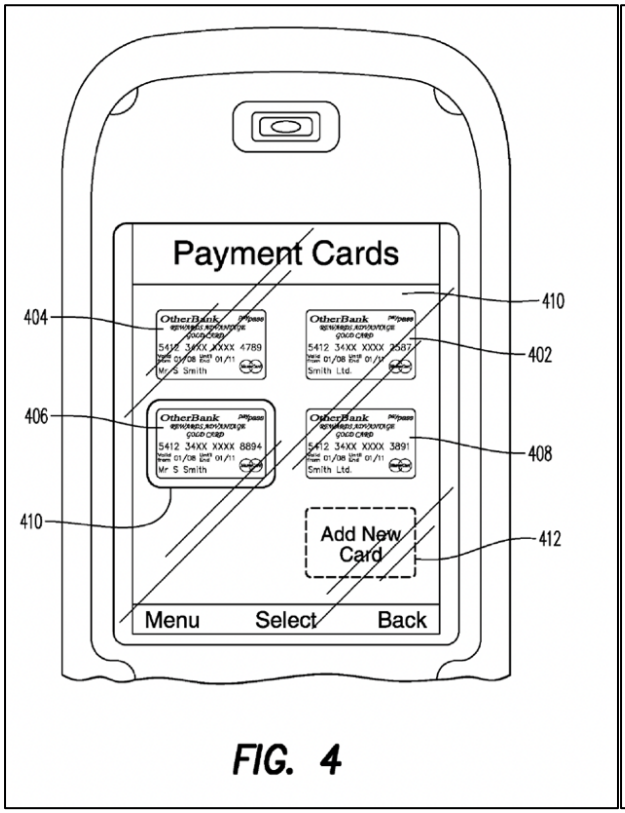


FIG. 4

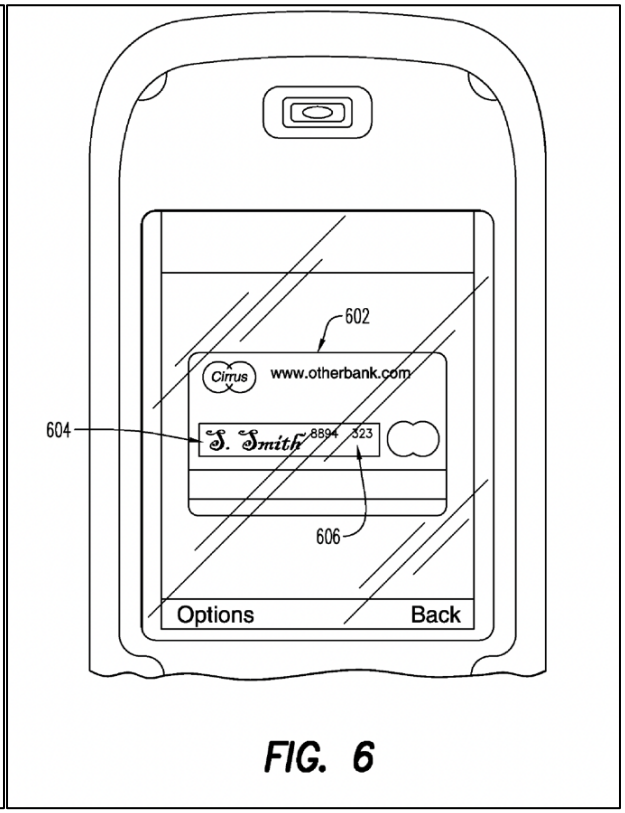
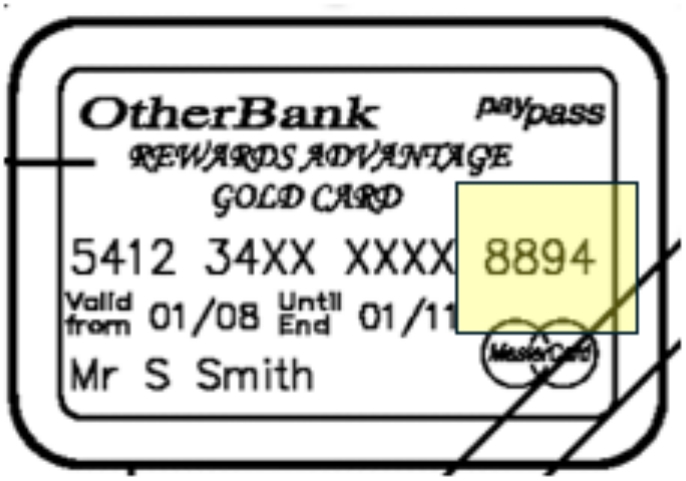


FIG. 6

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].

158. 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). As shown above Phillips 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*. It is worth noting that Phillips

(like Collinge) is assigned to MasterCard, references MasterCard's PayPass system, and it shares an inventor with the Collinge Provisionals (Mr. Simon Phillips).

6. Motivation to Combine

159. It would have been obvious, and a POSITA would have been motivated to configure Collinge's mobile payment application to display small images of payment cards including the card logo, iconography, partial payment number, and other card issuer provided payment information (such as a CVV) as described by Phillips. 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 as depicted by Phillips Fig. 4.

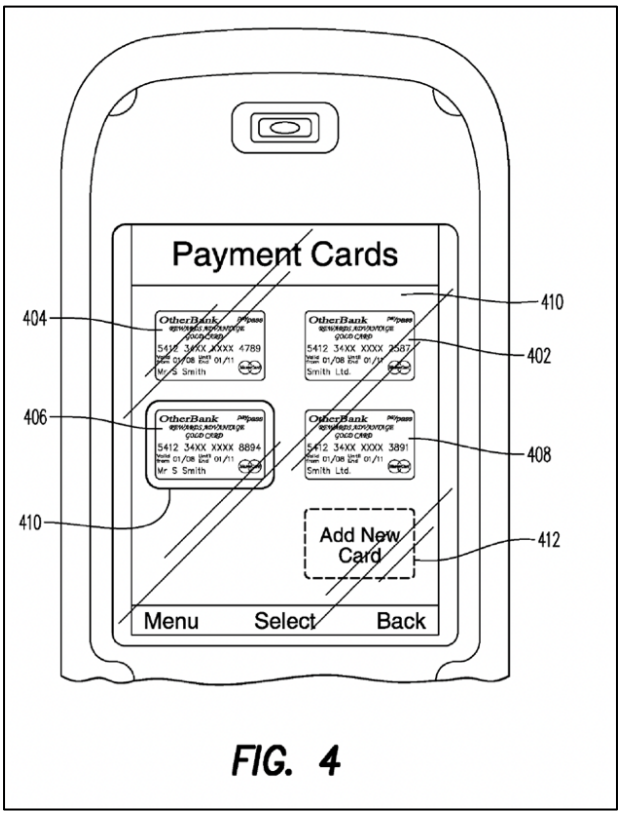


FIG. 4

Phillips, Fig. 4.

160. 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. A POSITA would have further understood, and Collinge already teaches, showing the user an image of the card being used when the user is about to make an NFC payment, which helps to serve as a "check" for the user that they are using the payment method that they intended to, decreasing the risk of an inadvertent user error.

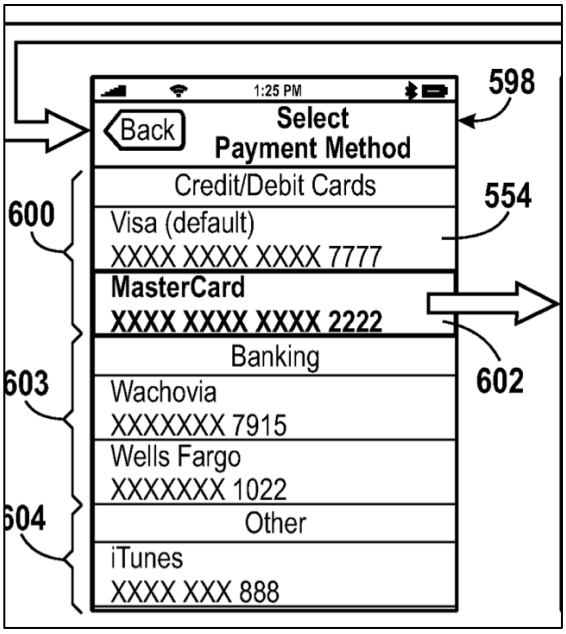


'098 Provisional (Ex.1008) at p. 100; *'248 Provisional (Ex.1006),* Figs. 2A-B.

161. Collinge does not provide detail on how the user interface of Collinge's mobile application would show multiple credit cards available to a user (though Collinge does teach that multiple cards would be available on the application), and a POSITA would have considered related MasterCard PayPass art—including art by the same inventors listed on Collinge and its Provisionals—including Phillips. *See Collinge*, [0038]; [0074]. 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 as shown in '098 Provisional (Ex.1008) at p. 100.

7. Lin's Teachings

162. It would have been obvious and a POSITA would have been motivated to show only the last 4-digits of the payment account number on the payment selection screen of Collinge's modified mobile payment application based on the teachings of Lin. As shown below 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.

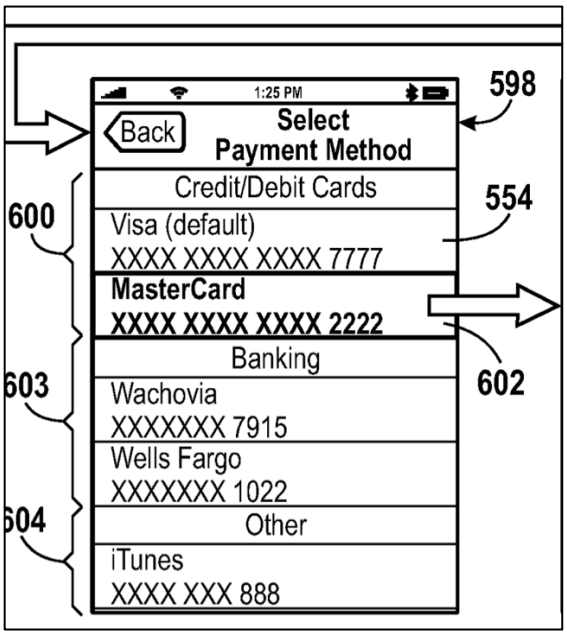


Lin, Fig. 14E. (excerpt).

8. Motivation to Combine

163. 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. 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 as demonstrated by Lins Visa, MasterCard, Wachovia, Wells Fargo, and iTunes payment methods in the figure below:



Lin, Fig. 14E. (excerpt).

164. 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. It was well known to limit the exposure of a consumers card number. For example, as of January 1, 2009, and in contrast to federal law, California Civil Code Section 1747.09 required that no more than the last five digits of a credit or debit card number be printed on both the electronically-printed card receipt retained by

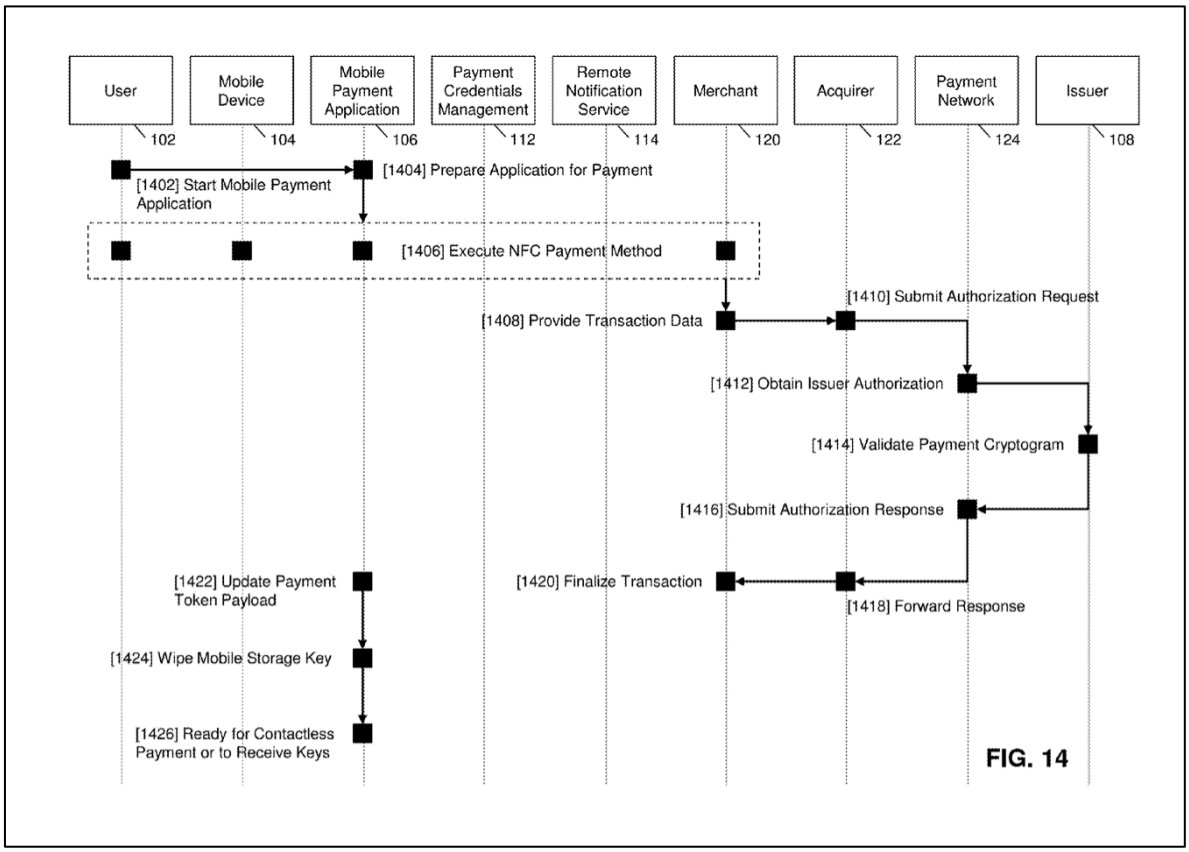
the business as well as the receipt provided to customers. (*See* CA CIVIL, Ex. 1050) Collinge in view of Lin teaches displaying a plurality of payment options including debit, credit, or prepaid and receiving a user-selection of a payment method for a transaction via said touch-screen display user-interface.

165. 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 distinguish between payment methods as demonstrated by both Lin and Phillips. 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.

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;"

166. Collinge's mobile payment application 106 is executed by the processor of mobile device 104. *Collinge* at [0041]. Referring to Figure 14, the method for conducting a payment transaction, Collinge teaches the mobile payment application 106 may retrieve the "generating key from the card profile 116 and the single use key 118" where the "generating key may used by the mobile payment

application 106 to generate a **payment cryptogram** for use in the payment transaction." *Collinge* at [0119].



Collinge at Figure 14. Collinge explains that in "step 1402, the user 102 may start the mobile payment application 106 on the mobile device 104" then the mobile payment application 106 "may prepare for payment." *Collinge* at [0119]. "To prepare for payment, the mobile payment application may regenerate the mobile storage key and may retrieve the payment credentials and generating key from the card profile 116 and the single use key 118 in the encrypted local storage 304." *Collinge* at [0119].

167. The "generating key" referenced by Collinge with respect to the method of Figure 14 is first introduced regarding the system of Figure 1. *Collinge* at [0050].

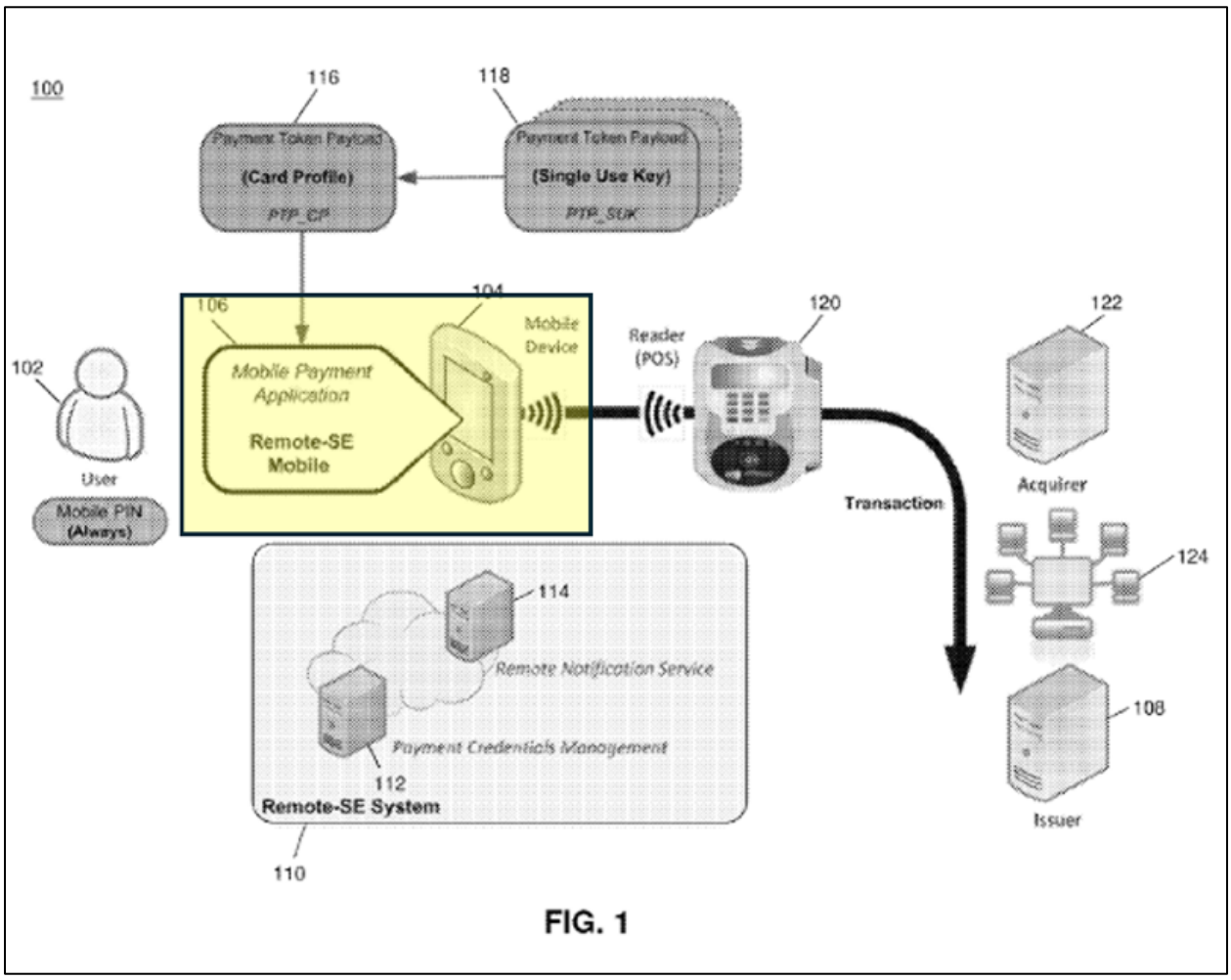


FIG. 1

Collinge, Fig. 1. (annotated)

168. The "generating key" may be included alongside an application transaction count (ATC) as part of single use key 118. *Collinge* at [0050]. "In one embodiment, the generating key 208 may generate a dynamic card validation code (CVC3) or an application cryptogram (AC)." *Collinge* at [0050].

169. Returning to the method of Figure 14, Collinge expressly teaches that the "generating key may be used by the mobile payment application 106 to **generate a payment cryptogram** for use in the payment transaction." *Collinge* at [0119] (emphasis added). In step 1406, "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." *Collinge* at [0120]. To execute the NFC payment, the point-of-sale terminal 120 provides "transaction data to the acquirer 122 including the payment credentials and payment cryptogram[,]" then the acquirer "may submit an authorization request including the transaction data" (i.e., including the payment cryptogram) to the payment network 124." *Collinge* at [0121]. The payment network 124 "may seek authorization from the issuer 108 for the payment transaction[,]" then in step 1414, the "issuer 108 may validate the payment cryptogram." *Collinge* at [0121]. "The issuer 108 may, once the payment cryptogram is validated, approve or deny the payment transaction[.]" *Collinge* at [0121].

170. Specifically, when teaching a method 1600 for generating a payment cryptogram, Collinge teaches in "step 1610, **a payment cryptogram valid for a single payment transaction** may be generated, by a **processing device**, based on at least the received single use key 118[.]" *Collinge* at [0131], [0135] (emphasis added). The payment cryptogram "may be an application cryptogram or a **dynamic card validation code**." *Collinge* at [0135] (emphasis added). The dynamic card

validation code "(CVC3)" may be generated based on "at least the supplied CVC3 value, the session key unpredictable number, the application transaction counter, and the reader unpredictable number." *Collinge* at [0142], [0145]. Collinge, in the '248 Provisional (Ex.1006), teaches generating the CVC3 using the session key unpredictable number, track data, the ATC, and the reader unpredictable number:

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 (Ex.1006) at Table 1.

171. The use of the application transaction counter in generating the dynamic card validation code (i.e., payment cryptogram) confirms that the payment cryptogram is dynamically generated, because the application transaction counter is a different number for each transaction. *See, e.g., Robers (Ex.1044)* at [0075] ("The application cryptogram returned in step 318 may be based, in part, on **the application transaction counter (ATC),** which is a counter in the chip card, two bytes long, **which increments every transaction**.") (emphasis added).

172. Collinge teaches "[t]he payment cryptogram may be, for example, an application cryptogram or a dynamic card validation code (CVC3)." *Collinge*, [0077]. It was well known that a type of payment cryptogram may be a CVC3. See Section VII. Additionally, Collinge's payment cryptogram (e.g., dynamic card

validation code) is a dynamically generated because it is valid only for a single transaction, meaning it is dynamically generated on per-transaction basis. Collinge's payment cryptogram (e.g., dynamic card validation code) is *limited-use payment information* because it is limited to one use per transaction and because it is used in a payment transaction. *Collinge* at [0135] (" a payment cryptogram valid for a single payment transaction may be generated"), [0119]("[t]o prepare for payment, the mobile payment application 106 may regenerate the mobile storage key and may retrieve the payment credentials and generating key from the card profile 116and the single use key 118 in the encrypted local storage 304. The generating key may be used by the mobile payment application 106 to generate a payment cryptogram for use in the payment transaction.") Dynamic card validation codes were well known in the art. For example, Visa's "contactless smart card specifications includes a code designated Dynamic Card Verification Value (dCVV) for each transaction." *Bona* at [0037] On the other hand, "MasterCard Inc.'s PAYPASS® Magstripes smart card specification has a similar code designated the CVC3." *Bona* at [0037] Both Visa's dCVV and Mastercard's CVC3 are a "one-time (i.e., dynamic) codes… unique to each transaction." *Bona* at [0037]. CVVs need to be present in a magstripe transaction. *Bona* at [0037]. ("magnetic stripe specifications for Track 1 and Track 2 contents require a specific static value called a CVV to be present.")A POSITA would have understood that Collinge, a MasterCard reference uses a dynamic card

validation code CVC3 in place of the standard card-issued CVV when conducting a payment transaction because as discussed above, it was well known in the prior art that Mastercard uses a CVC3 value to replace the static It was well-known at the time and a POSITA would have understood that an application cryptogram and CVC3 are dynamically generated alternatives to the static card issuer CVV found on the back of a traditional payment card. For example, Kranzley teaches "the 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]. Therefore, Collinge teaches *using said limited-use payment information* (payment cryptogram) *in place of said card issuer supplied payment information* (CVV). A POSITA would have appreciated that using a dynamic CVV, helps "eliminate both "card present" and "card not present" fraud." *Bona* at [0037]. ("Replacing the static CVV value with the dynamic dCVV or CVC3 codes (in the embodiments where the data is formatted for VISA® and MASTERCARD® transactions, respectively) and including any other necessary data used to verify the dCVV or CVC3 codes (e.g., Application Transaction Counter (ATC) value and dynamic data presence flag) would provide sufficient information in the payment authorization process to eliminate both "card present" and "card not present" fraud.")

173. A POSITA would have understood that Collinge's payment cryptogram is *generat[ed] by the processor* because Collinge teaches mobile payment application 106 generates the payment cryptogram, and mobile payment application 106 is executed by the processor of mobile device 104. Thus, Collinge teaches dynamically *generating, by the processor, limited-use payment information*.

174. 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] (methods for transmitting payment credentials and a payment cryptogram to a point-of-sale terminal are apparent to POSITAs).

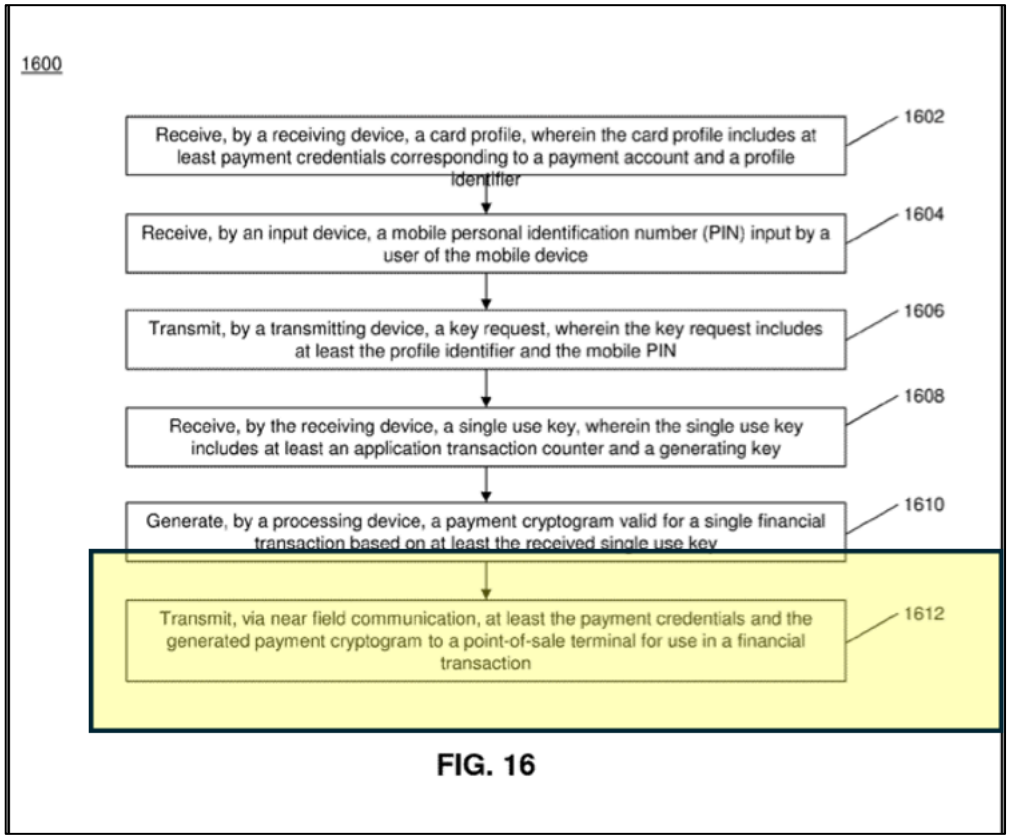


FIG. 16

Collinge, Fig. 16. (annotated).

175. Collinge's complete payment information is likewise used in place of the card issuer supplied payment information (complete payment credentials including a PAN+CVC) when performing a payment transaction. *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). As discussed above Collinge's payment cryptogram is used in place of the issuer supplied CVV.

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

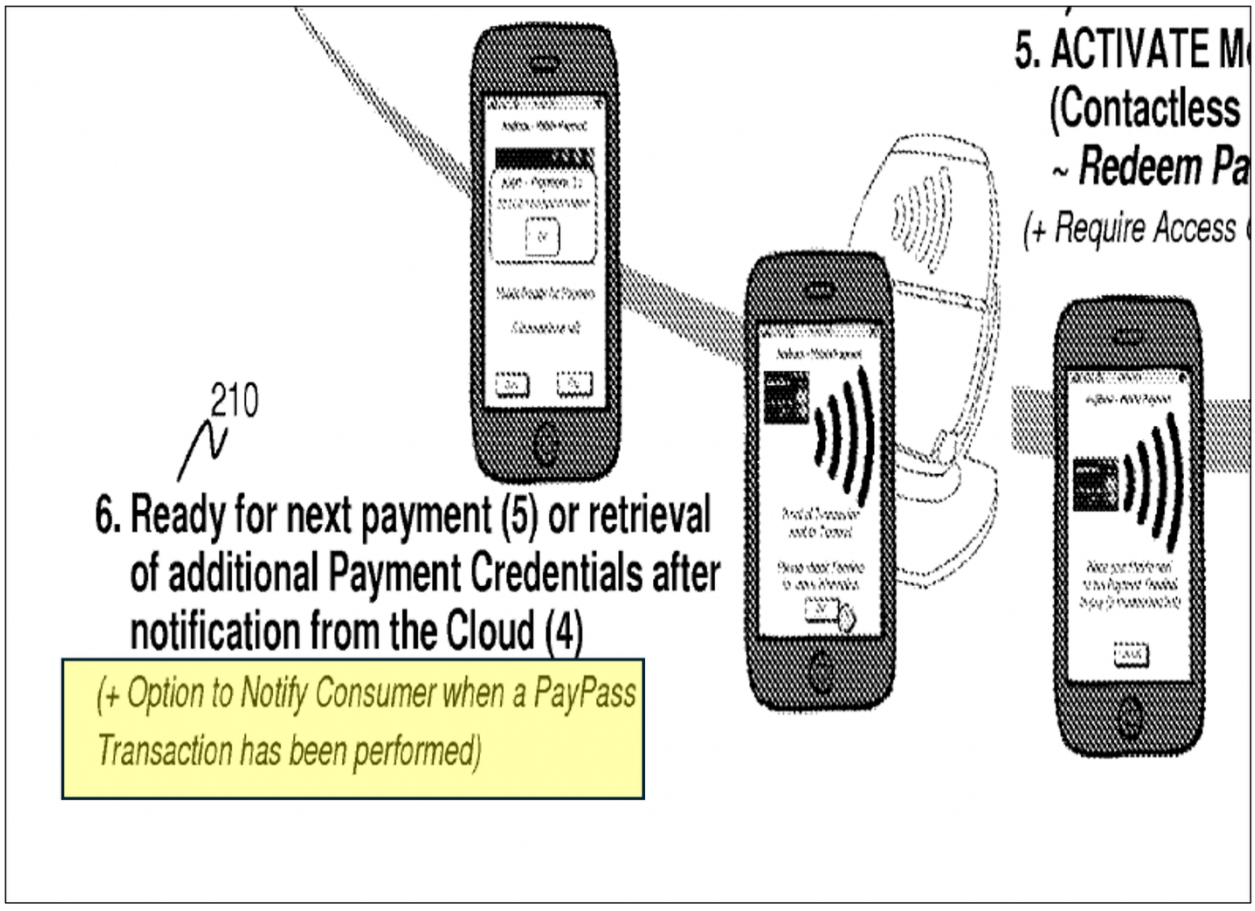
176. As discussed above, Collinge's payment cryptogram (i.e., CVC3) is generated on mobile device 104. *See* Claim 1(e). Collinge expressly teaches that the payment cryptogram (*said limited-use payment information*) is transmitted from mobile device 104 (*said electronic device*) to the point-of-sale terminal 120 (*for receipt by an NFC recipient*). *Collinge* at [0044] ("The mobile device 104 may be further configured to **transmit a generated payment cryptogram and payment credentials to a point-of-sale terminal 120 at a merchant**.") (emphasis added). "The point-of-sale terminal 120 may be any type of point-of-sale terminal or device suitable for receiving payment credentials via near field communication (NFC)." *Collinge* at [0044]. Thus, Collinge's point-of-sale terminal 120 is *an NFC recipient*

because it receives payment credentials and the payment cryptogram via NFC from mobile device 104. Additionally, Collinge's mobile device 104 comprises an NFC interface. *See* Claim 1(b)(2). A POSITA would understand that because Collinge teaches the mobile device 104 comprises an NFC interface, because the point-of-sale terminal 120 receives communications via NFC, and because mobile device 104 transmits the payment cryptogram to the point-of-sale terminal 120, that the transmission of the payment cryptogram from mobile device 104 is done from *via said NFC interface*. Accordingly, Collinge teaches *transmitting said limited-use payment information from said electronic device to an NFC recipient of the transaction via said NFC interface.*

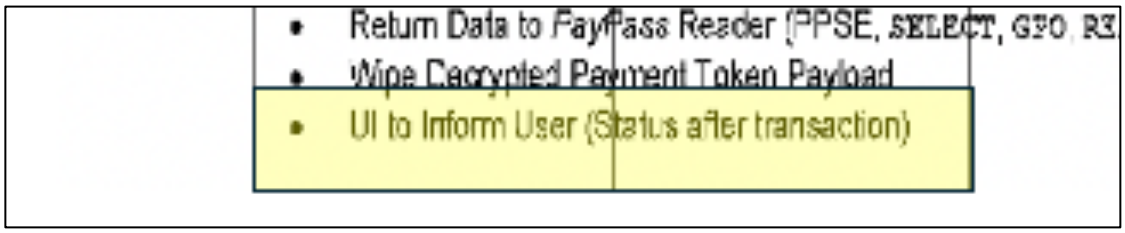
1(g): "visually conveying a status of said transaction via a user-interface displayed on said touch-screen display."

177. In the '248 Provisional (Ex.1006), which I understand is incorporated by reference into Collinge, teaches that after an NFC payment transaction is conducted between mobile device 104 and point-of-sale terminal, "step 210 can comprise notifying the user 113 when a PayPass transaction has been performed." *'248 Provisional (Ex.1006)* at [0074]. As I discussed above at claim 1(c), Collinge teaches that mobile device 104 receives information from and communicates with the point-of-sale terminal 120 via the NFC interface.

178. Additionally, at Figure 2B of the '248 Provisional (Ex.1006), Collinge teaches displaying the notification of the PayPass transaction being performed on the touch screen of mobile device 104. *'248 Provisional (Ex.1006)* at Figure 2B. A POSITA would have understood that notifying the consumer when a PayPass transaction has been performed on the touch screen of Collinge's mobile device 104 constitutes information reflecting *visually conveying a status of said* payment *transaction via a user-interface displayed on* Collinge's *touch-screen display.*

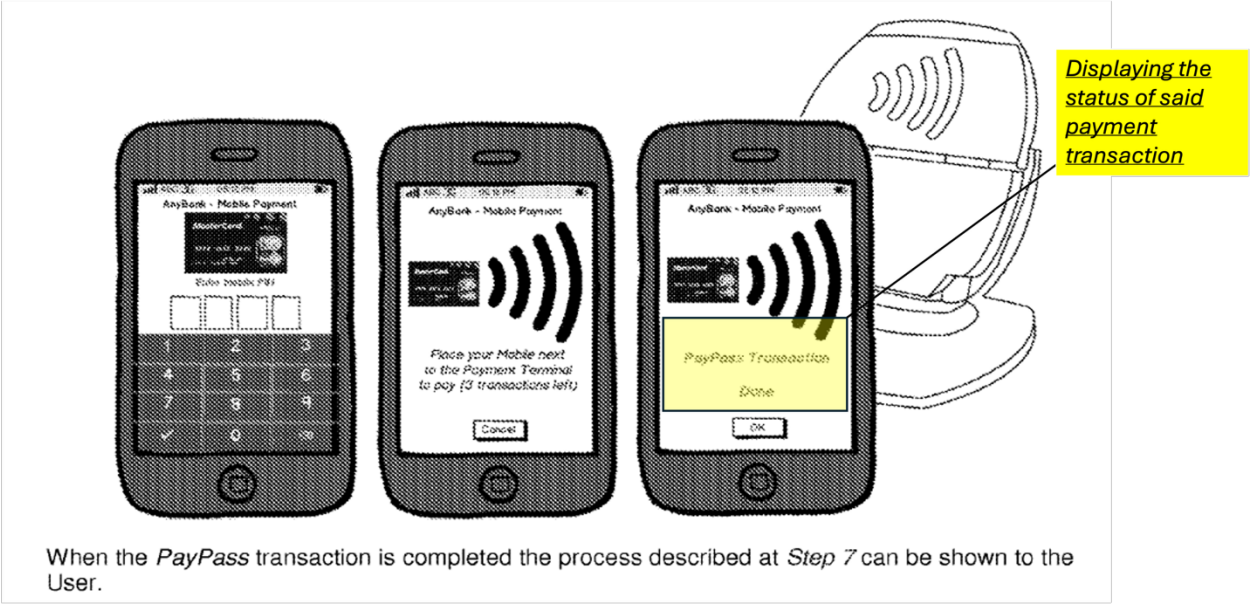


'248 Provisional (Ex.1006) at Figure 2B (annotated excerpt).



'248 Provisional (Ex.1006), Fig. 14 (excerpt).

179. Further, '248 Provisional (Ex.1006) expressly teaches that the UI, which a POSITA would have understood to be user interface, informs the user of the "status after the transaction." *'248 Provisional (Ex.1006)* at Figure 14, [0195]. A POSITA would understand that the UI would be displayed on the touch screen display of mobile device 104. Additionally, the '098 Provisional (Ex.1008), which I understand is incorporated by reference into Collinge, teaches displaying the status of a payment transaction on the touch screen of the mobile device.



When the *PayPass* transaction is completed the process described at *Step 7* can be shown to the User.

'098 Provisional (Ex.1008) at p. 99; *'248 Provisional (Ex.1006),* Figs. 2A-B.

180. As such, Collinge teaches and a POSITA would have understood that the notification of "PayPass Transaction Done" displayed on the UI of mobile device 104 is responsive to receiving information from the point-of-sale terminal 120 via the NFC interface. A POSITA would have understood that the information is received via the NFC interface because that is the structure that allows mobile device 104 to communicate with the point-of-sale terminal 120, and the point-of-sale terminal 120 would be what confirms a transaction is complete.

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… and a user identification entry."

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

182. 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].

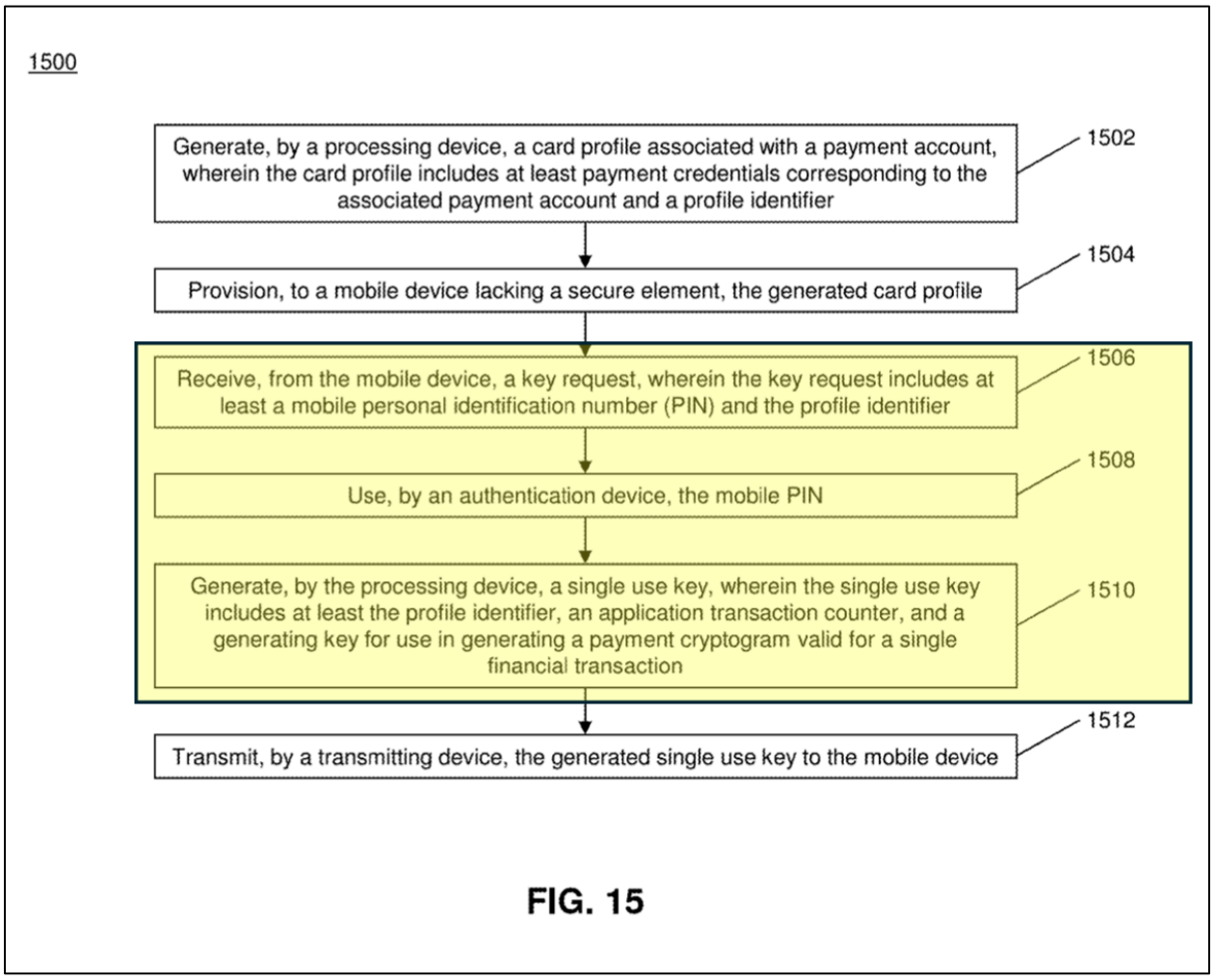


FIG. 15

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 106may then generate a payment cryptogram using the generating key included in the single use key118." *Collinge*, [0077].

183. Collinge teaches an application transaction counter (ATC) (*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 "**a device transaction sequence counter**" and is updated each transaction. A POSITA would have been very familiar with this use of an ATC, as an ATC is a common security feature, which ensures that the cryptogram generated is not a duplicate of a cryptogram previously generated. For example, U.S. Patent Appl. No. 2013/0246269 to Roberts et al. ("Roberts") teaches the following:

> The application cryptogram returned in step 318 may be based, in part, on the application transaction counter (ATC), which is a counter in the chip card, two bytes long, **which increments every transaction**, and is a fundamental security mechanism employed with both contacted and contactless chips. It is one wherein the card and issuer **can ensure that cryptograms received from the card are not "old" cryptograms**; i.e., the ATC can be used to ensure that a cryptogram produced by the card is not a previous cryptogram. Stated in another way, one of the things that would not be desirable is for a card to produce the same cryptogram that it produced for a previous transaction. By including the ATC in the cryptogram, it is ensured that the card will never produce a cryptogram that is the same as a previously-produced cryptogram.

Robers (Ex.1044), [0075]. *See also, Bona*, [0102] (discussing role of an ATC in transaction authorization).

184. Collinge is provisioned the ATC from the cloud system. The cloud system "identif[es] an encrypted payload based on a derived CVC3 key (KDCVC3), 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].

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 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[…]: payment issuer secrets; 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.

185. *See* Claim 1(e) and 2. Collinge further teaches *payment issuer secrets*. Collinge teaches that the issuer 108 validates a payment cryptogram. *Collinge (Ex. 1004),* [0141]. A POSITA would have been very familiar with methods of validating a payment cryptogram, as recognized by Collinge. *Collinge (Ex. 1004),* [0077]. Typically, the issuer will recompute the payment cryptogram and compare the issuer-generated payment cryptogram to the cryptogram received from the merchant.

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].

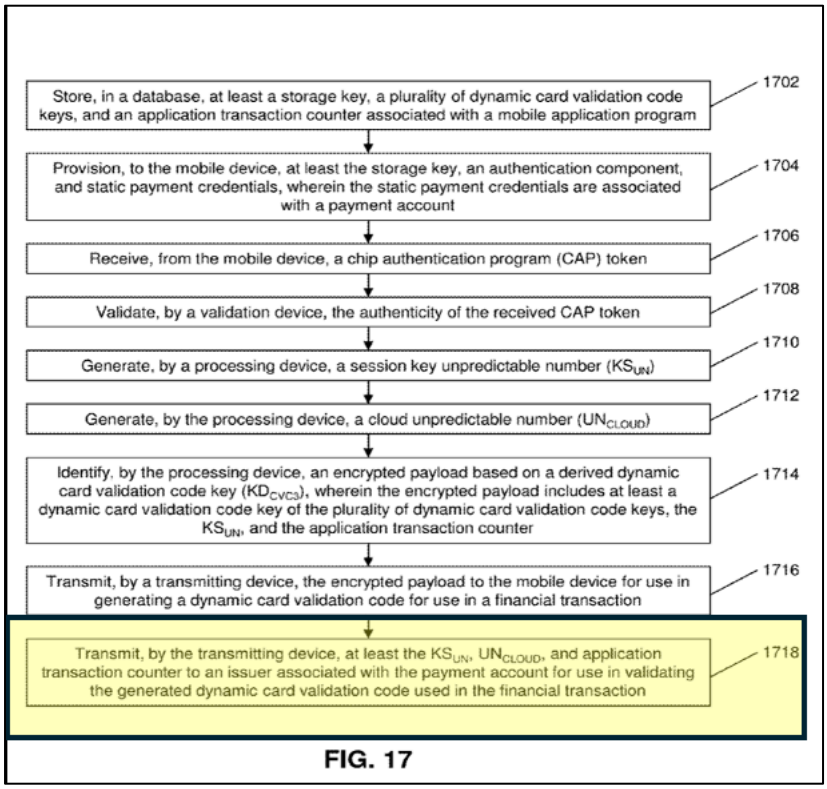


FIG. 17

Collinge (Ex. 1004), Fig. 17 (annotated); see also '248 Provisional (Ex.1006) (Ex. 1006), 54.

186. The issuer may then "authenticate the dynamic card validation code[.]" *Collinge (Ex. 1004),* [0056]. Collinge's provisional details how the issuer validates the payment cryptogram. Collinge teaches generating a CVC3 based on at least: "the supplied CVC3 value, the session key unpredictable number, the application

transaction counter, and the reader unpredictable number." *Collinge (Ex. 1004),* [0145]; *'248 Provisional (Ex. 1006)*, Table 1. A POSITA would have appreciated that the session key unpredictable number is distinct and generated each transaction and is only available to Collinge's system and the issuer. Therefore, a POSITA would have understood that the session key unpredictable number (K_{SUN}) are secret information shared between two parties (*secret)*

187. Specifically, based on the received information at the issuer above (KS_{UN}, UN_{CLOUD}, and ATC) the issuer will compute $Cloud\_CVC3_{TRACK1/2}$. *'095 Provisional (Ex. 1005)*, 24. Therefore, the UN_{CLOUD} is a secret between the issuer and Collinge's cloud system.

> *UN_{CLOUD} is **not** sent to the Mobile Payment Application.*
>
> *UN_{CLOUD} is part of the payload exchanged between the Cloud and the Issuer during the Synchronization process.*

'098 Provisional (Ex.1008), [0224].

188. The issuer also uses $IVCVC3_{TRACK1/2}$ which is a MAC calculated over track 1 and 2 data using KD_{CVC3} which is "kept in the Cloud/Issuer" *'095 Provisional (Ex. 1005)*, 21.

> The Issuer system is able to compute **Cloud_CVC3$_{TRACK1/2}$** using:
>
> - IVCVC3$_{TRACK1/2}$ (2 bytes)
> - UN$_{CLOUD}$ (4 bytes)
> - ATC (2 bytes)

'095 Provisional (Ex. 1005), 24. After computing $Cloud\_CVC3_{TRACK1/2}$, the issuer computes $CVC3_{TRACK1/2}$ which is directly used in generating the CVC3. *'095 Provisional (Ex. 1005)*, 25.

> The Issuer system is able to compute $\mathbf{CVC3_{TRACK1/2}}$ using:
>
> - Cloud_CVC3$_{\text{TRACK1/2}}$ (2 bytes)
> - UN$_{\text{READER}}$ (4 bytes)
> - ATC (2 bytes)
>
> The Issuer can validate the $\mathbf{CVC3_{TRACK1/2}}$.

'095 Provisional (Ex. 1005), 25. The issuer already has the rest of the values used when generating the CVC3 (KS_{UN}, UN_{CLOUD}, and ATC). *'095 Provisional (Ex. 1005)*, 24-25.

189. 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* at [0050]. The single use key is shared with issuer 108. *Collinge* at [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]. ("…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.") Therefore Collinge teaches the payment cryptogram CVC3 value (*limited-use payment information*) is generated based on the K_{SUN} and the generating key and values within the single use key 118 (*secrets*), and that the K_{SUN} and single use key 118 is secret information shared with issuer 108 (payment issuer secrets).

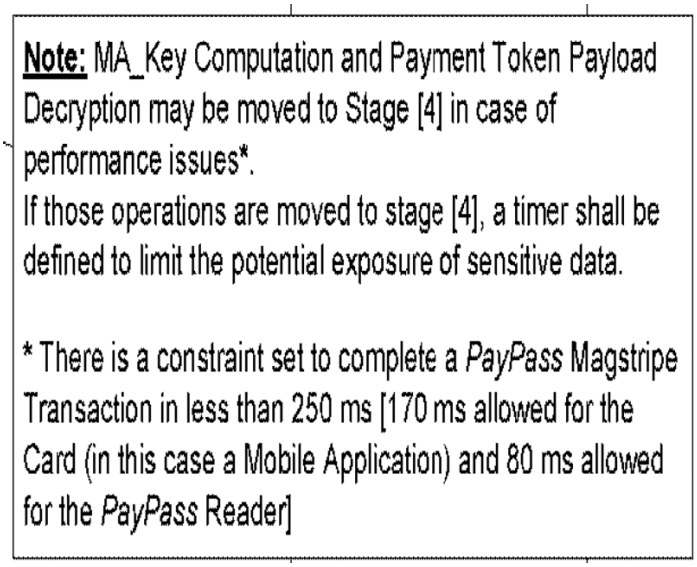
7. "The method of claim 1, wherein the receiving an input at an electronic device comprises receiving an input via a user interface from one of the set of user interfaces comprising: …a device touch-screen interface…:

190. As discussed above in Claim 1(a), 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).

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."

191. As will be discussed below, Collinge teaches 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.

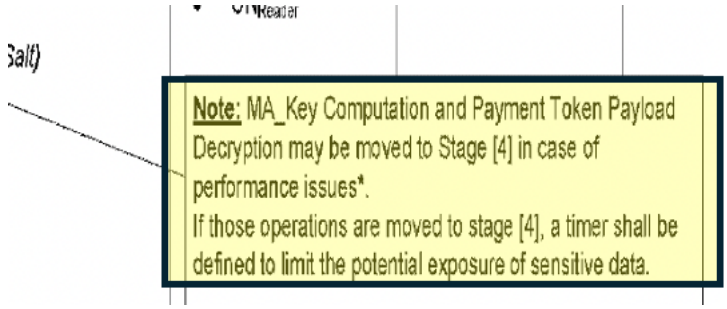
192. Collinge teaches setting a time constraint for completing a PayPass transaction with the Mobile Application of "less than 250 ms [170 ms allowed for the Card (in this case a Mobile Application) and 80 ms allowed for the PayPass Reader]" *'248 Provisional (Ex.1006)*, Fig. 14.



'248 Provisional (Ex.1006), Fig. 14. (excerpt). Even though 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 (Ex.1006)*, [0189], Fig. 14 (Step [5] "Enable NFC interface"; Step [6] "NFC Tap"). As discussed above in the background of technology section this was common in the prior art. *See* Section VII.

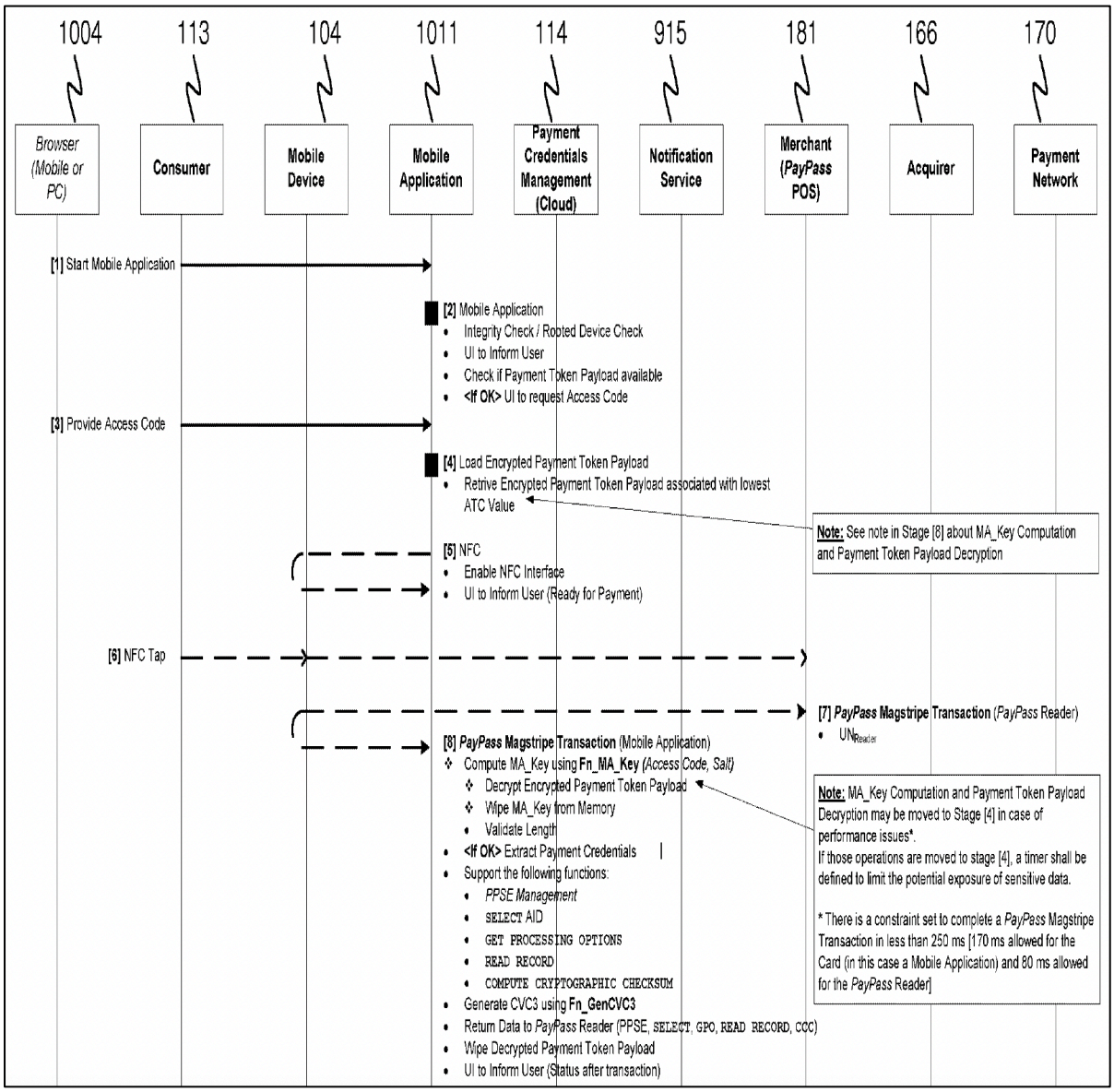
193. Collinge additionally teaches that if certain operations included in the [8] PayPass Magstripe Transaction are instead performed when the Payment Token Payload is loaded to the mobile application, then for that step, too, "a timer shall be

defined to limit the potential exposure of sensitive data." *'248 Provisional (Ex.1006)*, Fig. 14, [0197].



'248 Provisional (Ex.1006), Fig. 14. (annotated excerpt).

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



'248 Provisional (Ex.1006), Fig. 14. (excerpt).

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 transaction exceeding a pre-set amount limit; the transaction interval exceeding a pre-set time duration […] presenting the user with at least one of a set of selectable options comprising: […]requesting a transaction payment; selecting an alternate payment account; inputting a transaction denial"[…]

195. Collinge in view of Phillips teaches 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 transaction interval exceeding a pre-set time duration and presenting the user with at least one of a set of selectable options comprising: inputting an approval authorization and inputting a transaction denial.

9. Collinge's Teachings

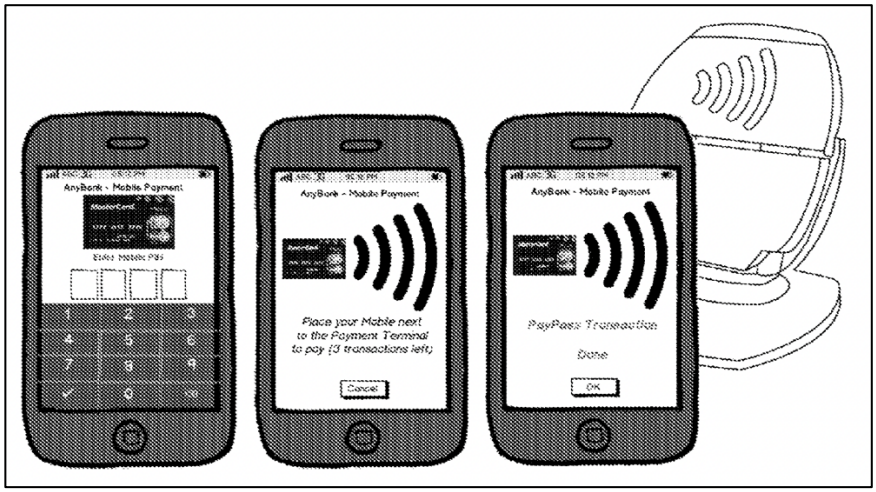
196. Collinge teaches *completing a transaction* on the mobile device if the payment transaction is approved "based on funds or credits in the payment account[.]" *Collinge*, [0045]. Collinge teaches the user must input their PIN and then place the mobile device next to the payment terminal. Once the user places their mobile device next to the payment terminal, the NFC transaction must complete within 170ms. *'248 Provisional (Ex.1006)*, Fig. 14. *See* Claim 10. As discussed in Claim 10, 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 (Ex.1006)*, 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 (Ex.1006), 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.



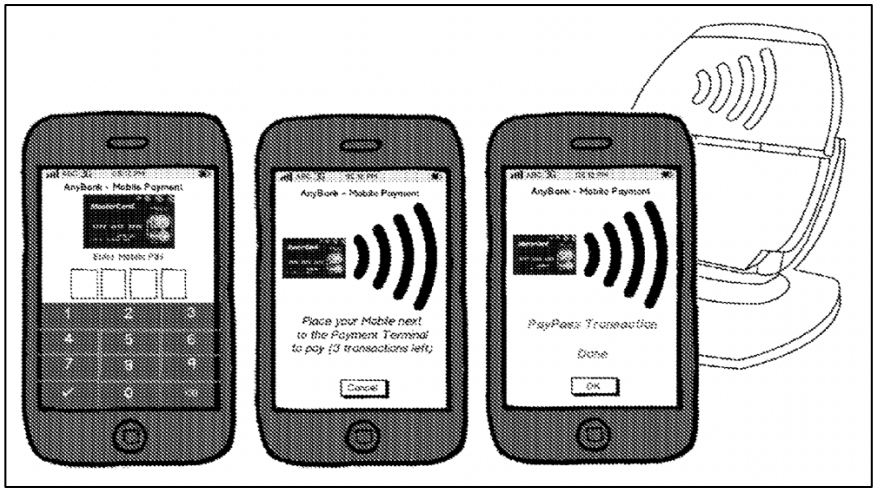
'098 Provisional (Ex.1008), 99; *see also '248 Provisional (Ex.1006)*, Fig. 2B.

10. Phillips' Teachings

197. 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].

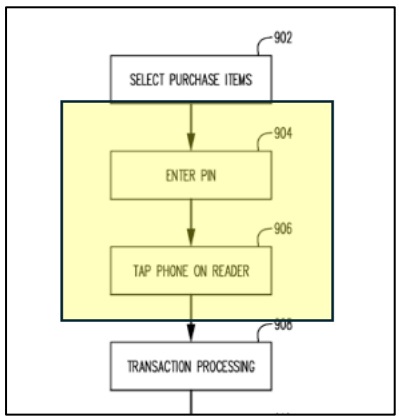
11. Motivation to Combine

198. 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. 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.



'098 Provisional (Ex.1008), 99; *see also '248 Provisional (Ex.1006)*, Fig. 2B. A POSITA would have appreciated that Phillips and Collinge both teach inputting a

PIN just before the user taps the phone on the reader. *'098 Provisional (Ex.1008)*, 99; *Phillips*, Fig. 9.



Phillips, Fig. 9. (annotated excerpt) It was well understood that credit cards will decline when a credit limit is reached as taught by Collinge. *See Collinge,* [0120], [0077]. A user may still need to complete their payment, for example, because the service being paid for has already been completed. It was well known that if a payment method fails that the user may want to retry, decline, or go through with a transaction. A POSITA would have appreciated that such a modification would increase transaction speed instead of making the user go back to the first step to perform 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.

> **12(a): "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: […]accepting a user input selection of a payment option, from said payment options, via said touch-screen display.

199. *See* Claims 1(a), (d).

12(b): "proceeding with a default payment option in said device payment transaction responsive to a user not selecting any of said payment options."

200. Collinge in view of Phillips teach proceeding with a default payment option in said device payment transaction responsive to a user not selecting any of said payment options.

201. Phillips teaches that 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].

12. Motivation to Combine

202. 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. 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 that many users have one card that they use considerably more often than other cards. Further, a POSITA would have appreciated that in the combination, the user is still given a choice of payment methods, if they prefer not to use their default method. For example, this was well known in the art. Lin teaches "a default payment account may be an account that is automatically selected for providing a payment when a transaction is initiated on the device 10." *Lin*, 25:22-26:7. 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.

19(Pre): "An electronic device comprising:"

203. *See* Claim 1(Pre).

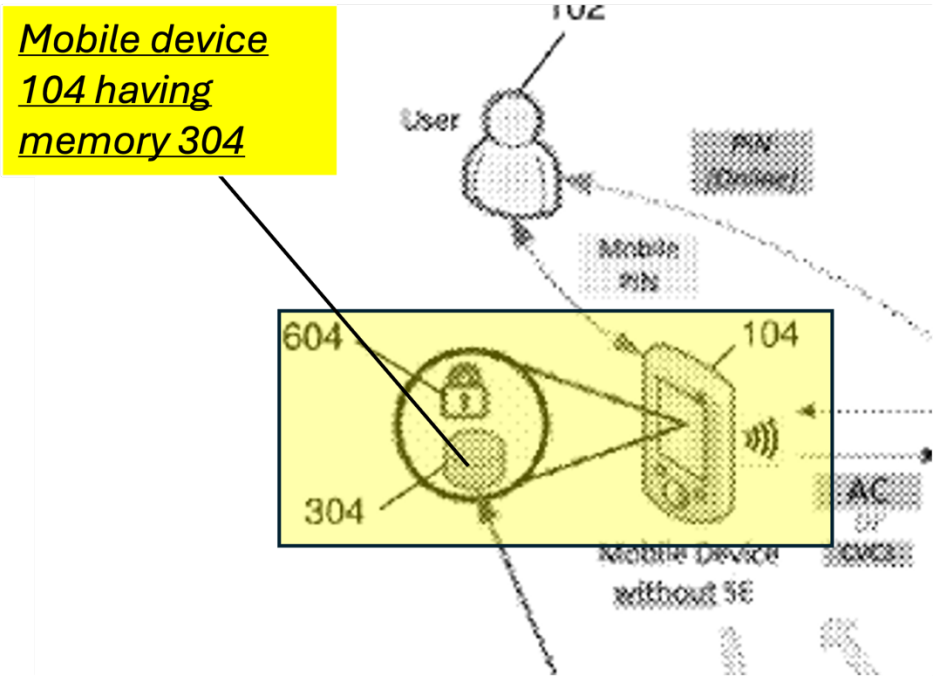
19(a): "at least one processor;"

204. *See* Claim 1(b).

19(b): "a memory coupled to the at least one processor;"

205. Because Collinge teaches that 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[,]" Collinge teaches that mobile device 104 includes *a memory*. Collinge further teaches that mobile device 104 comprises a "storage 304." *Collinge*

at [0073] ("The mobile payment application 106 may also…encrypt the **storage 304 on the mobile device 104**.") (emphasis added). Thus, Collinge teaches mobile device 104 comprising *a memory*.

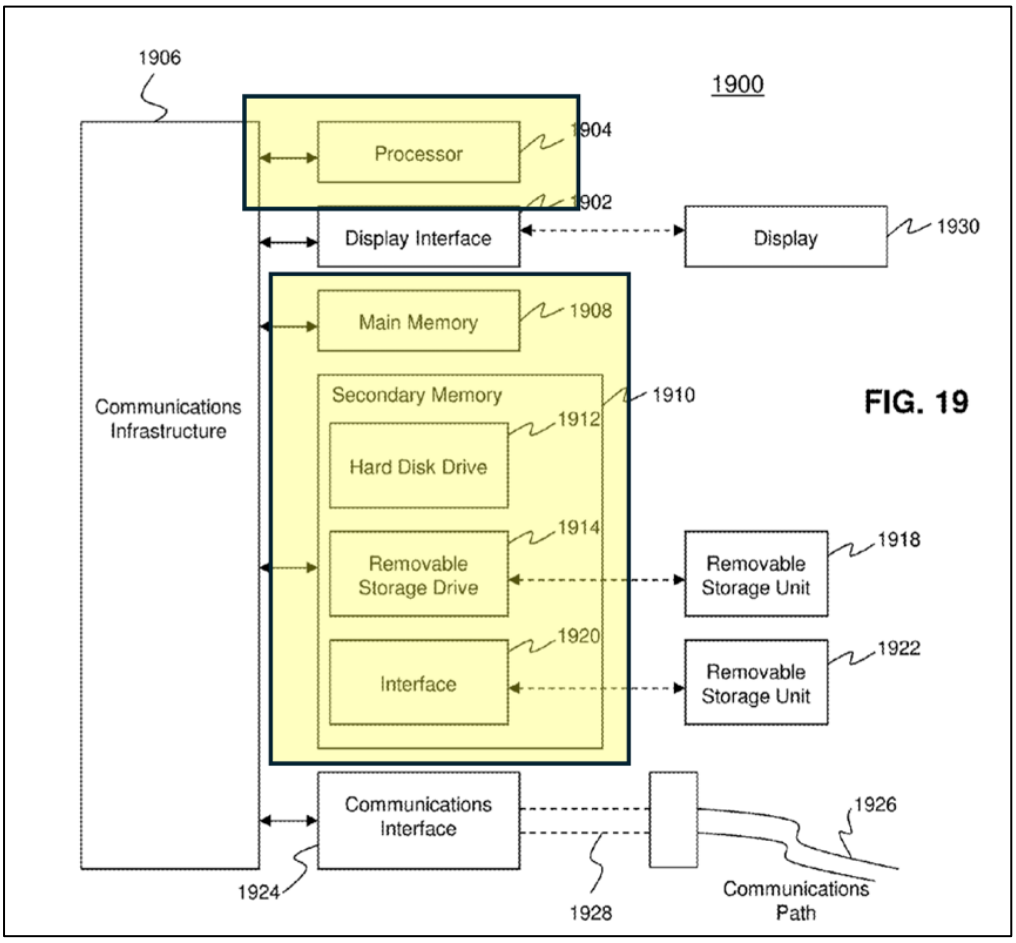


Collinge at Figure 6 (illustrating mobile device 104 having memory 304) (annotated excerpt).

206. A POSITA would understand that the processor and memory of mobile device are necessarily coupled because if the memory were not coupled to the processor, then the mobile payment application 106 executed by the processor on mobile device 104 would not be functional. It was well known that processors in electronic devices operate by reading instructions stored in memory. If the processor were not coupled to the memory, then the processor would not have any instructions

to read/follow and would be rendered inoperable to perform the functions of mobile device 104. Thus, Collinge renders obvious *a memory coupled to the processor*.

207. Additionally, a POSITA would have understood that Collinge's memory is coupled to the processor based on the teachings of Figure 19. A POSITA would have also understood and/or found obvious that Collinge's mobile device 104 would be implemented as the computer system 1900 based on the teachings of the '248 Provisional (Ex.1006) that teaches processor 1604 of Figure 16 (corresponding to processor 1904 in Figure 19 of Collinge) as carrying out the methods of Figures 2A-B, which are done on mobile device 104. I have reproduced Figure 19 of Collinge below, which illustrates main memory 1908 and secondary memory 1919 as being coupled to processor 1904 through communications infrastructure 1906. *Collinge* at Figure 19.



Collinge at Figure 19 (annotated).

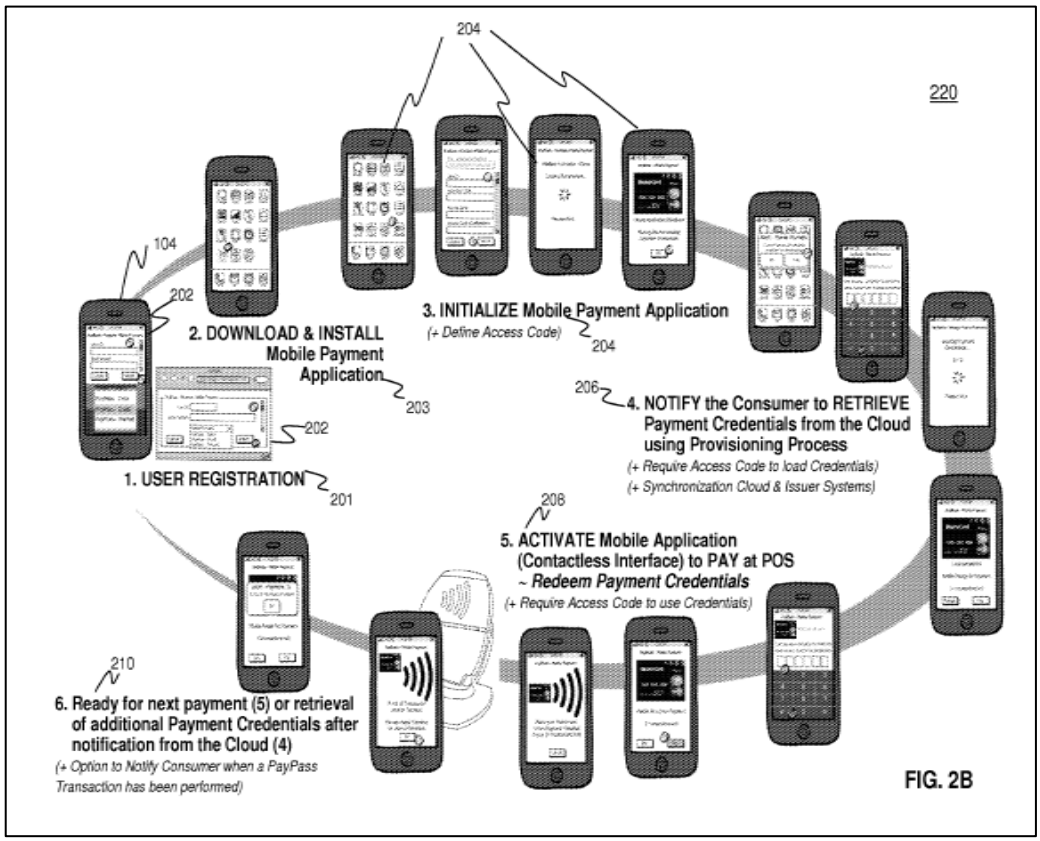
19(b): "a display operable to present a visual user-interface comprising device inputs;

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

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

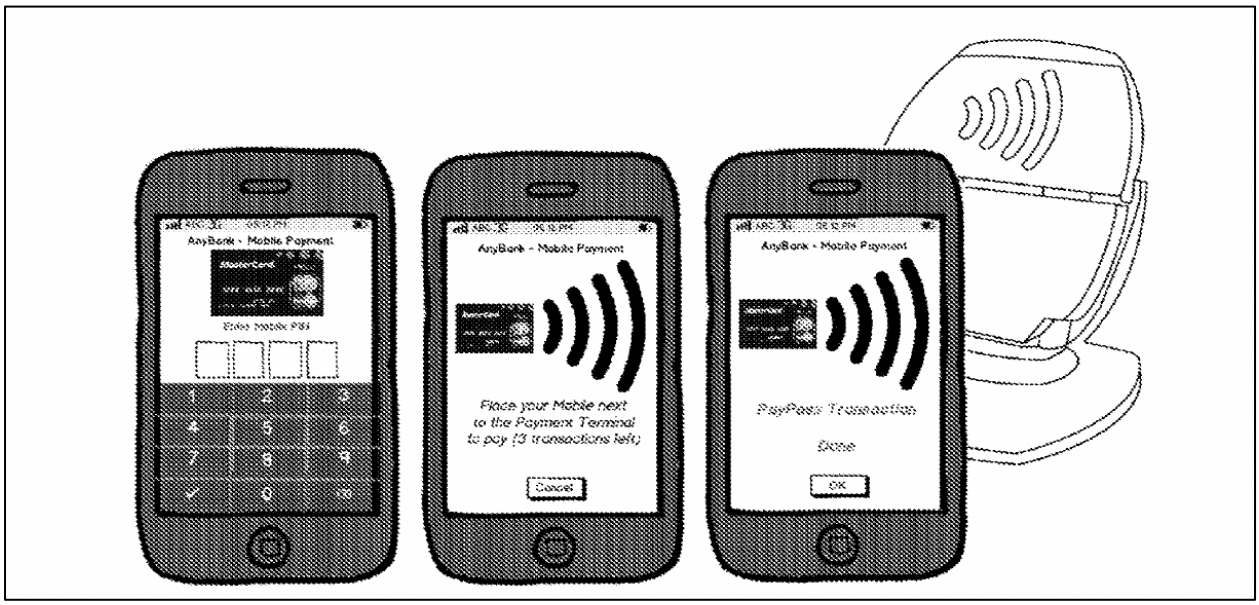
210. A POSITA would have understood that Collinge's touch screen (i.e., user-input device) would have physical hardware components and software components (e.g., a visual GUI component). *Mahapatra (Ex.1041)*, 37 ("[a] basic touch screen…is made up of 3 basic elements, a sensor, a controller and a software driver."). A POSITA would have understood that Collinge's touch screen includes a visual GUI component (for example, the GUI depicted in *'248 Provisional (Ex.1006)*, Fig. 2B below) that corresponds to the claimed "touch-screen user interface."

211. Collinge's '248 Provisional (Ex.1006) application (which I understand is incorporated by reference into Collinge) provides further examples of user interaction with the touch screen during the user registration and payment process. In the below image, Collinge teaches that the user interacts with the user-interface on the touch screen of the device to download and install the mobile payment application, input access codes (e.g., PIN numbers), make selections, and receive status information throughout the transaction.



'248 Provisional (Ex.1006), Fig. 2B.

212. As shown below, Collinge teaches that the user interface may direct the user to input a PIN, direct the user to place the mobile device near a payment terminal, and provide an indication to the user when the payment transaction is complete. *'098 Provisional (Ex.1008),* 99.



'098 Provisional (Ex.1008), 99; *'248 Provisional (Ex.1006),* Figs. 2A-B. Collinge further teaches that that registration process steps can also "be accomplished using input supplied by a cardholder or user" "via a GUI" of the mobile device 104. *'098 Provisional (Ex.1008),* [0063]. A POSITA would understand that all of the interactions depicted above during Collinge's registration and payment process are user payment interactions. In each instance, the user interacts with the visual user-interface on the touch screen of Collinge's mobile device 104 which displays information relating to Collinge's system for making payments using mobile device 104. As another example, Collinge teaches that the touch screen of mobile device 104 receives a user's input of a "mobile personal identification number (PIN)" prior to generation of a payment cryptogram. *Collinge*, [0133]

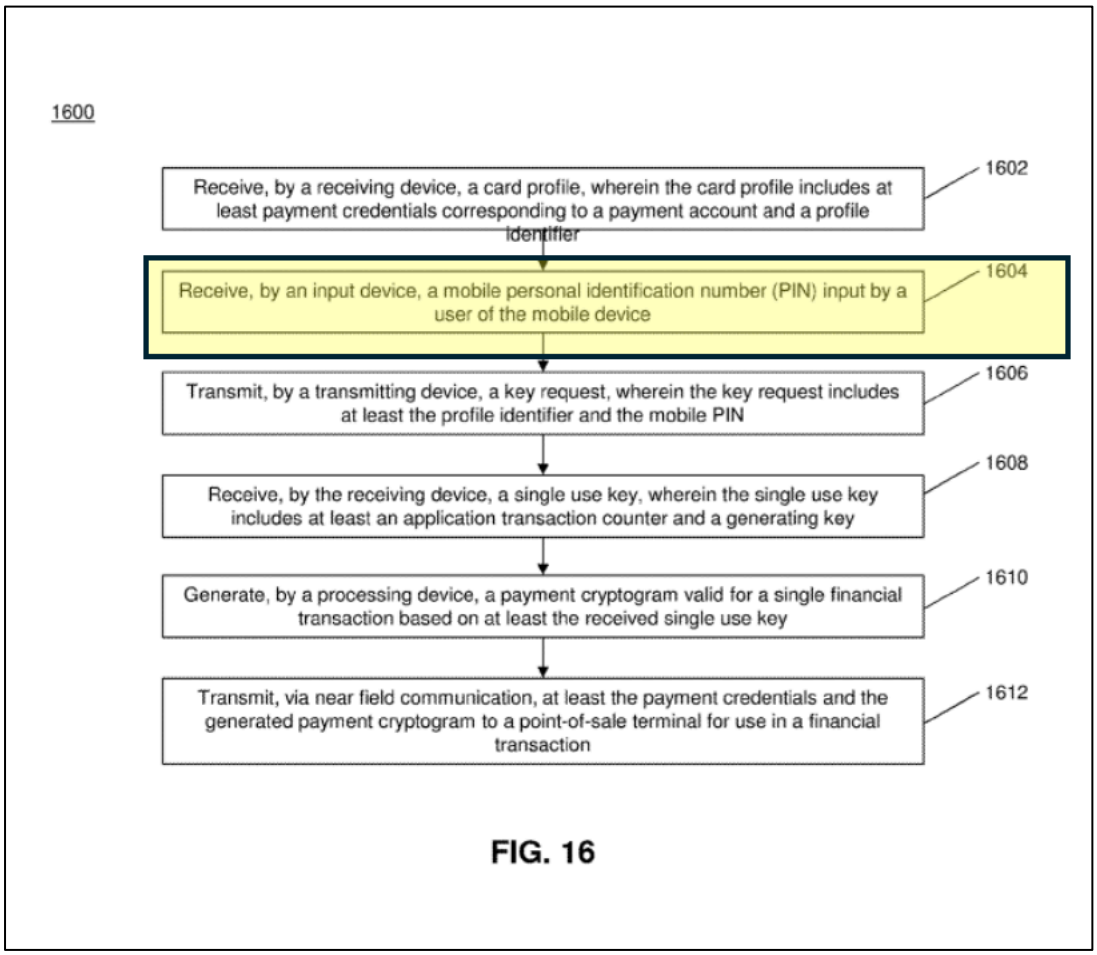
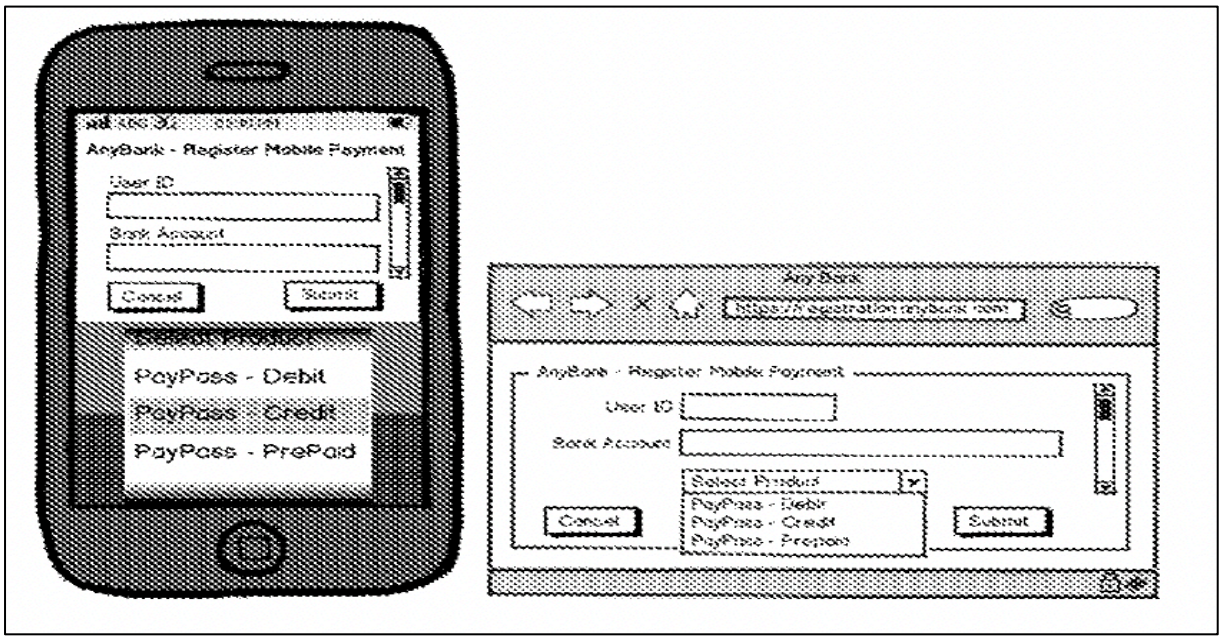


FIG. 16

Collinge, Fig. 16. (annotated)

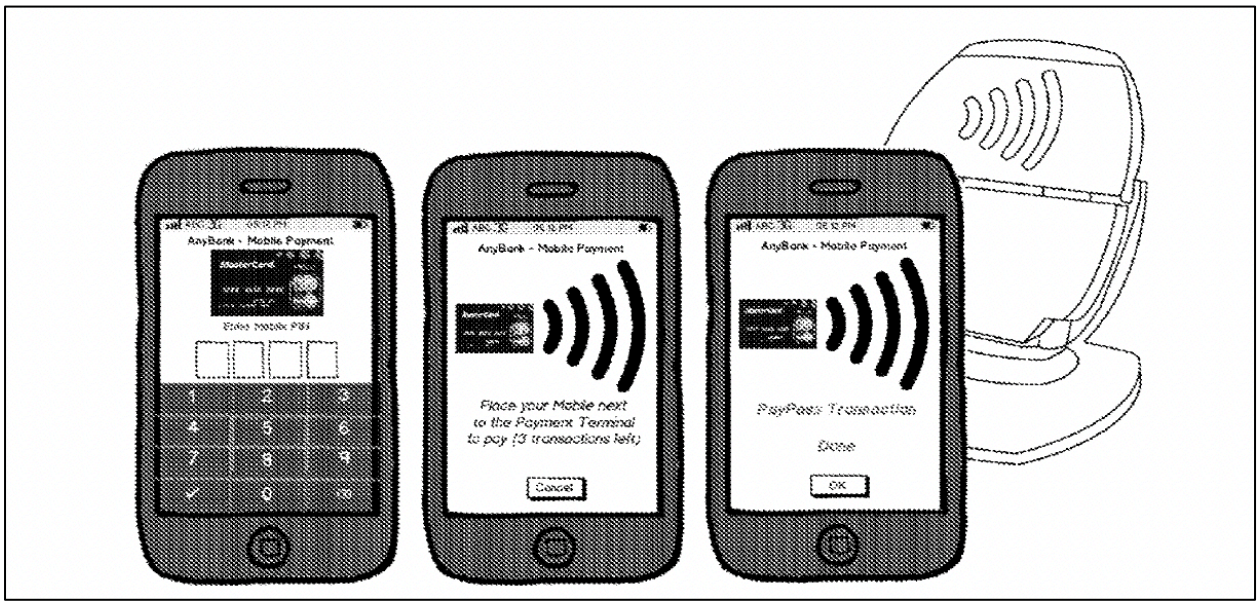
213. Collinge's registration process steps can likewise "be accomplished using input supplied by a cardholder or user" "via a GUI" of the mobile device 104. *Id.,* [0063]. Collinge's user-interface is also operable for a user selection, of at least one of issuer-provided payment methods via the touch-screen display interface.



'098 Provisional (Ex.1008), 96; *'248 Provisional (Ex.1006)*, Fig. 2A-2B.

19(b)(1): "display output;"

214. As shown above in Claim 19(b), Collinge teaches a *display output*. Collinge teaches that on the touch screen display, Collinge's display visually directs a user 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 as depicted in *'098 Provisional (Ex.1008),* 99.



'098 Provisional (Ex.1008), 99; *'248 Provisional (Ex.1006)*, Fig. 2A-2B. The registration process steps can likewise "using input supplied by a cardholder or user" via a GUI" of the mobile device 104. *'098 Provisional (Ex.1008),* 99, [0063].

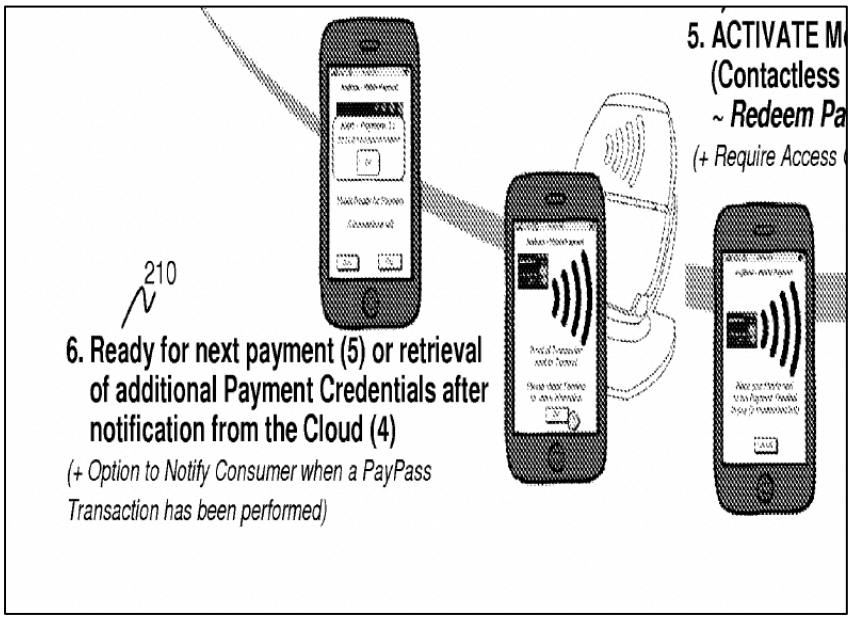
19(b)(2): "a device input;"

215. *See* Claim 19(b).

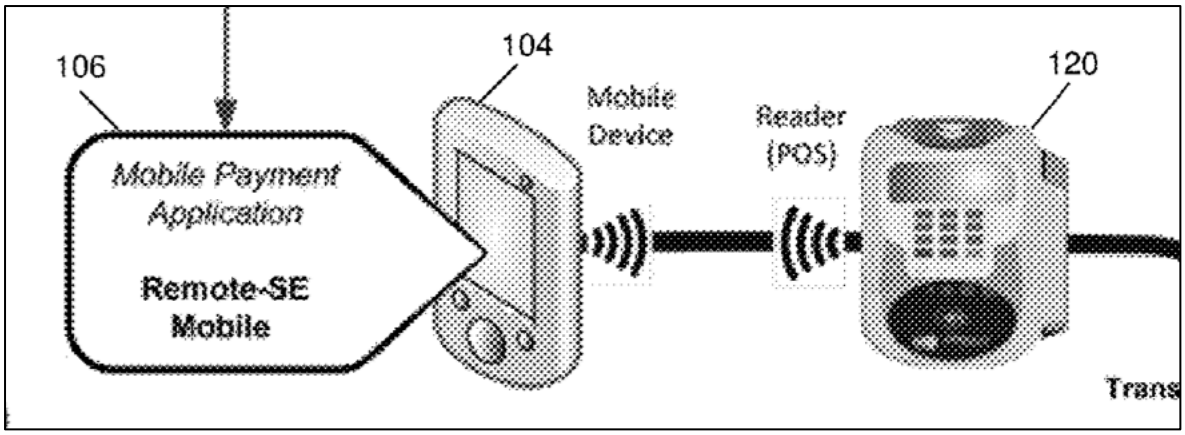
19(b)(3): "an NFC interface operable to receive a transaction request when in proximity to an NFC recipient;"

216. As I discussed 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).

217. A POSITA would have understood that Collinge's mobile device in Figure 1 is within "proximity" to an NFC recipient. *See also '248 Provisional (Ex.1006)*, Fig. 2B; *Collinge*, Fig. 1.



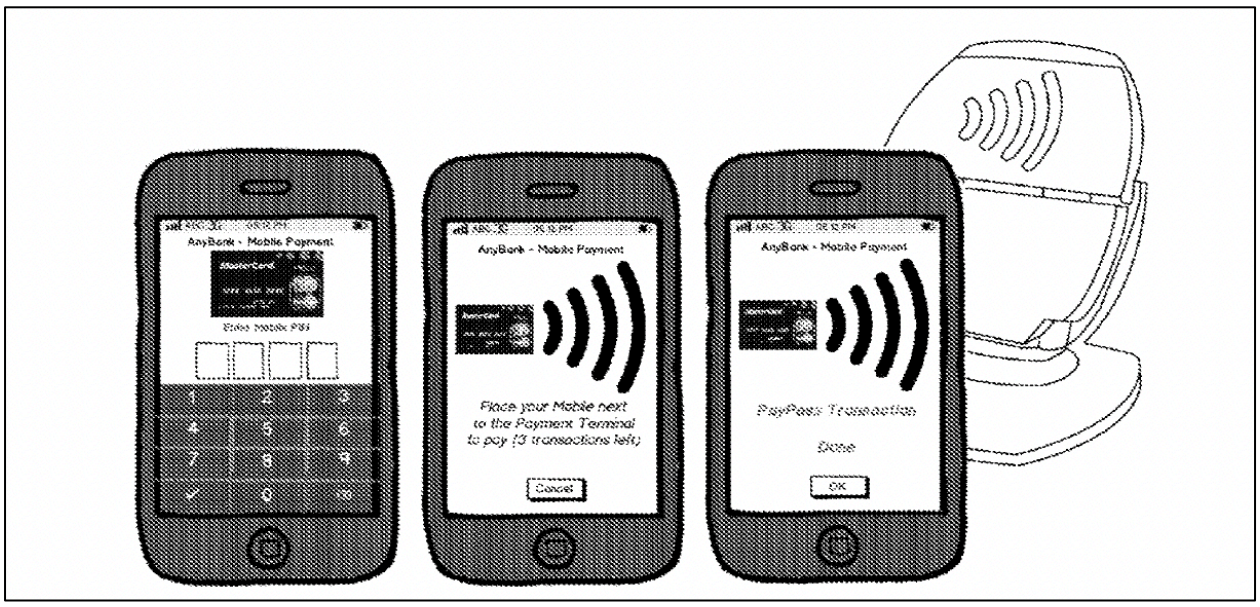
'248 Provisional (Ex.1006), Fig. 2B. (excerpt)



Collinge, Fig.1. (excerpt)

218. Further, it was well known that NFC transactions are performed within "proximity" to an NFC recipient. For example, Near Field Communication (NFC) "enables communication between an NFC enabled mobile phone at one end, and another NFC-enabled mobile phone, an NFC reader, or an NFC tag at the other end." *Coskun (Ex.1021)*, 1. In terms of distance, "NFC is restricted to within very close

proximity." *Coskun (Ex.1021)*, 1. This proximity is often "within 4 cm[.]" *Coskun (Ex.1021)*, 32.



'098 Provisional (Ex.1008), 99.

19(c): "wherein the processor is operable to execute a program to implement a method comprising:"

219. As discussed throughout, 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.")

19(d): "accepting a priming action of the electronic device by an identified device user, from the device input;"

220. *See* Claim 1(a).

19(e): "enabling the electronic device for imminent performance of a payment operation responsive to the priming action of a valid user;"

221. *See* Claim 1(a), 10.

19(f): "displaying a summary of selectable payment account options on the display;"

222. *See* Claim 1(d).

19(g): "receiving a payment selection and approval authorization from a valid device user via the device input; and"

223. *See* Claim 1(d).

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,"

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

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"

225. *See* Claim 1(f).

19(j): "wherein further the processor is operable to cause the display to visually convey a status of the transaction."

226. *See* Claim 1(g).

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 touch key-pad[…] and identifying a valid device user through an input detection, selected from at least one of a set comprising: a correct passcode entry sequence[…]: and receiving a correct user response input, from a security challenge presented on the display."

227. Collinge teaches receiving the *priming action* (e.g., activation code, PIN) of a valid user via the touch key pad on Collinge's 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*) that is displayed on the display of mobile device 104. As discussed above in the overview section, the'579 Patent discloses a priming operation may have several different examples. *See '579 Patent* (Ex. 1001), 11:34-42.

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[…]; 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."

228. 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. *See* Claim 1(e).

229. Collinge teaches that the "[p]rocessor device 1904 may be a special purpose or a general purpose processor device." Collinge, [0150]. Collinge also teaches that "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 (Ex.1006), [0006]. A POSITA would have understood that 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. In fact the "GlobalPlatform Trusted Execution Environment (TEE) defined a standardized isolation environment for Systems on Chip (SoC) in which sensitive code, data and resources are processed away from the main operating environment, software and memory on the device." *TPM (Ex. 1051), 3.* Running code "in the TEE and using protected resources (known as 'Trusted Application's') is cryptographically verified prior to execution, leading to high integrity assurance." *TPM (Ex. 1051), 3.* It was well known that a cryptographic processor is one that performs cryptographic operations, such as generating a payment cryptogram. Since the TEE "provides an isolated runtime environment

entirely inside the SoC (processor chip), the TEE enables advanced device or peripheral security use cases such as securing the user interface, or controlling access to an NFC chip." *TPM (Ex. 1051), 3.* Since Collinge does not have a Secure Element, the TEE behaves like a Secure Element would. As such "the TEE can be used as a distinct security coprocessor or to provide a trusted 'bridge' between the user and other security technologies such as secured UI or OS user permissions on one side, and Secure Element access control on the other" *TPM (Ex. 1051), 3.*

X. OPINIONS REGARDING GROUND 2: *COLLINGE* IN VIEW OF LIN AND KRANZLEY

5(a): "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: device secrets; issuer secrets;"

230. 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].

5(b): "and displaying the limited-use security number on the user-interface of the display."

231. 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*).

232. 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).

1. *Motivation To Combine*

233. It would have been obvious and a POSITA would have been motivated to modify Collinge's mobile payment application to display the Collinge's payment cryptogram on Collinge's display as taught by Kranzley. A POSITA would have recognized that 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 CVV-type value to be provided, as taught by Kranzley. *Kranzley,* [0011], [0040]. 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 that this would have been combining known elements to yield predicable results.

6: "The method of claim 1, wherein a payment processing authority verifies a limited-use number based on at least one information of the set of information comprising…a transaction sequence count information 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 and a use outside of a valid time window."

234. 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*), response to verifying a valid limited-use number, by the payment network (*payment processing authority)*, on at least one unverifiable condition, of a set of unverifiable conditions comprising: an invalid number generation and a use outside of a valid time window where the payment cryptogram appears in place of *card issuer information* (CVC).

2. Collinge's Teachings

235. 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].

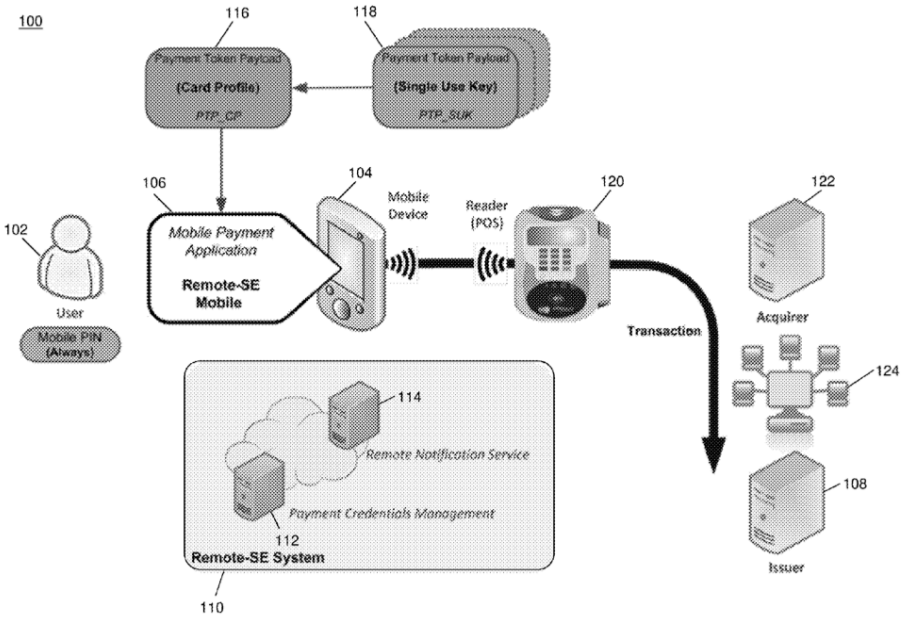


FIG. 1

Collinge, Fig. 1.

236. 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]. The issuer approves a transaction by "validat[ing] the application cryptogram." *Collinge*, [0077].

237. Collinge teaches that the single-use key is "protected based on a mobile personal identification number (PIN)[.]" *Collinge,* [0051]. To use the single-use key to generate a payment cryptogram, "user 102 may provide a mobile PIN for authentication." *Collinge,* [0051]. If the "mobile PIN provided is incorrect, an incorrect value of the single use key may be used by the mobile payment application 106. In such an instance, the issuer 108 will not authorize the payment transaction." *Collinge,* [0051]. A POSITA would have understood that an incorrect value of the mobile PIN used when generating a payment cryptogram is due to *invalid number generation*.

238. As another example, Collinge teaches that the issuer 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. *See '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 limited for a specified merchant category; and a spending limit for a duration.").

3. *Kranzley's Teachings*

239. Kranzley teaches that "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].

240. 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].

4. Motivation to Combine

241. 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*) validates a payment cryptogram as taught by Kranzley instead of Collinge's issuer validating the payment cryptogram. Collinge already teaches a payment network. *Collinge*, [0036]. Collinge's payment network already deals with 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 understood that one example of a payment processing authority would be Collinge's payment network.

242. A POSITA would have appreciated that 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]. A POSITA would have been motivated have Collinge's payment network (payment provider) approve a payment transaction in order to have a faster transaction since you would be reducing one step of forwarding the information to the issuer and would have had a reasonable expectation of success in making such a modification.

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. 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. 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.

XI. OPINOINS REGARDING GROUND 3: COLLINGE IN VIEW OF LIN, PHILLIPS, SMITH, AND KRANZLEY

4(Pre): "The method of claim 1, wherein a limited-use number comprises a device account number,"

244. 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.

245. In similar art, Smith (also assigned to MasterCard) teaches a "mobile device" that "may…be used…with a near field communications enabled purchasing transaction." *Smith*, Abstract.

246. 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].

247. 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]. The PPAN is a different number from the actual PAN. As discussed in greater detail below, a POSITA would have recognized and Smith teaches that it is beneficial to use a PPAN in place of traditional payment account credentials so that if the mobile device and mobile wallet are compromised (i.e. lost or stolen), the PAN associated with the user's payment device (i.e. credit card) is not compromised. *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.")

248. Smith therefore teaches (1) a mobile device with a mobile wallet, (2) assigning a user's PAN to a "PPAN" (*device account number*) to be used by the user in place of a PAN, and (3) allowing the user to present his/her mobile device with a PPAN at a point-of-transaction (POT) for payment. *Smith*, [0024].

249. In the combination, Smith's PPAN is used in place of Collinge's PAN.

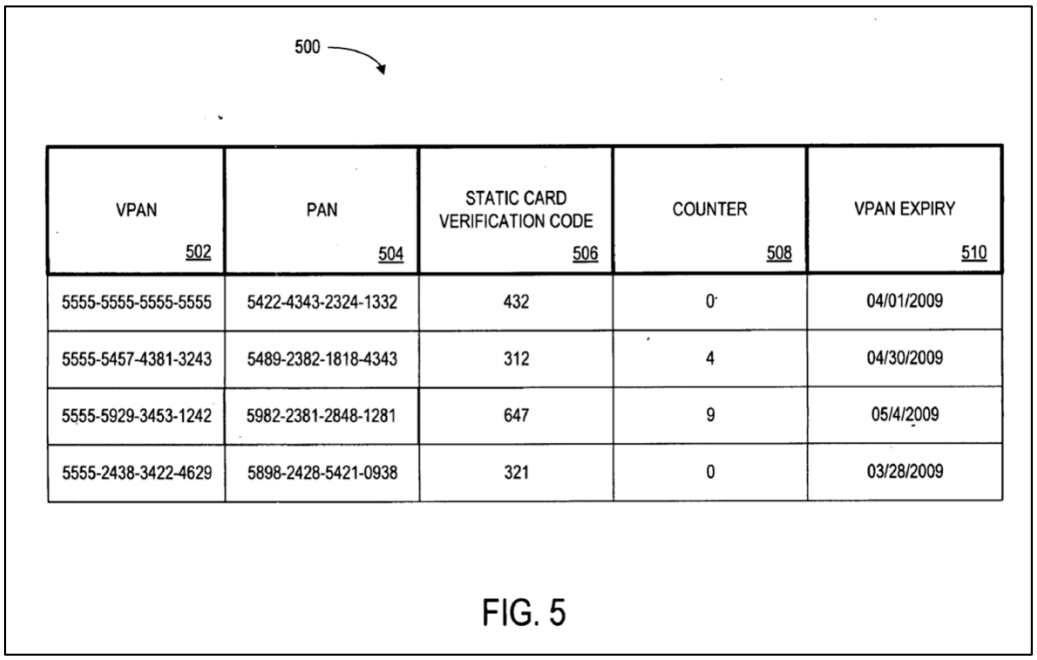
1. Collinge's Teachings

250. Collinge teaches that its mobile device is provisioned with a "card profile," including static payment credentials such as a PAN or Primary Account Number. *Collinge*, [0043], [0143]. *See also '098 Provisional (Ex.1008)*, [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."); [0048]-[0049] (emphasis added) ("The card profile 116 may include payment credentials…The common payment credentials 202 may include all data elements common to any type of payment transactions, such as both mag stripe and m/chip payment transactions. Such data elements may include **payment account number**, tracking data, and card layout description data."). As I explained above at Section VII, a PAN is the unique identifier number found on the front of a credit, debit, or prepaid card or the like.

251. Collinge further teaches that a virtual primary account number (VPAN) can be used as an alternative to the card PAN and PSN (PAN Sequence Number). *'098 Provisional (Ex.1008)*, 159-160. Collinge teaches that using a Virtual PAN is safer and can "mitigate the risk of any misuse of a PAN value." *Id.*

252. A POSITA would have been well-familiar with the concept of using a VPAN, or other PAN alternative for increased security, as this idea had been around for quite some time. As an example, U.S. Patent Appl. No. 2010/0125509 to Kranzley et al. ("Kranzley"), another Mastercard reference, taught using a VPAN is used in place of a PAN as depicted below:



VPAN 502	PAN 504	STATIC CARD VERIFICATION CODE 506	COUNTER 508	VPAN EXPIRY 510
5555-5555-5555-5555	5422-4343-2324-1332	432	0	04/01/2009
5555-5457-4381-3243	5489-2382-1818-4343	312	4	04/30/2009
5555-5929-3453-1242	5982-2381-2848-1281	647	9	05/4/2009
5555-2438-3422-4629	5898-2428-5421-0938	321	0	03/28/2009

FIG. 5

Kranzley, Fig. 5.

253. Collinge also teaches that a virtual primary account number (VPAN) can be used as an alternative to the card PSN (PAN Sequence Number). *'098 Provisional (Ex.1008)*, 159-160 ("The use of a Virtual PAN can allow an Issuer to mitigate the risk of any misuse of a PAN value") ("Virtual Pan can be used as a mechanism to provide segregation between the PAN (and PSN) value delivered to the Mobile Payment Application as part of a Card Profile[.]") A PSN was known in the art to differentiate multiple cards linked to the same PAN. For example, U.S. Patent Appl. No. 2013/0151292 to Deloo et al. ("Deloo") teaches that "[a] primary account hash sequence number (PSN) may be used to differentiate a primary card from an additional card on the same account." *Deloo (Ex.1045)*, [0078]. As another

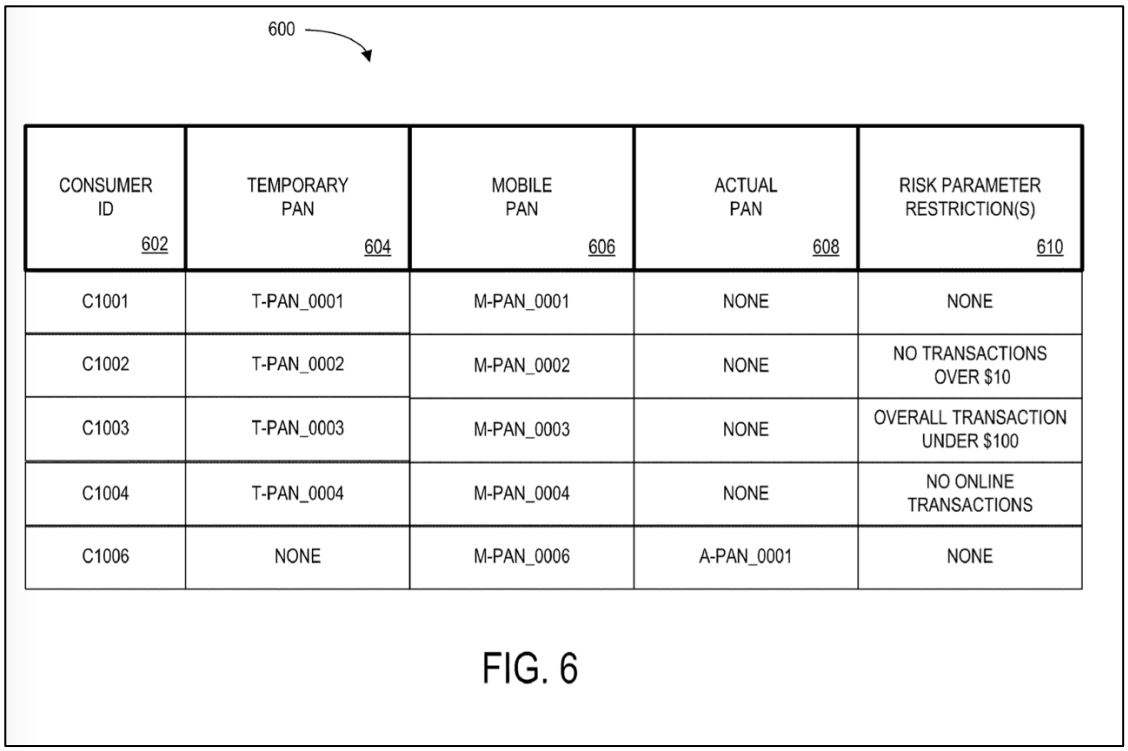
example, Roberts, a Mastercard patent teaches that "a PAN Sequence Number…in combination with the PAN uniquely identifies the card." *Robers (Ex.1044)*, [0074].

2. Smith's Teachings

254. Smith 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].

255. 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].

256. 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]. The PPAN is a different number from the actual PAN as depicted below.



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.

257. Smith's "PPAN" (*device account number*) is "assigned to the mobile device 104." *Smith*, [0016]. The PPAN is used in place of the actual PAN. *Smith*, [0040]. The PPAN is "stored in the mobile device 204." *Smith*, [0022]. A POSITA would have understood that since Smith's PPAN is specifically assigned to the mobile device it is *device account number.*

258. 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

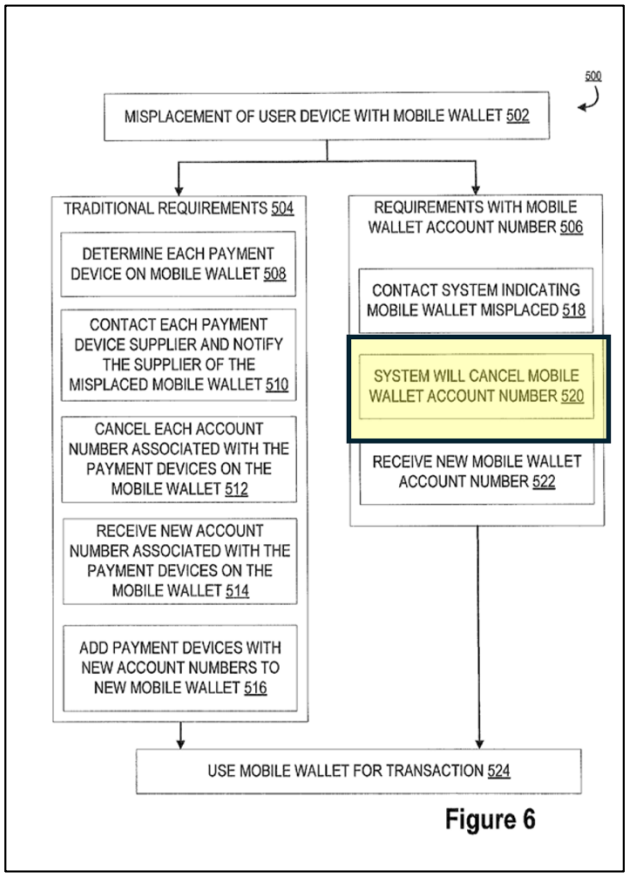
generation service 210." *Smith*, [0023]. Thus, supporting that the PPAN is different from the PAN.

259. The issuer can "implement dual account number structures" for "multiple NFC-enabled handsets may be managed for a single account." *Smith*, [0029]. It was well known that a dual account number has separate and distinct numbers for each device the overall account is used on. For example, U.S. Patent Appl. No. 2006/0186195 to Gray describes "[a]n additional benefit of having two separate but related numbers is that the consumer/cardholder may use the consumer account number to provide a third party the information to send the cardholder funds" via "a dual account number" *Gray (Ex.1046)*, [0035]. Accordingly, a POSITA would have understood Smith's PPAN is a distinct *account number* for a payment account on a particular "mobile device."

260. 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.") A POSITA would have appreciated that using Smith's teachings does not require the user to have to get a new PAN if a device is lost.

261. Smith's PPAN is a static number; Smith teaches the expiration date associated with the account may be updated without updating the PPAN. *Smith*,

[0041] ("update an NFC-enabled payment account (e.g., to update an expiration month and/or year") Therefore, a POSITA would have understood that Smith's PPAN is static for each PAN, in other words if a user registers multiple cards with underlying PANs, each PAN would have its own static PPAN. *See* '579 Patent, claim 21. This was well known in the art. For example, Grigg teaches "[i]f the user misplaces "the user device 204, the user 202 may request cancellation of the mobile wallet account number." *Grigg (Ex.1047),* [0074], Fig. 6.



Grigg (Ex.1047), Fig. 6. (annotated)

3. Motivation To Combine

262. For many reasons, 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 (Ex.1008)*, 159-160.

263. A POSITA would have found it obvious and would have been motivated to use Smith's PPAN in place of the PAN in Collinge's static payment credentials because both Collinge and Smith expressly recognize that it is beneficial to use an alternative to traditional financial institution account numbers when making a payment using a mobile device. Collinge teaches that an alternative payment number (which is calls a Virtual Primary Account Number or VPAN) is safer and can "mitigate the risk of any misuse of a PAN value"). *'098 Provisional (Ex.1008)*, 159-160. Smith teaches a "PPAN" (*device account number*) that is used in place of the PAN/account number. *Smith*, [0040]. Since Collinge already teaches using a VPAN, the issuer would have already been equipped to process and verify transactions when an alternate to the PAN was used.

264. A POSITA would have been motivated to use Smith's PPAN instead of Collinge's PAN so that Collinge's mobile device would not be required to store the PAN, which is a sensitive financial number. For example, Smith teaches the PPAN is "stored in the mobile device 204." *Smith*, [0022]. Smith also teaches the issuer has to "requests a look up of the related PAN from the PAN mapping/account

generation service 210." *Smith*, [0023]. Both supporting that the PAN does not need to be stored in Smith's device.

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. *See Ghosh (Ex.1048)*, 51. ("Without a secure infrastructure for computing on the device, achieving secure m-commerce may not be possible."); *Collinge*, [0003]-[0004]. ("In order to achieve this, mobile phones with secure element hardware (e.g., a Secure Element chip) are used to securely store payment account credentials, such as credit card credentials. However, not all mobile devices have secure elements. Furthermore, some issuers may not have access to a secure element on a mobile device, even if the mobile device has one available. As a result, a consumer who has a NFC-capable mobile device may not be able to use their device to conduct payment transactions if their mobile device lacks a secure element, and even in some cases where their mobile device has a secure element.") For example, a POSITA would have understood that it is valuable to remove all traditional payment device account numbers from a user device so that if the device were stolen, the thief would have access only to PayPass PAN(s). *Bona,* [0074]; A POSITA would have recognized that this is beneficial because if a user's device is lost or stolen, only the PPAN(s) would have to be

cancelled; automatic transactions using the traditional payment credentials (such as the credit card PAN) would not be impacted. *Bona,* [0007], [0014], [0074], Fig. 6. For example, Vizzarri (Ex.1032) teaches different techniques to guarantee security in m-payment systems. Classical methods are end-to-end encryption and tokenization. With tokenization an encrypted or random value, called token, replaces the card number (PAN) or the magnetic stripe track data in an electronic transaction. The token then becomes the reference number representing the card number, so all tokens can be referenced back to the original card number." *Vizzarri (Ex.1032)*, 5.

266. 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 as an alternative to the card PAN and PSN (PAN Sequence Number) and a POSITA would have been familiar with using PAN-alternatives, particularly when making mobile PayPass payments. *See '098 Provisional (Ex.1008)*, 159-160 In the combination, Smith's PPAN would perform the same function—provide an alternative account number that can be used for a payment transaction. *Smith*, [0023]-[0024]. A POSITA would have understood that using Smith's PPAN in place of Collinge's PAN would be combining prior art elements according to known methods to yield the predictable result of increased security. 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. Smith already teaches using "the PayPass® standard" when completing a transaction where "the point of sale device is provided with information including the PPAN stored in the mobile device 204" by using NFC. *Smith*, [0024].

267. In the proposed combination of Collinge and Smith, Collinge's mobile device would receive the assigned PPAN(s) taught by Smith, in place of PAN information in Collinge's payment credentials provisioned to the mobile payment application as part of Collinge's card profile 116. *Collinge,* [0048], Fig. 6, [0104] (card profile (PTP_CP)); *'098 Provisional (Ex.1008)*, [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.");

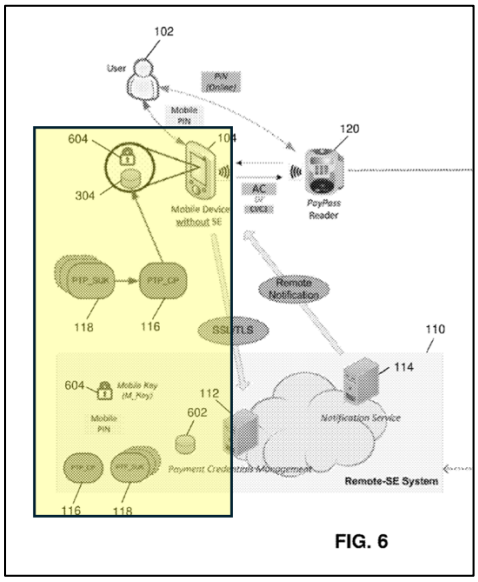
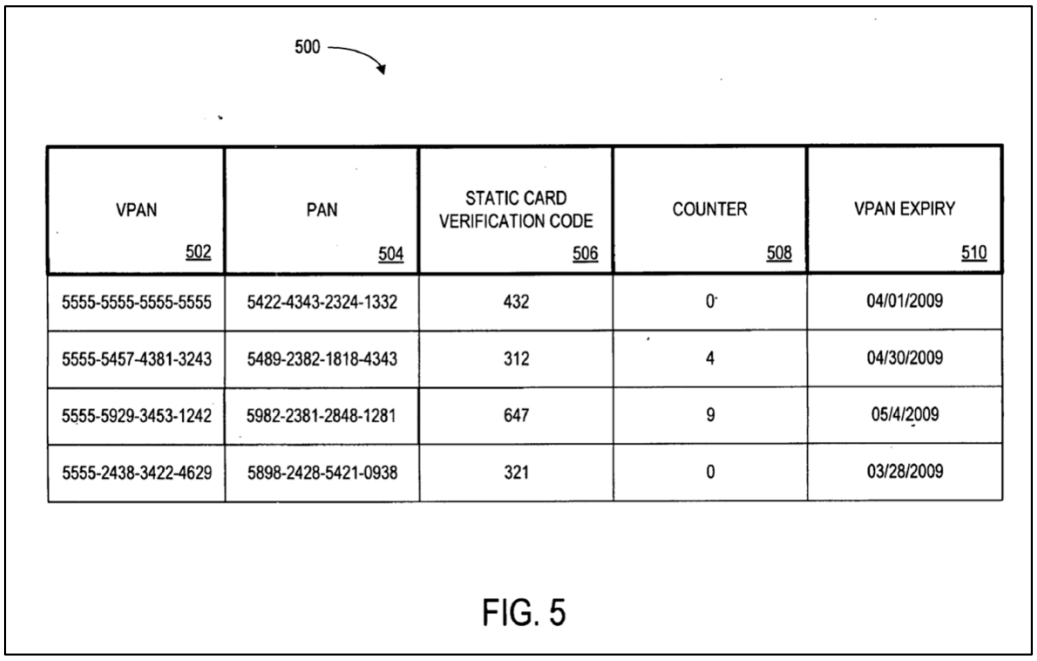


FIG. 6

Collinge, Fig. 6. (annotated excerpt). A POSITA would have appreciated that Smith already demonstrated feasibility of such a system. Collinge already receives the card profile (PTP_CP) through the remote-SE cloud system. *Collinge*, Fig. 6; [0104]. Further, it was well known in the art some Mastercard systems were already able to receive an alternative to the PAN from a payment provider/issuer/financial institution. For example, Kranzley teaches that in Figure 5 "[t]he table includes entries identifying VPANs that have been issued or assigned by the payment provider 110."



VPAN 502	PAN 504	STATIC CARD VERIFICATION CODE 506	COUNTER 508	VPAN EXPIRY 510
5555-5555-5555-5555	5422-4343-2324-1332	432	0	04/01/2009
5555-5457-4381-3243	5489-2382-1818-4343	312	4	04/30/2009
5555-5929-3453-1242	5982-2381-2848-1281	647	9	05/4/2009
5555-2438-3422-4629	5898-2428-5421-0938	321	0	03/28/2009

FIG. 5

Kranzley, Fig. 5.

268. 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.").

269. It was well known in the art that storing sensitive information such as a PAN in fewer locations can lessen the risks of the sensitive information being compromised. For example, PCI SSC teaches that "[s]toring tokens instead of PANs is one alternative that can help to reduce the amount of cardholder data in the environment[.]" *PCI SSC (EX.1031)*, 3. PCI SSC also teaches that "[o]ne of the primary goals of tokenization solution should be to replace sensitive PAN values with non-sensitive token values." *PCI SSC (EX.1031)*, 5. A POSITA would have understood that using Smith's PPAN in place of Collinge's PAN would be combining prior art elements according to known methods to yield the predictable result of increased security. It was well known in the art that storing sensitive information such as a PAN in fewer locations can lessen the risks of the sensitive information being compromised. Collinge already teaches that using a Virtual PAN is safer and can "mitigate the risk of any misuse of a PAN value." *'098 Provisional (Ex.1008)*, 159-160. 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.

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,"

270. As discussed in Claim 4(Pre), Collinge in view of Smith teach 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. 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)").

271. Collinge, Smith, and Kranzley teach wherein the device account number is of a limited time-duration of valid use. Kranzley teaches using a virtual PAN (VPAN) in place of the PAN. The VPAN "may have its own virtual expiry date." *Kranzley*, [0036].

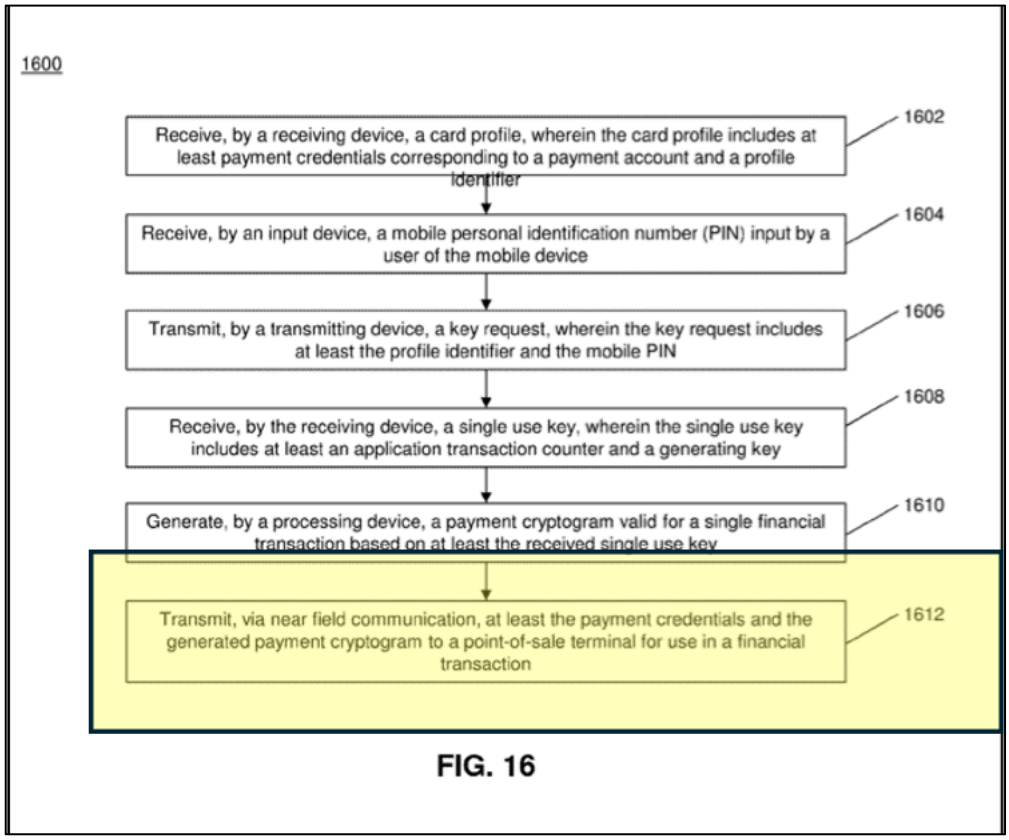
4. Motivation to Combine

272. 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 that 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. The modification is nothing more than the application of a known technique (assigning an expiration date) to a well-known device (mobile device) ready for improvement 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. A POSITA would have been motivated to make such a modification because the PPAN is associated with a payment account which typically is associated with an expiration date. *See, e.g., Smith* at [0029] ((“PPAN, an expiration date (e.g., an expiration month and year)”). Thus, a POSITA would have been motivated, for example, to correspond the PPAN expiration date with the expiration date of a payment card. The modification would have increased security of sensitive payment information, because when an expired PPAN is replaced, the likelihood of perpetrators having the ability to fraudulently use the PPAN is decreased. The modification is nothing more than the application of a known technique (assigning an expiration date) to a known device (virtual account number) ready for improvement to yield predictable results. The modification would have been straight forward and merely required assigning an expiration date to the PPAN, which would have been stored alongside the PPAN in the payment credentials as discussed in 4(Pre).

4(b): "and further comprising: performing payment transactions by the electronic device including the limited-use number;"

273. As shown below, Collinge teaches sending the dynamically generated CVC3 and payment credentials (which include the PAN, among other items) to a point-of-sale terminal in a payment transaction. *Collinge*, [0070], [0077]; [0135] ("at least the payment credentials and the generating payment cryptogram may be transmitted, via near field communication, to a point-of sale terminal (e.g., the point-of-sale terminal 120) for use in a financial transaction.").



Collinge, Fig. 16. (annotated); [0048]-[0049] (emphasis added) ("The card profile 116 may include payment credentials…The common payment credentials 202 may

include all data elements common to any type of payment transactions, such as both mag stripe and m/chip payment transactions. Such data elements may include **payment account number**, tracking data, and card layout description data.")

, Fig. 6, [0104] (card profile (PTP_CP)); *'098 Provisional (Ex.1008)*, [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.").

274. 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] ("the process of personalizing the mobile device 104 with the software (including the PPAN…[o]nce the personalization or loading of the payment application is complete, the customer 102 may use the mobile device **104** to complete payment transactions. ."). A POSITA would again have recognized that substitution of a PayPass PAN would have increased security since sensitive information like a PAN would therefore not be transmitted. *Smith*, [0023] ("the payment network 218 identifies the PPAN and requests a look up of the related PAN"). 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.

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.

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

4(c): "combining the limited-use number and said device account number within a device generated payment information; and"

276. 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 further teaches generating a payment cryptogram (CVC3) based, in part, on a PAN. Further, 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 (Ex.1006), Table 1;*'095 Provisional*, [0010]. ("some payment credentials …including track data…contain PAN information."); *'098 Provisional (Ex.1008)*, [0148] ("The generated encrypted payment token payload 112 contains sensitive data including Track Data, which in turn contains a PAN value.").

277. It was well known in the art that a dynamic card verification value (CVC3) is generated in part based on the PAN as demonstrated by Collinge. 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. Collinge's card profile includes "at least payment credentials corresponding to the associated payment account and a profile identifier[.]" *Collinge*, Abstract. Specifically, Collinge teaches that the "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." *'098 Provisional (Ex.1008),* [0101] (emphasis added); *Collinge*, [0048]-[0049] (emphasis added) ("The card profile 116 may include payment credentials…The common payment credentials 202 may include all data elements common to any type of payment transactions, such as both mag stripe and m/chip payment transactions. Such data elements may include **payment account number**, tracking data, and card layout description data.")

5. Smith's Teachings

278. 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.*

6. Motivation to Combine

279. *See* Claim 4(a). 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). 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 as discussed in Claim 4 when replacing the PAN. A POSITA would have appreciated that Smith's PPAN is linked to the cardholder's account but differs from the actual PAN. 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. Generating adynamic CVV was well known in the art. For example, U. S. Patent No. 7,740,168 to Hammad et al. ("Hammad") teaches "[t]he dCVV or a dynamic card verification value…can be generated using an algorithm which uses at least a counter and input data such as an account number, expiration date, and other information." *Hammad (Ex.1038)*, 1:46-50. 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. 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).

4(d): "conveying said device generated payment information, in place of card issuer information, when the device is performing payment transactions."

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

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.

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

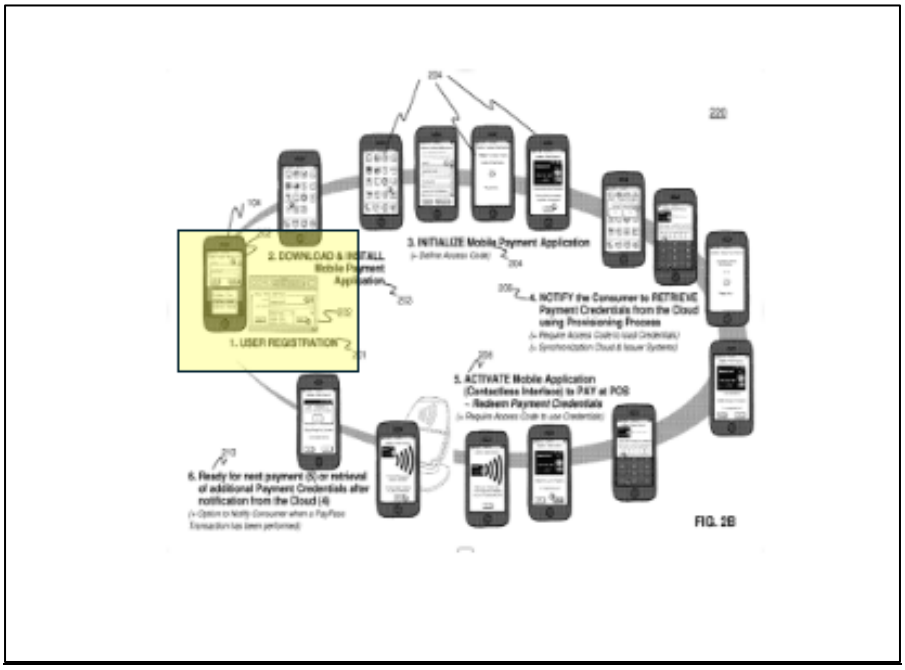
22. The electronic device of claim 19, wherein the memory is accessible to the processor, and wherein said memory comprises: a static device-specific device account information including a device account number of limited-use; and keys, wherein said device-specific device account information originates 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.

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

XII. OPINIONS REGARDING GROUND 4: *COLLINGE* IN VIEW OF LIN PHILLIPS AND AABYE

8(a): "The method of claim 1, wherein the priming operation comprises one operation of the set of operations comprising…a touch-screen touch…a user-interface selection of a payment method; and a user-interface selection initiating a payment-operation;"

283. As I discussed above in Claim 1(a) Collinge teaches a priming operation performed on the touch screen (inputting an activation code). As I discussed above in Claim 1(d), Collinge teaches the user selects a payment method. Collinge's further teaches a user selection of a payment method initiations a payment-operation as shown in step 1 in the figure below.



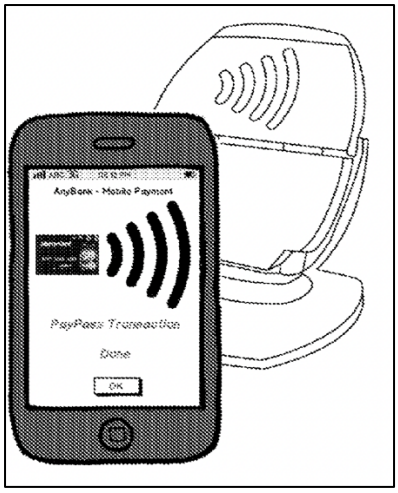
1. *'248 Provisional (Ex.1006), Fig. 2B. (annotated)*

8(b): "further comprising enabling the electronic device for payment via successfully completing at least one of a set of user-validations comprising: a user entry of a valid passcode; a device biometric sensing of a valid user identity; and a device biometric sensing the electronic device is continuously remaining in the proximity possession of a valid user.

284. As discussed above in Claim 1(a) 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. Collinge in view of Aabye further 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.

2. Collinge's Teachings

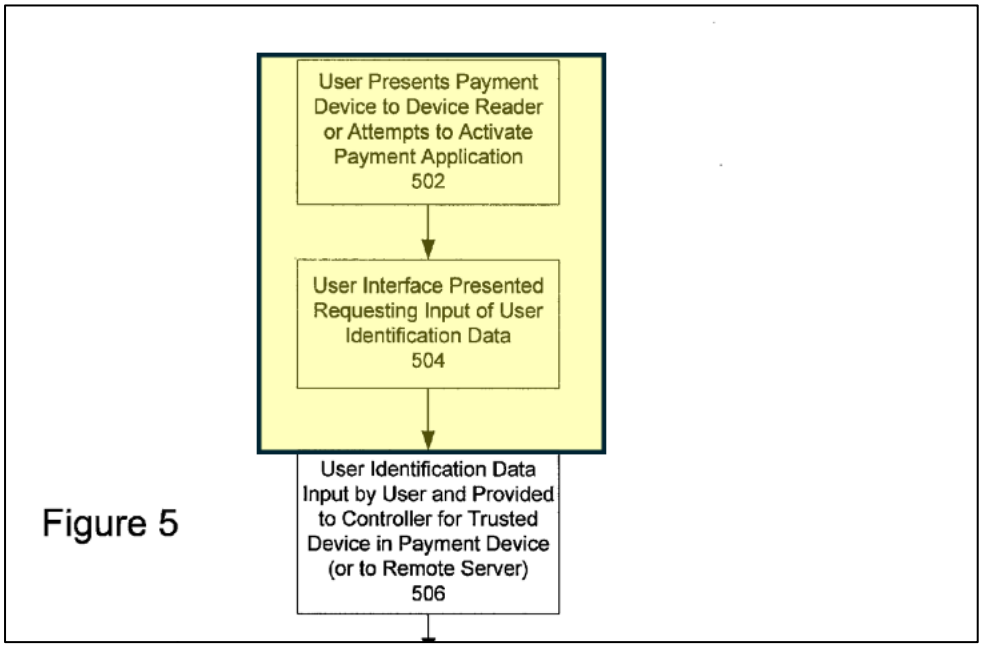
285. Collinge teaches the user may supply "a biometric identifier." *Collinge*, [0143].



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

3. Aabye's Teachings

286. In response to the user presenting the "payment device to device reader", "the user is presented with a user interface." *Aabye*, [0054]-[0055]. Aabye teaches the "the payment device may include a user data input element 402." *Aabye*, [0050]. The "input element 402" may be a "a fingerprint detector or sensor, a touchscreen, a biometric data sensor, etc." *Aabye*, [0050]. 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].



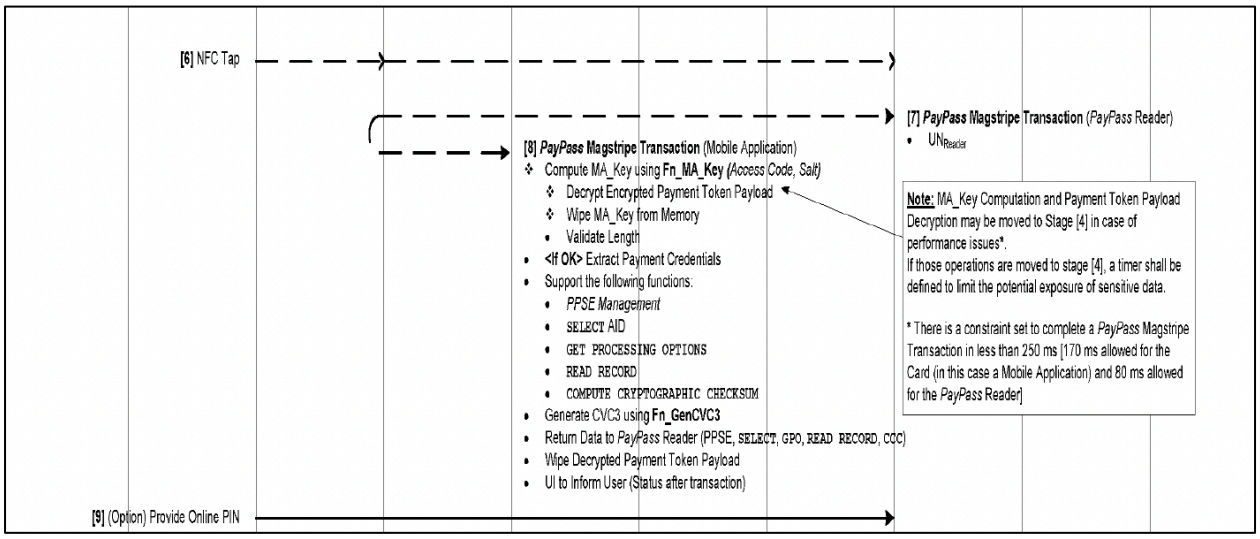
Aabye, Fig. 5. (annotated excerpt)

287. Aabye's 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]. 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. In terms of distance, "NFC is restricted to within very close proximity." *Coskun (Ex.1021)*, 1. This proximity is often "within 4 cm[.]" *Coskun (Ex.1021)*, 32. A POSITA would have understood that once the user's fingerprint is validated, the transaction is enabled the electronic device for payment.

4. Motivation to Combine

288. 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. 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 (Ex.1006), 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. Spoofing a fingerprint is significantly more difficult and requiring a fingerprint for a user to be able to complete a purchase, would provide additional security. Aabye already teaches granting access only if the user's fingerpaint matches. *Aabye*, [0057].

289. 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 know 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. Using a fingerprint sensor was well known in the art. For example 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].

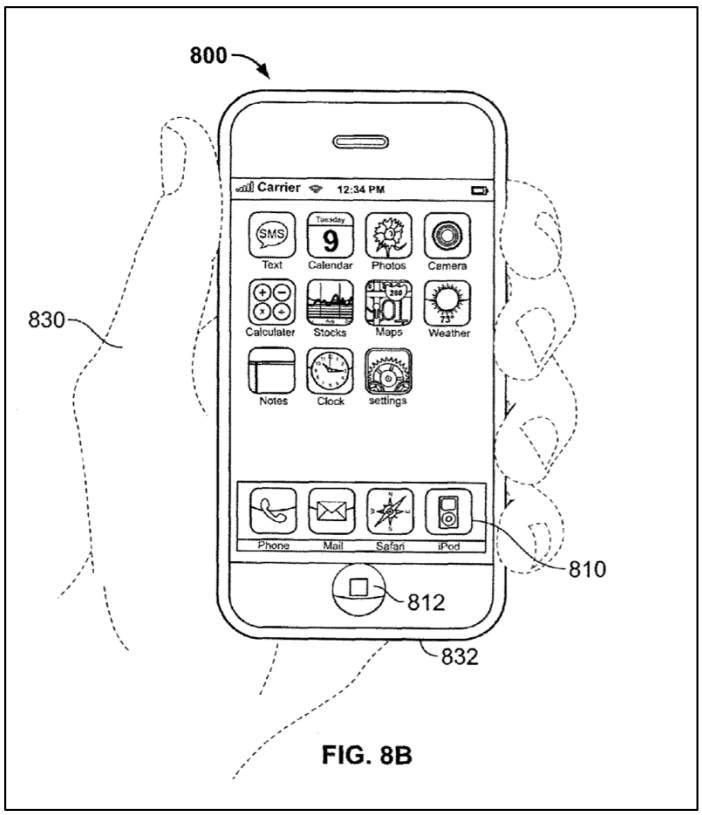


FIG. 8B

Fadell, Fig. 8B.

9(a): "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 touch-screen display interface....and a device biometric sensing the electronic device is continuously remaining in the proximity contact of a valid user; and"

290. As I discussed above in Claim 8(b), Collinge and Aabye teach a device biometric sensor operable to determine the electronic device continuously remains in contact with a valid user. Further, as shown in the figure below Collinge's *device touchscreen user interface* is operable to accept *a user approval* (selecting a pay option).



'098 Provisional (Ex.1008), 100; *'248 Provisional (Ex.1006)*, Fig. 2B.

9(b): "displaying, on the display, at least one information of a set of information comprising… a card image; and other payment iconography"

291. *See* Claim 1(d).

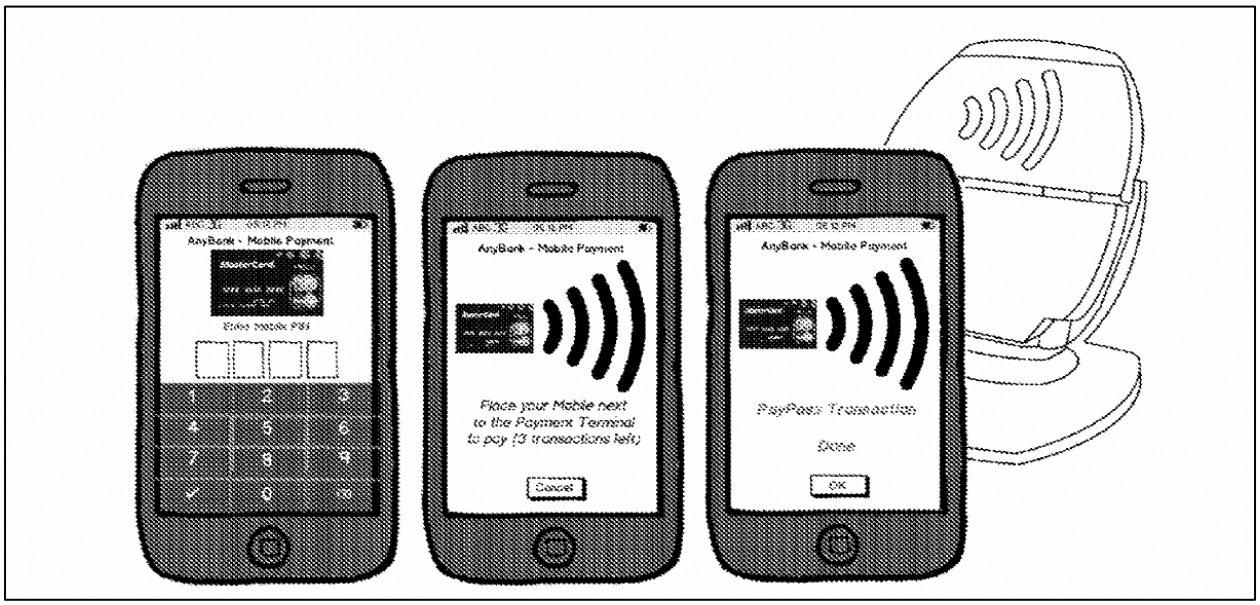
9(c): "receiving a user input of at least one user action, from a set of actions comprising: a payment method selection; a payment approval authorization; a payment denial"

292. Collinge receives a user input from a payment method selection (as discussed in Claim 1(d)), payment approval authorization, and payment denial.

293. As shown in the figures below 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).



'098 Provisional (Ex.1008), 100; *'248 Provisional (Ex.1006)*, Fig. 2B.



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

XIII. OPINIONS REGARDING GROUND 5: *COLLINGE* IN VIEW OF LIN AND AABYE

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

294. *See* Claim 1(Pre).

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;"

295. As discussed above 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. As

an example, Lin teaches the request is sent via NFC and that NFC communication must occur within "2 to 4 cm[.]" *Lin*, 19:26-27.

15(b): "displaying a summary of selectable payment account options at a touch-screen display user-interface of the electronic device;"

296. *See* Claim 1(d).

15(c): "receiving, from a valid device user, a payment selection and approval authorization input on the electronic device;"

297. *See* Claim 1(a).

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"

298. *See* Claim 1(e).

15(e): "transmitting said limited-use number from said electronic device to a transaction recipient via the NFC interface;"

299. *See* Claim 1(f).

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…"

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

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;"

301. *See* Claim 8(b).

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"

302. *See* Claim 1(d).

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."

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

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: an indication of a payment successfully completed."

304. *See* Claim 1(g).

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 users payment account information;…and receiving a user-selection of a payment method for a transaction via said touch-screen display user-interface."

305. *See* Claim 1(d).

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 user entry of a valid passcode; and a device biometric recognition of a valid user."

306. *See* Claims 1(a) and 8.

XIV. OPINIONS REGARDING GROUND 6: *COLLINGE* IN VIEW OF LIN, PHILLIPS, AABYE AND PISULA

13(a): " 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:

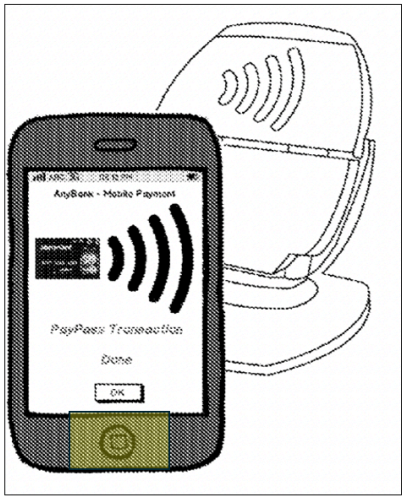
307. As I discussed above in Claim 8, Collinge in view of Aabye teaches a biometric sense of the device continuously remaining in the proximity contact of a valid user, since a last validation. Collinge in view of Pisula teaches a button double press.

1. Pisula's Teachings

308. 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) (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.

2. Motivation to Combine

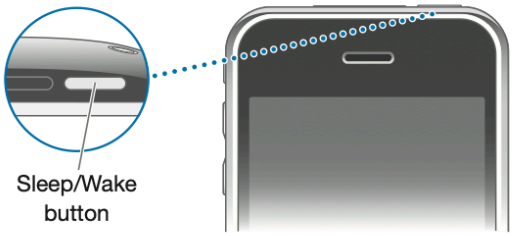
309. It would have been obvious and a POSITA would have been motivated to modify Collinge's mobile device to accept a double button press to turn on the display of Collinge's device and allow a user to access mobile applications based on the teachings of Pisula and because Collinge already teaches a button as shown in the figure below.



'098 Provisional (Ex.1008), 99 (excerpt, annotated); *Collinge*, Fig. 1.

310. 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. For example, the iPhone 2007 user guide discusses many uses of buttons as

depicted below.



Lock iPhone	Press the Sleep/Wake button.
Unlock iPhone	Press the Home ▢ button or the Sleep/Wake button, then drag the slider.
Turn iPhone completely off	Press and hold the Sleep/Wake button for a few seconds until the red slider appears, then drag the slider. When iPhone is off, incoming calls go straight to voicemail.
Turn iPhone on	Press and hold the Sleep/Wake button until the Apple logo appears.

iPhone (Ex.1052), 27. As another example, 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].

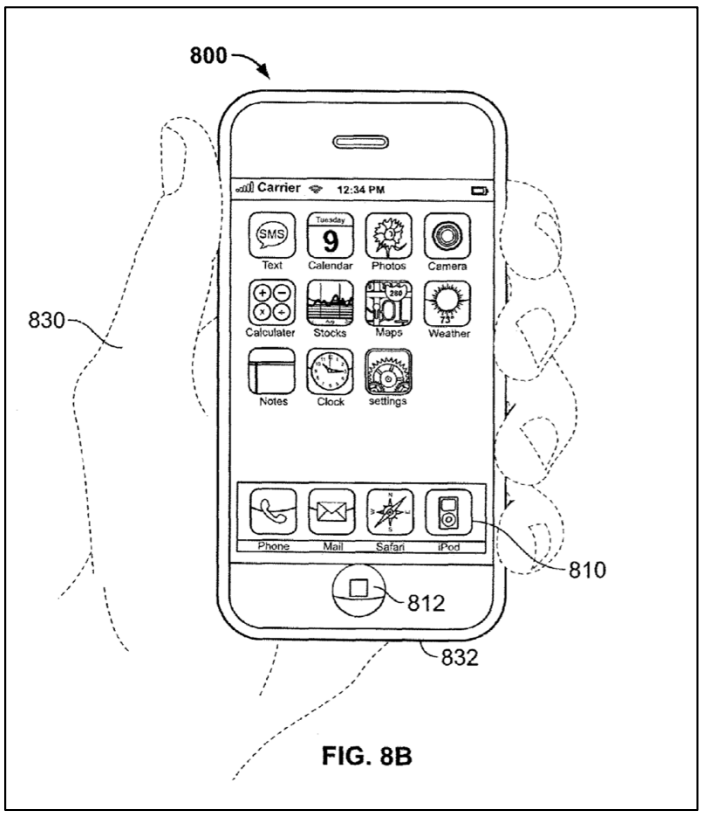


FIG. 8B

Fadell, Fig. 8B.

311. 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 as taught by *Pisula* at 16:53-56 ("keep[] the screen off…to present unnecessary battery drainage").

312. 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 changes of a user inadvertently powering the device on (and therefore wasting battery). As taught by Pisula, the long button press method saves battery power. *Pisula* at 16:53-56 ("keep[] the screen off…to present unnecessary battery drainage").

313. 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. 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 as demonstrated by Pisula and it would have been well-within the capabilities of a POSITA to implement such functions.

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;"

314. 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

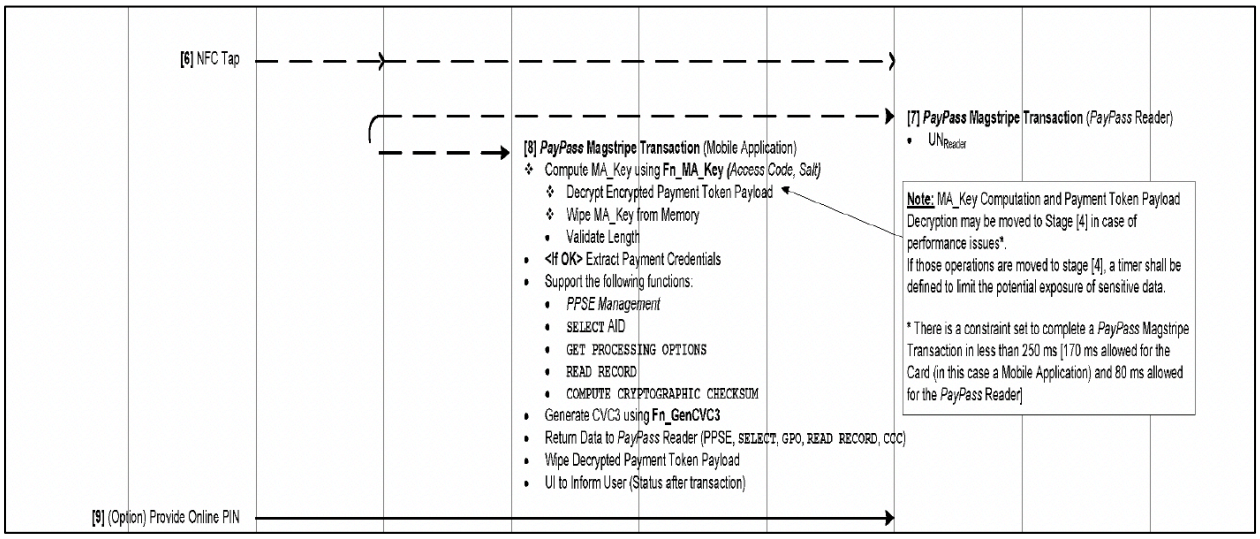
through Collinge's authentication process again and re-enter the activation code as discussed in Claim 1(a).

13(c): "disabling a device priming operation on further button pressing;"

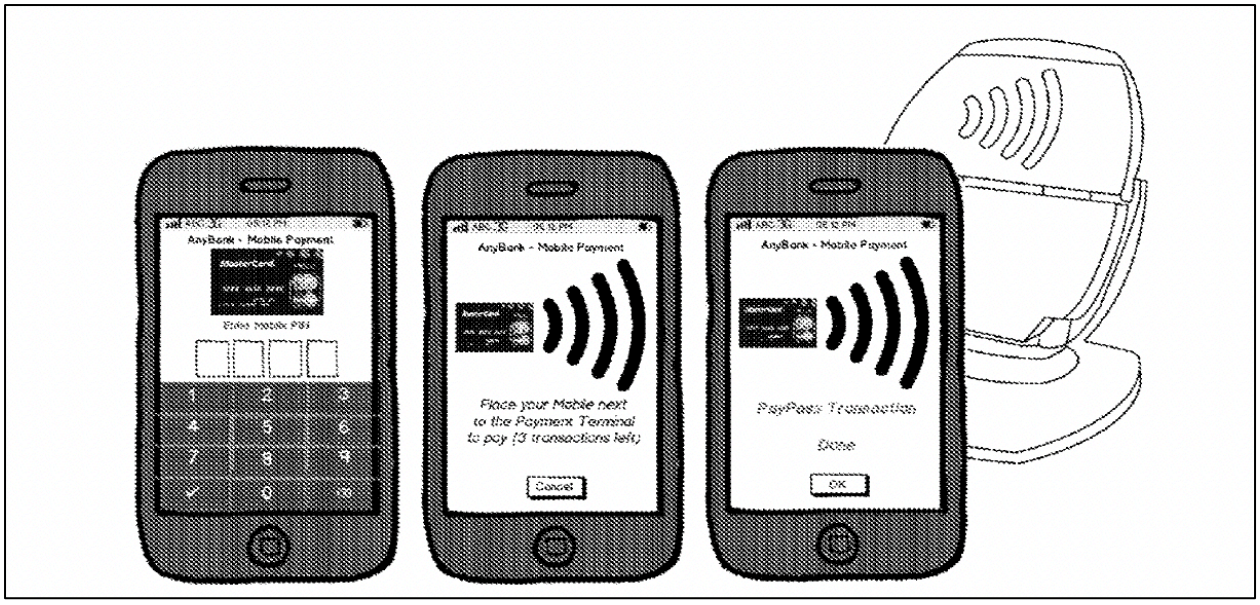
315. As the Collinge-Pisula combination teaches, if a user presses the button twice outside of the 0.3 second timeline, Collinge's device would not approve the button press. *See* Claim 13(a). Collinge-Pisula also teaches a "longer press of the push button (e.g., 206) may turn power to the device 100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

13(d): "disabling a payment priming operation after the expiration of a pre-set time duration from a successful priming action; and"

316. The Collinge and Aabye combination 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. The Collinge and Aabye combination was discussed in Claim 8(b). *See* Claim 8(b).



'248 Provisional (Ex.1006), Fig. 14 (excerpt).

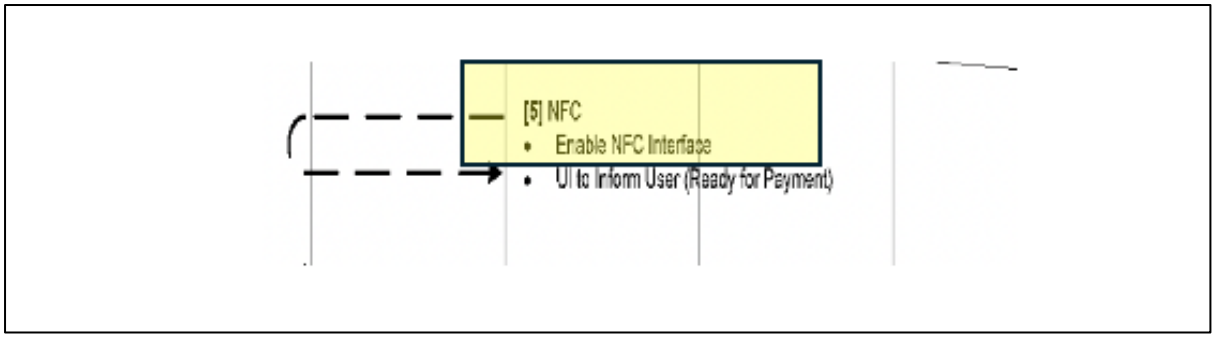


'098 Provisional (Ex.1008), 99; *'248 Provisional (Ex.1006)*, Fig. 2B

13(e): "disabling a device priming operation responsive to completing a transaction."

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

transaction (one transaction per priming (e.g., each time the device is brought near the NFC interface) as depicted in Collinge's *'248 Provisional (Ex.1006)*, Fig. 14 which as disused by above in Section VIII I understand to be incorporated by reference to Collinge.



'248 Provisional (Ex.1006), Fig. 14 (excerpt).

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

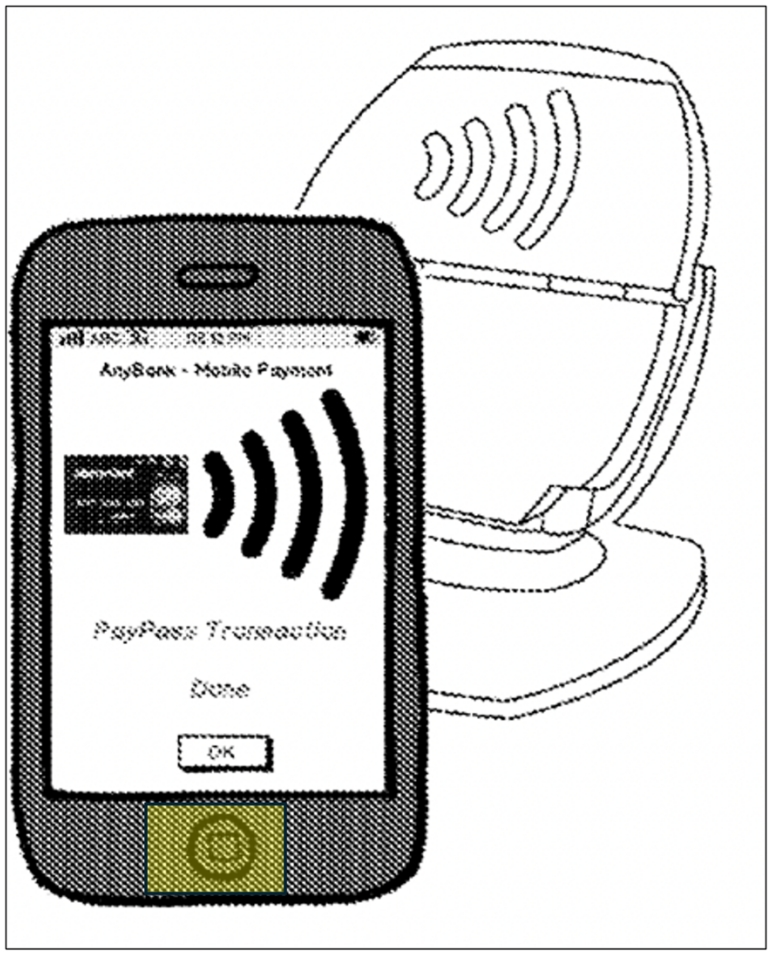
14(a): "A method of claim 1, wherein the priming operation is input after at least one of: a biometric sense of a touch contact of a valid user's skin on a touch ID button of the electronic device,

318. 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 before bring Collinge's mobile device within proximity of an NFC recipient (which may form part of a priming operation).

1. Collinge's Teachings

319. Collinge teaches that a user 102 "may supply additional authentication credentials, such as…a biometric identifier." *Collinge* at [0081], *see also* [0139],

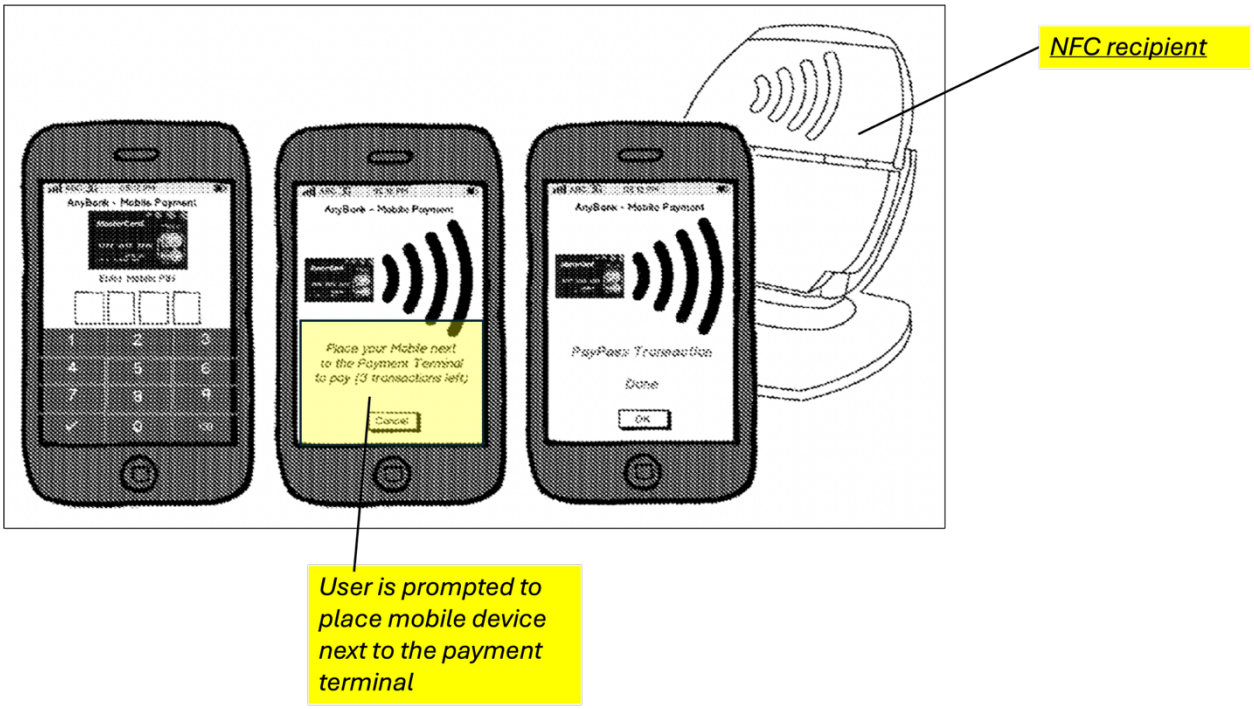
[0143]. Collinge further teaches, in the '098 Provisional (Ex.1008), that mobile device 104 comprises a button on the bottom of the device. *'098 Provisional (Ex.1008)* at p. 99.



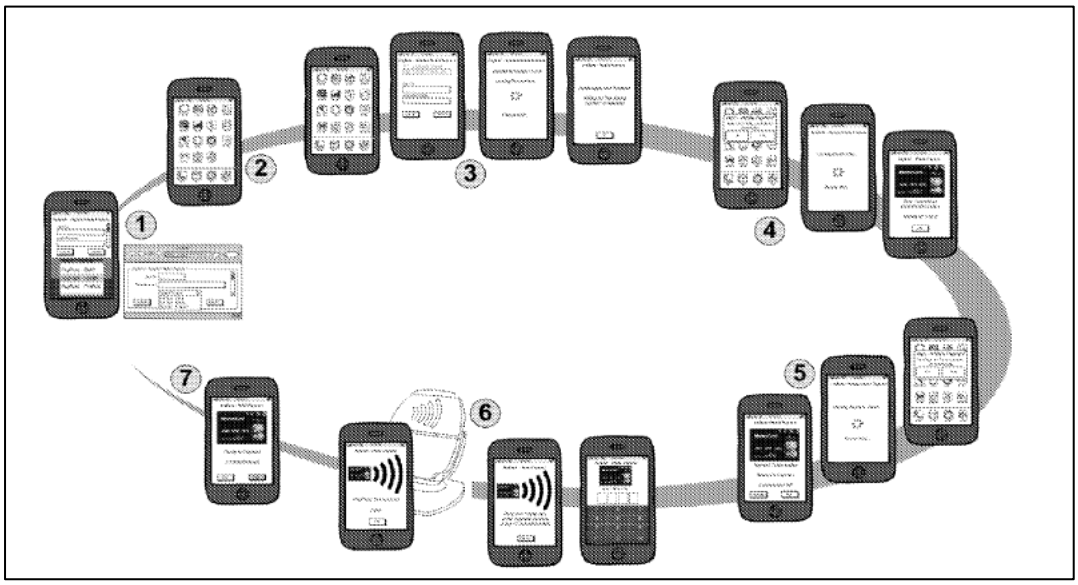
'098 Provisional (Ex.1008) at p. 99 (annotated excerpt); *see Collinge*, Fig. 1.

320. A POSITA would have understood that the button on Collinge's mobile device 104 would be used to sense a user's fingerprint as taught by Fadell. Detecting fingerprints on mobile devices were common practice before the priority date. *See, e.g., Birdwell (Ex.1036)* at [0006] ("A small number of mobile phones feature a

dedicated fingerprint scanner, namely the Fujitsu F-01A mobile phone and the recently introduced Motorola Atrix mobile telephones.") As can be seen in the below figure, the user of the mobile device inputs PIN into mobile device and then receives a notification on the display that says "Place your Mobile next to the Payment Terminal to pay (3 transactions left)[.]" *'098 Provisional (Ex.1008)* at p. 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* at [0133]. Using mobile device 104, the user "must always provide the Mobile PIN for all PayPass transactions[.]" *'098 Provisional (Ex.1008)* at p. 99.



'098 Provisional (Ex.1008) at page 99.



'098 Provisional (Ex.1008), 95; '248 Provisional (Ex.1006), Fig. 2B.

2. Fadell's Teachings

321. Fadell teaches an "electronic device for detecting a user's fingerprint[.]" *Fadell* at [0063]. The "electronic device 700 may include at least one sensor 720 operative to detect features of a user's fingerprint to identify the user." *Fadell* at [0064]. Sensor 720 "may be placed in, adjacent to or behind any button or other physical input that a user may press in an electric device[,]" for example "behind a home button of a portable media player or cellular telephone (e.g., button 812, FIG. 8B)." *Fadell* at [0065]. "In some embodiments, input mechanism 712 may include a sensor 720 embedded underneath some or all of the pad such that when a user places a finger on input mechanism 712…sensor 720 may detect the features of the user's finger for authenticating the user." *Fadell* at [0066]. "The user may then be authenticated by comparing the detected biometric attributes

with a library of biometric attributes stored by or accessible to the electronic device." *Fadell* at [0006]. "Received biometric information stored in the library may be retrieved when a user attempts to authenticate, and compared to the biometric information provided by the user. If the provided biometric authentication information matches information stored in the library…the electronic device may provide access to a restricted resource." *Fadell* at [0080].

322. Because Fadell teaches that "sensor 720 may detect the features of the user's finger for authenticating the user[,]" and that the "received biometric information" may be "compared to the biometric information provided by the user" to authenticate the user, Fadell teaches successfully validating the identified user comprises…successfully determining a match. A POSITA would have understood that comparing the fingerprint to the library of biometric attributes would be performed by the processor of the electronic device, because the library of biometric attributes would be stored in memory, and a processor would be required to perform any functions related to said biometric attributes. Additionally, Fadell's teaching of sensor 720 detecting the features of a user's finger is *a biometric sense of a touch contact of a valid user's skin on a touch ID button of the electronic device* because the user input is the fingerprint and it is received via the fingerprint sensor 720. A POSITA would have understood that Fadell's library of biometric attributes is predetermined user characteristics…as stored in the electronic device because the

library of biometric attributes would correspond to stored data of the user's fingerprint such that when the user wishes to gain access to the device and places their finger on the fingerprint sensor, the detected fingerprint is compared to the library.

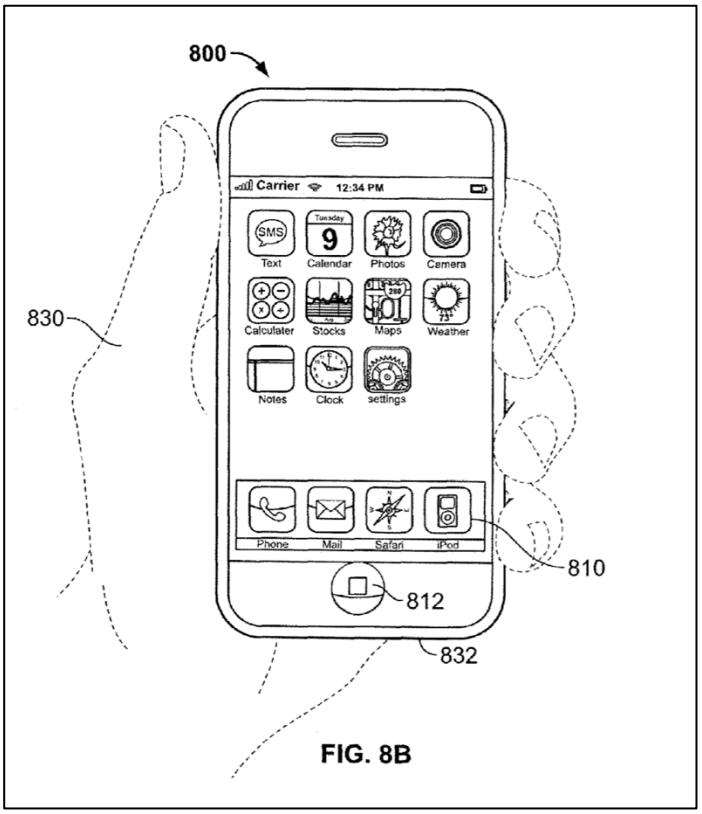


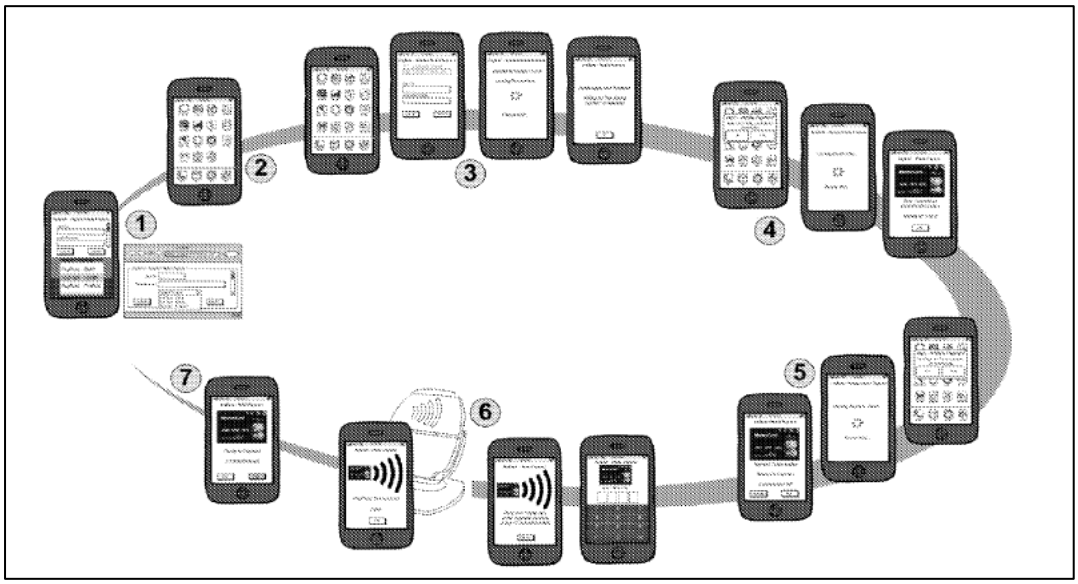
FIG. 8B

Fadell at Figure 8B.

3. Motivation to Combine

323. A POSITA would have found it obvious and been motivated to modify Collinge's mobile device 104 according to the teachings of Fadell such that mobile device 104 comprises a fingerprint sensor, which is one of a *set of user input sensors* alongside Collinge's touch screen. 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 (3 transactions left)" such as an initial step in Collinge's payment process. *'098 Provisional (Ex.1008)* at p. 99.



'098 Provisional (Ex.1008), 95; '248 Provisional (Ex.1006), Fig. 2B.

324. In the combination, the button on the bottom of Collinge's mobile device 104 comprises a fingerprint sensor, and the user of the mobile device may be authenticated based on a fingerprint. As taught by Fadell, the fingerprint biometric attributes would be stored in the memory of mobile device 104, such that when the user places their finger on the fingerprint sensor, the processor is able to compare the detected fingerprint to the "library of biometric attributes stored by or accessible to the electronic device." *Fadell* at [0006]. A POSITA would have found obvious to configure Collinge's memory and processor of mobile device 104 to store and compare, respectively, fingerprint biometric data from the user of mobile device 104

to increase security of a user accessing the contents of mobile device 104. Fingerprints are a biometric attribute that are unique to an individual, making it harder for malicious actors to gain access to the content of mobile device 104. *See, e.g., Chiu (Ex.1037)* at [0004] ("The biometric authentication is the latest technique of personal identification that uses the constant features of a person, such as voice print, fingerprint, iris pattern etc. The most important point is that these characteristics are unique to a person so that they cannot be stolen or denied in any circumstances.") Accordingly, a POSITA would have been motivated to decrease the likelihood of unknown users from accessing mobile device 104 by incorporating Fadell's teachings of a fingerprint sensor for user authentication into Collinge's mobile device 104. Collinge already recognized that a user may supply a "biometric identifier" as a means of authentication. *Collinge* at [0081]. 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. Additionally, the modification is the combination of prior art elements (fingerprint sensors, electronic devices) according to known methods to yield the predictable result of increasing security of Collinge's mobile device and would have had a reasonable expectation of success in making such a modification.

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." 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. Indeed, it was well known in the art that mobile devices employing fingerprint sensors, as demonstrated by Fadell and Birdwell. *See, e.g., Birdwell (Ex.1036)* at [0006] ("A small number of mobile phones feature a dedicated fingerprint scanner, namely the Fujitsu F-01A mobile phone and the recently introduced Motorola Atrix mobile telephones.") As such, the modification would have had a reasonable expectation of success.

14(b): "and validating a user passcode entry on the touch-screen display of the electronic device;"

326. *See* Claim 1(a).

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."

327. *See* Claim 13(a)-(d).

XVI. CONCLUSION

328. I declare that all statements made herein of my knowledge are true, and that all statements made on information and belief are believed to be true, and that these statements were made with the knowledge that willful false statements and the

like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Dated: 6/18/2025 By: 

Curriculum Vitae

(June 2025)

B. Clifford Neuman

Education:

- Ph. D. Computer Science, June 1992, University of Washington

  Thesis: The Virtual System Model, A Scalable Approach to Organizing Large Systems. Supervised by Professor Edward D. Lazowska

- M.S. Computer Science, May 1988, University of Washington

- S.B. Computer Science and Engineering June 1985, Massachusetts Institute of Technology

  Thesis: Sentry, A Discretionary Access Control Server.
  Supervised by Dr. David D. Clark

Employment:

- Research Scientist, Information Sciences Institute, University of Southern California, 1991-Present.

- Associate Division Director, Computer Networks Division, Information Sciences Institute, University of Southern California, 2001-June 2005.

- Director, Center for Computer Systems Security, University of Southern California, 2002-Present.

- Associate Professor of Computer Science Practice, Department of Computer Science, University of Southern California, 2016-.

- Research Associate Professor, Department of Computer Science, University of Southern California, 2008-2016.

- Research Assistant Professor, Department of Computer Science, University of Southern California, 1992-2008.

- Chief Scientist, CyberSafe Corporation, 1992 – 2001.

- Pre-Doctoral Research Associate, Department of Computer Science, University of Washington, 1987-1991.

- Project Athena, Massachusetts Institute of Technology 1985-1986.

- Systems Programmer, EECS Computer Facility, Massachusetts Institute of Technology 1982-1985.

Advisory Boards:

- NTT Communications Security Advisory Board, 2003-2006.
- Eyematic Corporation, 1999-2001.
- Net Research Inc / BayBuilder, 2000-2001.

Courses taught:

- DSci429/ENGR599, Security Privacy and Policy in the Age of the Internet. Fall 2019-2024.
- INF/DSci-523 Computer Systems Assurance, Spring 2016, Fall 2017-2024.
- INF 524 Distributed Systems and Network Security, Summer 2015
- INF-526 Secure System Administration, Summer 2016, Spring 2017, Spring 2021.
- INF 527 Secure Systems Engineering, Fall 2015
- INF/DSci-529 Privacy and Security for Informatics, Spring 2016-2025.
- CSci 530 Computer Security Systems (University of Southern California), Fall 2003-2024.
- CSci 555 Advanced Operating Systems (University of Southern California), Fall 1992-2003, 2006-2012, 2014, 2020.
- CSci599 Trusted Computing (University of Southern California), Spring 2007.
- CSci532 Hacking for Defense, Innovation for Defense Applications, Spring 2018-2020, Spring 2022- 2025.
- CSci 451 Operating Systems (for University of Washington Extension), Spring 1987.

Tutorials taught:

Electronic Payment Systems, presented at:

- Usenix Workshop on Electronic Commerce, New York, July 1995.
- Usenix Workshop on Electronic Commerce, Oakland, CA, November 1996.
- Internet Society Symposium on Network and Distributed Systems Security, March 1998.
- Usenix Workshop on Electronic Commerce, Boston, MA, September 1998.
- Internet Society Symposium on Network and Distributed Systems Security, February 1999.
- 8th International World Wide Web Conference, Toronto, Canada May 1999.

Web Security and Beyond: Protecting your Electronic Commerce Application, presented at:

- Internet Society Symposium on Network and Distributed Systems Security, March 1998.
- Internet Society Symposium on Network and Distributed Systems Security, February 1999.

Research Interests:

Dr. Neuman conducts research in distributed computer systems with emphasis on scalability and computer security, especially for cyber-physical systems and critical infrastructure.

In his research, Dr. Neuman works to design and develop scalable information, security, and computing infrastructure for the Internet. He is the principal designer of the Kerberos system, an encryption based authentication system used among other things as the primary authentication method for Microsoft's Windows 2000, XP and many other systems. He has used Kerberos as a base for more comprehensive computer security infrastructure providing authorization, accounting, and audit.

Recent research includes managing computer security policies in federated and coalition environments, and using policy as a unifying element for integrating all security services including authorization, audit, and intrusion detection with systems and applications. This work extends the application of trusted computing to protect mutually suspicious entities from one another and forms the basis for the TrustView security architecture.

Most recently, Dr. Neuman has focused on security for cyber-physical systems, with an emphasis on protection of critical infrastructure, including the power grid. Recent publications discuss cross-domain threat propagation in such systems, and mitigation techniques applied in both the cyber and physical domains.

Dr. Neuman has designed systems for network payment which build upon security infrastructure to provide a secure means to pay for services provided over the Internet. The NetCheque and NetCash systems, which are suitable for micropayments (payments on the order of pennies where the cost of clearing a credit card payment would be prohibitive). NetCheque provides accounting for the flow of funds through the system whereas NetCash supports anonymous transactions.

He is the principal designer of the Prospero system which is used to organize and retrieve information distributed on the Internet. The Prospero system applies the Virtual System Model to construct views of the information available on the network. Prospero is an embedded system that is used by several commercial products.

The Prospero Resource Manager (PRM) supports the management of computing resources in distributed systems. PRM provides multiple views of the available resources by supporting multiple resource managers, each controlling a subset of the resources in the system, independent of other managers of the same type. The functions of resource management are distributed across three types of managers: system managers, job managers, and node managers. The complexity of these management roles is reduced because each is designed to utilize information at an appropriate level of abstraction.

Awards

- InfoWorld Top Ten Technology Innovators, InfoWorld Magazine, February 2002.
- 2001 Usenix Software Tools User Group Award recipient for contributions to the development of Kerberos.
- DARPA Dynamic Coalitions Program 2003 award for excellence in academic research.
- Usenix Security 2022 Test of Time Award for Kerberos: An Authentication Service for Open Network Systems, Published in 1988 Winter USENIX Technical Conference Proceedings.

Memberships and Professional Activities:

Memberships

- Association for Computing Machinery (ACM) – Life member.
- Institute of Electrical and Electronic Engineers (IEEE) - Senior member
- IEEE Computer Society
- Internet Society (ISOC)
- Internet Engineering Task Force (IETF) - Participant
- Usenix Association

Program and General Chair

- Program Chair, Fourth Annual PKI R&D Workshop: “Multiple Paths to Trust”, Gaithersburg, MD. April 2005.
- General Chair, 2004 Internet Society Symposium on Network and Distributed System Security, San Diego, CA, February 2004.

IPR2025-01148
Apple EX1003 Page 262

- General Chair, 2003 Internet Society Symposium on Network and Distributed System Security, San Diego, CA, February 2003.

- Vice Program Chair, Security Track, International Conference on Distributed Computing Systems (ICDCS), Vienna Austria, 2002.

- Program Chair, 2002 Workshop on Accelerating Trustworthy Internetworking.

- General Chair, 2002 Internet Society Symposium on Network and Distributed System Security. San Diego, CA, February 2002.

- Program Chair, 4th ACM Conference on Computer and Communications Security, Zurich, Switzerland. April 1997.

- Program Chair, 4th Internet Society Symposium on Network and Distributed System Security, San Diego, CA, February 1997.

- Program Chair, 3rd Internet Society Symposium on Network and Distributed System Security, San Diego, CA, February 1996.

Editorial and Publication Advisory Boards

- Guest Editor, Journal of High Speed Networking, special issue on managing security policies, 2006.

- Contributed/Edited section of Report of the Workshop on Responding to the Unexpected, February 27, 2002, New York City.

- Editorial Board, International Journal of Electronic Commerce, June 1996 - Present.

- Editorial Board, ACM Transaction on Information and Systems Security, 1998 – 2001.

Program Committees

- Program Committee, 2015 Industrial Control Systems Security Workshop at ACSAC, December 2015, Los Angeles.

- Program Committee, 2015 IEEE International Conference on Intelligence and Security Informatics, May 2015. Baltimore MD, USA.

- Steering Group, 2013 Internet Society Symposium on Network and Distributed System Security, San Diego, CA, February 2014.

IPR2025-01148
Apple EX1003 Page 263

- Program Committee, 2012 IEEE International Conference on Intelligence and Security Informatics, Washington DC, June 2012.

- Program Committee, ACM SIGKDD Workshop on Intelligence and Security Informatics 2012 (ISI-KDD 2012), Beijing China.

- Steering Group, 2013 Internet Society Symposium on Network and Distributed System Security, San Diego, CA, February 2013.

- Steering Group, 2012 Internet Society Symposium on Network and Distributed System Security, San Diego, CA, February 2012.

- Steering Group, 2011 Internet Society Symposium on Network and Distributed System Security, San Diego, CA, February 2011.

- Program Committee, 2010 ACM Symposium on Access Control Models and Technologies (SACMAT2010). Pittsburgh, June 2010.

- Program Committee, 2011 IEEE International Conference on Intelligence and Security Informatics. 011, Beijing China.

- Program Committee, 2010 IEEE International Conference on Intelligence and Security Informatics. May 2010, Vancouver, BC, Canada.

- Program Committee, 9th Symposium on Identity and Trust on the Internet (IDtrust 2010), Gaithersburg, MD, April 2010.

- Steering Group, 2010 Internet Society Symposium on Network and Distributed System Security, San Diego, CA, February 2010.

- Program Committee, 2009 ACM Symposium on Access Control Models and Technologies (SACMAT2009). Stresa, Italy, June 2009.

- Program Committee, 2009 IEEE International Conference on Intelligence and Security Informatics. June 2009, Dallas TX, USA.

- Program Committee, 8th Symposium on Identity and Trust on the Internet (IDtrust 2009), Gaithersburg, MD, April 2009..

- Steering Group, 2009 Internet Society Symposium on Network and Distributed System Security, San Diego, CA, February 2009

- 2008 IEEE International Conference on Intelligence and Security Informatics. June 2008, Taipei, Taiwan.

IPR2025-01148
Apple EX1003 Page 264

- Program Committee, 7th Seventh Symposium on Identity and Trust on the Internet (IDtrust 2008), Gaithersburg, MD, March 2008.

- Program Committee, 2007 IEEE International Conference on Intelligence and Security Informatics. May 2007, New Brunswick NJ. USA.

- Program Committee, 6th Annual PKI R&D Workshop, Gaithersburg, MD. April 2007.

- Steering Group, 2007 Internet Society Symposium on Network and Distributed System Security, San Diego, CA, February 2007.

- The First Workshop on Security, Trust and Privacy in Grid Environments STPG2008), at The 8th IEEE International Symposium on Cluster Computing and the Grid (CCGRID2008), 19-22 May 2008, Lyon, France

- 2006 IEEE Workshop on Policies for Distributed Systems and Networks (Policy2006), London Ontario, June 2006.

- 11th ACM Symposium on Access Control Models and Technologies (SACMAT2006). Lake Tahoe, June 2006.

- 2006 IEEE International Conference on Intelligence and Security Informatics. May 2006, San Diego USA.

- Fifth Annual PKI R&D Workshop, Gaithersburg, MD. April 2006.

- Second International Workshop on Security in Distributed Computing Systems. (in conjunction with 25th International Conference on Distributed Computing Systems ICDCS-2005), Columbus, OH, USA. June 2005.

- 2005 IEEE International Conference on Intelligence and Security Informatics. May 2005, Atlanta USA.

- 2004 IEEE International Conference on Intelligence and Security Informatics. June 2004, Tucson USA.

- 2003 IEEE International Conference on Intelligence and Security Informatics. June 2003, Tucson USA.

- IEEE Sixth International Workshop on Policies for Distributed Systems and Networks (Policy2005). June 2005, Stockholm Sweden..

- IEEE Fifth International Workshop on Policies for Distributed Systems and Networks (Policy2004). June 2004, New York.

IPR2025-01148
Apple EX1003 Page 265

- Steering Group, Internet Society Symposium on Network and Distributed System Security, San Diego, CA, February 2001 to 2006.

- 21st International Conference on Distributed Computer Systems (ICDCS-21), Phoenix, AZ, April 2001,

- Ninth International World Wide Web Conference, Amsterdam, May 2000.

- 2001 Symposium on Applications and the Internet (SAINT), San Diego, CA, January 2001. (IEEE Computer Society).

- Eighth Internet Society Symposium on Network and Distributed System Security, San Diego, CA, February 2000.

- Sixth ACM Conference on Computer and Communications Security, Singapore, November 1999.

- First ACM Conference on Electronic Commerce (EC-99), Denver, CO, November 1999.

- Eighth International World Wide Web Conference, Toronto, May 1999.

- Third International Conference on Financial Cryptography, Anguilla, British West Indies, February 1999.

- Seventh IEEE International Symposium on High Performance Distributed Computing, Chicago, IL, July 1998.

- First International Conference on Financial Cryptography, Anguilla, British West Indies, February 1997.

- Second Usenix Workshop on Electronic Commerce, Oakland, CA, November 1996.

- 1996 Conference on The Convergence of Telecommunications and Distributed Computing Technologies (TINA), Heidelberg, Germany, September 1996.

- Sixth Usenix Security Symposium, San Jose, CA July 1996.

- Third ACM Conference on Computer and Communications Security, New Delhi, India, March 1996.

- First Usenix Workshop on Electronic Commerce, New York City, July 1995.

- Second Internet Society Symposium on Network and Distributed System Security, San Diego, CA, February 1995.

IPR2025-01148
Apple EX1003 Page 266

- Second ACM Conference on Computer and Communications Security, Fairfax VA, November 1994.

- First Internet Society Symposium on Network and Distributed System Security, San Diego, CA, February 1994.

- First ACM Conference on Computer and Communications Security, Fairfax VA, November 1993.

- PSRG Workshop on Network and Distributed System Security, San Diego, CA, February 1993.

Other positions

- Panel member, National Research Council, CSTB Committee on Computing and Communications Research to Enable Better Use of Information Technology in Government, October 2001.

- Publications Chair, 3rd ACM Conference on Computer and Communications Security, March 1996.

Publications (Journals):

- Wadhawan, Yatin, Clifford Neuman, and Anas AlMajali. "IGNORE: A Policy Server to Prevent Cyber-Attacks from Propagating to the Physical Domain." Applied Sciences 10, no. 18 (2020): 6236.

- AlMajali, Anas, Yatin Wadhawan, Mahmood S. Saadeh, Laith Shalalfeh, and Clifford Neuman. "Risk assessment of smart grids under cyber-physical attacks using Bayesian networks." International Journal of Electronic Security and Digital Forensics 12, no. 4 (2020): 357-385.

- Anas Al Majali, W. Yatin., Neuman, C, Saadeh. Mahmood, Shalalfeh. Laith. “Risk Assessment of Smart Grids under Cyber-physical Attacks using Bayesian Networks”. Accepted in 2019 for International Journal of Electronic Security and Digital Forensics

IPR2025-01148
Apple EX1003 Page 267

- Yatin Wadhawan , Anas Al Majali, Clifford Neuman. "A Comprehensive Analysis of Smart Grid Systems against Cyber-Physical Attacks", MDPI: A special issue of Electronics: Cyber-Physical Systems. 2018.

- Anas AlMajali, Arun Viswanathan, Clifford Neuman, Resilience Evaluation of Demand Response as Spinning Reserve under Cyber-Physical Threats. Electronics 6(1), 2016.

- B. Clifford Neuman. Prospero: A Tool for Organizing Internet Resources. (A retrospective) Electronic Networking: Research, Applications and Policy, 20(4): 408-419, Winter 2012. (refereed journal)

- B. Clifford Neuman. Prospero: A Tool for Organizing Internet Resources. A Tatyana Ryutov, Clifford Neuman, Li Zhou and Noria Foukia, *Initial Trust Formation in Virtual Organizations*, International Journal of Internet Technology and Security Transactions, 2007.

- Tatyana Ryutov, Clifford Neuman, Dongho Kim and Li Zhou. Integrated Access control and Intrusion Detection for Web Servers. IEEE Transaction on Parallel and Distributed Systems, Vol 14, No. 9, September 2003.

- R. Bajcsy, et. al. Cyber Defense Technology Networking and Evaluation, Communications of the ACM, March 2004.

- Tatyana Ryutov, Grig Gheorghiu, and Clifford Neuman, An Authorization Framework for Metacomputing Applications, Cluster Computing 2(1999), 165-175.

- B. Clifford Neuman and Theodore Ts'o. Kerberos: An Authentication Service for Computer Networks, IEEE Communications, 32(9):33-38. September 1994.

- B. Clifford Neuman and Santosh Rao. The Prospero Resource Manager: A scalable framework for processor allocation in distributed systems, Concurrency: Practice and Experience, 6(4):339-355, June 1994.

- B. Clifford Neuman. Enabling Commerce on the Internet, IEEE Computer29(4):91-92. April 1996.

- B. Clifford Neuman. Security, Payment, and Privacy for Network Commerce, IEEE Journal on Selected Areas in Communications, 13(8):1523-1531. October 1995.

- B. Clifford Neuman. The Prospero File System: A global file system based on the Virtual System Model. Computing Systems, 5(4):407-432, Fall 1992.

- Michael F. Schwartz, Alan Emtage, Brewster Kahle, and B. Clifford Neuman A Comparison of Internet Resource Discovery Techniques. Computing Systems, 5(4):461-493, Fall 1992.

- B. Clifford Neuman. Prospero: A Tool for Organizing Internet Resources. Electronic Networking: Research, Applications and Policy, 2(1): 30-37, Spring 1992. (refereed journal)

Publications (Other):

- C. Pandit, H. Kothari and C. Neuman, "Privacy in time of a pandemic," 2020 13th CMI Conference on Cybersecurity and Privacy (CMI) - Digital Transformation - Potentials and Challenges(51275), 2020, pp. 1-6, doi: 10.1109/CMI51275.2020.9322737.

- Yatin Wadhawan , Anas Al Majali, Clifford Neuman. "PSP: A Framework to Allocate Resources to Power Storage Systems under Cyber-Physical Attacks", 5th International Symposium for ICS-SCADA Cyber Security. 2018.

- Yatin Wadhawan , Anas Al Majali, Clifford Neuman. "A Systematic Approach to Analyze Multiple Cyber-Physical Attacks on Smart Grid", International Conference on Cyber Security of Cyber Physical Systems. 2018.

- Yatin Wadhawan , Dr. Clifford Neuman. "RL-BAGS: A Tool for Smart Grid Risk Assessment", International Conference on Smart Grid and Clean Energy Technologies (ICSGCE). 2018.

- Wadhawan, Yatin and Neuman, Clifford,“BAGS: A Tool to Quanify Smar-Grid Resilience”, September 2017, In Proceedigs of the 4th International Workshop on Cyber-Physical Systems at the Federated Conference on Computer Science and Information Systems, Prague, Czech Repulic.

- Wadhawan, Yatin and Neuman, Clifford, and AlMajali, Anas “Analyzing Cyber-Physical Attacks on Smart Grid Systems”, 2017 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES), April 2017, Pittsburgh.

- Wadhawan, Yatin and Neuman, Clifford, “Evaluating Resilience of Gas Pipeline Systems Under Cyber-Physical Attacks: A Function-Based Methodology”, ACM Workshop on Cyber-Physical Systems Security and Privacy (CPS-SPC) 2016.

- Yatin Wadhawan and Clifford Neuman. Defending Cyber-Physical Attacks on Oil Pipeline Systems: A Game-Theoretic Approach Yatin Wadhawan and

Clifford Neuman. International Workshop on AI for Privacy and Security (PRAISE) from 29 August to 2 Septembe 2016, at the Haugue, Netherlands.

- Yatin Wadhawan and Clifford Neuman, A Roadmap to Evaluate Resilience of Oil and Gas Cyber-Physical Systems. 2015 ACSAC Workshop on Industrial and Control System Security, Los Angeles, December 2015.

- Tatyana Ryutov, Anas AlMajali, Clifford Neuman, Modeling Security Policies for Mitigating the Risk of Load Altering Attacks on Smart Grid Systems, in Proceedings of the 2015 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES) (IEEE), Seattle, April 2015.

- Anas AlMajali, Eric Rice, Arun Viswanathan, Kymire Tan, Clifford Neuman, *A Systems Approach to Analysing Cyber-Physical Threats in the Smart-Grid*, in Proceedings of the 4th International Conference on Smart Grid Communications (IEEE SmartGridComm), Vancouver, October 2013.

- Arun Viswanathan, Kymie Tan, Clifford Neuman, *Deconstructing the Assessment of Anomaly-Based Intrusing Detectors for Critical Applications*, in Proceedings of the16th International Symposium on Research in Attacks , Intrusions, and Defenses (RAID2013) St. Lucia, October 2013.

- Hashem Alayed, Fotos Frangoudes, and Clifford Neuman, *Behavioral-Based Cheating Detection in Online First Person Shooters using Machine Learning Techniques*, in Proceedings of IEEE 2013 Conference on Computational Intelligence in Games, Niagara Falls, Canada, August 2013.

- Anas AlMajali, Arun Viswanathan, and Clifford Neuman, *Analyzing Resiliency of the Smart Grid Communication Architectures under Cyber Attack*, in Proceedings of the 5th Workshop on Cyber Security Experimentation and Test (CSET'12) Bellevue, Washington, August 2012.

- Clifford Neuman and Kymie Tan, *Mediating Cyber and Physical Threat Propagation in Security Smart Grid Architecture*, in Proceedings of the 2nd International Conference on Smart Grid Communications (IEEE SmartGridComm), Brussels, October 2011.

Clifford Neuman, *Challenges in Security for Cyber-Physical Systems*, DHS Workshop on Future Directions in Cyber-Physical Systems Security, Newark, NJ, July 22-24, 2009.

- Arun Viswanathan, Clifford Neuman, Secure System Views: A new Paradigm for Secure Usable Sysems. USC-ISI Tehnical Report Number ISI-TR-654, January 2009.

- Terry Benzel, Robert Braden, Dongho Kim, Clifford Neuman, Anthony Joseph, Keith Sklower, Ron Ostrenga, Stephen Schwab, Design Deployment

and use of the DETER testbed.. In Proceedings of the DETER Community Workshop on Cyber-Security and Test, August 2007, Boston.

- Tatyana Ryutov, Clifford Neuman, A Trust Based Approach for Improving Data Reliability in Industrial Sensor Networks, in proceedings of the joint ITRUST and PST Conference on Privacy, Trust Management, and Security, New Brunswick Canada, August 2007. Also, ISI-TR-631, January 2007.

- Tatyana Ryutov, Clifford Neuman, Situational Identity: A Person-centered Identity Management Approach, USC ISI Technical report ISI-TR-630, January 2007.

- Tatyana Ryutov, Clifford Neuman, Ronak Shah, Automated Management of Vulnerability Mitigation Prescriptions. USC ISI Technical report ISI-TR-630, January 2007.

- Clifford Neuman, Managing Multiple Perspectives on Trust, *in proceedings of the 2007 Cyber Security and Information Infrastrcture Research Workshop*, Oak Ridge Tennessee, May 2007.

- Clifford Neuman. *Understanding Trust in SCADA Systems.* Proceedings of Beyond SCADA: Network Embedded Control for Cyber-Physical Systems. Pittsburgh, November 9, 2006. (Refereed Workshop Position Statement)

- Sukumal Kitisin and Clifford Neuman. *Reputation-Based Trust-Aware Recommender System*. Proceedings of the 2nd IEEE Workshop on the Value of Security Through Collaboration (SECOVAL), September 2006, Baltimore. (refereed workshop)

- Ho Chung and Clifford Neuman. *Modeling the Relative Strength of Security Protocols*. Proceedings of the 2nd ACM CCS Workshop on Quality of Protection, October 2006, Alexandria VA. (refereed workshop)

- Clifford Neuman, Chinmay Shah, Kevin Lahey. *Running Live Self-Propagating malware on the DETER Testbed.* Proceedings of the DETER Community Workshop, Arlington VA, June 2006.

- Noria Foukia, Liz Zhou and Clifford Neuman. *Multilateral Decision for Collaborative Defense Against Unsolicited Bulk e-mail*. Proceedings of the 4th International Conference on Trust Management. Pisa, Italy, May 2006. (refereed conference)

- Terry Benzel, Bob Braden, Dongho Kim, Clifford Neuman Anthony Joseph and Keith Sklower Ron Ostrenga and Stephen Schwab, *Experience with DETER: A Testbed for Security Research.* Second IEEE Conference on testbeds and Research Infrastructures for the Development of Networks and Communities (TridentCom2006), March 2006, Barcelona. (refereed conference)

IPR2025-01148
Apple EX1003 Page 271

- L. Li, I. Hamadeh, S. Jiwasurat, G. Kesidis, P. Liu, C. Neuman, *Emulating Sequential Scanning Worms on the DETER Testbed,* In Proceedings of 2nd International IEEE/CreateNet Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities (TridentCom2006), March 2006. (refereed conference)

- Tatyana Ryutov, Clifford Neuman, Li Zhou and Noria Foukia, *Establishing Agreements in Dynamic Virtual Organizations*, in Proceedings of the Workshop on the Value of Security through Collaboration, part of IEEE SecureComm, September 2005, Athens. (refereed workshop)

- Tatyana Ryutov, Clifford Neuman, Noria Foukia, Travis Leithead, Kent Seamons, Li Zhou, *Adaptive Trust Negotiation and Access Control for Grids*. 6th IEEE/ACM International Workshop on Grid Computing, Seattle, November 2005. (refereed workshop)

- Sultan Almuhammadi and Clifford Neuman, "Security and Privacy using One-Round Zero Knowledge Proofs", 7th IEEE Conference on E-Commerce Technology, Munich, July 2005. (refereed conference)

- Tatyana Ryutov, Li Zhou, Clifford Neuman, Travis Leithead, and Kent E. Seamons, "**Adaptive Trust Negotiation and Access Control**," *in Proceedings of the ACM Symposium on Access Control Models and Technologies* (SACMAT'05), Stockholm, June 1-3, 2005. (refereed conference)

- Tatyana Ryutov, Clifford Neuman, Dongho Kim and Li Zhou. Integrated Access control and Intrusion Detection for Web Servers. In proceedings of the 23rd International Conference on Distributed Computing Systems, Providence, Rhode Island, May 2003. (refereed conference)

- Tatyana Ryutov, Clifford Neuman and Dongho Kim. Dynamic Authorization and Intrusion Response in Distributed Systems. Proceedings of the 3rd DARPA Information Survivability Conference and Exposition (DISCEX III), April 2003. (refereed conference)

- Tatyana Ryutov and Clifford Neuman. The Specification and Enforcement of Advanced Security Policies. To be published In Proceedings of the Third International Conference on Policies for Distributed Systems and Networks (POLICY 2002), June 2002, in Monterey, California. (refereed conference)

- Tatyana Ryutov and Clifford Neuman, The Set and Function Approach to Modeling Authorization in Distributed Systems, in Proceedings of the Information Assurance in Computer Networks Methods, Models, and

IPR2025-01148
Apple EX1003 Page 272

Architectures for Network Security, May 2001, St. Petersburg, Russia, 189-206. (refereed conference)

- Tatyana Ryutov and Clifford Neuman, Representation and Evaluation of Security Policies for Distributed System Services, in Proceedings of the DARPA Information Survivability Conference and Exposition, January 2000. Hilton Head, SC. (refereed conference)

- Sukumal Imudom and B. Clifford Neuman, A Framework Supporting Collaborative Filtering for Internet Information, AAAI-98 Workshop on Recommender Systems, Madison, WI, July 1998. (refereed conference)

- G. Gheorghiu, T. Ryutov, and B. Clifford Neuman, Authorization for Metacomputing Applications, in Proceedings of the 7th IEEE Symposium on High Performance Distributed Computing, Chicago, IL, July 1998. (refereed conference)

- Sung-Wook Ryu and B. Clifford Neuman, Garbage Collection for Distributed Persistent Objects, in Proceedings of the Workshop on Compositional Software Architectures, Monterey, CA January 1998. (referred conference)

- B. Clifford Neuman and Gennady Medvinsky. Requirements for Network Payment: The NetCheque Perspective In Proceedings of IEEE COMPCON'95. March 1995. (referred conference)

- Clifford Neuman and Genaddy Medvinsky, *NetCheque, NetCash, and the Characteristics of Internet Payment Services*, MIT Workshop on Internet Economics, March, 1995

- Charlie Lai, Gennady Medvinsky, and B. Clifford Neuman. Endorsements, Licensing, and Insurance for Distributed System Services, In Proceedings of 2nd the ACM Conference on Computer and Communication Security. November 1994. (refereed conference)

- B. Clifford Neuman. How to Trust a Distributed System. In Proceedings of the National Computer Security Conference. Baltimore MD, October 1994. (invited conference)

- Gennady Medvinsky and B. Clifford Neuman. Electronic Currency for the Internet, Electronic Markets 3(9/10):23-24, October 1993. Also appeared in Connexions 8(6):19-23, June 1994. (unrefereed journal)

- Gennady Medvinsky and B. Clifford Neuman. NetCash: A design for practical electronic currency on the Internet. In Proceedings of the 1st ACM Conference

IPR2025-01148
Apple EX1003 Page 273

on Computer and Communication Security. November 1993. (refereed conference)

- B. Clifford Neuman, Steven Seger Augart, and Shantaprasad Upasani. Using Prospero to support integrated location independent computing. In Proceedings of the Symposium on Mobile and Location Independent Computing, August 1993. (refereed conference)

- B. Clifford Neuman. Prospero: A base for building information infrastructure. In Proceedings of INET'93, August 1993. (referred conference)

- B. Clifford Neuman and Santosh Rao. Resource Management for Distributed Parallel Systems. In Proceedings of the 2nd International Symposium on High Performance Distributed Computing, July 1993. (refereed conference)

- B. Clifford Neuman. Proxy-Based Authorization and Accounting for Distributed Systems. In Proceedings of the 13th International Conference on Distributed Computing Systems, pages 283-291, May 1993. (refereed conference)

- B. Clifford Neuman and Stuart G. Stubblebine. A Note on the Use of Timestamps as Nonces. Operating Systems Review, 27(2):10-14, April 1993. (unrefereed)

- B. Clifford Neuman. Prospero: A virtual directory service for the Internet, Connexions 6(7):2-9, July 1992. (unrefereed)

- B. Clifford Neuman. The Prospero File System: A global file system based on the Virtual System Model. In Proceedings of the 1st Usenix Workshop on Filesystems May 1992. (refereed conference)

- B. Clifford Neuman. Protection and Security Issues for Future Systems. In Proceedings of the Workshop on Operating Systems of the 90s and Beyond . Dagstuhl Castle, Germany. July 1991.(invited workshop)

- B. Clifford Neuman. The Need for Closure in Large Distributed Systems. Operating Systems Review, 23(4): 28-30, October 1989. (unrefereed)

- B. Clifford Neuman. Workstations and the Virtual System Model. In Proceedings of the 2nd IEEE Workshop on Workstation Operating Systems, pages 91-95, September 1989. (refereed conference)

- B. Clifford Neuman and Jennifer G. Steiner. Authentication of Unknown Entities on an Insecure Network of Untrusted Workstations. In Proceedings of the Usenix

IPR2025-01148
Apple EX1003 Page 274

Workshop on Workstation Security, Portland, OR. August 1988. (refereed conference)

- J. G. Steiner, B. Clifford Neuman, and J.I. Schiller. Kerberos: An Authentication Service for Open Network Systems. In Proceedings of the Winter 1988 Usenix Conference. February, 1988. (Version 4) (refereed conference)

- B. Clifford Neuman and Wayne Yamamoto. Adding Packet Radio to the Ultrix Kernel. In Proceedings of the Winter 1988 Usenix Conference February, 1988. (refereed conference)

- B. Clifford Neuman. Packet Radio and IP for the Unix Operating System. In Proceedings of the Sixth ARRL Computer Networking Conference, Redondo Beach, CA. August, 1987. (refereed conference)

Book Chapters:

- Sanjay Goel, Stephen F. Bush, Clifford Neuman, Smart Grid Security (Chapter 10) in IEEE Vision for Smart Grid Communications: 2030 and Beyond, IEEE Standards Association, 2013.

- Frank Siebenlist, Nataraj Nagaratnam, Von Welch, Clifford Neuman, Security for Virtual Organizations: Federating Trust and Policy Domains. in The GRID 2: Blueprint for a New Computing Infrastructure (edited by Kesselman and Foster), Morgan, Kauffman Publishers, 2004. (invited)

- Clifford Neuman, Security and Privacy, in Cancer Informatics: Essential Technologies for Clinical Trials, Springer-Verlag Inc, 2002. (invited)

- B. Clifford Neuman, Security, Accounting, and Assurance, in The GRID: Blueprint for a New Computing Infrastructure (edited by Kesselman and Foster), Morgan, Kauffman Publishers, 1999. (invited)

- B. Clifford Neuman and Gennady Medvinsky, Internet Payment Services, in Internet Economics, MIT Press. 1997. (refereed conference -> book)

- Charlie Lai, Gennady Medvinsky, and B. Clifford Neuman, Endorsements, Licensing, and Insurance for Distributed Services, in Internet Economics, MIT Press. 1997. (refereed conference -> book)

- B. Clifford Neuman, A Flexible Framework for Network Payment, in Readings in Electronic Commerce, Addison-Wesley. 1996. (invited)

IPR2025-01148
Apple EX1003 Page 275

- B. Clifford Neuman, Scale in Distributed Systems, Readings in Distributed Computing Systems, IEEE Computer Society Press, 1994. (refereed book chapter)

- John T. Kohl, B. Clifford Neuman, and Theodore Y. T'so, The Evolution of the Kerberos Authentication System. In Distributed Open Systems, pages 78-94. IEEE Computer Society Press, 1994. (refereed conference -> book)

Theses, Technical Reports, and Working Documents:

- Clifford Neuman, Tom Yu, Sam Hartman, Ken Raeburn, The Kerberos Network Authentication System, RFC 4120. July 2005 (standards specification).

- Dongho Kim and B. Clifford Neuman. Reconstructing Interconnections on Disconnected Mobile Hosts, ISI Technical Report ISI-TR-528, University of Southern California / Information Sciences Institute, April 2000

- John Kohl and B. Clifford Neuman. The Kerberos Network Authentication Service (Version 5). Internet Request for Comments RFC-1510. September 1993.

- B. Clifford Neuman, The Virtual System Model: A Scalable Approach to Organizing Large Systems, Ph.D. Thesis, University of Washington, Department of Computer Science and Engineering Technical Report 92-06-04, June 1992.

- B. Clifford Neuman. Proxy-Based Authorization and Accounting for Distributed Systems. Technical Report 91-02-01, Department of Computer Science and Engineering, University of Washington, March 1991.

- B. Clifford Neuman. The Virtual System Model: A Scalable Approach to Organizing Large Systems (A Thesis Proposal). Technical Report 90-05-01, Department of Computer Science and Engineering, University of Washington, May 1990.

- B. Clifford Neuman. The Virtual System Model for Large Distributed Operating Systems. Technical Report 89-01-07, Department of Computer Science, University of Washington, April, 1989.

- S.P. Miller, B. C. Neuman, J. I. Schiller, and J.H. Saltzer. Section E.2.1: Kebreros Authentication and Authorization System. Project Athena Technical Plan, MIT Project Athena, Cambridge, Massachusetts, October 1988. (Describes Version 4)

- B. Clifford Neuman. Sentry: A Discretionary Access Control Server. Bachelor's Thesis, Massachusetts Institute of Technology, June 1985.

IPR2025-01148
Apple EX1003 Page 276

Students who completed Ph.D. under Dr. Neuman

- Ho Chung, - Ph.D. USC 2009. Modeling the Relative Strength of Security. Now a researcher at Samsung.
- Li Zhou, - Ph.D. USC 2006. Negotiation of Multilateral Security Decisions. Now a researcher at Microsoft, Redmond WA.
- Sultan Almuhammadi – Ph.D. USC 2005, Security and Privacy Using One-Round Zero-Knowledge Proofs, now faculty at King Fahd University, Saudi Arabia.
- Noria Foukia (postdoc at USC 2004/05), currently Lecturer at University of Otago, Dunedin NZ.
- Xuhua Ding, Ph.D. USC 2003 (co-advisor with Gene Tsudik). Fine-grained control of security services. Now assistant professor at Singapore Management University.
- Yongdae Kim, Ph.D. USC 2002 (co-advisor with Gene Tsudik). Group Key Agreement: Theory and Practice, now faculty at University of Minnesota.
- Tatyana Ryutov - Ph.D. USC 2002, The Condition-driven Authorization Model for Distributed System Services, Now at USC Information Sciences Institute
- Dongho Kim – Ph.D. USC 2001, Reconstructing Interconnections on Disconnected Mobile Hosts, Now at USC Information Sciences Institute
- Sukumal Imudom – Ph.D. USC 2001, Distributed Annotation Framework Supporting Collaborative Filtering of Information, now faculty at Kasetsart University, Thailand.
- Eul Gyu Im - Ph.D. USC 2001, A Flexible Framework for Replication in Distributed Systems, now at National Security Research Institute, South Korea.
- Gennady "Ari" Medvinsky - Ph.D. USC 1996, Electronic Payment Services To CyberSafe Corporation, to Excite - @ Home, to Keen.com, to Microsoft.
- Santosh Rao - Ph.D. USC 1996, Resource Management, Parallel Debugging, and PRM, Now at Veritas Software
- Brenda Timmerman - Ph.D. USC - Traffic Flow Confidentiality, Faculty at Cal State Northridge
- Sung-Wook Ryu - Ph.D. USC - Garbage Collection for Prospero, Now at Veritas Software

IPR2025-01148
Apple EX1003 Page 277

- Konstadinos Kutsikos – Ph.D. USC - Electronic Commerce and Economics, now faculty at University of the Aegean, Greece.

- Anas Almajali – Ph.D. USC – Analysis of Threats in Cyber-Physical Systems. Now faculty at Hashemite University, Jordan.

- Hashem Alayed – Ph.D. USC – Security in Online games, now faculty at King Saud University, Saudi Arabia.

- Arun Viswanathan – Ph.D. USC – Situational Awareness and Intrusion Detection in Cyber-physical systems. Now working for NASA Jet Propulsion Lab.

- Yatin Wadhawan – Ph.D. USC - Analyzing Cyber-Physical Attacks on Industrial Control Systems. Now working at Microsoft.

- Abdulla Alwabel – Ph.D. USC Overcoming Challenges Facing Malware Behavioral Analysis.

IPR2025-01148
Apple EX1003 Page 278