UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,

Petitioner

v.

CARDWARE INC.,

Patent Owner

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

DECLARATION OF DR. CLIFFORD NEUMAN

TABLE OF CONTENTS

I. INTRODUCTION 34

A. Educational Background and Professional Experience 34

II. MATERIALS CONSIDERED 37

III. OVERVIEW AND LEGAL STANDARDS 40

A. Person of Ordinary Skill in the Art 41

B. Obviousness 42

C. Claim Construction 47

D. Printed Subject Matter 48

IV. LEVEL OF A PERSON OF ORDINARY SKILL 48

V. OVERVIEW OF THE '634 PATENT 49

A. Summary of the '634 Patent 49

B. Field of Endeavor 49

C. Problem Purportedly Solved by the Inventors of the '634 Patent 50

D. File History of the '634 Patent 51

VI. BACKGROUND OF TECHNOLOGY 51

A. The Evolution of Payment Cards 52

1. Magnetic Stripe Cards 52
2. Smart/Chip Cards 55
2. Near Field Communications 57
3. Active Mode 59
4. Passive Mode 61
5. The Development of Near Field Communications 62
6. Contactless EMV Payment Cards 62
7. Mobile Devices and Mobile Wallets 63
8. Card Emulation Mode 66

B. Payment Credential Security Features 69

1. Alternatives to a Payment Account Number (PAN) 69

2. Alternatives to Static Card Verification Values 73

VII. SUMMARY OF THE PRIOR ART REFERENCES.....75

A. Collinge.....75

1. Collinge is Analogous Art 78
2. Collinge is Prior Art 80
3. Support for Collinge in Collinge Provisionals 107

B. Lin 111

1. Lin is Analogous.....114

C. Sahota 115

1. Sahota is Analogous 117

D. Smith 118

1. Smith is Analogous.....119

E. Kranzley 120

1. Kranzley is Analogous.....120

F. Fadell 122

1. Fadel is Analogous 123

G. Yu 124

1. Yu is Analogous 125

VIII. SUMMARY OF UNPATENTABILITY 126

IX. OPINIONS REGARDING GROUND 1: COLLINGE IN VIEW OF LIN AND SAHOTA. 127

1. Claim 1 (Pre): "A method of generating and using limited-use payment information for performing a payment transaction, the method comprising:" 127
2. 1(a): "receiving an input at an electronic device, wherein the input comprises a priming operation, and, wherein the electronic device comprises:".....131
3. 1(a)(1): "a processor;" 138
4. 1(a)(2): "a touch-screen display coupled to the processor; and".....138
5. 1(a)(3): "a near field communications (NFC) interface coupled to the processor;" 143

6. 1(b): "responsive to said priming operation, readying said device to perform a payment transaction by an identified user;" 150

7. 1(c): "receiving a payment request for the payment transaction at said electronic device;" 153

8. 1(d): "displaying, on the touch-screen display, information reflecting the payment request, and an image representing a selected issued payment account;" 159

9. 1(e): "dynamically generating, by the processor, limited-use payment information; 164

10. 1(f): "wherein said limited-use payment information is dynamically generated based on a per-transaction sequential parameter originating from the electronic device;" 170

11. 1(g): "using said limited-use payment information in connection with the payment transaction in place of issued payment information associated with said selected issued payment account;" 174

12. 1(h): "transmitting said limited-use payment information from said electronic device via said NFC interface for receipt by an NFC recipient;" 174

13. 1(i): "responsive to the transmitting the limited-use payment information, receiving via the NFC interface information reflecting a status of said payment transaction; and displaying the status of said payment transaction via said touch-screen display." 175

14. Claim 2 "The method of claim 1, wherein the limited-use payment information comprises a cryptogram number." 179

15. Claim 7: "The method of claim 1, wherein the priming operation comprises bringing the electronic device within receiving proximity of an NFC recipient." 179

16. D. Claim 8(a): "The method of claim 7, wherein said readying said device to perform a payment transaction comprises: identifying said proximity NFC recipient is an NFC payment facility; successfully validating the

identified user as authorized to perform the payment transaction via said electronic device; and" 179

17. Claim 8(b): "receiving a user approval for performing the payment transaction." 182

18. Claim 9(Pre): "The method of claim 8, wherein said user approval for performing a payment transaction comprises displaying a request for user input at said electronic device, for both said identifying and said user approval of said payment transaction, and further comprising:" 183

19. Claim 9(a): "the processor identifying that said user input matches a known authorized user of the electronic device, before said readying said device to perform a payment transaction; and," 184

20. Claim 9(b): "disallowing the payment transaction by the device until said readying said device to perform the payment transaction is successfully completed." 185

21. Claim 10.1: The method of claim 8, wherein said successfully validating the identified user comprises the processor successfully determining a match between: firstly, a user input received via at least one of a set of user input sensors of the electronic device; and, secondly, at least one of the set consisting of: predetermined user characteristics, and challenge-responses of an authorized user, as stored in the electronic device. 187

22. Claim 11: "The method of claim 10, wherein said user input received via at least one set of a set of user input sensors of the electronic device comprises a passcode entry sequence performed by a user input via the touch-screen display." 190

23. Claim 15: "The method of claim 1, wherein the input comprising a priming operation is a user input." 191

24. Claim 27: "The method of claim 1, wherein the dynamically generating further comprises dynamically generating the limited-use payment information based on payment processing authority secret information." 191

25. Claim 28(Pre): "The method of claim 27 wherein the limited-use payment information is based on at least one secret information shared by both the electronic device and the payment processing authority; and" 191

26. Claim 28(a): "further wherein the at least one secret information is not exchanged when p[er]forming the payment transaction." 191

27. Claim 39 (Pre): "An electronic device for completing a payment transaction, the electronic device comprising:" 197

28. 39(a): "a processor;" 199

29. 39(b): "a memory coupled to the processor," 199

30. 39(b)(1): "wherein the memory is operable to store information associated with use of an issued payment account and wherein the payment authority information comprises a secret information;" 201

31. 39(c): "a near field communications (NFC) interface coupled to the processor and operable to receive a payment request associated with the payment transaction;" 203

32. 39(d): "a user interface coupled to the processor;" 204

33. 39(e): "a user input device coupled to the processor; and," 209

34. 39(f): "wherein said processor is operable to: responsive to a priming operation, wherein the priming operation is operable to ready the device to perform the payment transaction," 209

35. 39(g): "cause the display of information associated with the payment request;" 210

36. 39(h): "cause the display of an image representing at least one user-selectable issued payment account; and," 210

37. 39(i): "dynamically generate a limited-use payment information based on a per-transaction sequential parameter originating from the electronic device, and secret information associated with a selected issued payment account; and," 211

38. 39(j): "cause the transmission, via said NFC interface, a payment information combination comprising the dynamically generated limited-use payment information and said payment authority information, for receipt by an NFC recipient;" 212

39. 39(k): "wherein the NFC interface is operable, in response to transmitting said payment information combination, to receive status information reflecting a transaction processing status of said payment transaction; and wherein the user interface is operable to provide an indication of the status information." 213

40. Claim 41: "The device of claim 39 wherein the payment authority information comprises a secret information shared by both the electronic device and a payment processing authority." 214

41. Claim 44: "The device of claim 39 wherein the processor is operable to cause the transmission of issued payment account information and in response thereto, to receive the processing authority information." 214

42. Claim 45: "The device of claim 39 wherein the dynamically generated limited-use payment information comprises a cryptogram number, and further wherein the processor is operable to cause transmission, via said NFC interface, of a payment information combination comprising the dynamically generated limited-use payment information and at least a portion of said payment authority information in connection with the payment transaction in place of at least a portion of the payment information associated with said selected issued payment account." 214

43. Claim 46: "The device of claim 45 wherein the processor is operable to cause the transmission of issued payment account information and in response thereto, receive the processing authority information." 215

44. Claim 49: "The device of claim 39, wherein said user interface comprises a display and wherein said user input device comprises a touch panel disposed adjacent to said

display and wherein further the processor is operable to identify an authorized user by validating a valid user passcode input to the touch panel." 215

45. Claim 50: "The device of claim 39, wherein said user interface comprises a display and wherein said user input device comprises a touch panel disposed adjacent to said display and wherein further the processor is operable to identify an authorized user by displaying a security challenge question presented on the display and receiving a correct user response thereto." 216

46. Claim 55(a): "The device of claim 39, wherein the processor is operable to: receive a user-selection of an issued payment account presented on the user interface, received the user input device coupled to the processor, and" 217

47. Claim 55(b): "responsive thereto, select from the memory a specific processing authority information corresponding to the user-selected issued payment account information, and" 217

48. Claim 55(c): "use at least a portion of said specific processing authority information in place of at least a portion of the issued payment account information to generate a combined payment information to complete a payment transaction per the input user-selection." 218

49. Claim 56(Pre): "An electronic device for completing a payment transaction, the electronic device comprising:" 218

50. 56(a): "a processor;" 218

51. 56(b): "a memory coupled to the processor," 219

52. 56(b)(1): "wherein the memory stores a payment authority information associated with a user-selectable issued payment account, and wherein the payment authority information includes a secret information;" 219

53. 56(c): "a near field communications (NFC) interface coupled to the processor and operable to receive a payment request associated with the payment transaction; 219

54. 56(d): "a user interface coupled to the processor;" 219

55. 56(e): "a user input device coupled to the processor; and,".....219

56. 56(f):" wherein said processor is operable to: responsive to a priming operation, wherein the priming operation is operable to ready the device to perform the payment transaction,".....219

57. 56(g): "cause the display of information associated with the payment request;" 219

58. 56(h): "cause the display of an image representing the user-selectable issued payment account; and,".....219

59. 56(i): "dynamically generate a limited-use payment information based on a per-transaction sequential parameter originating from the electronic device, and the secret information associated with the user-selectable issued payment account; and," 220

60. 56(j): "cause the transmission, via said NFC interface, of a payment information combination comprising, the dynamically generated limited-use payment information and at least a portion of said payment authority information, for receipt by an NFC recipient;" 220

61. 56(k): "wherein the NFC interface is operable, in response to transmitting said payment information combination, to receive status information reflecting a transaction processing status of said payment transaction; and wherein the user interface is operable to provide an indication of the transaction status information.".....220

62. Claim 60: "The device of claim 56, wherein the secret information is shared by both the electronic device and a payment processing authority." 220

63. Claim 61: "The device of claim 56, wherein the processor is operable to cause the transmission of issued payment account information and in response thereto, to receive the payment authority information.".....220

64. Claim 62: "The device of claim 56, wherein the dynamically generated limited-use payment information comprises a cryptogram number, and further payment information combination is used in place of at least a portion of fixed payment information associated with said user-selectable issued payment account." 220

65. Claim 63: "The device of claim 62, wherein the processor is operable to cause the transmission of issued payment account information and in response thereto, receive the payment authority information." 221

66. Claim 66: "The device of claim 56, wherein said user interface comprises a display and wherein said user input device comprises a touch screen interface of the display, and wherein further the processor is operable to identify an authorized user by validating a valid user passcode input to the touch screen interface." 221

67. Claim 67: "The device of claim 56, wherein said user interface comprises a display and wherein said user input device comprises a touch screen interface of the display, and wherein further the processor is operable to identify an authorized user by displaying a security challenge question presented on the display and receiving a correct user response via said touch screen interface of the display." 221

68. Claim 72(Pre): "The device of claim 56, wherein the processor is operable to receive, via the user input device, a user-selection of said user-selectable issued payment account presented on the user interface, and" 222

69. Claim 72(a): "in response thereto, is further operable to select from memory the payment authority information corresponding to selected user-selectable issued payment account, and" 222

70. Claim 72(b): "is further operable to use said payment information combination in place of at least a portion of fixed payment information associated with said selected user-selectable issued payment account." 222

X. OPINIONS REGARDING GROUND 2: COLLINGE IN VIEW OF LIN, SAHOTA, AND SMITH.....223

1. Claim 29(Pre): "A system for completing a payment transaction, the system comprising:".....223
2. 29(a): "an electronic device operable to receive a priming operation, wherein the priming operation is operable to ready said device for performing a payment transaction by an identified user, and, wherein the electronic device further comprises:" 224
3. 29(b):" a processor;".....224
4. 29(c): "a near field communications (NFC) interface coupled to the processor and operable to receive a payment request associated with the payment transaction; and,".....225
5. 29(d): "a touch-screen display coupled to the processor, and".....225
6. 29(e): "wherein the electronic device is operable to cause the display of information reflecting device-readiness, the payment request, and an image representing at least one selected issued payment account;" 225
7. 29(f): "wherein the electronic device is operable to dynamically generate limited-use payment information based on a sequential counter count from the electronic device;".....225
8. 29(g): "wherein the electronic device is operable to store a static device-specific user account information;".....226
9. 29(h): "wherein the electronic device is operable to transmit a combination of said dynamically generated limited-use payment information and said static device-specific user account information to an NFC recipient via, said NFC interface for use in connection with payment transaction in place of information associated with said selected issued payment account;".....241
10. 29(i): "wherein the electronic device is operable, subsequent to transmission of said combination, to receive a status information reflecting a status of said

payment transaction; and, wherein the touch-screen display is operable to display as indication of said status information.”.....244

11. 3(a): “The method of claim 2, further comprising: prior to the priming operation, transmitting the issued payment information for receipt by a payment processing authority; and,” 245

12. Claim 3(b): “in response to said transmitting issued payment information, receiving a static device account information that is unique to the electronic device.”.....247

13. Claim 4(a): “The method of claim 3 further comprising: combining said limited-use payment information and said static device account information, to [produce] a combined payment information;”.....248

14. Claim 4(b): “transmitting said combined payment information, in place of the issued payment account information, via said NFC [interface] for receipt by an NFC recipient; and”.....248

15. Claim 4(c): “receiving, via the NFC interface, and in response to transmitting said combined payment information, transaction processing information reflecting a status of said payment transaction.” 249

16. Claim 5: “The method of claim 3, wherein the dynamically generating [further] comprises dynamically generating the limited-use payment information based on payment processing authority secret information.”.....249

17. Claim 6: “The method of claim 5, wherein the limited-use payment information is based on at least one secret information shared by both the electronic device and the payment processing authority.” 252

18. Claim 17(a): “The method of claim 1, further comprising: prior to the priming operation, transmitting the issued payment information for receipt by a payment processing authority; and,” 252

19. Claim 17(b): "in response to said transmitting issued payment information, receiving a static device account information that is unique to the electronic device." 252

20. Claim 18(a): "The method of claim 17 further comprising: combining said limited-use payment information and said static device account information, to produce a combined payment information;" 253

21. Claim 18(b): "transmitting said combined payment information, in place of the issued payment account information said NFC interface for receipt by an NFC recipient; and" 253

22. Claim 18(c): "receiving, via the NFC interface, and in response to transmitting said combined payment information, transaction processing information reflecting a status of said payment transaction." 253

23. Claim 19: "The method of claim 18, wherein the dynamically generating further comprises dynamically generating the limited-use payment information based on payment processing authority secret information." 253

24. Claim 20: "The method of claim 19, wherein the limited-use payment information is based on at least one secret information shared by both the electronic device and the payment processing authority." 253

25. Claim 21: "The method of claim 17, wherein the dynamically generating further comprises dynamically generating the limited-use payment information based on payment processing authority secret information." 253

26. Claim 22: "The method of claim 21, wherein the limited-use payment information is based on at least one secret information shared by both the electronic device and the payment processing authority." 254

27. Claim 23(a): "The method of claim 1, further comprising: prior to the priming operation, transmitting the issued payment information, user information and device-specific information; and," 254

28. Claim 23(b): "in response to transmitting said issued payment information, user information and device-specific information, receiving a payment processing authority supplied secret information." 259

29. Claim 24: "The method of claim 23 wherein said payment processing authority supplied secret information comprises static device account information." 259

30. Claim 30: "The system of claim 29, wherein the dynamically generated limited-use payment information comprises a cryptogram number." 259

31. Claim 31: "The system of claim 29, wherein the device-specific user account information comprises static device account information." 259

32. Claim 32: "The system of claim 31, wherein the static device account information comprises a static device account number that is unique to the electronic device." 260

33. Claim 34: "The system of claim 32 wherein the sequential counter count is changed per payment transaction." 260

34. Claim 35: "The system of claim 34 wherein the electronic device is operable to transmit issued payment account information and in response thereto, to receive the static device account information." 260

35. Claim 36(Pre): "The system of claim 29 wherein the electronic device is further operable to dynamically generate the limited-use payment information based on a shared information: from said user, information associated with said electronic device, information associated with said selected, issued payment account, and at least one secret; and," 260

36. Claim 36(a): "wherein said shared information is shared by both the electronic device and a payment processing authority." 260

37. Claim 37: "The system of claim 36 wherein the electronic device is further operable to dynamically

generate the limited-use payment information based on payment processing authority secrets." 260

38. Claim 38: "The system of claim 29 wherein the electronic device is further operable to dynamically generate the limited-use payment information based on payment processing authority secrets." 260

39. Claim 40: "The device of claim 39 wherein the payment authority information comprises information that is unique to the electronic device." 261

40. Claim 42: "The device of claim 41 wherein the processing authority information comprises a static device account number." 261

41. Claim 47: "The device of claim 46 wherein the processing authority information comprises a static device account number." 261

42. Claim 57: "The device of claim 56, wherein the payment authority information comprises information that is unique to the electronic device." 261

43. Claim 58: "The device of claim 57, wherein the payment authority information comprises a static device account number." 261

44. Claim 64: "The device of claim 63, wherein the payment authority information comprises a static device account number." 261

XI. OPINIONS REGARDING GROUND 3: COLLINGE IN VIEW OF LIN, SAHOTA, SMITH, AND KRANZLEY.....262

1. Claim 25: "The method of claim 24 wherein said static device account information comprises a static device account number and a static device-specific expiration date." 262

2. Claim 26: "The method of claim 25 wherein the static device account number is associated with the selected issued payment account on said electronic device." 264

3. Claim 33: "The system of claim 32 wherein the static device account information further comprises a static device account expiration date." 264

4. Claim 43: "The device of claim 42 wherein the processing authority information further comprises a static device account expiration date." 264

5. Claim 48: "The device of claim 47 wherein the processing authority information further comprises a static device account expiration date." 264

6. Claim 59: "The device of claim 58, wherein the payment authority information further comprises a static device account expiration date." 264

7. Claim 65: "The device of claim 64, wherein the payment authority information further comprises a static device account expiration date." 264

XII. OPINIONS REGARDING GROUND 4: COLLINGE IN VIEW OF LIN, SAHOTA, AND FADELL..... 264

1. Claim 10.2: "The method of claim 8, wherein said successfully validating the identified user comprises the processor successfully determining a match between: firstly, a user input received via at least one of a set of user input sensors of the electronic device; and, secondly, at least one of the set consisting of: predetermined user characteristics, and challenge-responses of an authorized user, as stored in the electronic device." 264

2. Claim 12: "The method of claim 10, wherein said predetermined user characteristics stored within the electronic device comprise known user biometric touch characteristics." 271

3. Claim 13: "The method of claim 10, wherein said predetermined user characteristics stored within the electronic device comprise a known user touch gesture." 272

4. Claim 16(Pre): "The method of claim 15, wherein said readying said device to perform a payment transaction comprises:" 272

5. Claim 16(a): "successfully identifying said identified user from said user input; and," 272

6. Claim 16(b): "wherein said user input further comprises a user approval for performing the payment transaction received from said identified user; and," 272

7. Claim 16(c): "wherein said successfully identifying further comprises said electronic device validating an authorized user of said electronic device by comparing a user-touch input received via a touch input sensor on the electronic device with a recognized valid user-touch, stored in a memory of the electronic device; and," 272

8. Claim 16(d): "wherein said user approval for performing the payment transaction further comprises:" 273

9. Claim 16(e): "visually presenting information of the payment transaction on the touch screen display of said electronic device;" 273

10. Claim 16(f): "visually presenting a request for user approval of the payment transaction via touch input at said electronic device; and," 276

11. Claim 16(g): "subsequent to receiving a user-touch input from an identified user, approving performance of said payment transaction via said electronic device." 277

12. Claim 51: "The device of claim 39, wherein said user input device comprises a biometric sensor operable to detect a user touch of said electronic device and wherein further the processor is operable to identify an authorized user by biometric sensing of a continuous user touch." 278

13. Claim 52: "The device of claim 39, wherein said user interface comprises a display and wherein said user input device comprises a touch panel disposed adjacent to said display and wherein further the processor is operable to identify an authorized user by biometric sensing of a user touch at the touch panel." 278

14. Claim 53: "The device of claim 39, wherein said user interface comprises a display and wherein said user input device comprises a touch panel disposed adjacent to said

display and wherein further the processor is operable to identify an authorized user by biometric recognition of a valid user identification." 279

15. Claim 68: "The device of claim 56, wherein said user input device comprises a biometric sensor operable to detect a user touch of said electronic device and wherein further the processor is operable to identify an authorized user by biometric sensing of said user touch." 279

16. Claim 69: "The device of claim 56, wherein said user interface comprises a display and wherein said user input device comprises a touch screen interface of the display and wherein further the processor is operable to identify an authorized user by biometric sensing of a user touch at the touch screen interface." 279

17. Claim 70: "The device of claim 56, wherein said user interface comprises a display and wherein said user input device comprises a touch input of the electronic device and wherein further the processor is operable to identify an authorized user by biometric recognition of a valid user identification via the touch input."....279

XIII. OPINIONS REGARDING GROUND 5: COLLINGE IN VIEW OF LIN, SAHOTA, AND YU. 280

1. Claim 10.3: "The method of claim 8, wherein said successfully validating the identified user comprises the processor successfully determining a match between: firstly, a user input received via at least one of a set of user input sensors of the electronic device; and, secondly, at least one of the set consisting of: predetermined user characteristics, and challenge-responses of an authorized user, as stored in the electronic device." 280

2. Claim 14: "The method of claim 10, wherein said predetermined user characteristics stored within the electronic device comprise a known user motion of the device." 285

3. Claim 54: "The device of claim 39, wherein said user input device comprises an army of motion sensors and wherein further the processor is operable to identify an

authorized user by detecting a recognized user displacement of the array of motion sensors." 285

4. Claim 71: "The device of claim 56, wherein said user input device comprises an array of motion sensors and wherein further the processor is operable to identify an authorized user by detecting a recognized user displacement of the array of motion sensors." 286

XIV. CONCLUSION*.....*286

CLAIM LISTING

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

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

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

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

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

Claim Designation	Claim Language
Claim 27	The method of claim 1, wherein the dynamically generating further comprises dynamically generating the limited-use payment information based on payment processing authority secret information.
Claim 28(Pre)	The method of claim 27 wherein the limited-use payment information is based on at least one secret information shared by both the electronic device and the payment processing authority; and
Claim 28(a)	further wherein the at least one secret information is not exchanged when preforming the payment transaction.
Claim 29(Pre)	A system for completing a payment transaction, the system comprising:
Claim 29(a)	an electronic device operable to receive a priming operation, wherein the priming operation is operable to ready said device for performing a payment transaction by an identified user, and, wherein the electronic device further comprises:
Claim 29(b)	a processor;
Claim 29(c)	a near field communications (NFC) interface coupled to the processor and operable to receive a payment request associated with the payment transaction; and,
Claim 29(d)	a touch-screen display coupled to the processor, and
Claim 29(e)	wherein the electronic device is operable to cause the display of information reflecting device-readiness, the payment request, and an image representing at least one selected issued payment account;
Claim 29(f)	wherein the electronic device is operable to dynamically generate limited-use payment information based on a sequential counter count from the electronic device;
Claim 29(g)	wherein the electronic device is operable to store a static device-specific user account information;
Claim 29(h)	wherein the electronic device is operable to transmit a combination of said dynamically generated limited-use payment information and said static device-specific user account information to an NFC recipient via, said NFC interface for use in connection with payment transaction in place of information associated with said selected issued payment account;

Claim Designation	Claim Language
Claim 29(i)	wherein the electronic device is operable, subsequent to transmission of said combination, to receive a status information reflecting a status of said payment transaction; and, wherein the touch-screen display is operable to display as indication of said status information.
Claim 30	The system of claim 29, wherein the dynamically generated limited-use payment information comprises a cryptogram number.
Claim 31	The system of claim 29, wherein the device-specific user account information comprises static device account information.
Claim 32	The system of claim 31, wherein the static device account information comprises a static device account number that is unique to the electronic device.
Claim 33	The system of claim 32 wherein the static device account information further comprises a static device account expiration date.
Claim 34	The system of claim 32 wherein the sequential counter count is changed per payment transaction.
Claim 35	The system of claim 34 wherein the electronic device is operable to transmit issued payment account information and in response thereto, to receive the static device account information.
Claim 36(Pre)	The system of claim 29 wherein the electronic device is further operable to dynamically generate the limited-use payment information based on a shared information: from said user, information associated with said electronic device, information associated with said selected, issued payment account, and at least one secret; and,
Claim 36(a)	wherein said shared information is shared by both the electronic device and a payment processing authority.
Claim 37	The system of claim 36 wherein the electronic device is further operable to dynamically generate the limited-use payment information based on payment processing authority secrets.

Claim Designation	Claim Language
Claim 38	The system of claim 29 wherein the electronic device is further operable to dynamically generate the limited-use payment information based on payment processing authority secrets.
Claim 39(Pre)	An electronic device for completing a payment transaction, the electronic device comprising:
Claim 39(a)	a processor;
Claim 39(b)	a memory coupled to the processor,
Claim 39(b)(1)	wherein the memory is operable to store information associated with use of an issued payment account and wherein the payment authority information comprises a secret information:
Claim 39(c)	a near field communications (NFC) interface coupled to the processor and operable to receive a payment request associated with the payment transaction;
Claim 39(d)	a user interface coupled to the processor;
Claim 39(e)	a user input device coupled to the processor; and,
Claim 39(f)	wherein said processor is operable to: responsive to a priming operation, wherein the priming operation is operable to ready the device to perform the payment transaction,
Claim 39(g)	cause the display of information associated with the payment request;
Claim 39(h)	cause the display of an image representing at least one user-selectable issued payment account; and,
Claim 39(i)	dynamically generate a limited-use payment information based on a per-transaction sequential parameter originating from the electronic device, and secret information associated with a selected issued payment account; and,
Claim 39(j)	cause the transmission, via said NFC interface, a payment information combination comprising the dynamically generated limited-use payment information and said payment authority information, for receipt by an NFC recipient;

Claim Designation	Claim Language
Claim 39(k)	wherein the NFC interface is operable, in response to transmitting said payment information combination, to receive status information reflecting a transaction processing status of said payment transaction; and wherein the user interface is operable to provide an indication of the status information.
Claim 40	The device of claim 39 wherein the payment authority information comprises information that is unique to the electronic device.
Claim 41	The device of claim 39 wherein the payment authority information comprises a secret information shared by both the electronic device and a payment processing authority.
Claim 42	The device of claim 41 wherein the processing authority information comprises a static device account number.
Claim 43	The device of claim 42 wherein the processing authority information further comprises a static device account expiration date.
Claim 44	The device of claim 39 wherein the processor is operable to cause the transmission of issued payment account information and in response thereto, to receive the processing authority information.
Claim 45	The device of claim 39 wherein the dynamically generated limited-use payment information comprises a cryptogram number, and further wherein the processor is operable to cause transmission, via said NFC interface, of a payment information combination comprising the dynamically generated limited-use payment information and at least a portion of said payment authority information in connection with the payment transaction in place of at least a portion of the payment information associated with said selected issued payment account.
Claim 46	The device of claim 45 wherein the processor is operable to cause the transmission of issued payment account information and in response thereto, receive the processing authority information.
Claim 47	The device of claim 46 wherein the processing authority information comprises a static device account number.

Claim Designation	Claim Language
Claim 48	The device of claim 47 wherein the processing authority information further comprises a static device account expiration date.
Claim 49	The device of claim 39, wherein said user interface comprises a display and wherein said user input device comprises a touch panel disposed adjacent to said display and wherein further the processor is operable to identify an authorized user by validating a valid user passcode input to the touch panel.
Claim 50	The device of claim 39, wherein said user interface comprises a display and wherein said user input device comprises a touch panel disposed adjacent to said display and wherein further the processor is operable to identify an authorized user by displaying a security challenge question presented on the display and receiving a correct user response thereto.
Claim 51	The device of claim 39, wherein said user input device comprises a biometric sensor operable to detect a user touch of said electronic device and wherein further the processor is operable to identify an authorized user by biometric sensing of a continuous user touch.
Claim 52	The device of claim 39, wherein said user interface comprises a display and wherein said user input device comprises a touch panel disposed adjacent to said display and wherein further the processor is operable to identify an authorized user by biometric sensing of a user touch at the touch panel.
Claim 53	The device of claim 39, wherein said user interface comprises a display and wherein said user input device comprises a touch panel disposed adjacent to said display and wherein further the processor is operable to identify an authorized user by biometric recognition of a valid user identification.
Claim 54	The device of claim 39, wherein said user input device comprises an army of motion sensors and wherein further the processor is operable to identify an authorized user by detecting a recognized user displacement of the array of motion sensors.

Claim Designation	Claim Language
Claim 55(a)	The device of claim 39, wherein the processor is operable to: receive a user-selection of an issued payment account presented on the user interface, received the user input device coupled to the processor, and
Claim 55(b)	responsive thereto, select from the memory a specific processing authority information corresponding to the user-selected issued payment account information, and
Claim 55(c)	use at least a portion of said specific processing authority information in place of at least a portion of the issued payment account information to generate a combined payment information to complete a payment transaction per the input user-selection.
Claim 56(Pre)	An electronic device for completing a payment transaction, the electronic device comprising:
Claim 56(a)	a processor;
Claim 56(b)	a memory coupled to the processor,
Claim 56(b)(1)	wherein the memory stores a payment authority information associated with a user-selectable issued payment account, and wherein the payment authority information includes a secret information;
Claim 56(c)	a near field communications (NFC) interface coupled to the processor and operable to receive a payment request associated with the payment transaction;
Claim 56(d)	a user interface coupled to the processor;
Claim 56(e)	a user input device coupled to the processor; and,
Claim 56(f)	wherein said processor is operable to: responsive to a priming operation, wherein the priming operation is operable to ready the device to perform the payment transaction,
Claim 56(g)	cause the display of information associated with the payment request;
Claim 56(h)	cause the display of an image representing the user-selectable issued payment account; and,
Claim 56(i)	dynamically generate a limited-use payment information based on a per-transaction sequential parameter originating from the electronic device, and the secret information associated with the user-selectable issued payment account; and,

Claim Designation	Claim Language
Claim 56(j)	cause the transmission, via said NFC interface, of a payment information combination comprising, the dynamically generated limited-use payment information and at least a portion of said payment authority information, for receipt by an NFC recipient;
Claim 56(k)	wherein the NFC interface is operable, in response to transmitting said payment information combination, to receive status information reflecting a transaction processing status of said payment transaction; and wherein the user interface is operable to provide an indication of the transaction status information.
Claim 57	The device of claim 56, wherein the payment authority information comprises information that is unique to the electronic device.
Claim 58	The device of claim 57, wherein the payment authority information comprises a static device account number.
Claim 59	The device of claim 58, wherein the payment authority information further comprises a static device account expiration date.
Claim 60	The device of claim 56, wherein the secret information is shared by both the electronic device and a payment processing authority.
Claim 61	The device of claim 56, wherein the processor is operable to cause the transmission of issued payment account information and in response thereto, to receive the payment authority information.
Claim 62	The device of claim 56, wherein the dynamically generated limited-use payment information comprises a cryptogram number, and further payment information combination is used in place of at least a portion of fixed payment information associated with said user-selectable issued payment account.
Claim 63	The device of claim 62, wherein the processor is operable to cause the transmission of issued payment account information and in response thereto, receive the payment authority information.
Claim 64	The device of claim 63, wherein the payment authority information comprises a static device account number.

Claim Designation	Claim Language
Claim 65	The device of claim 64, wherein the payment authority information further comprises a static device account expiration date.
Claim 66	The device of claim 56, wherein said user interface comprises a display and wherein said user input device comprises a touch screen interface of the display, and wherein further the processor is operable to identify an authorized user by validating a valid user passcode input to the touch screen interface.
Claim 67	The device of claim 56, wherein said user interface comprises a display and wherein said user input device comprises a touch screen interface of the display, and wherein further the processor is operable to identify an authorized user by displaying a security challenge question presented on the display and receiving a correct user response via said touch screen interface of the display.
Claim 68	The device of claim 56, wherein said user input device comprises a biometric sensor operable to detect a user touch of said electronic device and wherein further the processor is operable to identify an authorized user by biometric sensing of said user touch.
Claim 69	The device of claim 56, wherein said user interface comprises a display and wherein said user input device comprises a touch screen interface of the display and wherein further the processor is operable to identify an authorized user by biometric sensing of a user touch at the touch screen interface.
Claim 70	The device of claim 56, wherein said user interface comprises a display and wherein said user input device comprises a touch input of the electronic device and wherein further the processor is operable to identify an authorized user by biometric recognition of a valid user identification via the touch input.
Claim 71	The device of claim 56, wherein said user input device comprises an array of motion sensors and wherein further the processor is operable to identify an authorized user by detecting a recognized user displacement of the array of motion sensors.

Claim Designation	Claim Language
Claim 72(Pre)	The device of claim 56, wherein the processor is operable to receive, via the user input device, a user-selection of said user-selectable issued payment account presented on the user interface, and
Claim 72(a)	in response thereto, is further operable to select from memory the payment authority information corresponding to selected user-selectable issued payment account, and
Claim 72(b)	is further operable to use said payment information combination in place of at least a portion of fixed payment information associated with said selected user-selectable issued payment account.

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. 11,620,634 (the "'634 Patent"). I understand that the Challenged Claims are 1-72, 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.

A. 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. 11,620,634 (the "'634 Patent")
1002	File History of the '634 Patent ("the '634 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	Intentionally left blank
1010	U.S. Patent Publication No. 2010/0125508 to Smith (“Smith)”)
1011	U.S. Patent Publication No. 2005/0043997 to Sahota et al. (“Sahota”)
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 Publication No. 2009/0320123 to Yu et al. (“Yu”)
1015	U.S. Patent Publication No. 2009/0083850 to Fadell et al. (“Fadell”)
1016	CardWare Inc.’s Preliminary Proposed Claim Constructions
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.pd

	f, [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	Intentionally left blank
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	Intentionally left blank
1042	U.S. Patent Publication No. 2006/0097991 to Hotelling et al. ("Hotelling")
1043	U.S. Patent No. 7,580,898 to Brown et al. ("Brown")
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")

11. I have considered these materials from the viewpoint of a POSITA as of the priority date of the '634 Patent. For the purposes of this declaration, I have been asked to assume that the earliest priority date of the '634 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 '634 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 '634 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.

A. Person of Ordinary Skill in the Art

13. I understand that the ’634 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.

B. 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.

C. 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 for purposes of this proceeding, Petitioner has adopted the following constructions, proposed by Patent Owner in the underlying litigation. Ex. 1016.

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

D. 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 ’634 Patent, the cited prior art, and the ordinary skill factors described in this section, a POSITA in the field of the ’634 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 '634 PATENT

A. Summary of the '634 Patent

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

B. Field of Endeavor

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 '634 Patent defines the "FIELD OF THE INVENTION" as relating to "electronic or smart payment devices and, more specifically, to more secure, smart

multi-function smart tokenizing electronic payment devices and transaction processing thereof." *'634 Patent* at 1:25-31. For these reasons, a POSITA would understand that the field of endeavor of the '634 Patent includes more secure payment cards, devices and systems.

34. The '634 Patent's specification criticizes existing systems due to being "susceptible to theft and/or compromise" *'634 Patent* at 1:66-2:3 For these reasons, a POSITA would have understood that the '634 Patent is trying to solve the problem of providing payment solutions that limit opportunities for theft or compromise of payment credentials.

C. Problem Purportedly Solved by the Inventors of the '634 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 '634 Patent and determine the problem that the inventors were trying to solve.

36. The '634 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." *'634 Patent* at 1:65–2:3. The '634Patent also notes 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." *'634 Patent* at 2:3-7. 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." *'634 Patent* at 2:17-21. The "Summary of the Invention" further describes a method of performing a transaction that includes "generating…a limited duration credit card number." *'634 Patent* at 2:66–3:7. Thus, a POSITA would understand that the '634 Patent is directed to solving the problem of providing payment solutions that limit opportunities for theft or compromise of payment credentials.

D. File History of the '634 Patent

37. I have reviewed the prosecution history for the '634 Patent. The '634 Patent claims priority to Provisional Application No. 61/794,891, filed March 15, 2013. The '634 Patent did not face any prior art rejections during prosecution. *'634 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 '634 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 ’634 Patent.

39. As described below, all 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 ’634 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.

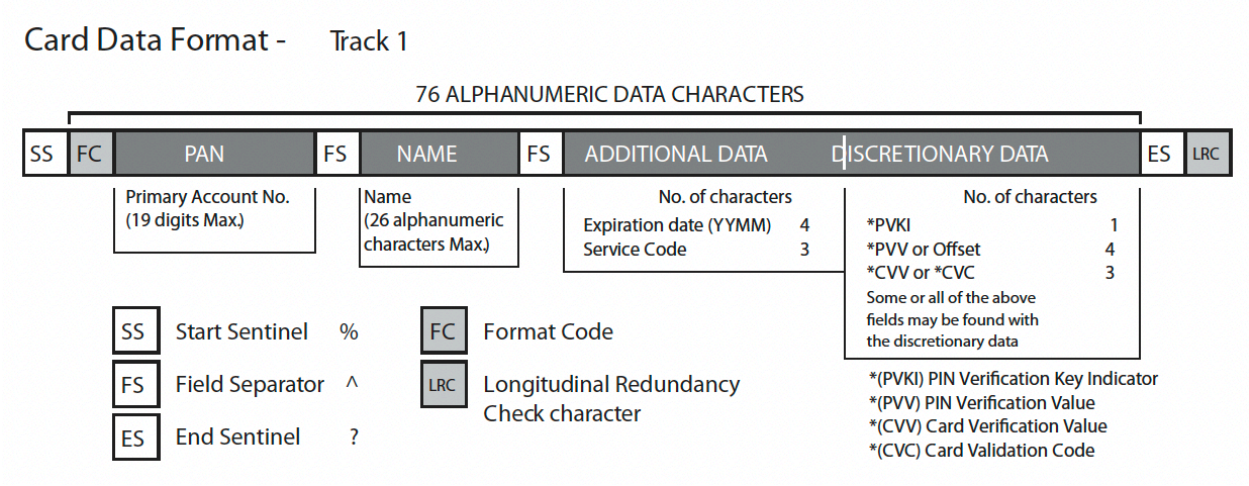
A. The Evolution of Payment Cards

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*, 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*, 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:

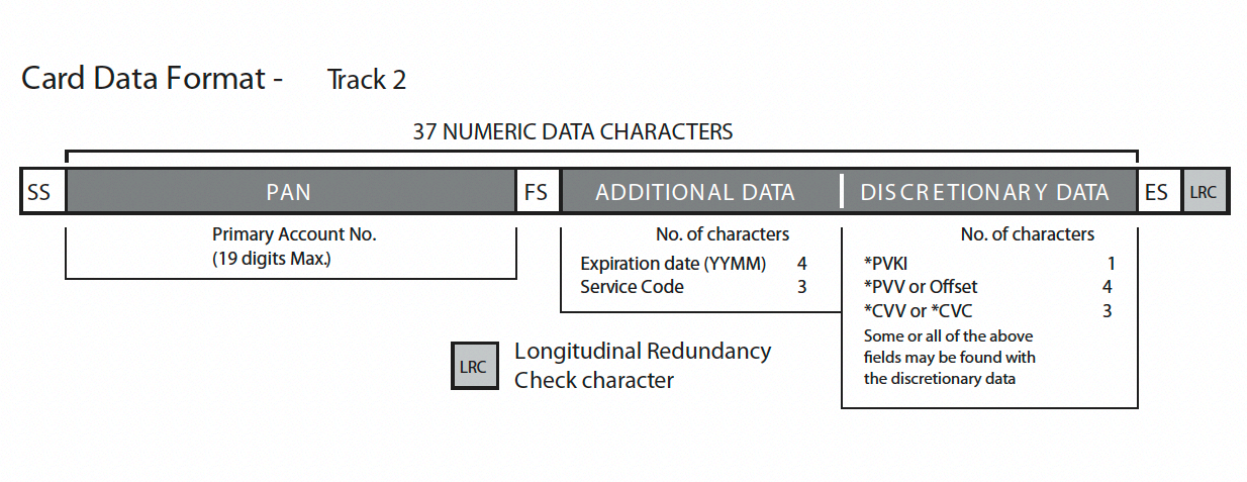


MagTek (Ex.1022), 1. On a card's track:

> "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 (Ex.1049), [0102]. Track 2 data includes the following data:



Magtek, 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.

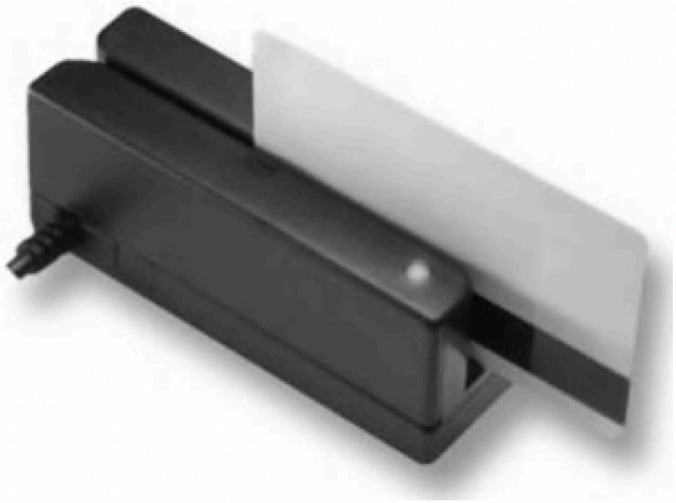


Figure 2.15 Magnetic stripe card.

Coskun, 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.

a) 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.

b) Contactless Payments

2. 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." *Finkenzelller*, 57.

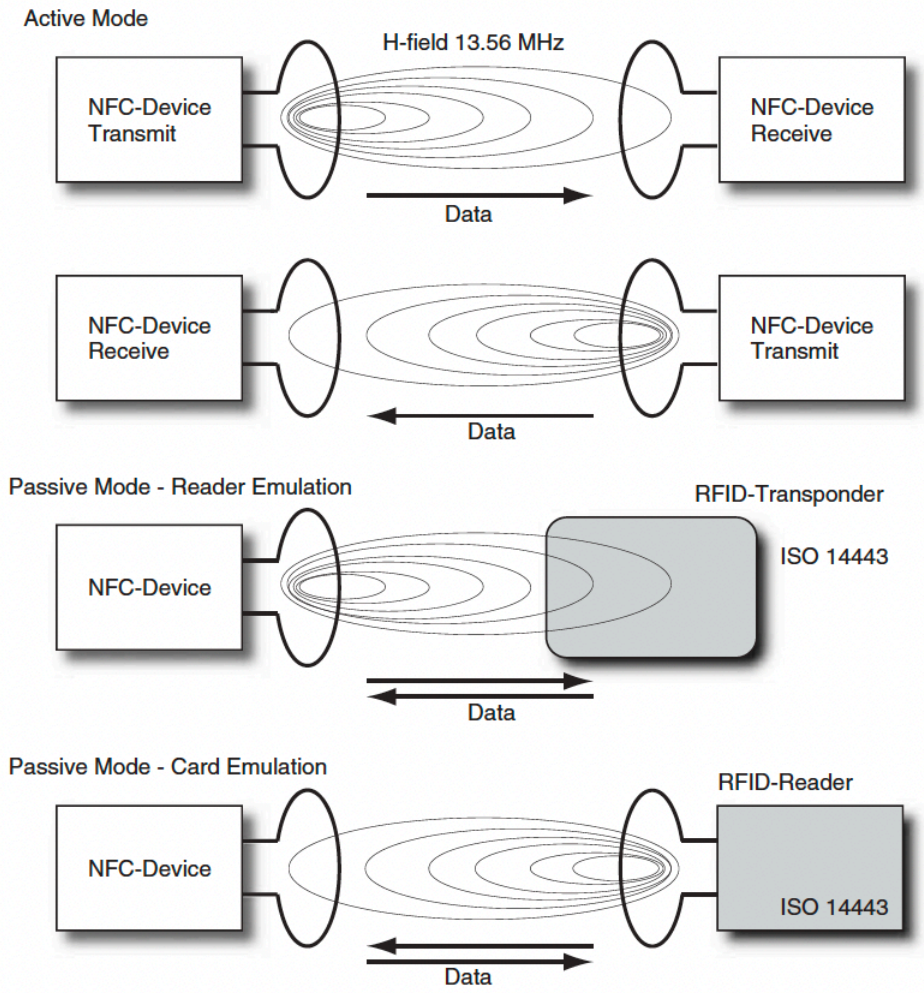


Figure 3.33 NFC distinguishes between three different operating modes: active mode (i); and passive mode in the operating modes reader emulation (ii); and card emulation (iii)

Finkenzelller, 58.

3. 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.

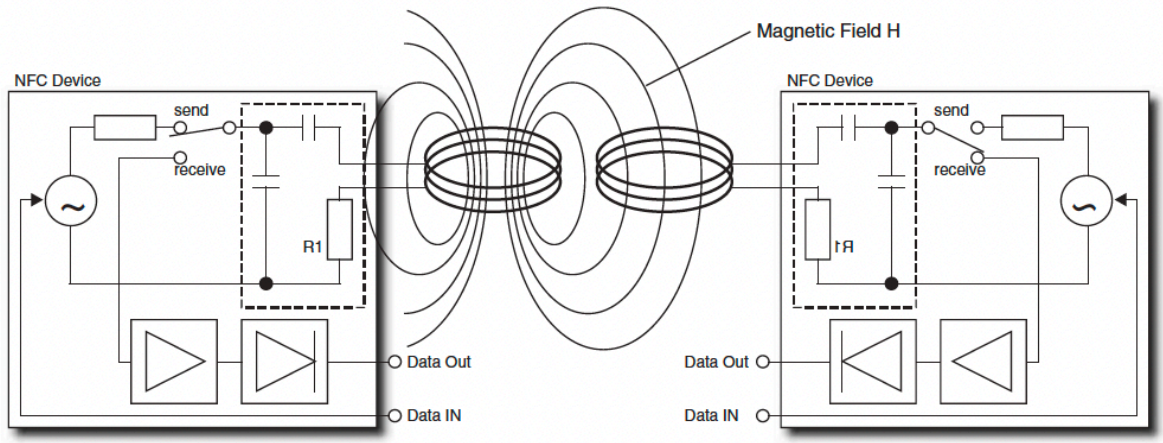


Figure 3.32 In active mode, the NFC interfaces alternately emit magnetic fields for data transmission

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.

4. 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.

5. 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.

6. 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.

7. 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].

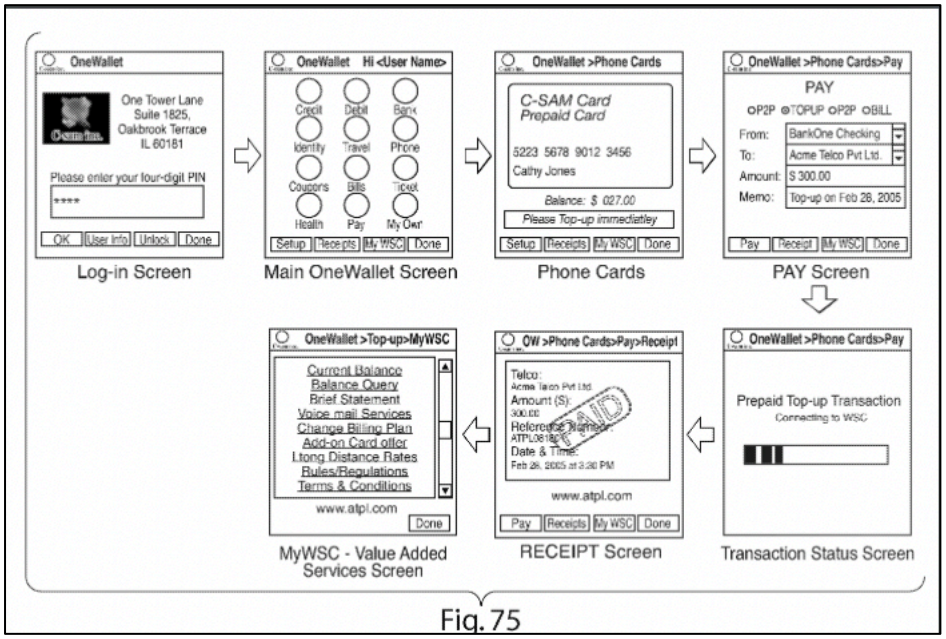


Fig. 75

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.

8. 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.

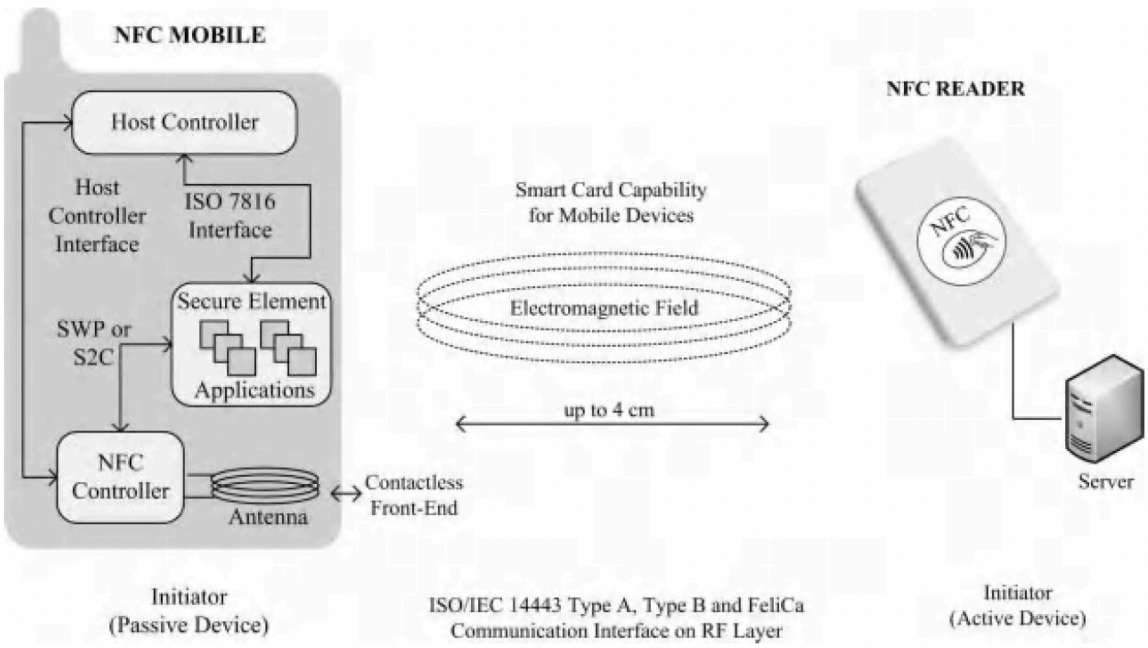


Figure 3.32 Communication architecture of card emulation operating mode.

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'].

B. 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.

1. 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 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."

500

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 (Ex.1047), [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 (Ex.1047), [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 (Ex.1047), [0002], [0006]. Grigg notes that each payment device has a "different mobile wallet account number[.]" Grigg (Ex.1047), [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 (Ex.1047), [0053]. This mobile wallet number "may be permanently associated with the mobile wallet" Grigg (Ex.1047), [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 (Ex.1047), [0043].

2. 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 (Ex.1049)*, [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 (Ex.1049) notes that "[t]hese one-time (i.e., dynamic) codes are generated by the smart card chip and are unique to each transaction." *Bona (Ex.1049)*, [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 (Ex.1049)*, [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

A. Collinge

77. Collinge Ex. 1004 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"). Collinge was neither cited nor discussed during prosecution of the '579 Patent. Ex. 1002, (56). 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.

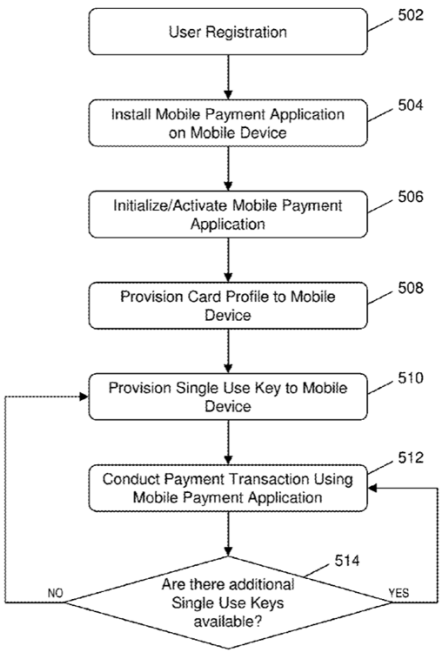
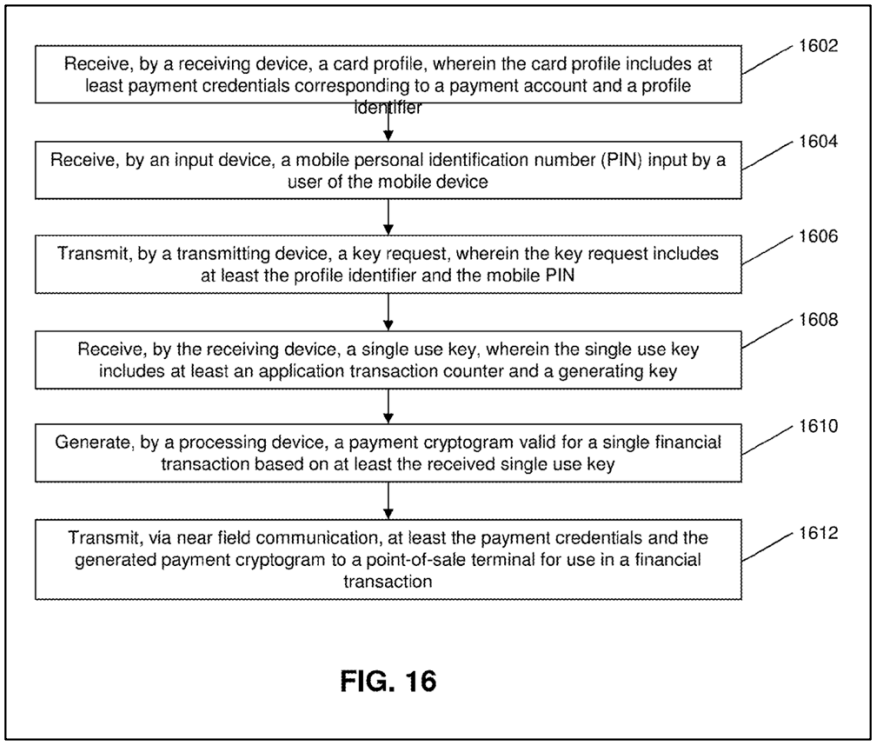


FIG. 5

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].



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 '634 Patent because both Collinge and the '634 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* at [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* at [0043]. The mobile device can then use the single use key to generate a payment cryptogram (either an application cryptogram (AC) or dynamic card validation code (CVC3)) for use in a financial transaction. *Collinge* at [0070]; [0050]. The '634 Patent similarly describes payment devices and transaction processing that can be utilized with near field communications. Ex. 1001 ('634 Patent) at 1:25-31, 2:66–3:7 . Similar to Collinge, the '634 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. Ex. 1001 ('634 Patent) at 10:48-53. Additionally, a POSITA would have found Collinge reasonably pertinent to the problem faced by the inventors of the '634 Patent because both Collinge and the '634 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 '634 Patent describes that its invention "address[es] security concerns of a payment card owner" for use in RFID transactions. Ex. 1001 ('634 Patent) at 9:35-37, 12:3-9. Accordingly, a POSITA would have considered Collinge analogous art to the '634 Patent.

2. Collinge is Prior Art

80. Collinge was filed on March 14, 2013, and is therefore prior art because it was filed earlier than the priority date of ’634 Patent’s provisional application, filed on March 15, 2013.

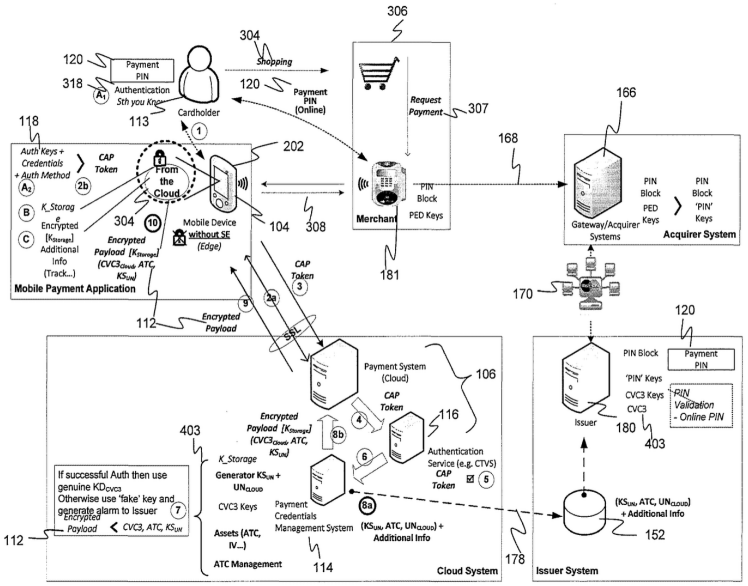
81. In the event that Cardware attempts to demonstrate that it is entitled to a date earlier than March 13, 2013, based on a showing of earlier conception and reduction to practice, it is additionally my understanding that Collinge is entitled to a prior date at least as early as April 18, 2012, based on Collinge provisional applications 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”).

82. I understand that for Collinge to be entitled to the April 18, 2012, filing date of the ’248 Provisional (Ex.1006), 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 provide 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 (“CVC3”), 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 CVC3, 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 CVC3for use in a financial transaction; and, transmitting the session key and cloud unpredictable number and ATC to an issuer for use in validating the CVC3 generated by the mobile device, which is similar to the level of disclosure in Collinge itself. In my opinion, the 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.

83. 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	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

mobile device lacking a secure element, comprising:	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."[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, Fig. 5

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

storing, in a database, at least a storage key, a plurality of dynamic card validation code keys, and an application transaction counter associated with a mobile application program;	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 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

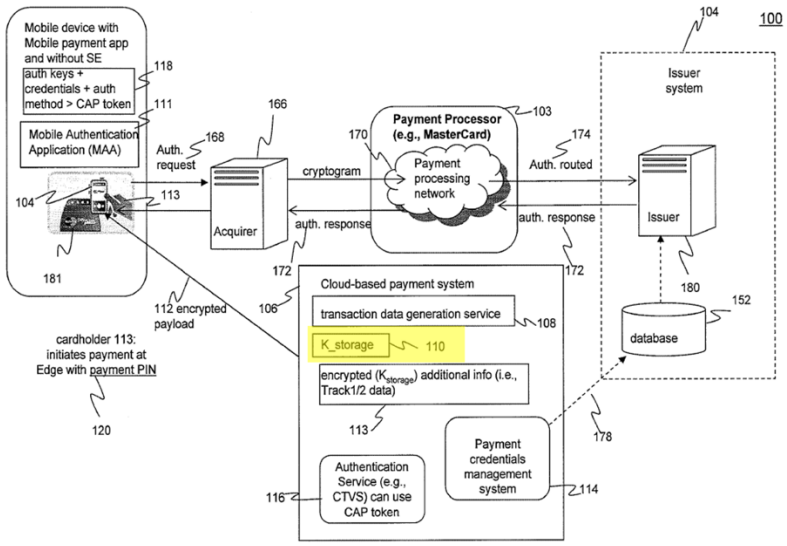
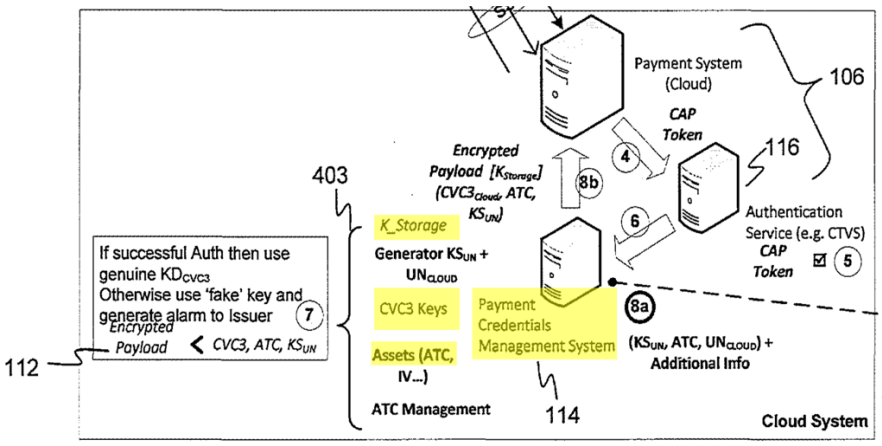
<table>
<tr>
<td></td>
<td>


FIG. 1

’095 Provisional (Ex. 1005), Fig. 1.



’095 Provisional (Ex. 1005), Fig. 5 (annotated excerpt);
’095 Provisional, Figs. 4, 6-8
</td>
</tr>
<tr>
<td>provisioning, to the mobile device, at least the storage key, an authentication component, and static payment</td>
<td>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</td>
</tr>
</table>

<table>
<tr>
<td>credentials, wherein the static payment credentials are associated with a payment account;</td>
<td>
<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

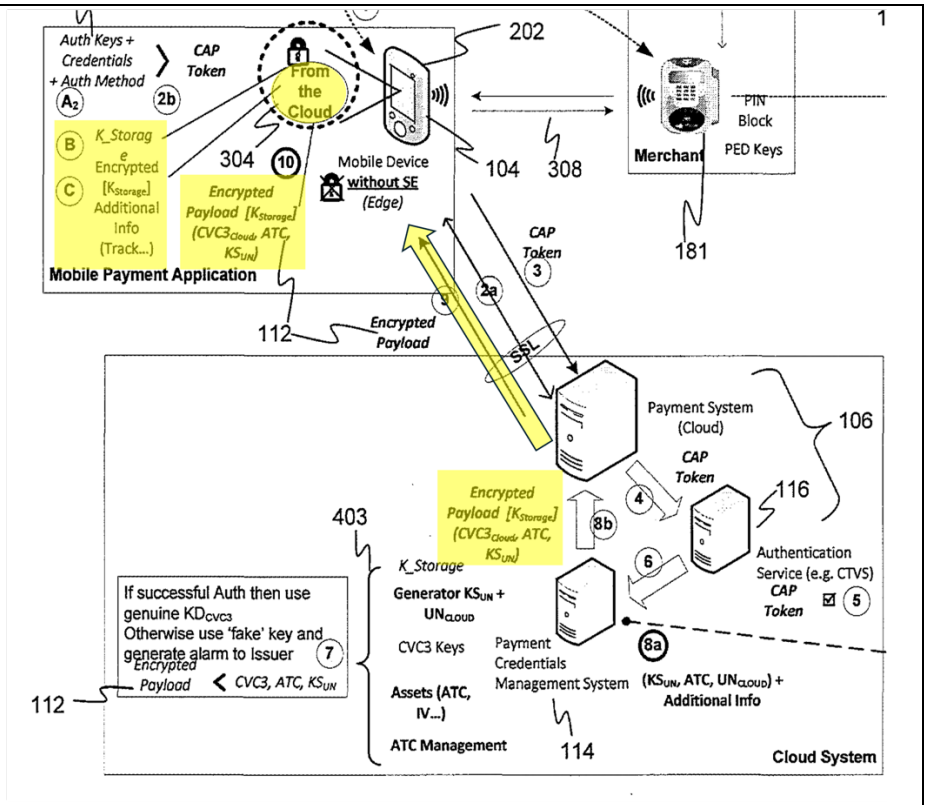
“Exemplary solutions and embodiments disclosed herein can incorporate several core principles outlined below:
► Storage Key ($K_{storage}$) defined at time of authentication profile and static Payment credentials provisioning.
► Authentication credentials protected using MAA rules (e.g. Key Camouflage) (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.

***
</td>
</tr>
</table>

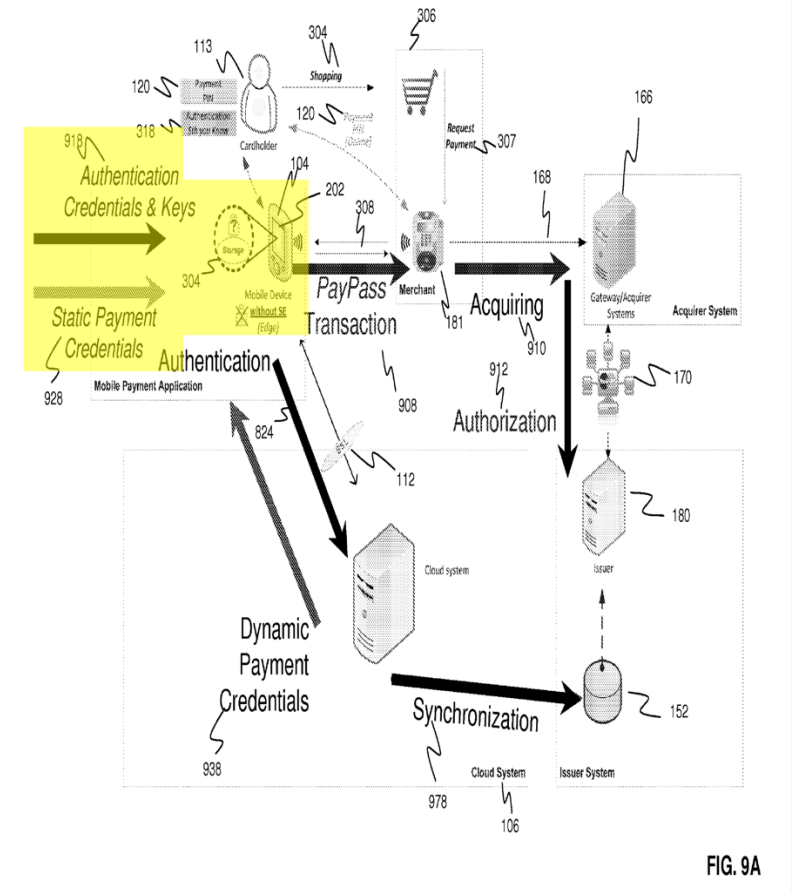
	► Delivery of Encrypted Payload [using $K_{storage}$] (KS_{UN}, Cloud_$CVC3_{TRACK1/2}$ and ATC) to Mobile Payment Application" '095 Provisional (Ex. 1005), ¶0068 "<u>(Static) Information known by the Mobile Payment Application</u> ◊ FCI (PPSE) ◊ AID (Application Identifier) ◊ FCI (File Control Information) ◊ 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



’248 Provisional (Ex. 1006), Fig. 9A

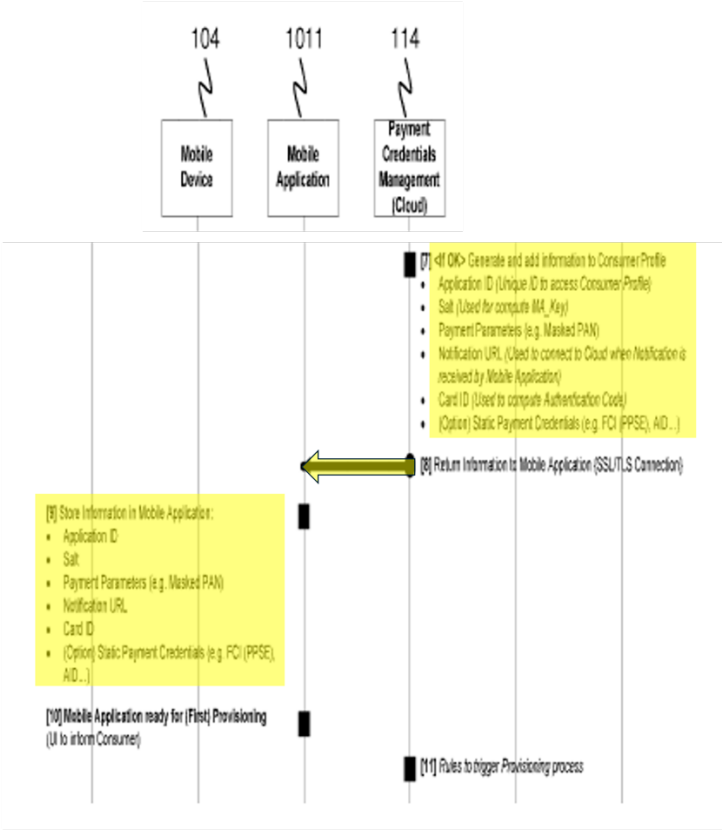
“The communications sequence depicted in Figure 11 encompasses pushing the following parameters/data to the mobile application 1011 as part of stage [7]: an application ID, which is a unique ID used to access the consumer profile (i.e., the profile for the user 113); a salt, which is a value used (in 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, 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

<table>
<tr>
<td>validating, by a validation device, the authenticity of the received CAP token;</td>
<td>The Collinge Provisionals disclose an authentication service validating the authenticity of the CAP token sent by the mobile device.

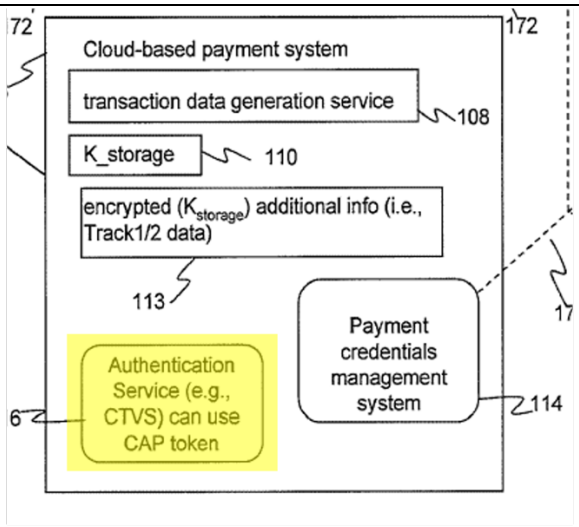
“A method for providing technical solutions for processing electronic payments initiated from a mobile device without requiring a secure element (SE) in a mobile device, comprising: …sending a token from a mobile authentication application (MAA) component of the mobile payment application to the Cloud; 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

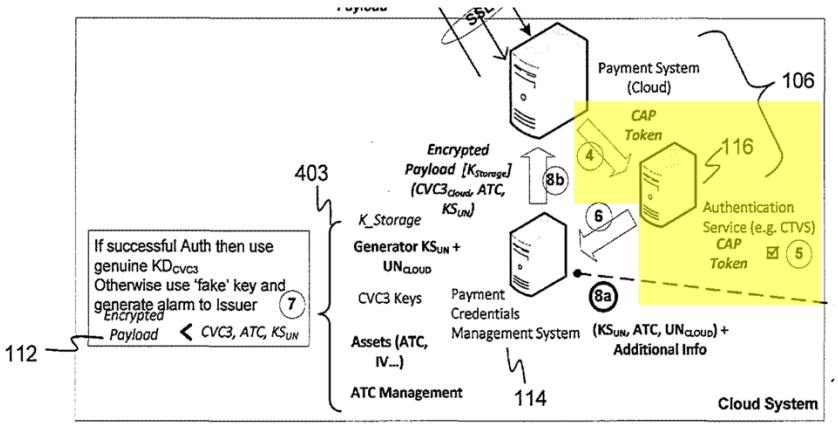
“In the exemplary embodiment of Figure 1, the authentication service 116 is configured to perform CVTS CAP Token validation (CTVS) and can use a Chip Authentication Program (CAP) token for authentication.”
’095 Provisional (Ex. 1005), ¶0038

“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

<table>
<tr><td>4</td><td>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.</td></tr>
<tr><td>5</td><td>The CTVS validates the CAP Token.
The CTVS can be operated by MasterCard or by the Issuer.</td></tr>
</table>
’095 Provisional (Ex. 1005), Table 1 (p. 24)</td>
</tr>
</table>



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



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

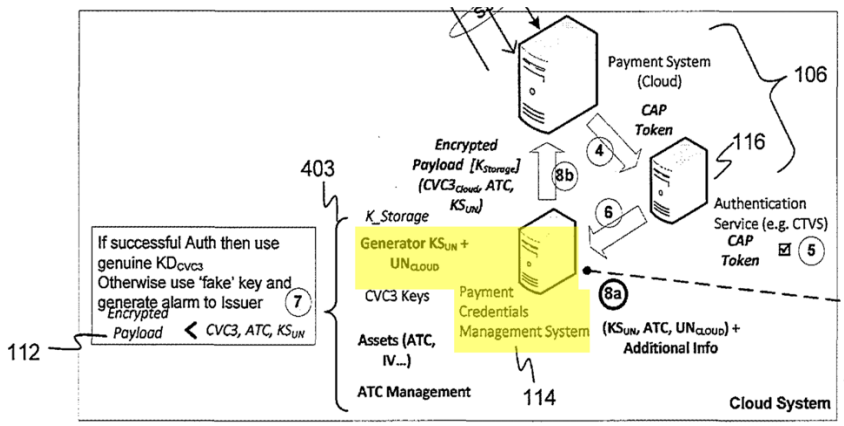
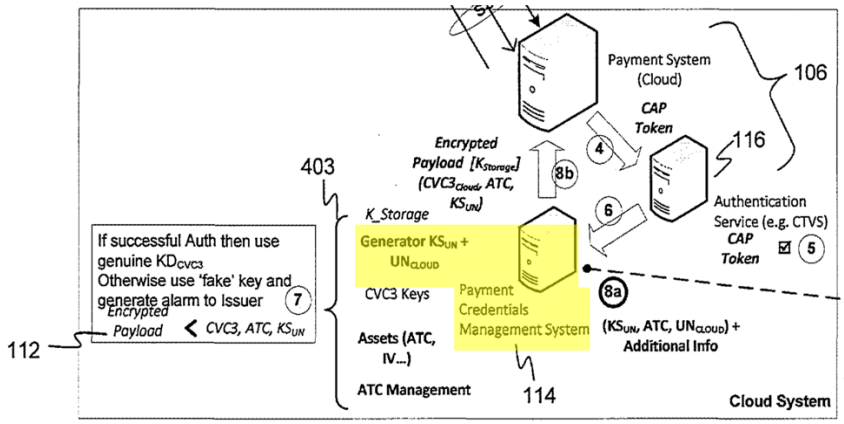
	Cloud). This encompasses the generation of KS_{UN} and UN_{CLOUD}, and the application transaction counter (ATC) management." '248 Provisional, ¶0077 (Ex. 1006); '095 Provisional (Ex. 1005), ¶0056 (p.13)  '095 Provisional (Ex. 1005), Fig. 1 (annotated excerpt); '095 Provisional, Fig. 7
generating, by 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, ¶0077 (Ex. 1006); '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

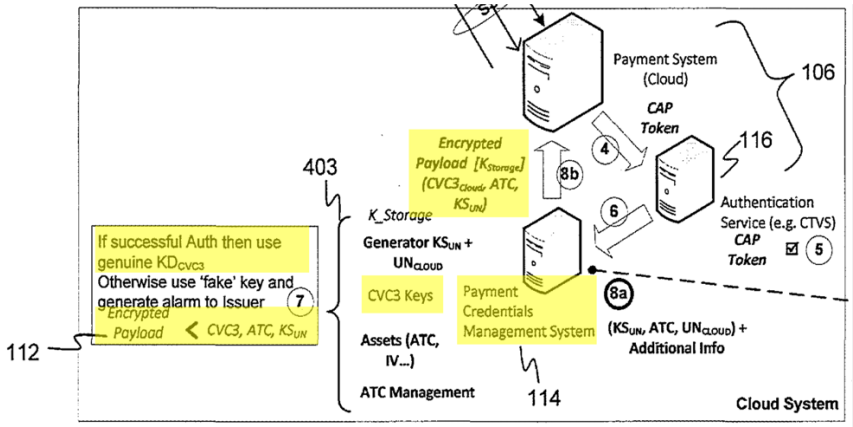
Stage	Description
***	
UN	Unpredictable Number

’095 Provisional, Table 2 (p. 25)



’095 Provisional (Ex. 1005), Fig. 5 (annotated excerpt);
’095 Provisional, Fig. 4, 6-7

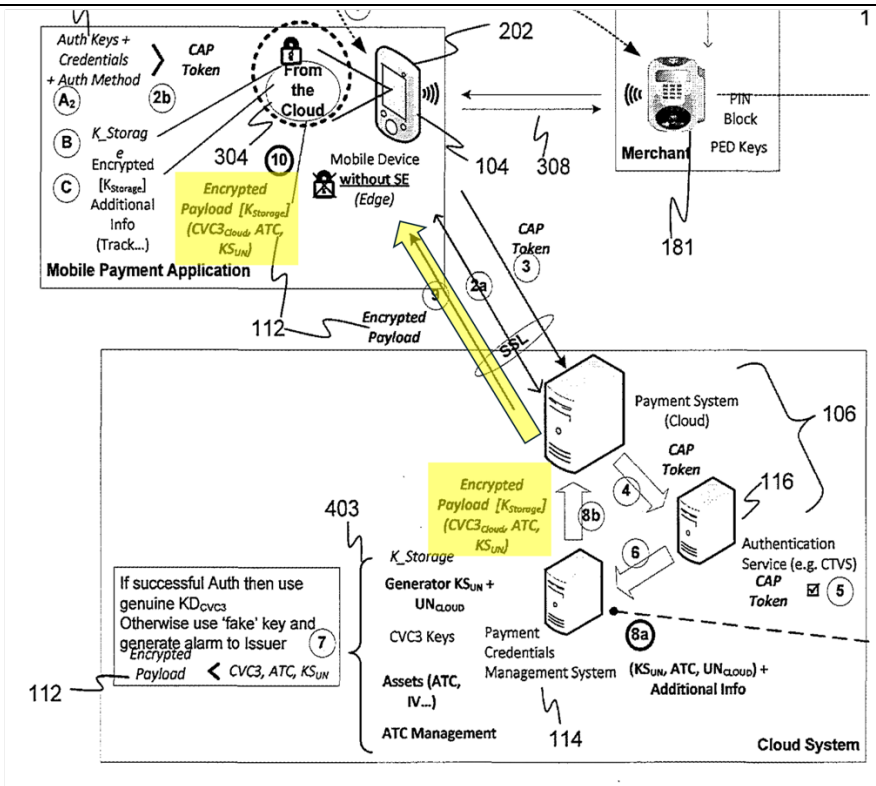
identifying, by the processing device, an encrypted payload based on a derived dynamic card validation code key (KD_{CVC3}), wherein the encrypted payload includes at least a dynamic card validation code key of the plurality of	The Collinge Provisionals disclose the cloud-based transaction data generation 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, 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. "<u>Encrypted (using $K_{Storage}$) Payload sent to the Mobile Payment Application (Valid for one contactless payment transaction)</u> ◊ $Cloud_CVC3_{TRACKI/2}$ ◊ 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



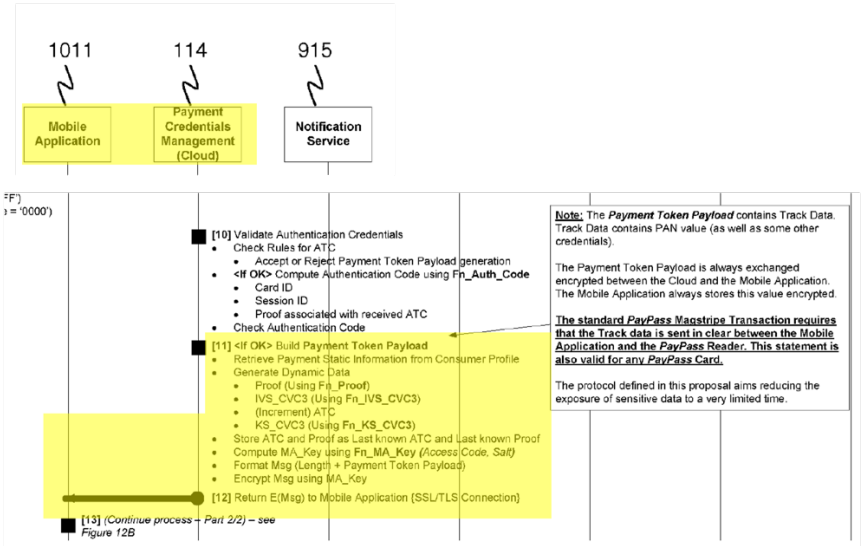
’095 Provisional (Ex. 1005), Fig. 5 (annotated excerpt);
’095 Provisional, Figs. 1, 6-8

“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.”

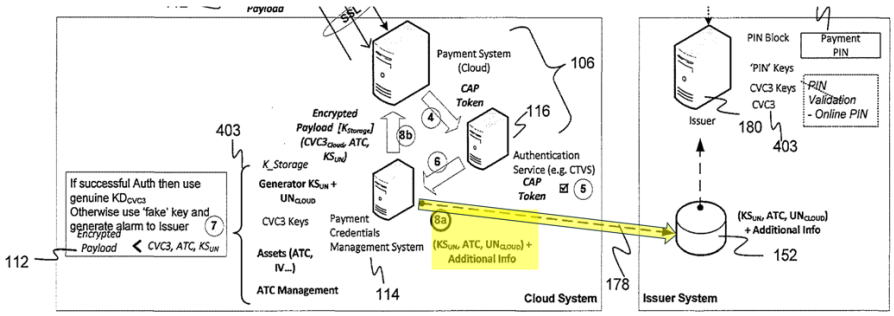
’248 Provisional (Ex. 1006), ¶0166

<table>
<tr>
<td></td>
<td>


’248 Provisional (Ex. 1006), Fig. 12A (annotated excerpt)
</td>
</tr>
<tr>
<td>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.</td>
<td>
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, Table 1 (p. 16)



’095 Provisional (Ex. 1005), Fig. 5 (annotated excerpt);
’095 Provisional, Figs. 6-7
</td>
</tr>
</table>

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)

“<u>Payload sent to the Issuer</u>
◊ 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:

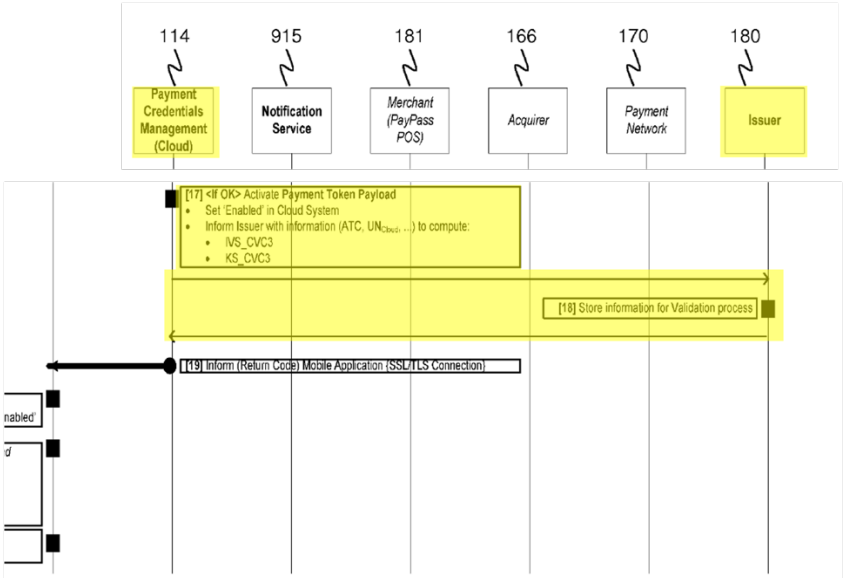
- $Cloud_CVC3_{TRACK1/2}$ (2 bytes)
- UN_{READER} (4 bytes)
- ATC (2 bytes)

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 (Ex. 1006), ¶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. "**<u>Fn ValCVC3</u>** 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 (Ex. 1006), ¶¶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)

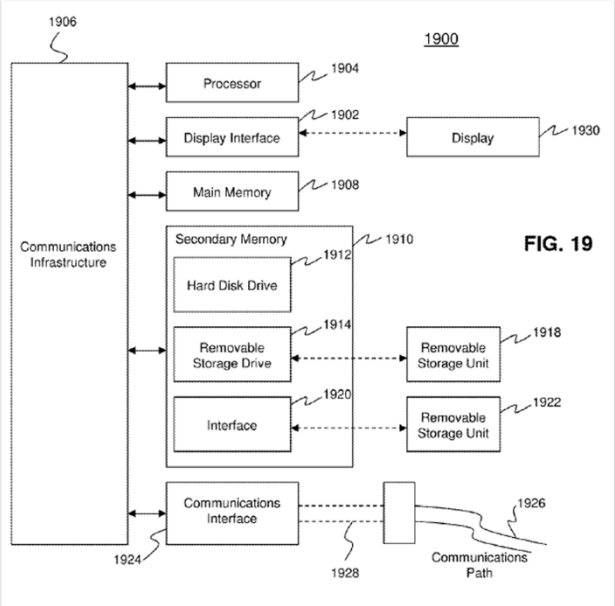
3. Support for Collinge in Collinge Provisionals

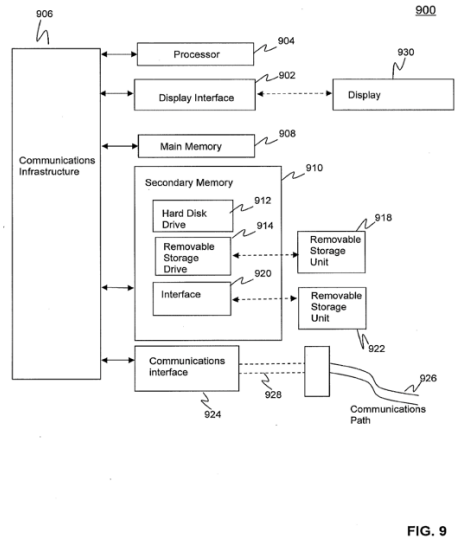
84. I have been informed that for Collinge to be §102(e) prior art as of the filing date of the Collinge Provisionals, the Collinge Provisionals must provide written description support for the subject matter relied upon in the petition. *See In re Giacomini*, 612 F.3d 1380, 1383 (Fed. Cir. 2010). "To 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*)."

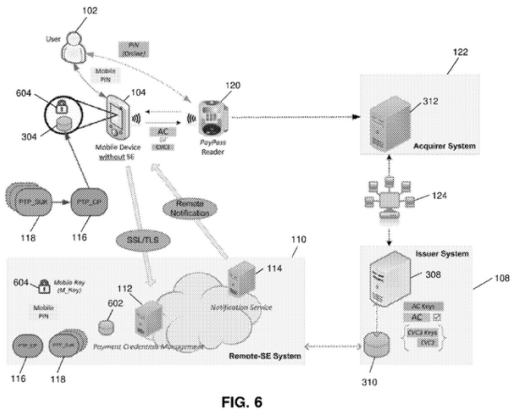
85. My opinion relies on many disclosures from Collinge, each of which a POSITA would have understood to be disclosed by the Collinge Provisionals.

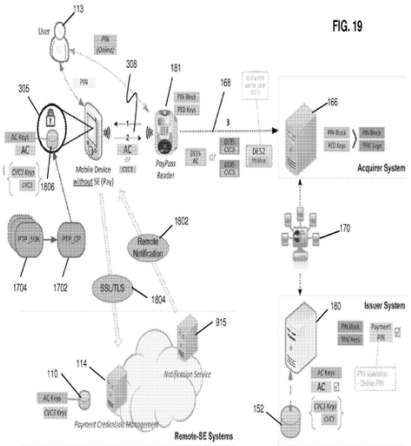
86. All portions of Collinge cited in the proposed grounds below appear substantially identically in Collinge Provisionals. I have endeavored to include citations to corresponding disclosures in the Collinge Provisionals below. Accordingly, the disclosure relied on to meet challenged claim limitations 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.





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]. A POSITA would have found it obvious and would have been motivated to incorporate these disclosures into Collinge's payment system because implementing Collinge's payment system requires various display screens with user-selectable softbuttons and Collinge's Provisional provide details regarding layout and softbutton functions that would assist a POSITA in implementing Collinge's teachings with a reasonable chance of success. *'248 Provisional (Ex. 1006),* Fig. 2B.

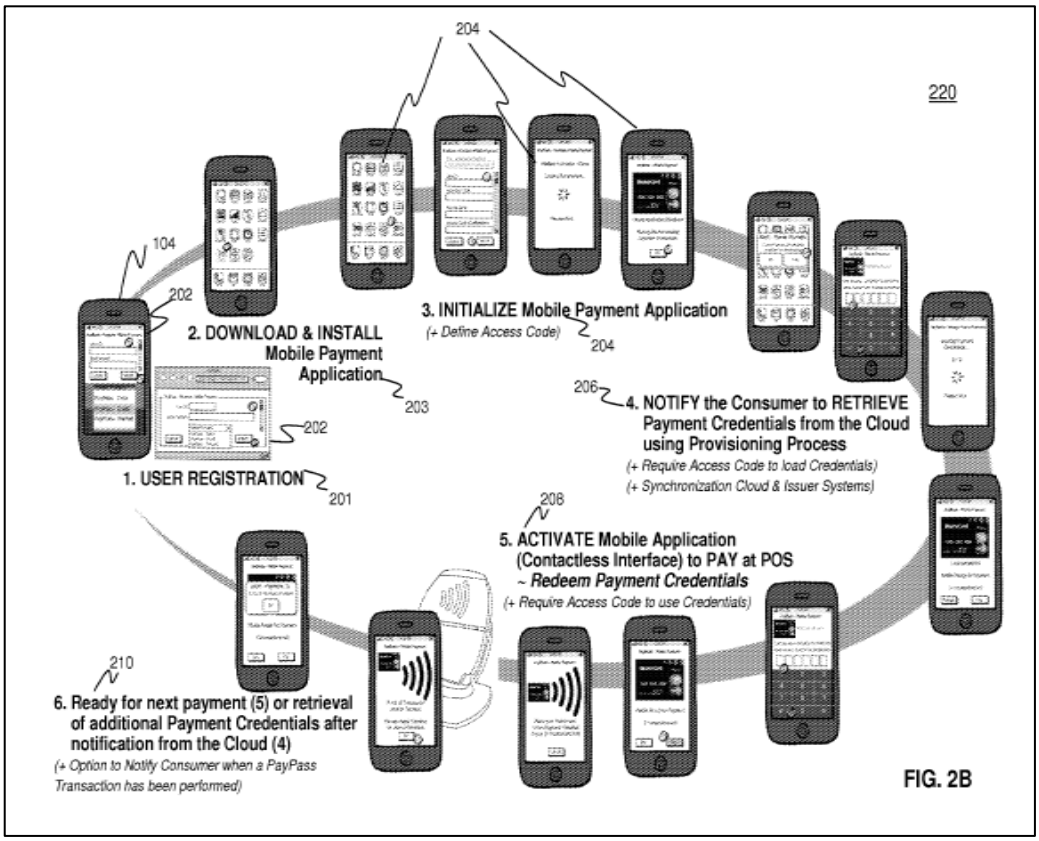


FIG. 2B

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

B. Lin

87. 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.

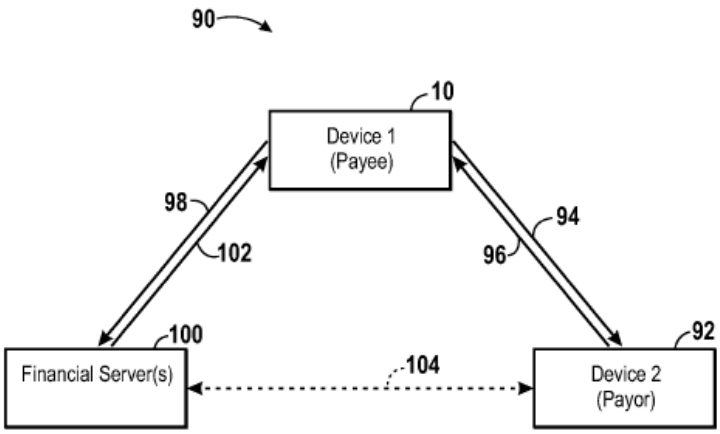


FIG. 4

Lin at Figure 4.

88. 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.

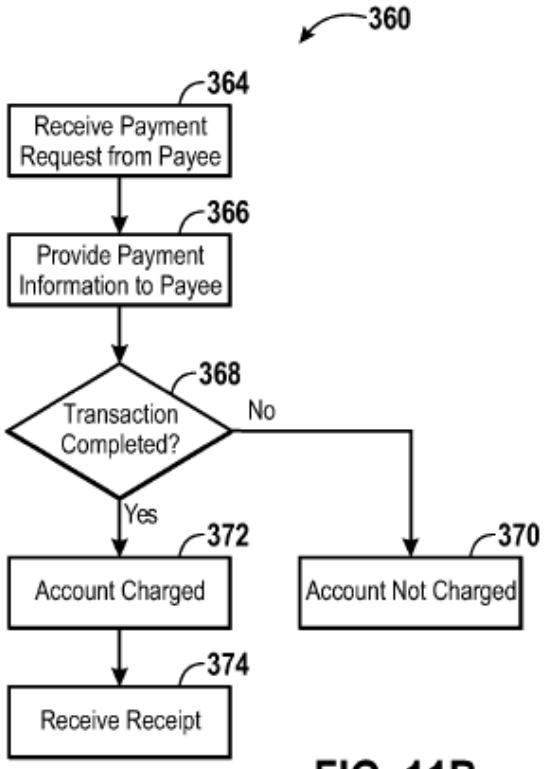


FIG. 11B

Lin at Figure 11B.

89. 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.

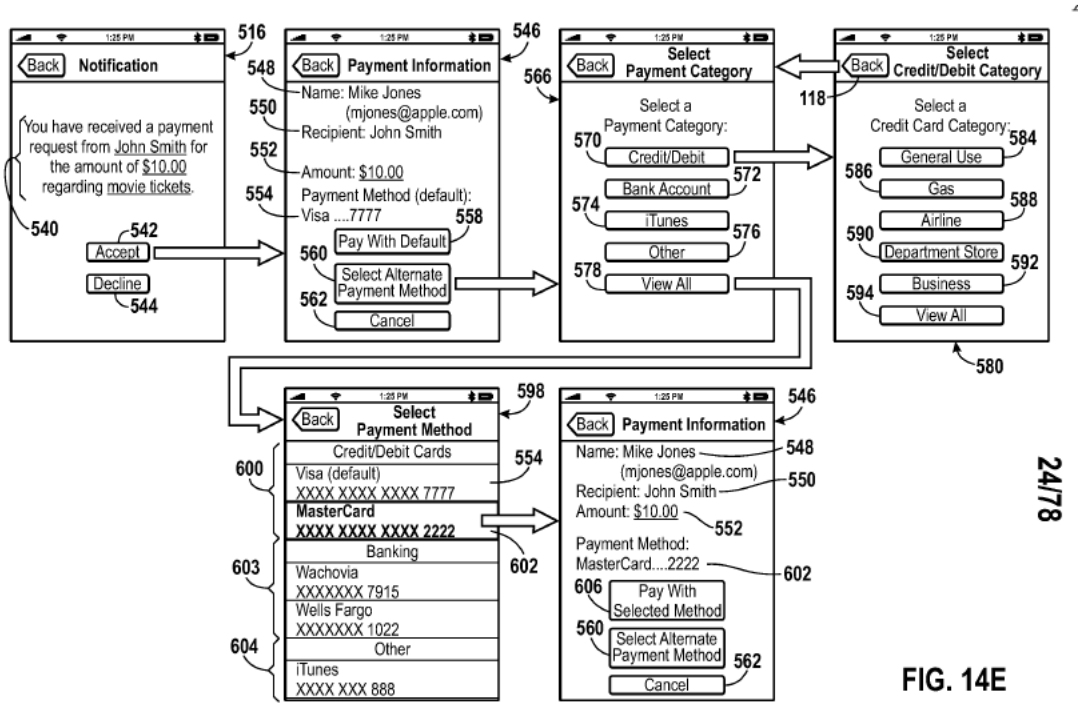


FIG. 14E

Lin at Figure 14E.

1. Lin is Analogous

90. Lin is analogous art to the '634 Patent because it is from the same field of endeavor. Like the '634 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 '634 patent* at Abstract, 1:31-26, Fig. 1 *with Lin* at Abstract, 68:13-25, Fig. 14C.

91. Lin is also reasonably pertinent to at least one problem addressed by the '634 Patent. Like the '634 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 '634 Patent,* 1:31-26, 2:4-12, 9:63-10:2 *with Lin*, 26:26-28-15.

C. Sahota

92. Sahota teaches "[m]ethods and systems for dynamically generating a verification value for a transaction and for utilizing such value to verify the authenticity of the payment service application." *Sahota* at Abstract. Referring to Figure 1, "the method of generating a dCVV for each transaction[,]" Sahota describes "[i]nitially, a numeric string of predetermined length is created. This numeric string is created by overlaying 101 the ATC 102 over the corresponding

leftmost digits of the account number for the payment service or PAN 104." *Sahota* at [0029]. Regarding the ATC, Sahota teaches the "payment device will also maintain an application transaction counter (ATC). The ATC will initially be set by the service provider to a predetermined value. Thereafter, the ATC will be incremented with each transaction." *Sahota* at [0028].

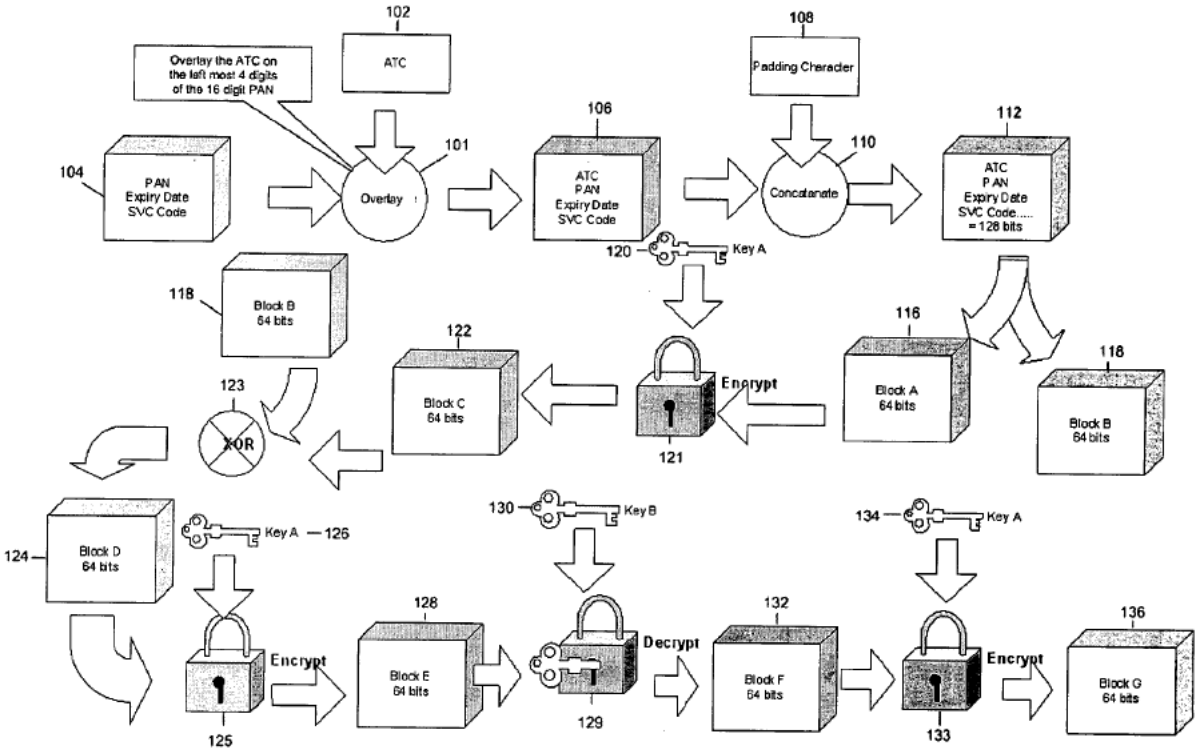


FIG. 1

Sahota at Figure 1.

93. During a payment transaction, if "the service provider computer determines that the transaction was contactless, the service provider computer compares the ATC received from the payment device to the corresponding ATC

stored on the service provider computer to determine if the received ATC is the expected next ATC 365. If the ATC received from the payment device is not the expected next ATC, the payment service deployed on the payment device has potentially been skimmed 640." *Sahota* at [0038].

1. Sahota is Analogous

94. Sahota is analogous art to the '634 Patent because it is from the same field of endeavor. Like the '634 Patent, Sahota is concerned with conducting secure payment transactions. *See, e.g., Sahota* at Abstract ("The embedded verification value is used by a service provider to verify the authenticity of the transaction."), [0008] ("The transaction is disapproved if the service provider generated verification value does not match the payment device generated verification value."), Figure 1. *Compare '634 patent*, Abstract, 1:26-31, Fig. 1 *with Sahota,* Abstract, [0008], Fig. 1.

95. Sahota is also reasonably pertinent to at least one problem addressed by the '634 Patent. Like the '634 Patent, Sahota is concerned with increasing security of payment transactions. *See, e.g., Sahota* at [0004] ("Also, one of the more insidious forms of skimming involved line tapping wherein the communication lines between the terminal and the credit card issuer is tapped and the card data extracted from the communications string."), [0021] ("…provides methods and systems for dynamically generating a card verification value for each transaction and for

utilizing such value to verify that the payment service is authentic and has not been skimmed."), [0028] ("…this corresponding ATC is used to identify payment services which may have been skimmed. In an alternate embodiment, a cryptogram, digital signature, or hash value based on a transaction data may be used in place of or in conjunction with the ATC."). *Compare '634 Patent,* 1:66-2:3 *with Sahota*, [0004], [0021], [0028].

D. Smith

96. 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.

97. 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].

600

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

FIG. 6

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

1. Smith is Analogous

98. Smith is analogous art to the '634 Patent because it is from the same field of endeavor. Like the '634 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]. *Compare '634 patent*, Abstract, 1:26-31, Fig. 1 *with Smith,* Abstract, [0021]-[0023].

99. Smith is also reasonably pertinent to at least one problem addressed by the '634 Patent. Like the '634 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 '634 Patent,* 1:66-2:3 *with Smith*, [0002], [0015], [0020].

E. Kranzley

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

1. Kranzley is Analogous

101. Kranzley is analogous art to the '634 Patent because it is from the same field of endeavor. Like the '634 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

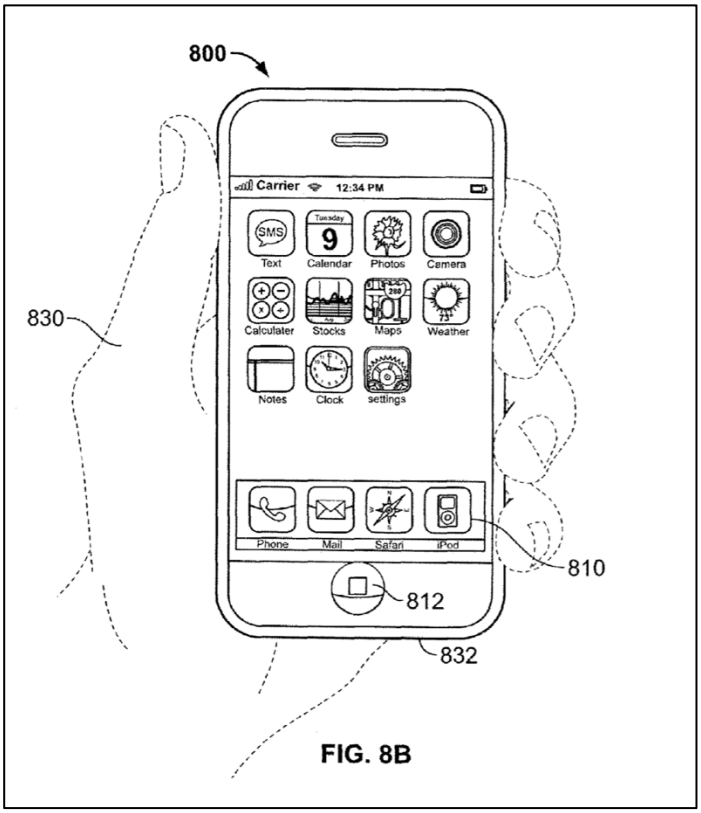
which include…a dynamic verification code generated by the payment application[.]"), [0003] ("It would further be desirable to provide mobile payment transactions which are secure and in which the cardholder's presence may be confirmed."), [0010] ("…and means for conducting a payment transaction include…at 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 '634 Patent*, Abstract, 1:26-31, Fig. 1 *with Kranzley,* Abstract, [0010], Fig. 1.

102. Kranzley is also reasonably pertinent to at least one problem addressed by the '634 Patent. Like the '634 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 ‘634 Patent,* 1:66-2:3 *with Kranzley*, [0003], [0065].

F. Fadell

103. 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].



Fadell at Figure 8B.

104. 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].

1. Fadel is Analogous

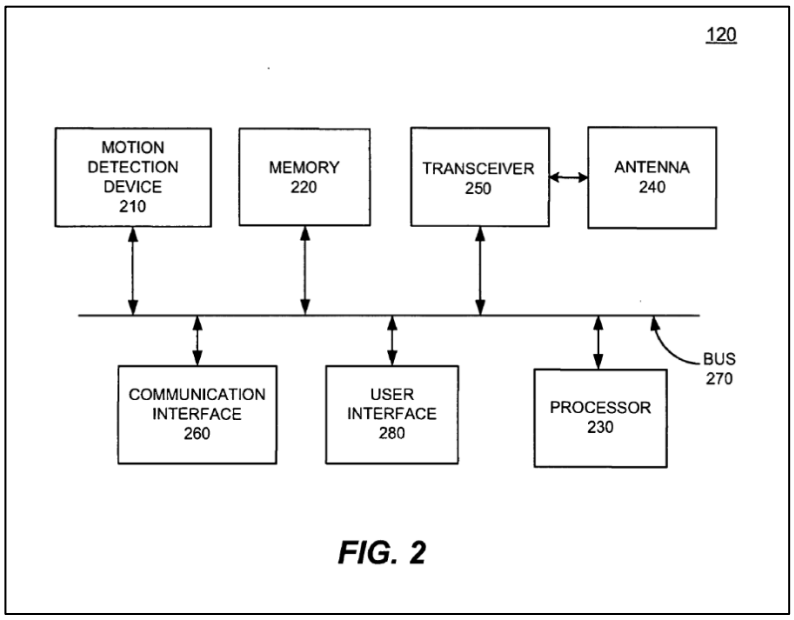
105. Fadell is analogous art to the '634 Patent because it is from the same field of endeavor. Like the '634 Patent, Fadell is concerned with authentication systems for an electronic device such as a mobile phone, including authenticating a user for accessing restricted information such as "transaction 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 '634 patent* at Abstract, 1:26-31, 11:63-12:12, Fig. 1 *with Fadell* at Abstract, [0031].

106. Fadell is also reasonably pertinent to at least one problem addressed by the '634 Patent. Like the '634 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 '634 Patent,* 1:66-2:3, 11:63-12:12 *with Fadell*, [0004], [0054], [0064].

G. Yu

107. Yu teaches a "mobile device" that includes a "motion detection device 210[.]" *Yu* at [0027].



Yu, Fig. 2.

108. Yu's mobile phone motion detection device "can comprise one or more accelerometers, gyros, inclinometers, cameras, tilt sensors, or any other sensors that can determine the motion of a device within N degrees of freedom[.]" *Yu* at [0028].

The output of the "motion detection device 210 can be processed by processor 230 with instructions in memory 220 to extract features from the movement of the mobile device to verify both the identity and presence of a mobile user." *Yu* at [0028]. If the user is verified "control passes to action 410 for further processing. In action 410 access to the service or device is granted. Access includes providing admission to mobile internet services, mobile banking or e-commerce, usage of the mobile communication device 120, usage of selected services or software in the device, or right to use selected hardware resources." *Yu* at [0038].

1. Yu is Analogous

109. Yu is analogous art to the '634 Patent because it is from the same field of endeavor. Like the '634 Patent, Yu is concerned with authentication systems for an electronic device such as a mobile phone, including secure systems for accessing "mobile banking or e-commerce[.]" *Yu* at [0038]. *See, e.g., Yu* at [0004] ("Mobile applications and services including mobile commerce, banking, and blogging or messaging often require authentication of the mobile user accessing them."), [0025] ("A mobile device such as mobile communication device 120 can further include a transceiver to access one or more services 130 over network 110. A service often requires user authentication. Instances of services 130 include mobile commerce, banking…"). *Compare '634 patent* at Abstract, 1:26-31, Fig. 1 *with Yu* at [0004], [0025].

110. Yu is also reasonably pertinent to at least one problem addressed by the '634 Patent. Like the '634 Patent, Yu is concerned with increasing security of payment transactions. *See, e.g., Yu* at [0008] ("A user is authenticated only if the two values coincide."); [0018] ("The user's motion patterns can be extracted from data captured by the motion sensors and then used as part of the authentication protocol."): [0038] ("If the user is verified "control passes to action 410 for further processing. In action 410 access to the service or device is granted. Access includes providing admission to mobile internet services, mobile banking or e-commerce, usage of the mobile communication device 120, usage of selected services or software in the device, or right to use selected hardware resources.") *Compare '634 Patent,* 1:66-2:3 *with Yu*, [0007]-[0008], [0018], [0038].

VIII. SUMMARY OF UNPATENTABILITY

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

Ground	Claim(s)	References
1	1-2, 7-11, 15, 27-28, 39, 41, 44-46, 49-50, 55-56, 60-63, 66-67, 72	Collinge, Lin, Sahota
2	29, 3-6, 17-24, 30-32, 34-38, 40, 42, 47, 57-58, 64	Collinge, Lin, Sahota, Smith
3	25-26, 33, 43, 48, 59, 65	Collinge, Lin, Sahota, Smith, Kranzley
4	10, 12-13, 16, 51-53, 68-70	Collinge, Lin, Sahota, Fadell
5	10, 14, 54, 71	Collinge, Lin, Sahota, Yu

IX. OPINIONS REGARDING GROUND 1: *COLLINGE IN VIEW OF LIN AND SAHOTA.*

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

112. Illustrated in Figure 14 below, Collinge teaches a method of generating and using a limited-use cryptogram for 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].

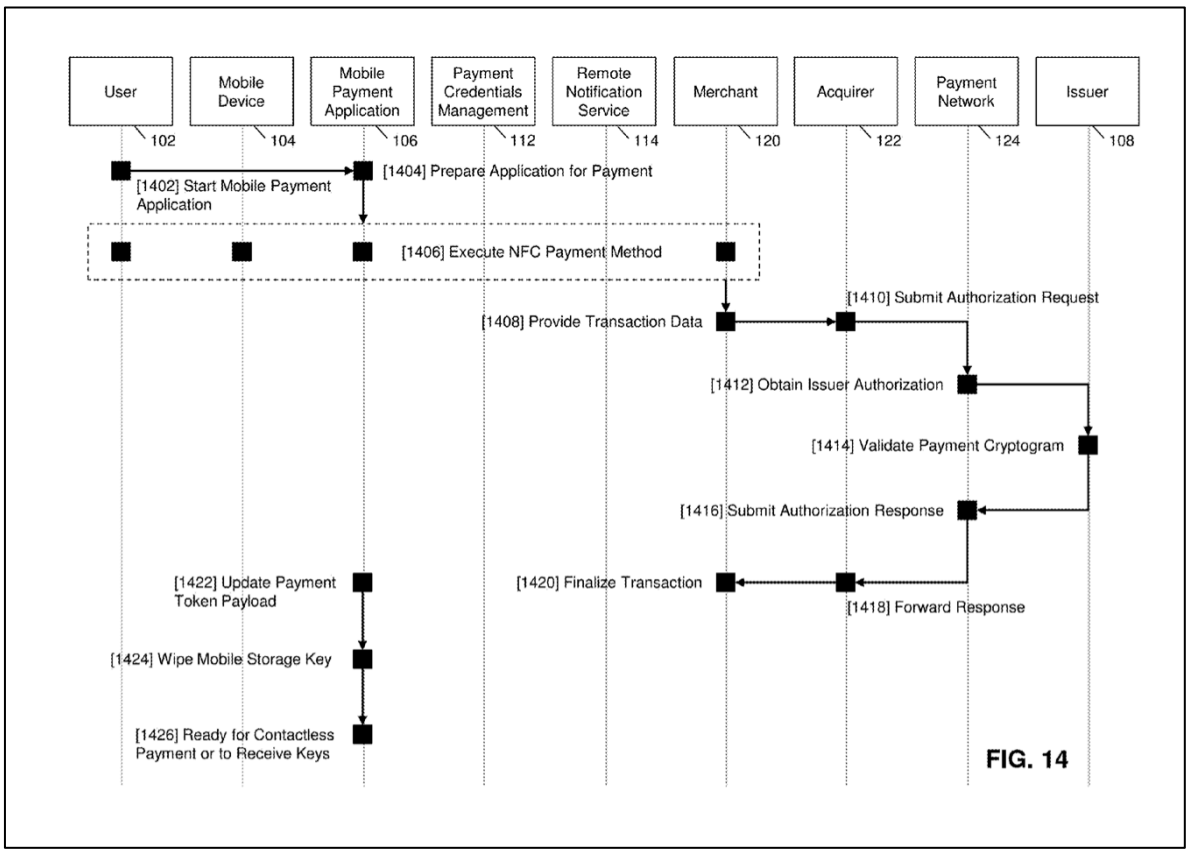


FIG. 14

Collinge at Figure 14.

113. 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].

114. 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].

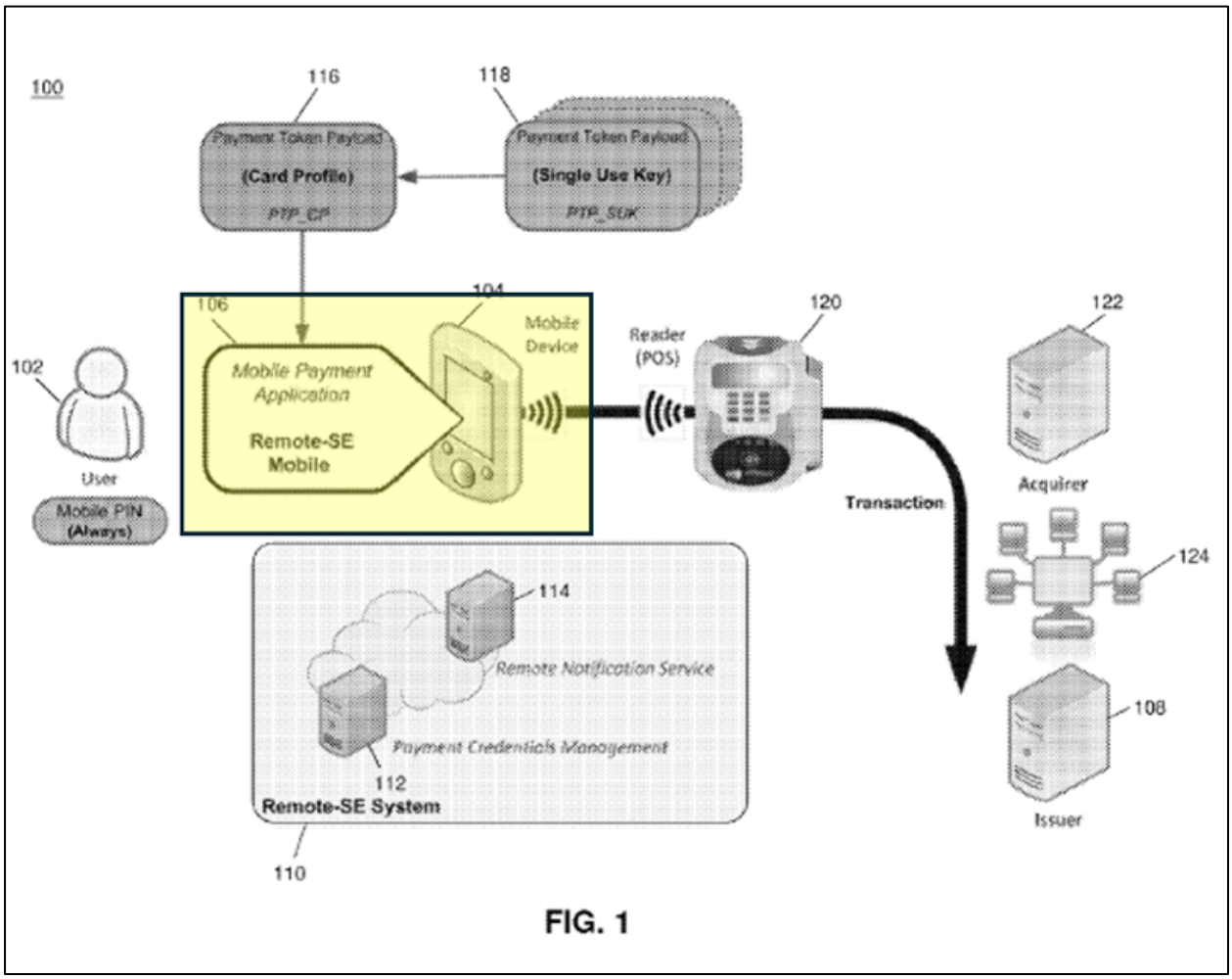


FIG. 1

Collinge, Fig. 1. (annotated)

115. 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].

116. 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*, [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*, [0121].

117. Described in more detail below, Collinge's CVC3 payment cryptogram is *limited-use payment information* because it is "valid for a single payment transaction[.]" *Collinge,* [0050], [0077], [0135], [0128].

118. Thus, because Collinge teaches "generat[ing] a payment cryptogram for use in the payment transaction" and because the payment cryptogram is used by the issuer to approve or deny a payment transaction, Collinge teaches *a method of generating and using limited-use payment information for performing a payment transaction*. *Collinge,* [0119], [0121].

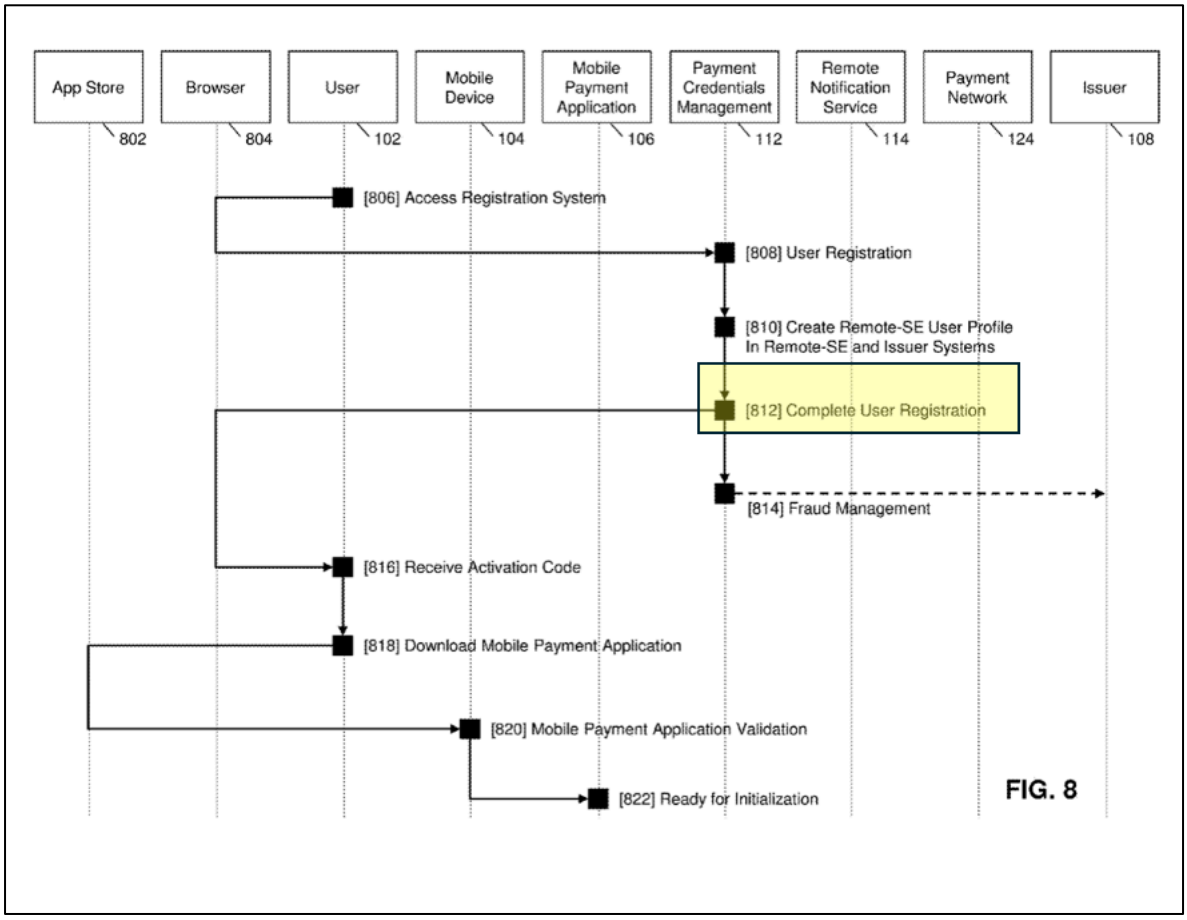
2. 1(a): "receiving an input at an electronic device, wherein the input comprises a priming operation, and, wherein the electronic device comprises:"

119. 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,* [0089].

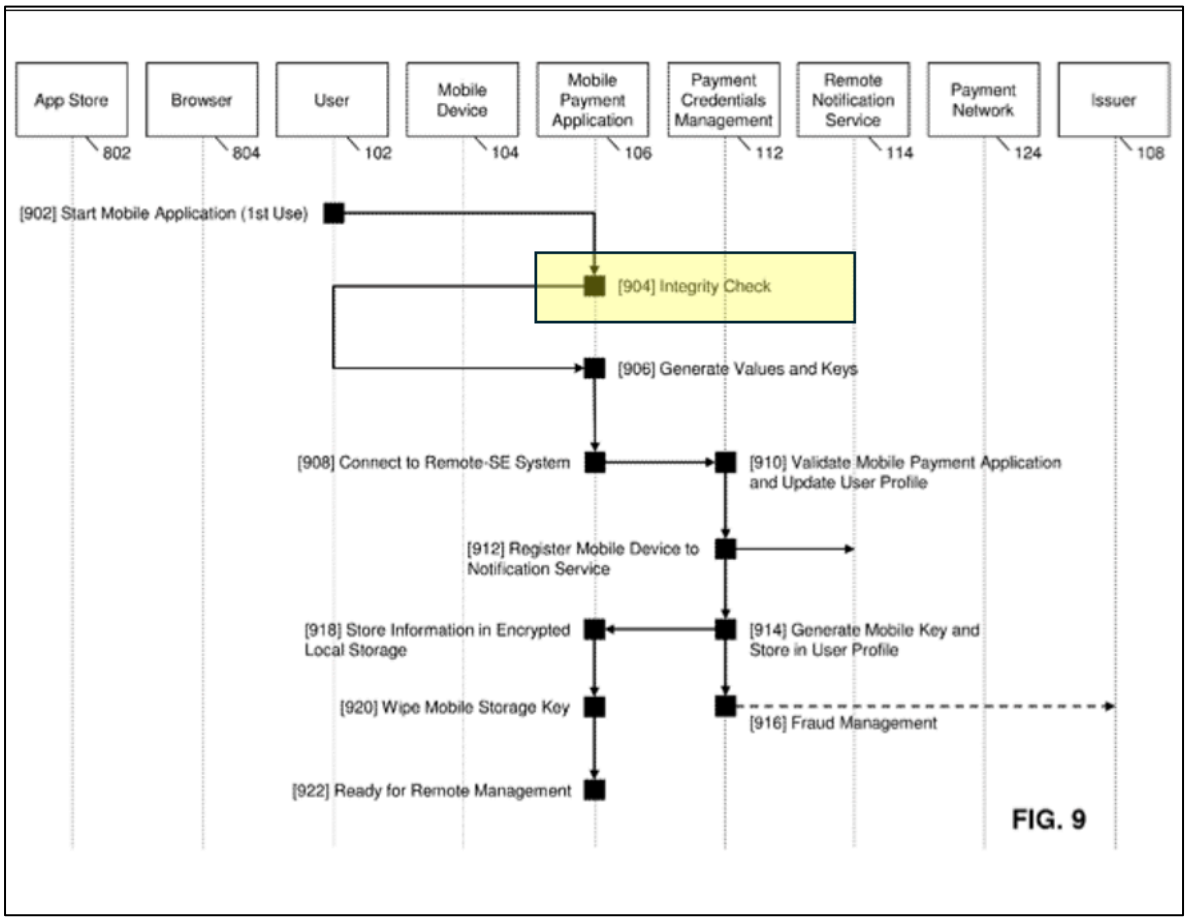
120. At step 808 "the user 102 may register with the payment credentials management service 112" then the payment credentials management service 112 "may create a user profile for the user 102[.]" *Collinge,* [0090]. "As part of the creation of the user profile, the payment credentials management service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

121. 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,* [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,* [0093], Figure 9.



Collinge, Fig. 8. (annotated)



Collinge, Fig. 9.

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

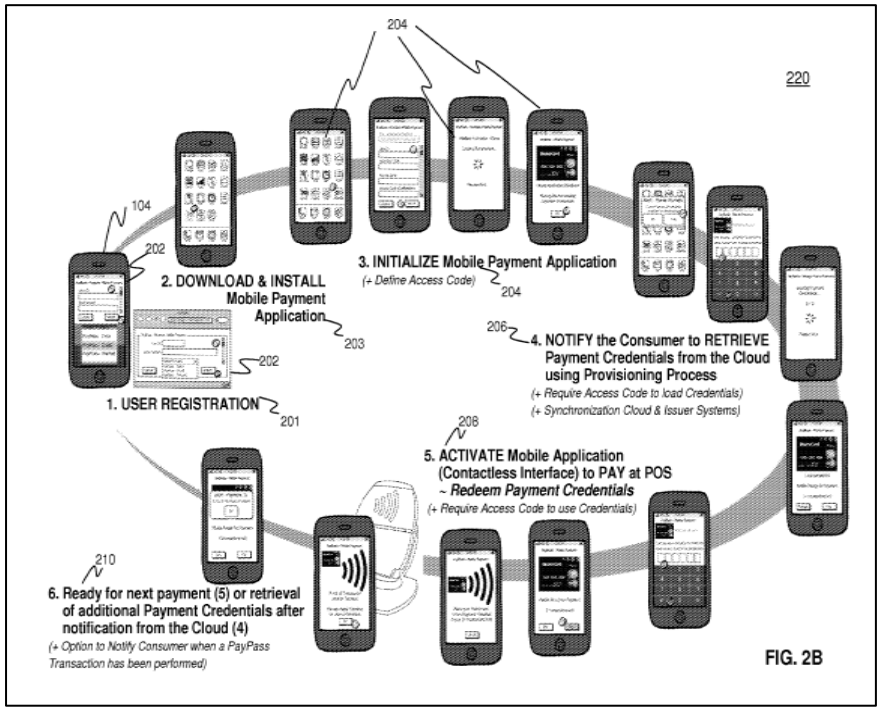


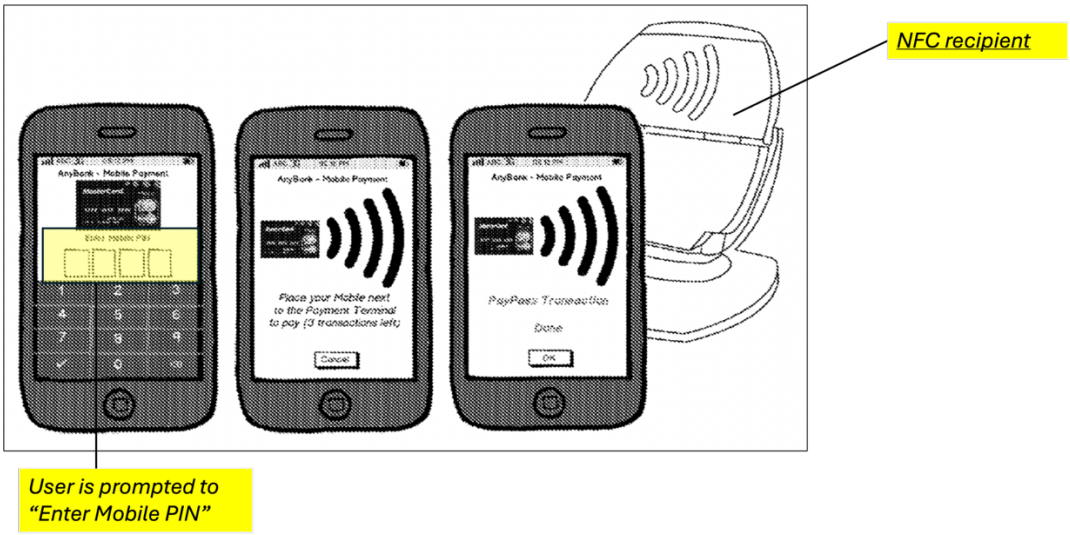
FIG. 2B

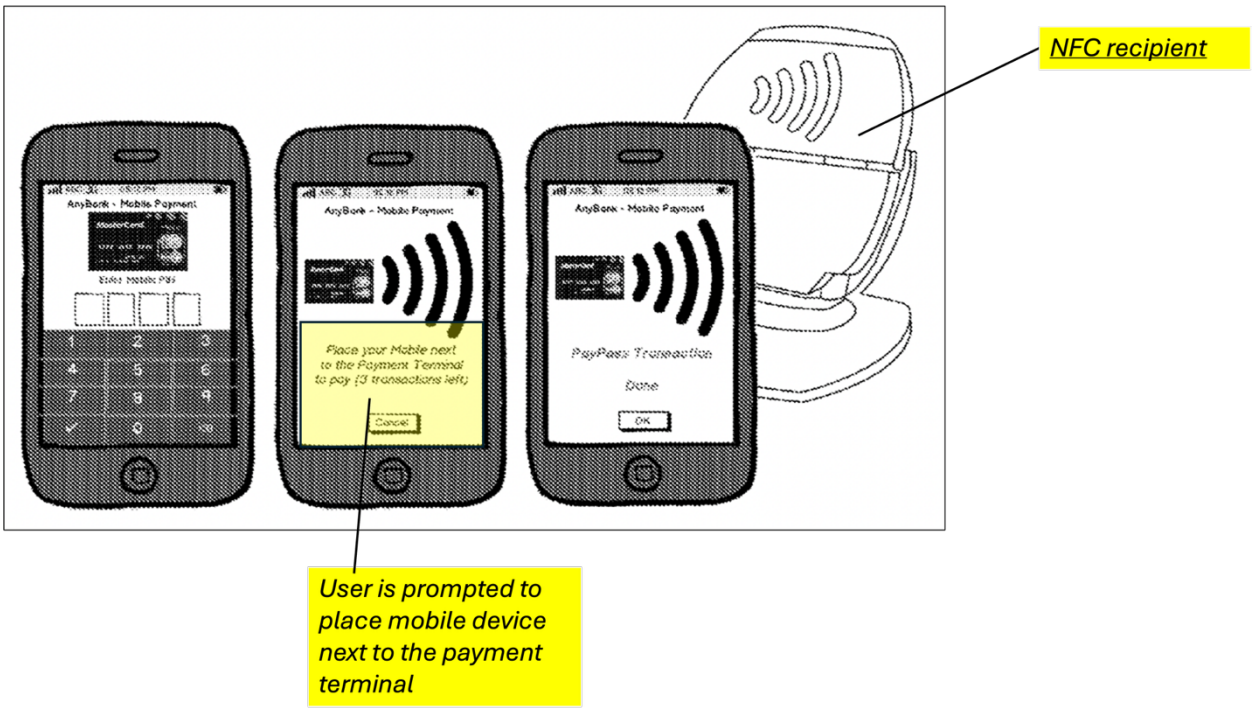
'248 Provisional (Ex.1006) at Figure 2B. As shown above, Collinge teaches the correct access code is required to load credentials. *'248 Provisional*, Fig. 2B.

123. Collinge teaches receiving an activation code (i.e., *input*) at the mobile device 104 (*electronic device*). A POSITA would have further understood that inputting an activation code by the user is a *priming operation*. The '634 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…" *'634 Patent* at 12:4-6. 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 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*.

124. 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.

125. 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)*, p. 99. A POSITA would have understood that input of "a mobile personal identification number (PIN)" before a payment cryptogram is generated is a *priming operation* because after the PIN is input, the mobile device is primed to perform a payment transaction. *Collinge,* [0133]. Using mobile device 104, the user "must always provide the Mobile PIN for all PayPass transactions[.]" *'098 Provisional (Ex.1008),* p. 99.

126. A POSITA would have further understood that bringing mobile device 104 in proximity to point-of-sale terminal 120 (NFC recipient) further may form part of a *priming operation* because it is part of preparing mobile device 104 to complete a payment transaction, thus priming mobile device 104. 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 is

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.

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

127. 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").

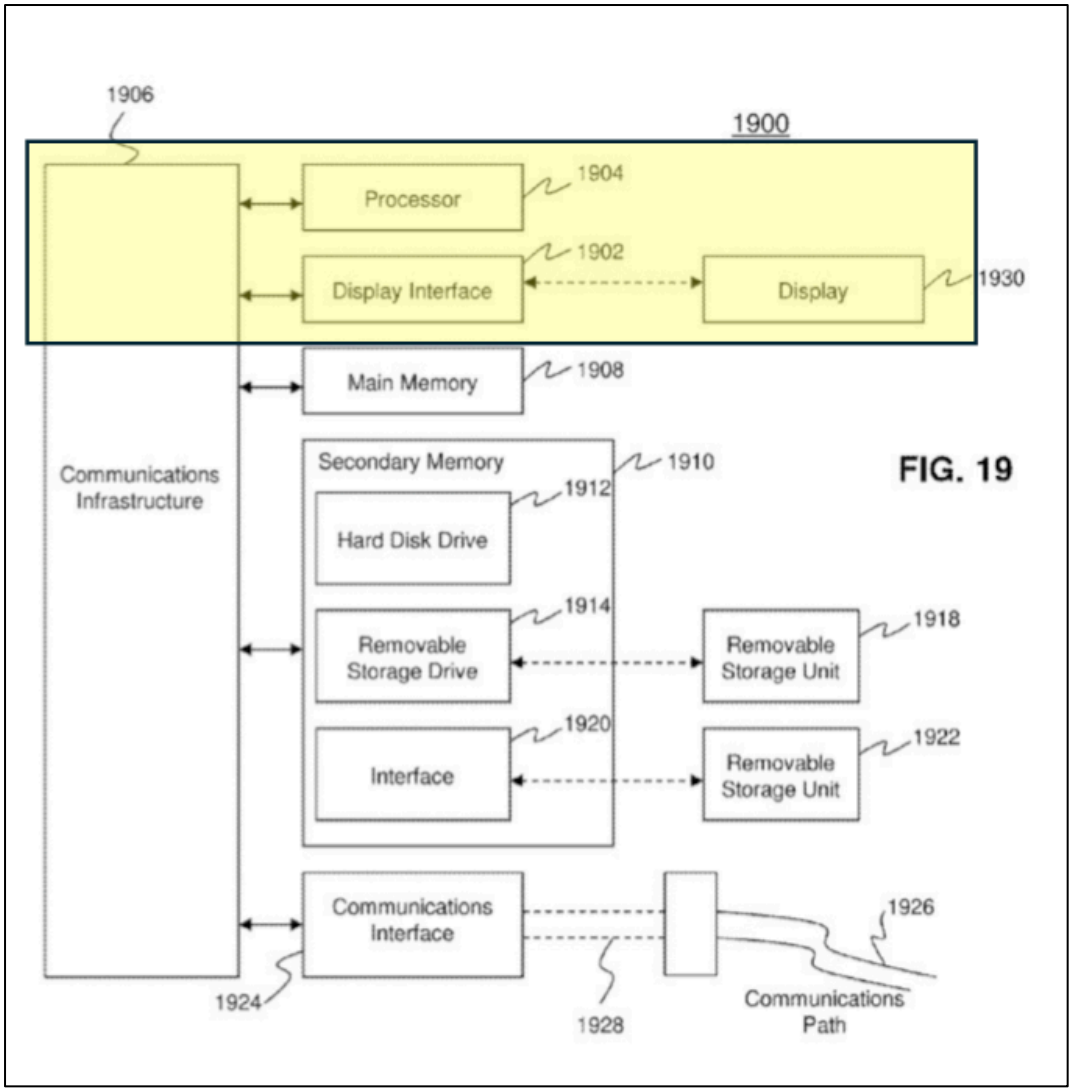
4. 1(a)(2): "a touch-screen display coupled to the processor; and"

128. 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. *See* Claim 1(a)(a). Therefore, Collinge's touch screen is a user input device.

129. 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,* [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*.

130. 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. (Ex.1042, "Hotelling") teaches that "[t]he computer system 50 also includes a touch screen 70 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.

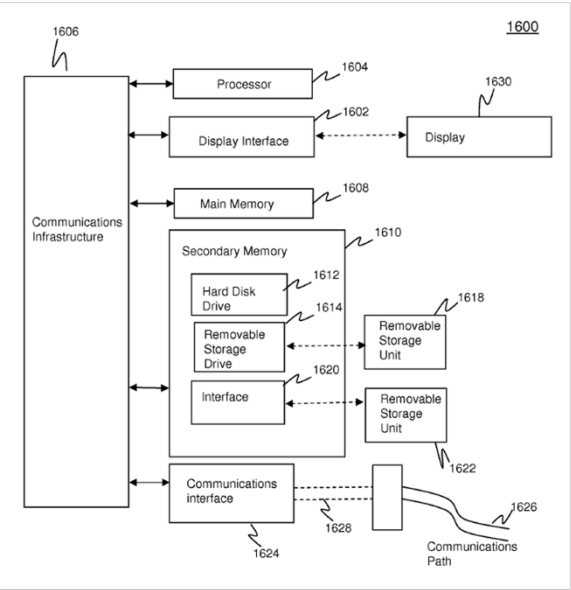
131. Additionally, Collinge teaches that "at least one processor device" is used to implement Collinge's payment system. *Collinge,* [0147]. System 1900, shown in Figure 19 below, further confirms that the mobile device 104's touch screen is "coupled" to the processor by the communications infrastructure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

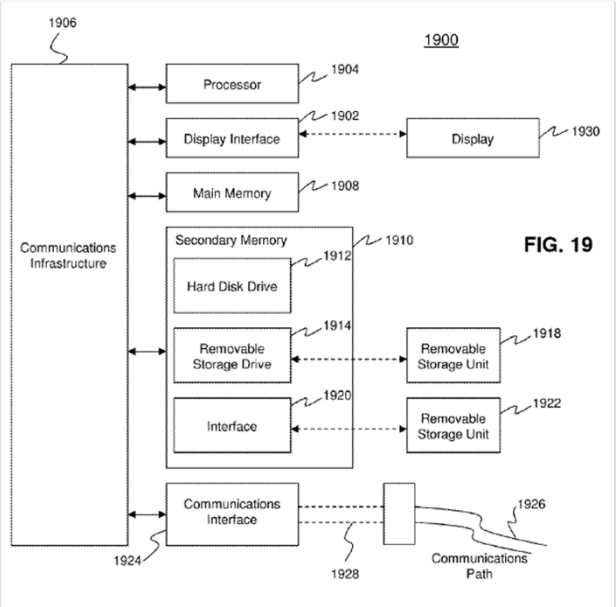


Collinge at Figure 19 (annotated).

132. 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].

133. 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).

134. 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].

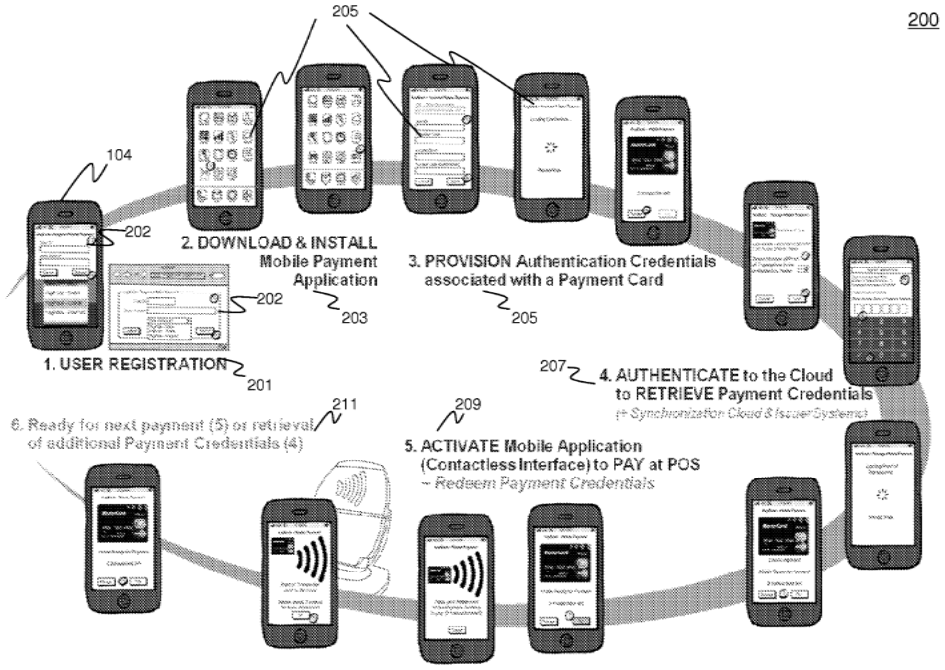


FIG. 2A

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

135. 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 corresponds to a processor 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 applies to mobile device 104 (the *electronic device*).

136. Additionally, a POSITA would have understood that in Figure 19, display interface 1902 is Collinge's touchscreen. It was well-known that a touch screens of a mobile device was used for 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 allow 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.

137. 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. Therefore, Collinge teaches a user interface (display) coupled to a processor.

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

138. Collinge teaches that "system 100…enable[s] the user 102 to use the mobile device to conduct NFC payment transactions[.]" *Collinge,* [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, and 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],[0120].

139. 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. Paus (Ex.1040), 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.* 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.

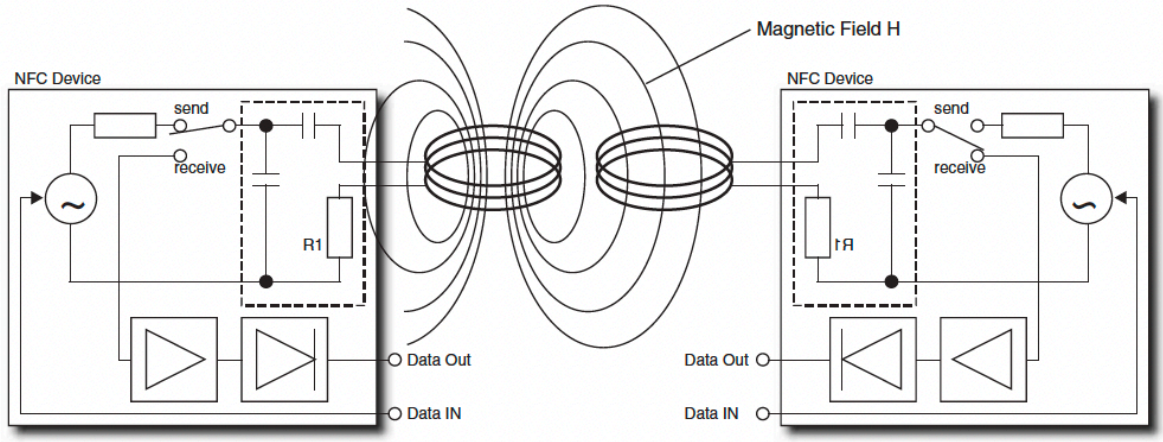
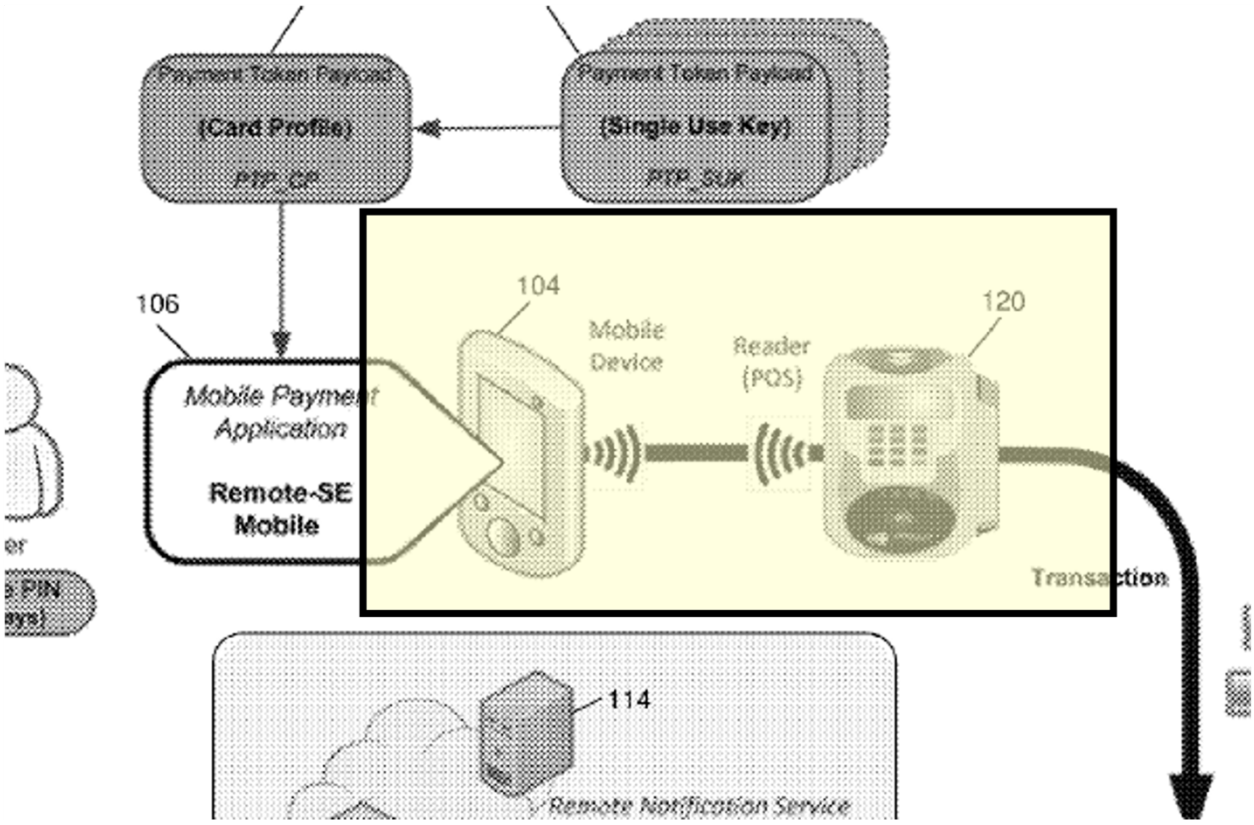


Figure 3.32 In active mode, the NFC interfaces alternately emit magnetic fields for data transmission

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 (Ex.1040),* 5.

140. 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),* [0067], [0184]. For this additional reason, Collinge teaches the mobile device 104 (*the electronic device*) having *a near field communications (NFC) interface*.



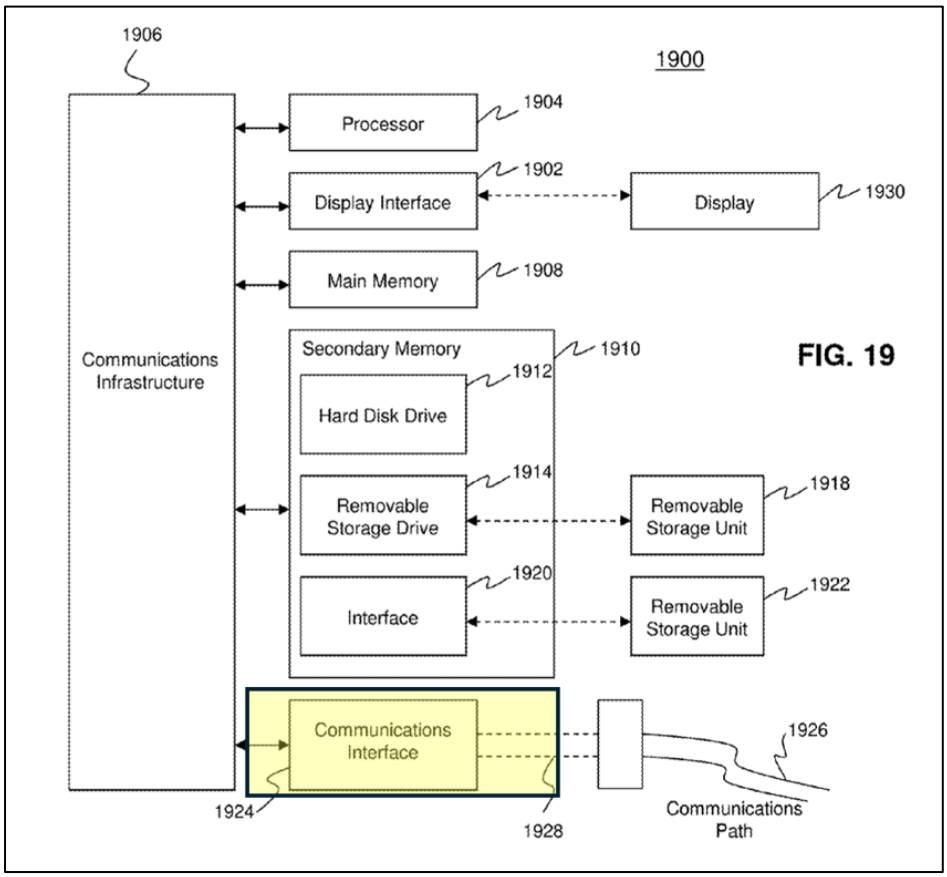
Collinge at Figure 1 (illustrating mobile device 104 communicating with a merchant point-of-sale terminal 120) (annotated excerpt).

141. A POSITA would understand that Collinge's NFC interface is coupled to the processor of mobile device 104. Collinge 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 <u>*processor*</u>). *Collinge,* [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.

142. 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 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.

143. 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).

144. "The communications interface 1924 may be configured to allow software and data to be transferred between the computer system 1900 and external devices[.]" *Collinge,* [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,* [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*.

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

145. In Claim 1(a) a user of mobile device 104 with mobile payment application 106 inputs an activation code to the mobile device 104 as part of "the integrity check" performed by mobile payment application 106 to authenticate user 102. *Collinge* at [0067], [0093]. As I discussed above in Claim 1(a), the user inputting the activation code is a *priming operation*.

146. Regarding Figure 5, which illustrates "a method 500 for initialization and use of the mobile payment application 106 in the mobile device 104[,]" Collinge teaches that after the user 102 enters the activation code (step 506), the "remote-SE system 100" transmits card profile 116 and single use key 118 to the mobile payment application 106. *Collinge,* [0068]-[0069]. Transmission of card profile 116 (step

508) and single use key 118 (step 510) is followed by step 512, where "the mobile device 104 may conduct a contactless/NFC payment transaction using the mobile payment application 106 and the single use key 118." *Collinge,* [0070].

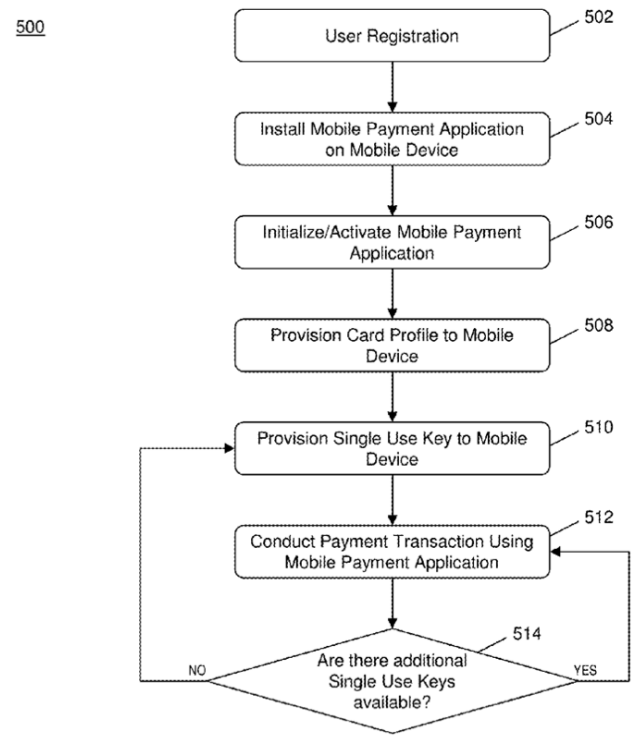


FIG. 5

Collinge at Figure 5. *See also* Figures. 9, 14.

147. In other words, Collinge teaches that responsive to the user inputting the activation code (*priming operation*), card profile 116 and single use key 118 are transmitted to mobile device 104. The transmission of card profile 116 and single use key 118 *read[ies] said device to perform a payment transaction by an identified*

user. As I described above, the user of mobile device 104 is authenticated by input of the activation code. *See* Claim 1(a). Transmission of card profile 116 and single use key readies mobile device 104 to perform a payment transaction because as shown in Figure 5, after steps 508 and 510, a payment transaction is conducted using mobile payment application 106, which is executed by the processor of mobile device 104. *Collinge* at Figure 5, [0041]. A POSITA would further understand that transmission of card profile 116 and single use key 118 readies mobile device 104 for a payment transaction because Collinge teaches that "[t]o prepare for payment, the mobile payment application 106 may…retrieve the payment credentials and generating key from the card profile 116 and the single use key 118[.]" *Collinge* at [0119]. Thus, card profile 116 and single use key 118 are required to conduct a payment transaction. As such, because Collinge teaches that card profile 116 and single use key are transmitted to mobile device 104 in response to the user inputting the activation code, and because card profile 116 and single use key are needed to prepare for a payment transaction, Collinge teaches *responsive to said priming operation, readying said device to perform a payment transaction by an identified user*.

148. Collinge teaches an additional priming operation, where the user of mobile device 104 inputs a PIN into mobile device 104 and then is instructed to position mobile device 104 next to the payment terminal. *See* Claim 1(a). A POSITA

would have understood that responsive to the user inputting the PIN and placing the mobile device next to the payment terminal (*responsive to said priming operation*), that mobile device 104 is readied to perform a payment transaction. The '098 Provisional (Ex.1008) expressly teaches that the "user must always provide the Mobile PIN for all PayPass Transactions[,]" so a POSITA would have understood that if the PIN is not provided, or if an incorrect PIN is provided, the payment transaction would not be completed. Thus, the user inputting the PIN and placing mobile device 104 next to the payment terminal *read[ies] said device to perform a payment transaction* because inputting the PIN and placing the mobile device next to the payment terminal is required to successfully complete a payment transaction. Additionally, a POSITA would have understood that the user is an *identified user* because both the correct activation code and correct PIN are known by the authenticated user.

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

a) Collinge's Teachings

149. Collinge teaches that mobile device 104 (*said electronic device*) may communicate with a point-of-sale terminal 120. *See, e.g., 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."),

[0070] ("The mobile payment application 106 may generate a payment cryptogram…and may transmit the generated cryptogram and payment credentials to a point-of-sale terminal 120."), Figure 1. Notably, Collinge teaches that mobile device 104 may receive data from a point-of-sale terminal 120. *Collinge* at [0145] ("…a reader unpredictable number may be received, via near field communication, form a point-of-sale terminal (e.g., the point-of-sale terminal 120).")

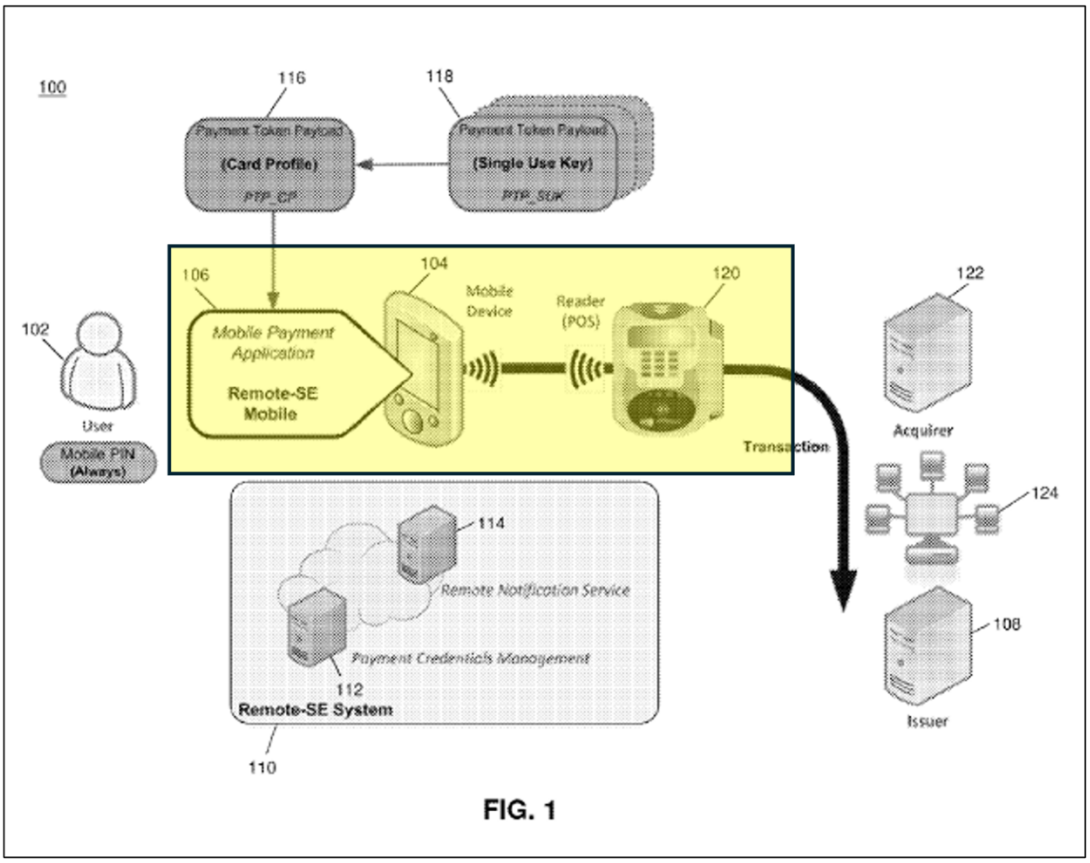


FIG. 1

Collinge at Figure 1 (illustrating mobile device 104 communication with point-of-sale terminal 120).

150. Mobile device 104 and point-of-sale terminal 120 may communicate to conduct a payment transaction. *Collinge* at [0120] ("In step 1406, a NFC payment method be executed between the user 102, the mobile device 104, the mobile payment application 106, and the point-of-sale terminal 120."), *see also Collinge,* [0145]. However, Collinge does not expressly teach how the transaction is initiated.

b) Lin's Teachings

151. Lin teaches techniques for "carrying out peer-to-peer financial transactions using one or more electronic devices 10, 92[.]" *Lin,* 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,* 30:18-19. "Initially, the payee device 10 may transmit a payment request, illustrated herein by reference numeral 94, to the payor device 92." *Lin,* 30:19-21.

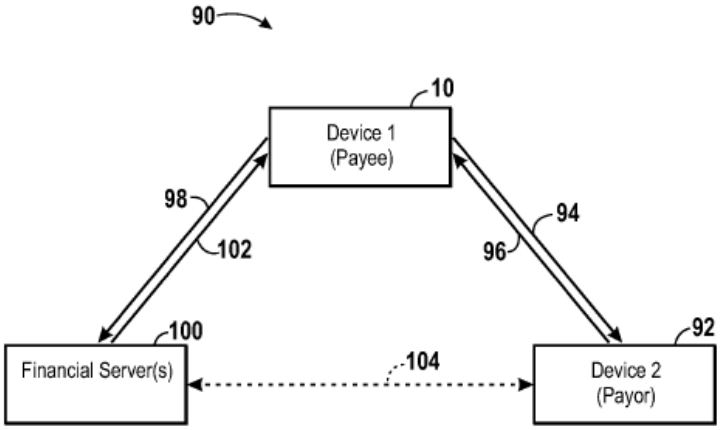


FIG. 4

Collinge at Figure 4.

152. 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,* 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,* 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,* 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,* 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,* 52:27-30. Because Lin teaches a payor device receiving a payment request from a payee device, Lin teaches *receiving a payment request for the payment transaction at said electronic device*.

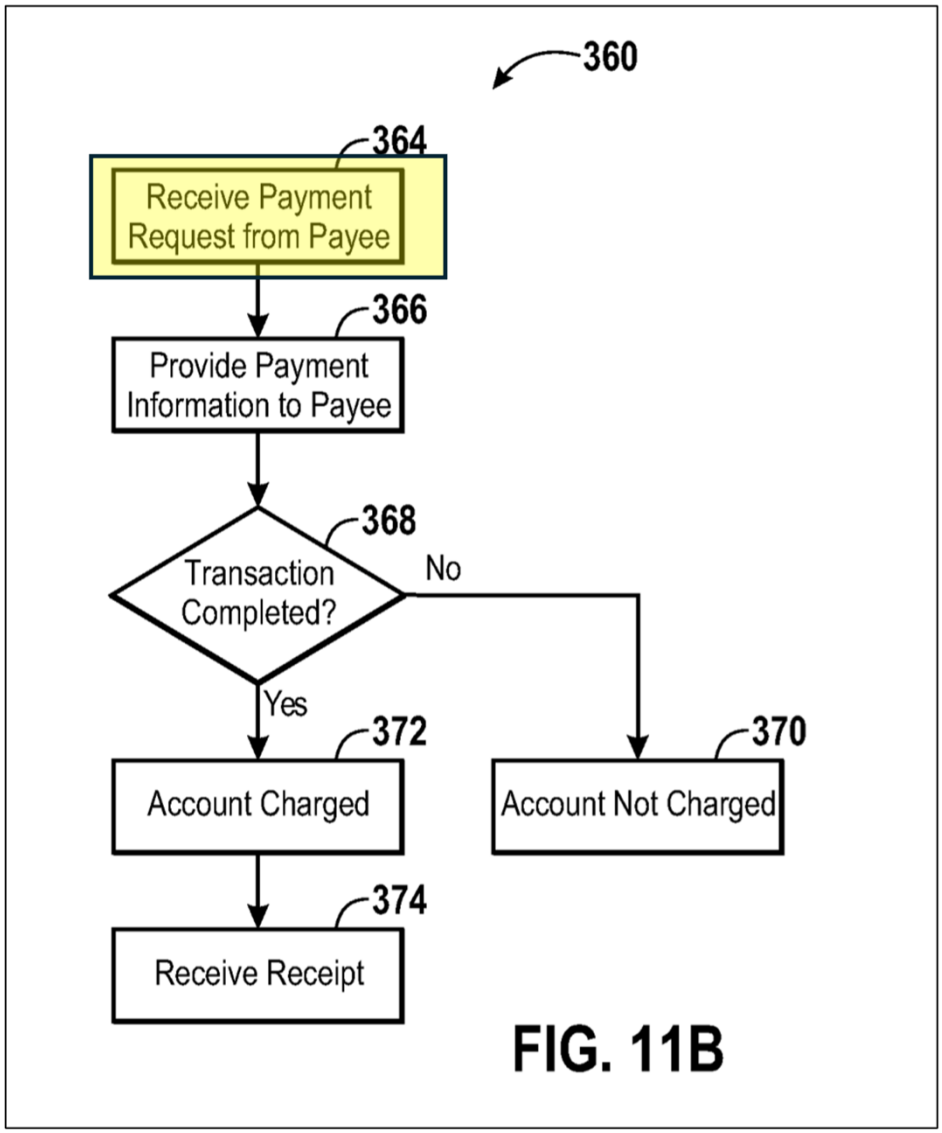
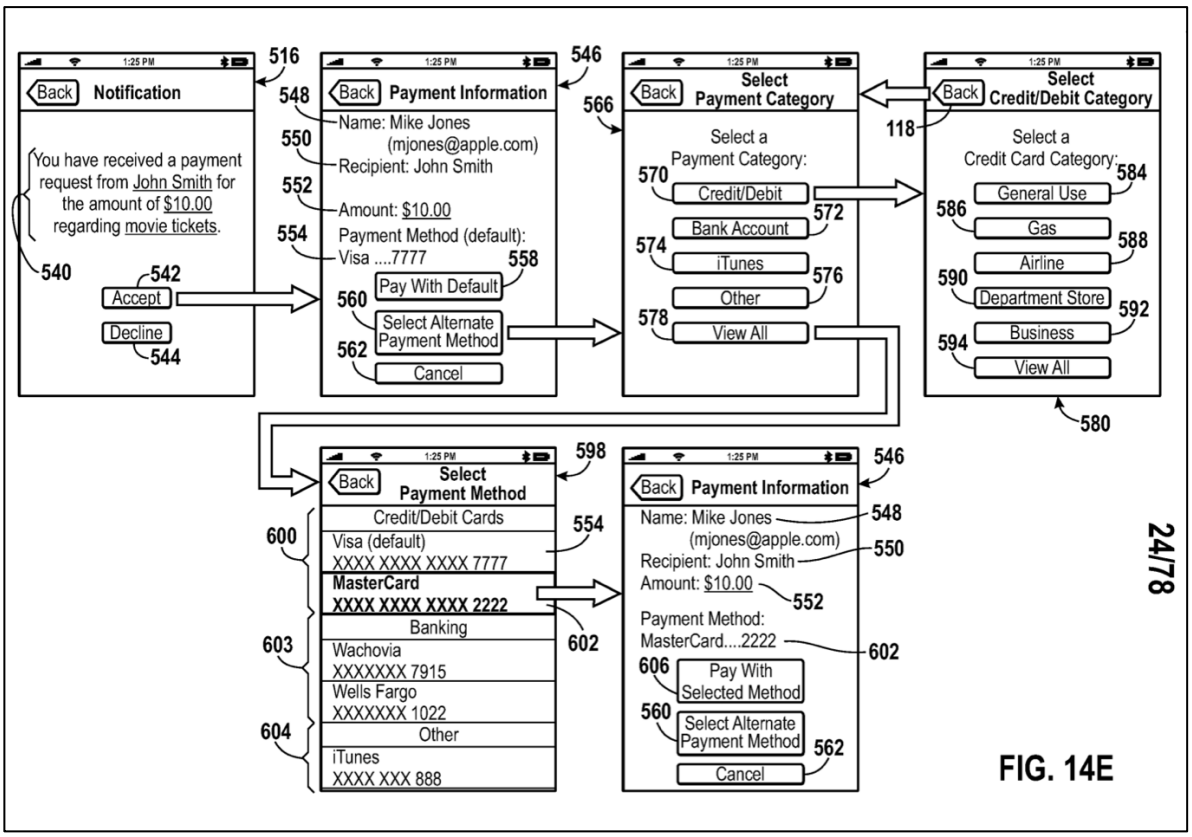


FIG. 11B

c) Motivation to Combine

153. A POSITA would have found it obvious and been motivated to configure Collinge according to the teachings of Lin such that a payment request would be received by Collinge's mobile device 104 (*said electronic device*) during a payment transaction via Collinge's NFC interface as taught by Lin. *Lin* at 56:25-28.



Lin, Fig. 14E. 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 another 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.")

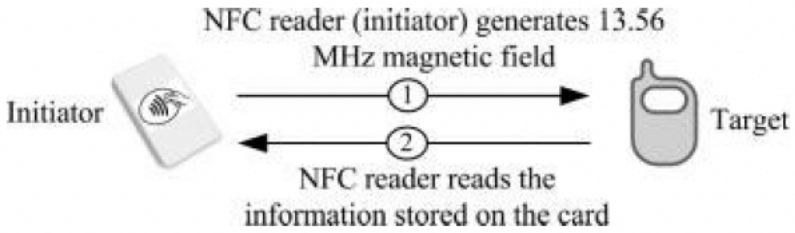


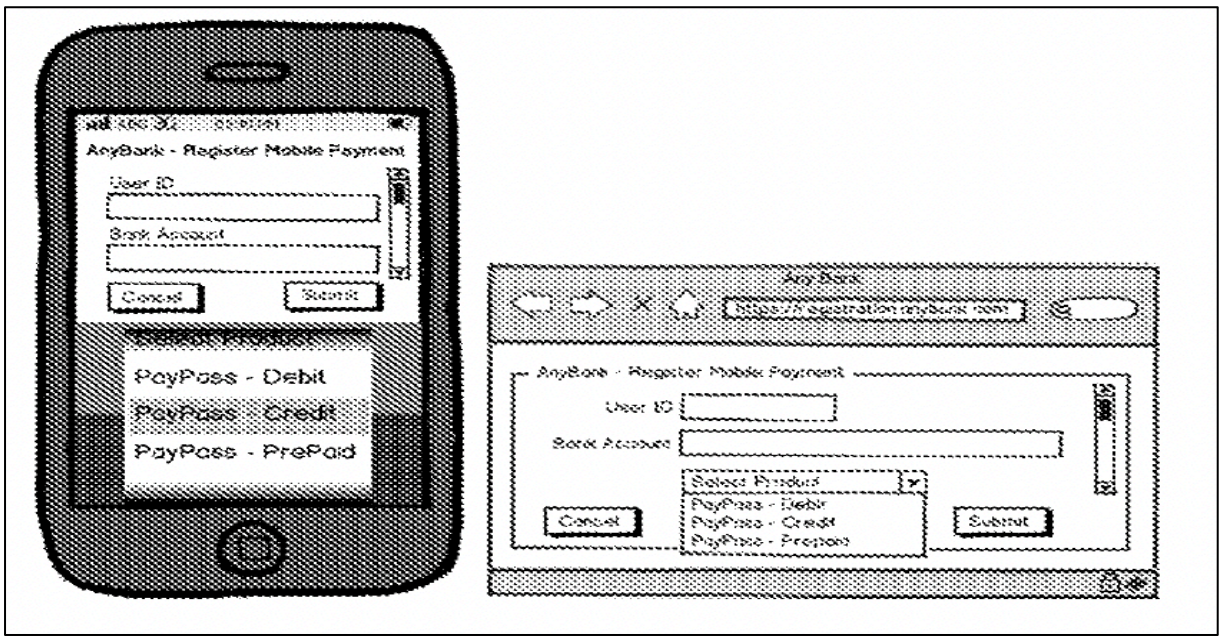
Figure 4.17 Card emulation mode.

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. *Collinge,* [0145]. ("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…may generate a payment CVC3 based on at least the supplied CVC3 value, the session key unpredictable number, the application transaction counter, and the reader unpredictable number.")

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

a) Collinge's Teachings

154. 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. Collinge further teaches in the '098 Provisional (Ex.1008), which I understand is incorporated by reference in Collinge, 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 an *issued 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.

155. Additionally, the '098 Provisional 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 image representing a selected issued payment account*), illustrated below.

'098 Provisional (Ex.1008) at p. 100 (illustrating the mobile device displaying a MasterCard payment account on the touch screen of the mobile device).

b) Lin's Teachings

156. As I discussed above in Claim 1(c), 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. Also discussed above, Lin teaches 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*, 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*, 71:7-10. Thus, Lin teaches <u>*displaying, on the touch-screen display, information reflecting the payment request*</u>. Lin also teaches displaying <u>*an image representing a selected issued payment account*</u> because, as can be seen in the annotated Figure 14E below, Lin teaches displaying the "presently selected payment account 554." *Lin,* 71:24-25.

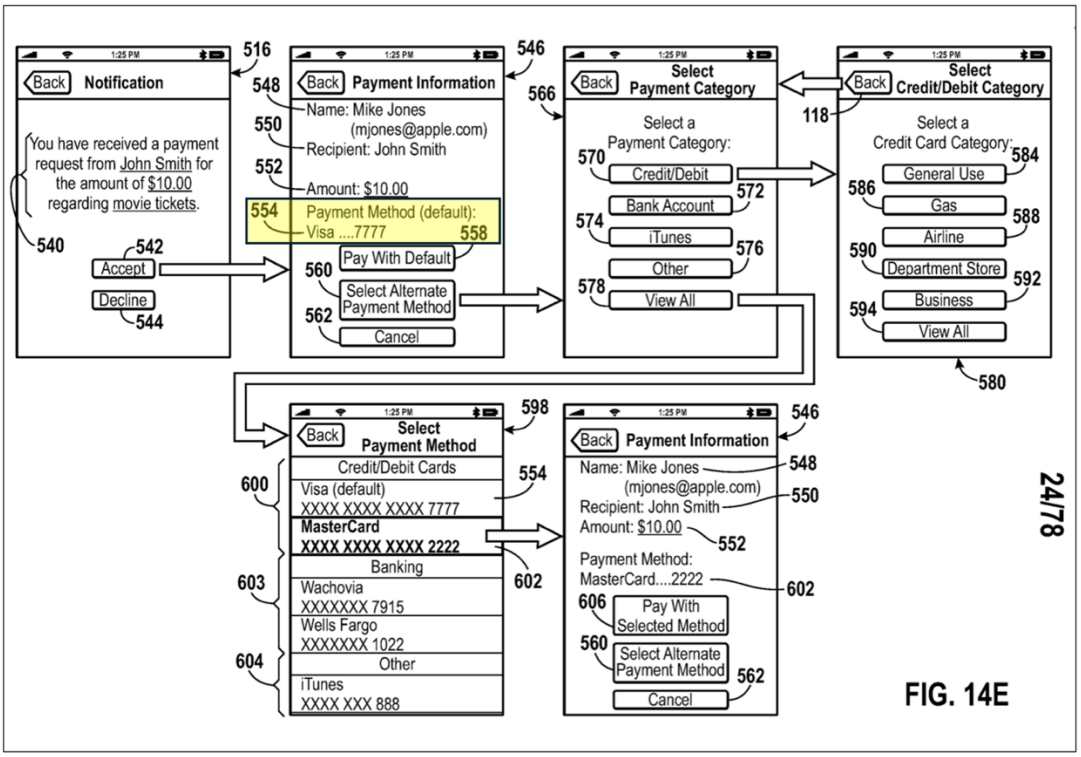
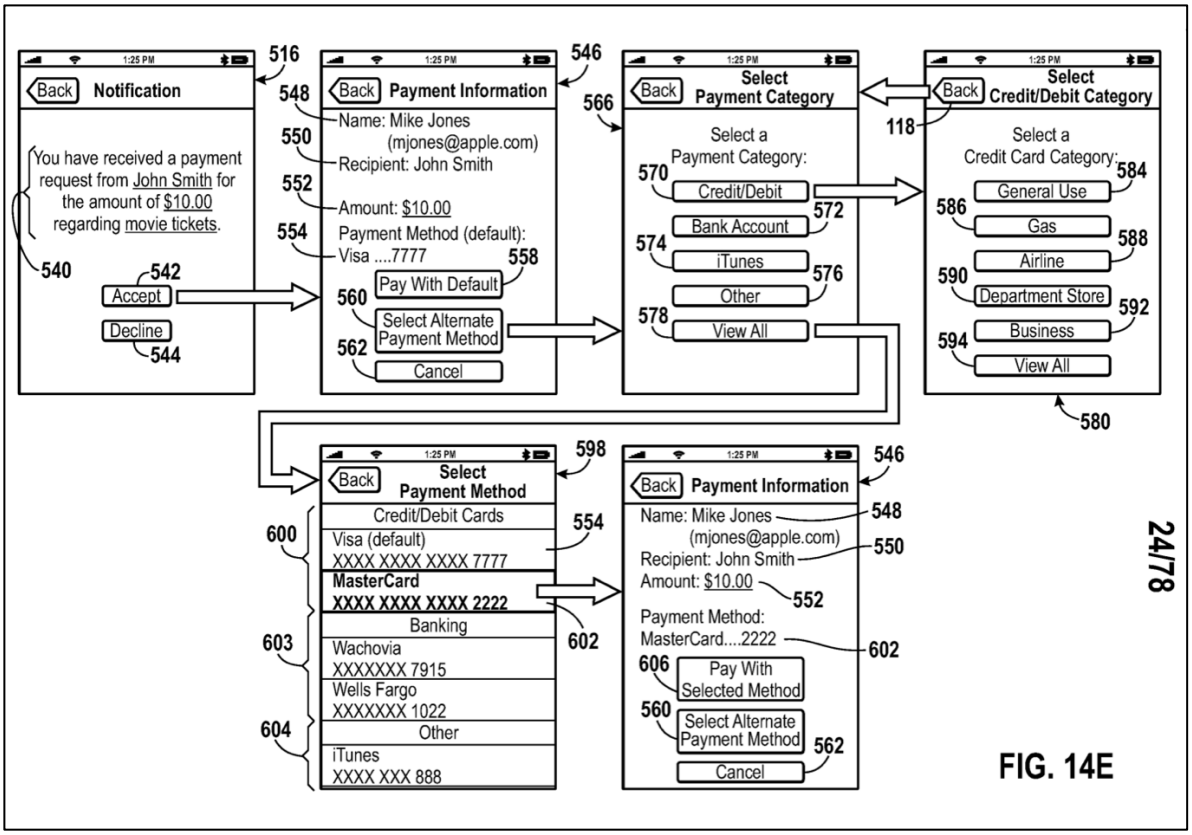


FIG. 14E

Lin at Figure 14E.

c) Motivation to Combine

157. A POSITA would have found it obvious and been motivated to modify Collinge such that mobile device 104 would display information reflecting the payment request (including the payment amount and payee) and an image representing a selected issued payment account, as taught by Lin. *See* Lin, Fig. 22C; Claim 1(c).



Lin, Fig. 14E. A POSITA would have been motivated to combine the prior art elements of Collinge's mobile device having a GUI and touchscreen interface with Lin's teaching of displaying information reflecting a payment request to yield the predictable result of a user being able to view the selected payment card, the payment amount, and the payee associated with the transaction. The modification would have

simplified user experience because a user of mobile device 104 would quickly and easily view payment transaction details such as the amount requested by point-of-sale terminal 120 and the account information from which a payment will be made. A POSITA would further recognize that the modification would increase payment security by allowing the user to check that the payment amount and payee are accurate in real-time, and would be able to immediately spot discrepancies or attempted fraud (such as if the payment amount was increased without notice). A POSITA would have had a reasonable expectation of success in making such a modification because displaying additional known information relating to a transaction on a display would have been well-within the capabilities of a POSITA. The combination is nothing more than the use of a known technique (displaying payment transaction information) to improve similar devices (mobile devices for conducting payment transactions) in the same way.

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

158. Collinge's mobile payment application 106 is executed by the processor of mobile device 104. *Collinge,* [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,* [0119]. Next, 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,* [0131], [0135] (emphasis added). The payment cryptogram "may be an application cryptogram or a **dynamic card validation code**." *Collinge,* [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,* [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. The supplied CVC3 is an input to the computation and the generated CVC3 as an output to the computation.

159. The use of the application transaction counter in generating the dynamic card validate code (CVC3 payment cryptogram) confirms that the payment cryptogram is <u>*dynamically*</u> generated, because the application transaction counter is

a different number for each transaction. *See, e.g., Roberts (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).

160. A POSITA would have understood that Collinge's CVC3 is used instead of the card issuer's CVC in a transaction. 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 application cryptograms are used in chip transactions and dynamic card validation codes are used in magstripe transactions (even in mobile phones). '098 Provisional (Ex.1008), 58. ("Application Cryptogram (AC) when using PayPass M/Chip or to generate a dynamic Card Validation Code (CVC3) when using PayPass Mag Stripe."); *Collinge*, [0048]-[0049]. As Collinge teaches the CVC3 is generated based in part on track data, which is found in a traditional magstripe. See Section VI; *Collinge*, [0050].

> The Mobile Payment Application use a specific process to generate the CVC3 using (KS_{UN}, $Cloud_CVC3_{TRACK1/2}$, ATC and UN_{READER})

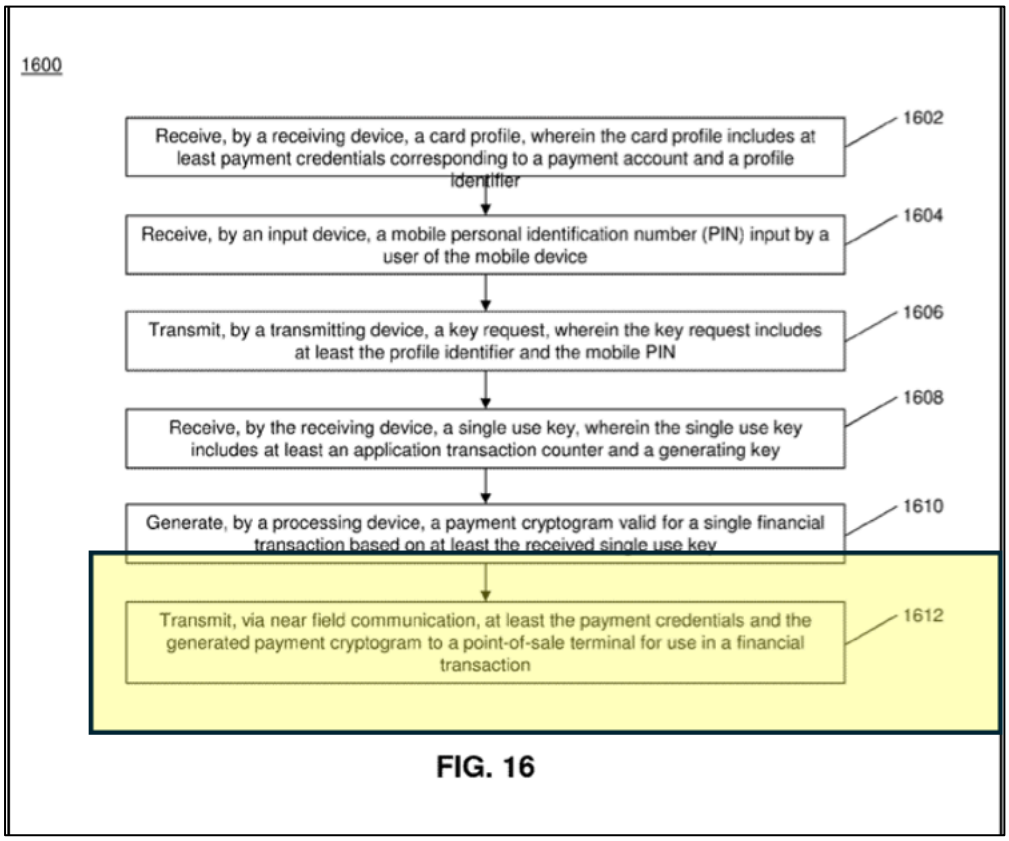
'248 Provisional (Ex.1006) at Table 1. Collinge teaches a type of payment cryptogram may be a CVC3. See Section VI; *Collinge*, [0050]. Additionally,

Collinge's CVC3 payment cryptogram 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], [0119]. *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 (Ex.1049)* at [0037] On the other hand, "MasterCard Inc.'s PAYPASS® Magstripes smart card specification has a similar code designated the CVC3." *Bona (Ex.1049)* at [0037] Both Visa's dCVV and Mastercard's CVC3 are a "one-time (i.e., dynamic) codes… unique to each transaction." *Bona (Ex.1049)* at [0037]. CVVs need to be present in a magstripe transaction. *Bona (Ex.1049)* 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 CVC 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]. It was well known that a CVC is what MasterCard calls a card verification code and a CVV is what Visa calls a card verification value. *See* Section VI; *Bona (Ex.1049)* at [0037]; *Kranzley*, [0066]. (“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.”) Therefore, Collinge teaches using said limited-use payment information (payment cryptogram) in place of said card issuer supplied payment information (CVC). A POSITA would have appreciated that using a dynamic CVV or CVC, helps “eliminate both “card present” and “card not present” fraud.” *Bona (Ex.1049)* 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.")

161. 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*. Likewise, Collinge's CVC3 is combined with additional payment credentials, and the combined complete payment information (which is also *limited-use payment information*) is used in place of an issuer-provided PAN and CVV.



Collinge, Fig. 16. (annotated), [0048], [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.").

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

a) Collinge's Teachings

162. As I discussed above in claim 1(e), Collinge teaches using the application transaction counter to generate the CVC3 payment cryptogram (*limited-use payment information*). The application transaction counter is a *per-transaction*

sequential parameter because it is a number assigned to a single transaction in sequential order. *See, e.g.,* Collinge teaches that the ATC "may be a count of transactions used for **fraud management and authentication[**.]" *Collinge,* [0050]; *Roberts (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). Collinge teaches that "the single use key 118" may "include an application transaction counter[,]" and that the single use key is provisioned to mobile device 104 in the form of a payment token payload. *Collinge* at [0050], [0047]-[0048]. Further, Collinge teaches that an "encrypted payload" including the application transaction counter is transmitted "to the mobile device 104 for use in generating a CVC3 value for use in a financial transaction." *Collinge* at [0140]-[0141]. Thus, Collinge's application transaction counter (*per-transaction sequential parameter* is generated on the cloud outside of mobile device 104 then transmitted to mobile device 104 to be stored in storage 304. *Collinge* at [0050] ("The single use key may include an application transaction counter[.]"), [0076] ("…transmit the generated single use key 118 to the mobile device 104, which may then store the single use key 118 in the local encrypted database 304.").

b) Sahota's Teachings

163. Sahota teaches "methods and systems for dynamically generating a verification value for a transaction and for utilizing such value to verify the authenticity the payment service application." *Sahota* at Abstract. "The dynamically generated Card Verification Value (referred to herein as the "dCVV") is generated on the payment device[.]" *Sahota* at [0021]. "Payment device" may include "a cellular telephone, a personal digital assistant, a mobile electronic device, or a computer." *Sahota* at [0024]. "Each time the payment service is initiated, a dCVV is generated on the payment device" and the dCVV is generated based on the application transaction counter. *Sahota* at [0029]. Notably, Sahota teaches that "**the payment device will also maintain an application transaction counter (ATC)**. The ATC will initially be set by the service provider to a predetermined value. Thereafter, the ATC will be incremented with each transaction." *Sahota* at [0028] (emphasis added). Thus, Sahota teaches *a per-transaction sequential parameter originating from the electronic device*.

c) Motivation to Combine

164. A POSITA would have found it obvious and been motivated to modify Collinge's mobile device to maintain an application transaction counter (ATC) according to the teachings of Sahota. Collinge teaches that the ATC "may be a count of transactions used for **fraud management and authentication[**.]" *Collinge,* [0050]. In the combination, Collinge's mobile device 104 (*the electronic device*)

maintains its own application transaction counter as taught by Sahota. *Sahota* at [0038]. A POSITA would have been motivated to modify mobile device 104 to maintain its own application transaction counter for use in generating the CVC3 in order to enhance the security of Collinge's payment system. For example, it provides an additional security barrier because even if a bad actor managed to intercept the encrypted payload provisioned to Collinge's mobile device, they would need to know the next transaction count number to be able to use the credentials in any way. Sahota states "service provider computer compares the ATC received from the payment device to the corresponding ATC stored on the service provider computer to determine if the received ATC is the expected next ATC 635." *Sahota* at [0038]. By comparing the ATC of mobile device 104 to the ATC transmitted to mobile device 104, increased security is achieved because if the ATCs do not match, then that is an indication of fraudulent activity. *Sahota* at [0038] ("If the ATC received from the payment device is not the expected next ATC, the payment service deployed on the payment device has potentially been skimmed 640."), [0003] ("One of the primary sources of fraud which is prevalent in the credit card industry is skimming, which refers to the electronic copying of the card's magnetic stripe data to create counterfeit cards."). A POSITA would have had a reasonable chance of success in including ATC tracking in Collinge's mobile device because at the time

it was already common for devices to track an ATC and a POSITA would have been well-familiar with how a device-tracked ATC would be implemented.

165. The modification would have been straight forward and merely required storing an initially set ATC value into encrypted storage 304 on mobile device 104, then configuring mobile device 104 to incrementally increase the ATC upon each conducted payment transaction. Accordingly, the modification would have had a reasonable expectation of success.

11. 1(g): "using said limited-use payment information in connection with the payment transaction in place of issued payment information associated with said selected issued payment account;"

166. As I discussed above at Claim 1(e), a POSITA would understand that the Collinge's payment cryptogram (i.e., CVC3) used to conduct a payment transaction (*using said limited-use payment information in connection with the payment transaction*) is used instead of a standard, static CVV code (*issued payment information associated with said selected issued payment account*) associated with the payment account used in Collinge's payment transaction.

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

167. As discussed in Claim 1(e), Collinge's payment cryptogram (i.e., CVC3) is generated on mobile device 104. Collinge expressly teaches that the

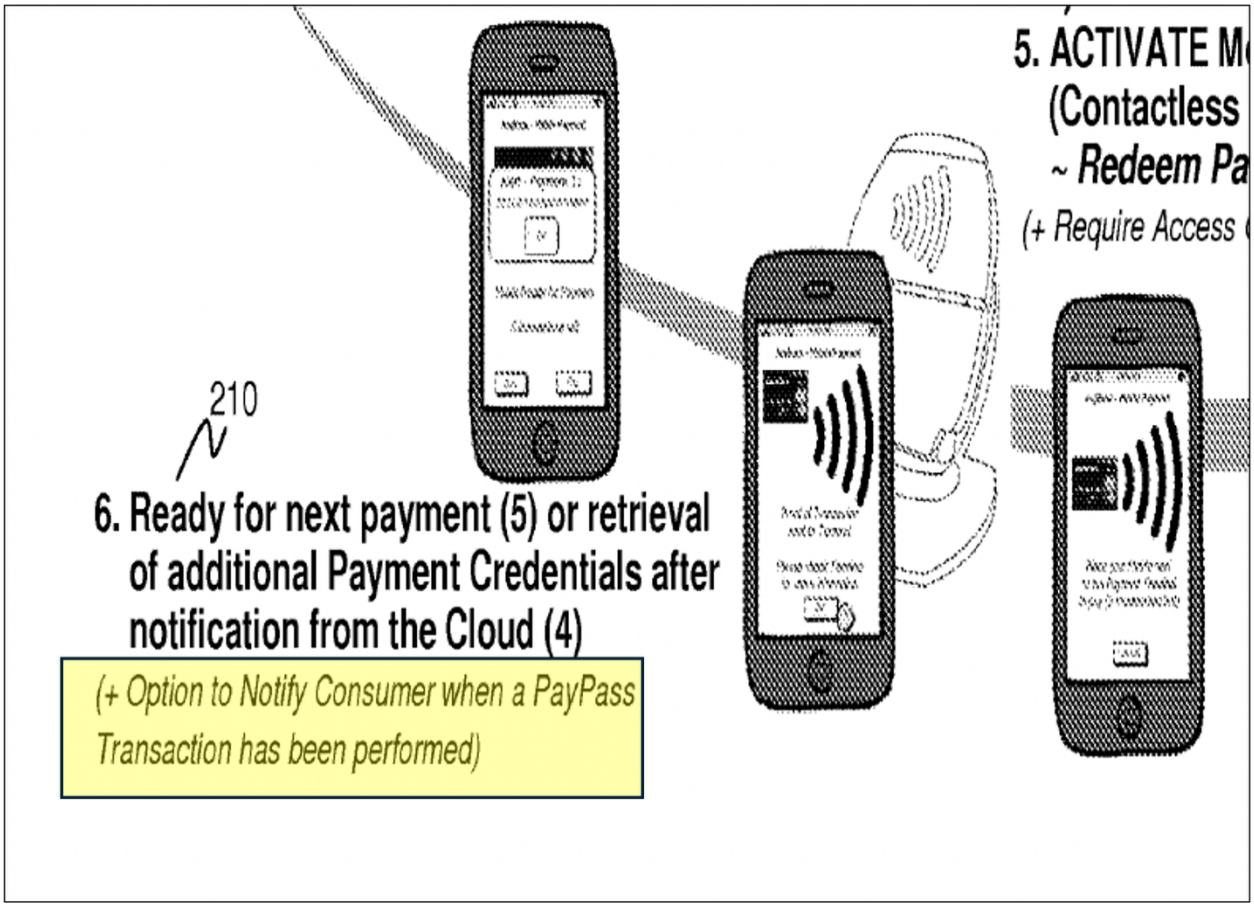
payment cryptogram (*said limited-use payment information*) is transmitted from mobile device 104 (*said electronic device*) to the point-of-sale terminal 120 (*for receipt by an NFC recipient*). *Collinge* at [0044] ("The mobile device 104 may be further configured to **transmit a generated payment 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, as discussed above Collinge's mobile device 104 comprises an NFC interface. *See* Claim 1(a)(3). 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 via said NFC interface for receipt by an NFC recipient*.

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

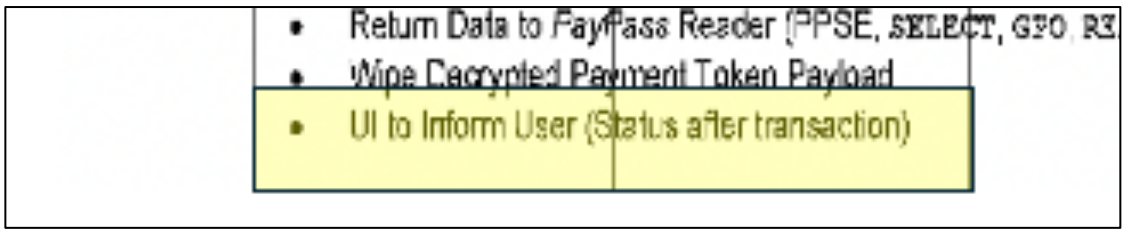
> *the status of said payment transaction via said touch-screen display."*

168. In the '248 Provisional, 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.

169. Additionally, at Figure 2B of the '248 Provisional, 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 a status of said payment transaction; and displaying the status of said payment transaction via said touch-screen display*.



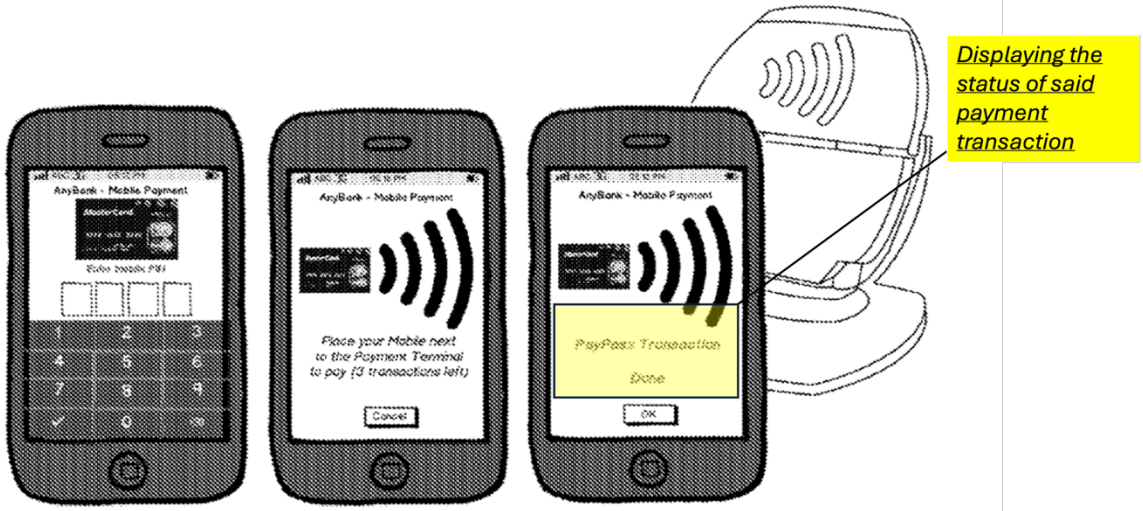
'248 Provisional (Ex.1006) at Figure 2B (annotated excerpt).



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

170. Further, the 248 Provisional 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, 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.

171. 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.

14. Claim 2 "The method of claim 1, wherein the limited-use payment information comprises a cryptogram number."

172. *See* Claim 1(e).

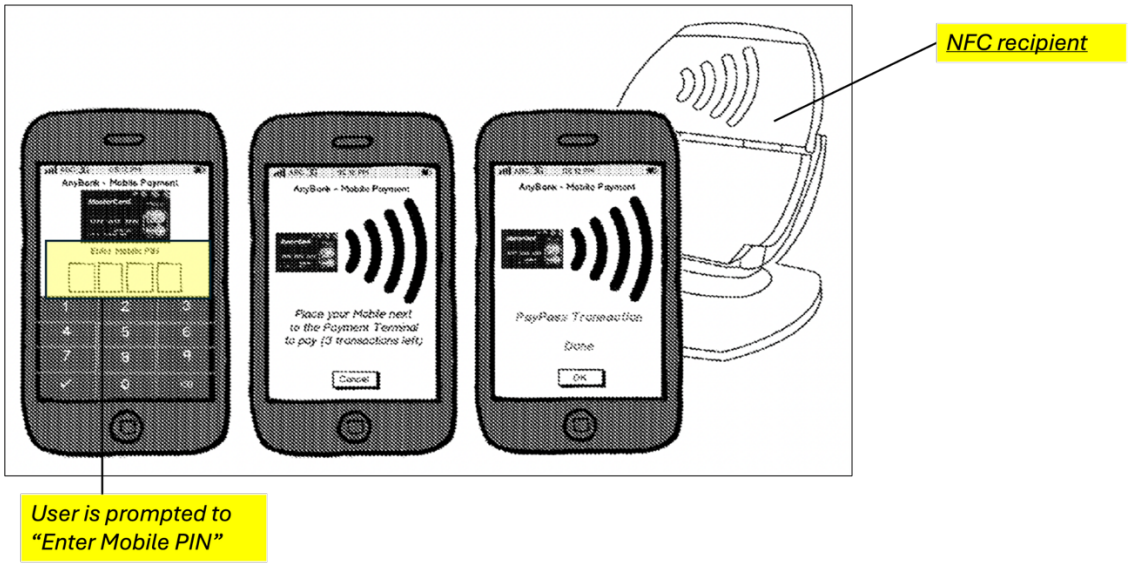
15. Claim 7: "The method of claim 1, wherein the priming operation comprises bringing the electronic device within receiving proximity of an NFC recipient."

173. See Claim 1(a).

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

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

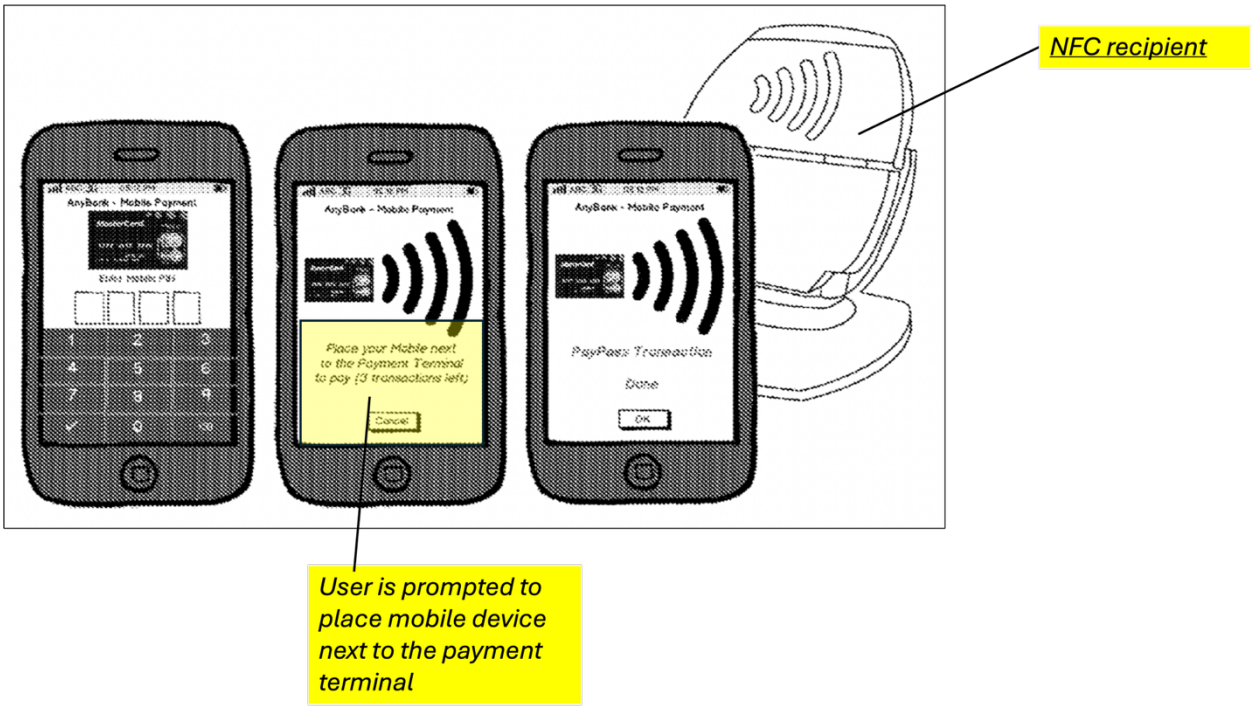
175. *See* Claim 1(a). In the '098 Provisional, which I understand is incorporated by reference into Collinge, the user of mobile device 104 is instructed to input a PIN using the user interface of mobile device 104.



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

176. A POSITA would have understood that a user inputting a correct PIN constitutes *successfully validating the identified user as authorized to perform the payment transaction via said electronic device* because PINs were well-known to be used to authenticate a user during a payment transaction. *See, e.g., Bona (Ex.1049)* at [0007] ("…where credit/debit cards contain an embedded microchip and are authenticated automatically using a PIN."). In other words, a POSITA would have understood that a when the user inputs the correct PIN into mobile payment application 106 on mobile device 104, that the user would be *successfully validat[ed]* as *authorized to perform the payment transaction via said electronic device* because if the user did not input the correct PIN, then the payment transaction would not be conducted. Per the '098 Provisional, the user "must always provide the Mobile PIN for all PayPass transactions[.]" *'098 Provisional (Ex.1008)* at p. 99.

177. Additionally, the '098 Provisional teaches instructing the user of mobile device 104 to "place your Mobile next to the Payment Terminal to pay[.]" *'098 Provisional (Ex.1008)* at p. 99.



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

178. A POSITA would have understood that when mobile device 104 is placed next to the NFC recipient, the NFC recipient is identified as *an NFC payment facility*. As I discussed above in Claim 1(e), NFC-enabled devices, such as Collinge's mobile device 104 are able to communicate by exchanging a magnetic field. When a mobile device receives an NFC payment request, as discussed above at Claim 1(c), transmission of data occurs in order from the NFC initiator to the NFC target. In the combination of Collinge-Lin I discussed above, the point-sale-terminal

120 sends a payment request to mobile device 104 using NFC. *See* claim 1(c). Therefore, Collinge-Lin teaches and a POSITA would understand that the point-of-sale terminal 120 is an NFC initiator and mobile device 104 is an NFC target. *See* Section VI. As I described in the background of technology section, if the NFC receives signals and the corresponding commands of an NFC initiator, the NFC interface automatically adopts the roll of the NFC target. *See* Section VI. Because the NFC interface of mobile device 104 (NFC target) receives a payment request from the point-of-sale terminal 120 (*NFC recipient*), which initiates the payment request, a POSITA would understand that the point-of-sale terminal 120 is identified as *an NFC payment facility* because only the *NFC payment facility* would have details of the payment request, such as the amount of requested payment and the identity of the requesting payee.

17. Claim 8(b): "receiving a user approval for performing the payment transaction."

179. Collinge teaches that mobile device 104 displays a display for the user of mobile device 104 to approve a payment transaction. The user has the option to choose between "quit" and "pay" on the user interface when performing a payment transaction. *'098 Provisional (Ex.1008)* at p. 100. A POSITA would have understood that when the user of mobile device 104 chooses "pay" that the payment transaction would be approved (*receiving a user approval for performing the*

<u>*payment transaction*</u>) and that when the user chooses "quit" that the payment transaction would not proceed.

'098 Provisional (Ex.1008) at p. 100.

> 18. *Claim 9(Pre): "The method of claim 8, wherein said user approval for performing a payment transaction comprises displaying a request for user input at said electronic device, for both said identifying and said user approval of said payment transaction, and further comprising:"*

180. As I discussed above at Claims 1(a) and 8, Collinge teaches displaying a request for user to input a PIN/code (<u>*identifying*</u>) and that user approval is obtained

by displaying a request to the user of mobile device 104, where the user has the option to click "quit" or "pay[.]"

'098 Provisional (Ex.1008) at p. 100.

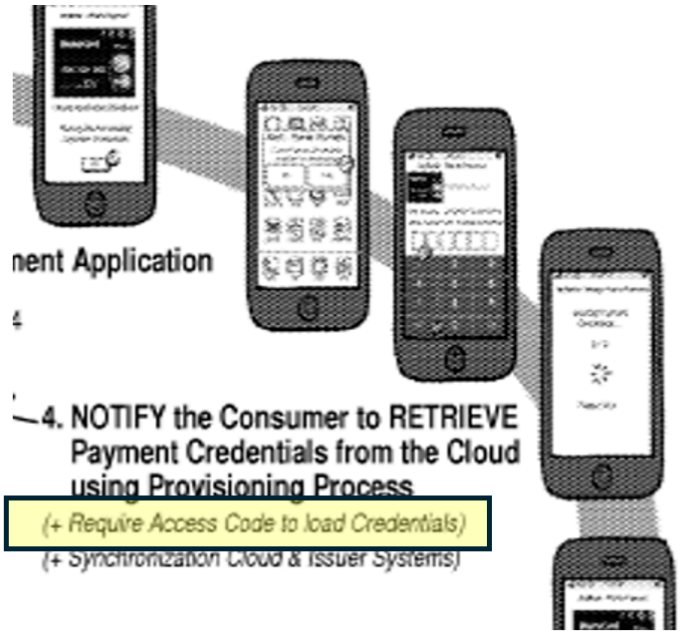
> *19. Claim 9(a): "the processor identifying that said user input matches a known authorized user of the electronic device, before said readying said device to perform a payment transaction; and,"*

181. As I discussed above at Claim 1(a), Collinge teaches that mobile payment application 106 on mobile device 104 may request the activation code to "authenticate the user 102." *Collinge* at [0093]. A POSITA would have understood that *the processor*, specifically, authenticates the user because mobile payment

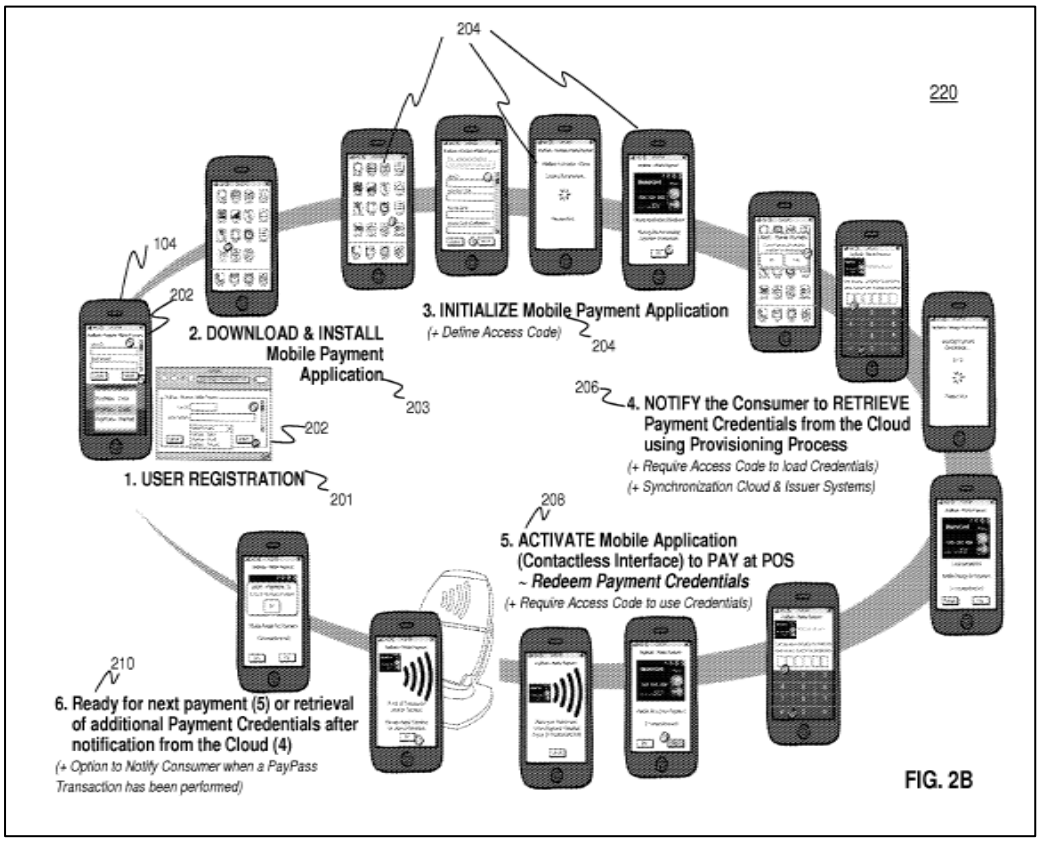
application 106 is executed by the processor of mobile device 104. *Collinge* at [0041]. Additionally, Collinge teaches that the correct PIN is required perform a payment transaction. As I discussed above at Claim 1(a), the code/PIN are required before a device is readied to perform a payment transaction. Thus, Collinge teaches *the processor identifying that said user input matches a known authorized user of the electronic device, before said readying said device to perform a payment transaction*.

20. Claim 9(b): "disallowing the payment transaction by the device until said readying said device to perform the payment transaction is successfully completed."

182. Because Collinge teaches that the user is required to input the activation code prior to loading payment credentials, a POSITA would have understood that if the user does not input the activation code or inputs an incorrect activation code, the payment transaction would be disallowed. *'248 Provisional (Ex.1006)* at Figure 2B ("Require Access Code to load Credentials).



'248 Provisional (Ex.1006) at Figure 2B. (annotated excerpt) Similarly, a POSITA would have understood that if the user does not input the PIN or inputs an incorrect PIN, the payment transaction would not be allowed. Thus Collinge teaches and a POSITA would have understood that Collinge teaches *disallowing the payment transaction by the device until said readying said device to perform the payment transaction is successfully completed*.



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

> 21. *Claim 10.1: The method of claim 8, wherein said successfully validating the identified user comprises the processor successfully determining a match between: firstly, a user input received via at least one of a set of user input sensors of the electronic device; and, secondly, at least one of the set consisting of: predetermined user characteristics, and challenge-responses of an authorized user, as stored in the electronic device.*[2]

---

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

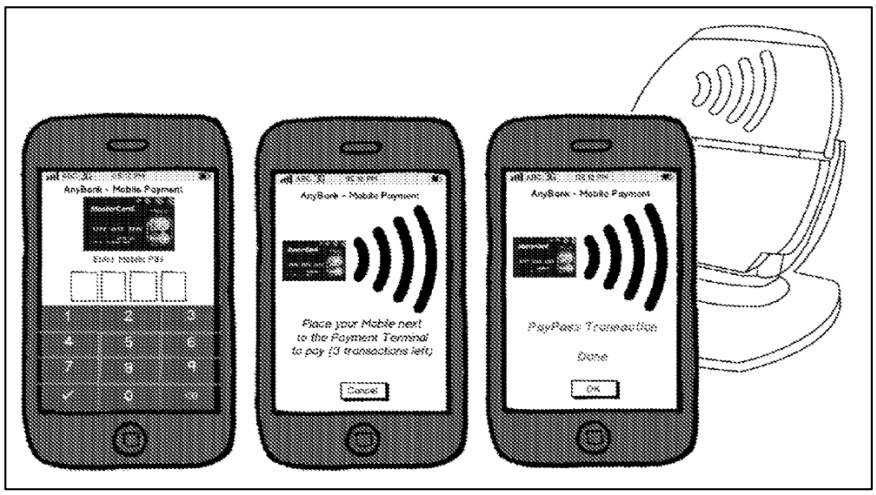
183. Collinge in view of Smith teaches validating a user if Collinge's processor is able to match a user's input of a PIN with a PIN stored in the memory of Collinge's mobile device.

a) Collinge's Teachings

184. Collinge's mobile device includes a touch screen and a button which are a <u>*user input sensors*</u>. *See* claim 1(a); *'098 Provisional (Ex.1008)*, 99. A user of mobile device 104 may input a PIN into mobile device 104 using the touch screen. *See* Claim 39(d).

185. Indeed, Collinge teaches that a user "must always provide the Mobile PIN for all PayPass transactions [.]" *'098 Provisional (Ex.1008)* at p. 99; *Collinge* at [0123] ("require authentication by the user 102 at both the mobile device 104 (e.g., entering of the mobile PIN) and the point-of-sale terminal 120 (e.g., entering of an online PIN or signature.") Collinge teaches validating a user via the input of a PIN via "an input device (e.g., of the mobile device 104, such as a touch screen) that may "receive a mobile personal identification number (PIN) input by a user (e.g., the user 102) of the mobile device 104." *Collinge*, [0133]. Collinge teaches a user "must always provide the Mobile PIN for all PayPass transactions[.]" *'098 Provisional*, 99. *Collinge,* [0123] ("require authentication by the user 102 at both the mobile device 104 (e.g., entering

of the mobile PIN) and the point-of-sale terminal 120 (e.g., entering of an online PIN or signature).")



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

b) Smith's Teachings

186. To the extent Collinge does not teach storing the valid PIN on mobile device 104 (<u>*and challenge-responses of an authorized user, as stored in the electronic device*</u>), Collinge in view of Smith teaches such. Specifically, Smith teaches that a transaction may be "offline" and in an offline transaction "the transaction is authorized by the payment application in the mobile device without transmission of an authorization request to the issuer 206[.]" *Smith* at [0022].

c) Motivation to Combine

187. A POSITA would have found it obvious and been motivated to modify Collinge's mobile device 104 according to the teachings of Smith such that

Collinge's mobile device would store a PIN and validate a user based on that stored PIN if the user enters the PIN correctly. A POSITA would recognize that Collinge teaches use of a PIN before supplying payment credentials to Collinge's payment device. If the mobile device declines to even send a request for payment credentials because an incorrect PIN has been entered (indicating a bad actor may have access to the device), then the bad actor cannot gain access to useful payment information because it was not provided to the mobile device to be retrieved or intercepted. Further, it would be faster for the device to validate the PIN itself, and would allow Smith's offline authentication mode to be used on the mobile device. The combination is nothing more than the use of a known technique (authenticating a user using a PIN) to improve similar devices (electronic devices) in the same way. Additionally, the modification is the combination of prior art elements (PINs, electronic devices) according to known methods to yield the predictable result of increasing security of Collinge's mobile device. In the combination, the PIN would be stored in Collinge's memory which is already accessible to Colinge's processor as discussed at Claim 39(b).

22. *Claim 11: "The method of claim 10, wherein said user input received via at least one set of a set of user input sensors of the electronic device comprises a passcode entry sequence performed by a user input via the touch-screen display."*

188. As I discussed above at Claim 1(a) and 10.1, Collinge teaches that a user may input an activation code and/or a mobile PIN using the touch screen of mobile device 104. Because the touch screen is *at least one set of a set of user input sensors of the electronic device* (touch screen, fingerprint sensor) and because the touch screen is used to input the mobile PIN and code (*passcode entry sequence*), Collinge teaches *wherein said user input received via at least one set of a set of user input sensors of the electronic device comprises a passcode entry sequence performed by a user input via the touch-screen display*.

23. Claim 15: "The method of claim 1, wherein the input comprising a priming operation is a user input."

189. *See* Claim 1(a).

24. Claim 27: "The method of claim 1, wherein the dynamically generating further comprises dynamically generating the limited-use payment information based on payment processing authority secret information."

190. *See* Claim 5.

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

191. *See* Claim 5.

26. Claim 28(a): "further wherein the at least one secret information is not exchanged when p[er]forming the payment transaction."

192. The generating key, part of single use key 118 (at least one secret information) is not exchanged (sent or received) to or from the point-of-sale terminal 120 when performing the payment transaction, rather the payment cryptogram and payment credentials are sent to the point-of-sale terminal 120 during the payment transaction. Collinge at [0050] ("The single use key may include an application transaction counter (ATC) and a generating key 208…The generating key 208 may be a key used to generate a payment cryptogram used in a financial transaction…the generating key 208 may generate a dynamic card validation code (CVC3) [.]"); [0070], [0121].

193. The reader unpredictable number is received from the point-of-sale terminal before Collinge's NFC interface is activated, notably the reader unpredictable number is not the generating key within the single use key (secret) identified above. *Collinge* at [0145]. ("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.")

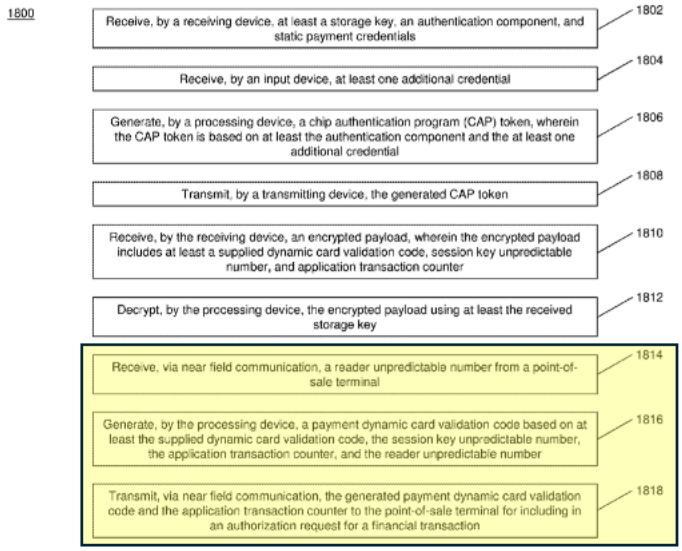
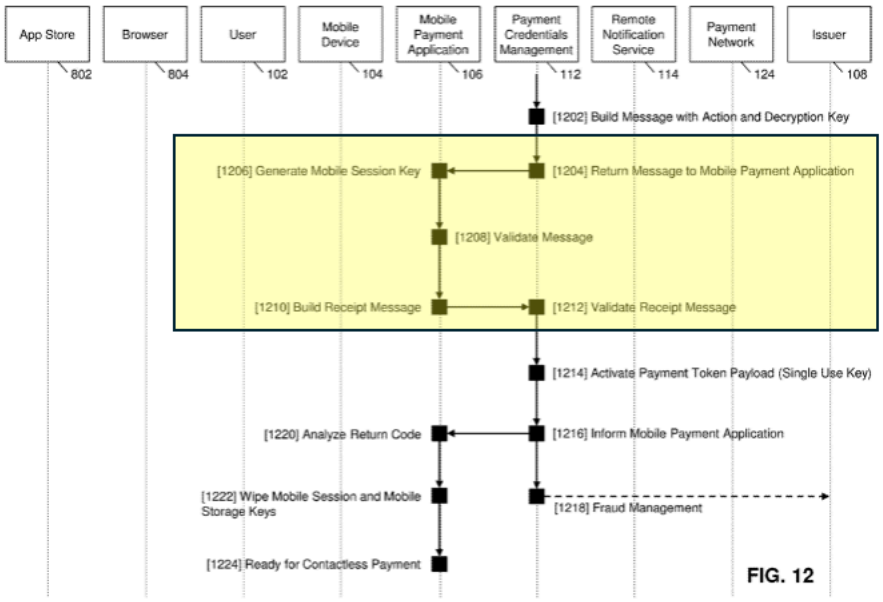


FIG. 18

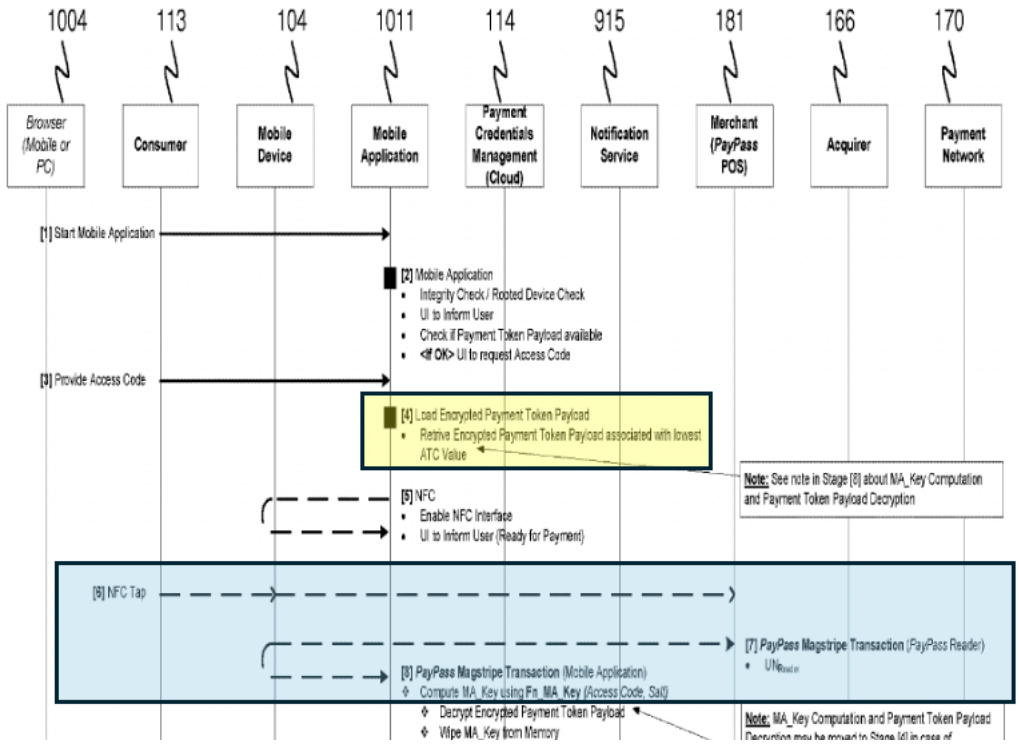
Collinge, Fig. 18. (annotated).

194. Notably the generating key within the single use key (secret) is not received from the point-of-sale terminal. As shown in the figures below, in step 1201 the "payment credentials management service 112 may build a message with an action to activate (e.g., decrypt) the previously provisioned single use key 118…in step 1204 transmit the message...to the mobile payment application 106[.]" *Collinge*, [0111].



Collinge, Fig. 12. (annotated)

195. Collinge's mobile payment application at step 1208 "decrypt[s] the single use key 118...and updates a status to indicate that the single use key 118 is successfully received and stored and that the mobile payment application 106 is ready to conduct a payment transaction." *Collinge*, [0109]. In step 1218 "the payment credentials management service 112 may synchronize the user profile including activation of the single use key 118 with the issuer 108 for fraud management." *Collinge*, [0111]. After this synchronization, the NFC interface is enabled. Fig. 14. *'248 Provisional (Ex.1006)*, Fig. 14 (excerpt).



'248 Provisional (Ex.1006), Fig. 14 (excerpt). Using the generating key within the single use key, Collinge's mobile device "generate[s] 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.") *Collinge*, [0145]; *Collinge*, [0050] ("The single use key may include an application transaction counter (ATC) and a generating key 208…The generating key 208 may be a key used to generate a payment cryptogram used in a financial transaction…the generating key 208 may generate a dynamic card validation code (CVC3) [.]")

196. Alternatively, to the extent this claim requires shared secret information to not be exchanged with an issuer, Collinge teaches wherein at least one secret

information (CVC) shared with Collinge's system and the issuer is not exchanged when performing the payment transaction since Collinge uses a dynamic CVC instead of the static CVC. Collinge teaches that the user provides "account information for the payment account with which the user 102 wants to use for payment transactions using the mobile device 104." *Collinge*, [0065]. A POSITA would have understood that in Collinge a user would already have to provide their CVC during the card registration process as the Collinge's CVC3 payment cryptogram is used in place of the card issuers CVC. For example, Kranzley (another MasterCard reference) teaches "the PAN 504 and the static card verification code 506 are obtained from a cardholder when the cardholder registers to use a payment card[.]" *Kranzley* at [0066].

500

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. A POSITA would have understood that a card's CVC is a secret that is shared between Collinge's system and an issuer (e.g., MasterCard). Since Collinge performs transactions using a CVC3 payment cryptogram in place of a static CVC, Collinge therefore does not exchange the ate least one secret information shared with an issuer (CVC) during a transaction. Instead, the issuer would receive the CVC during a card registration process. *Kranzley* at [0066].

27. Claim 39 (Pre): "An electronic device for completing a payment transaction, the electronic device comprising:"

197. Collinge teaches a mobile device 104 included in system 100, wherein 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].

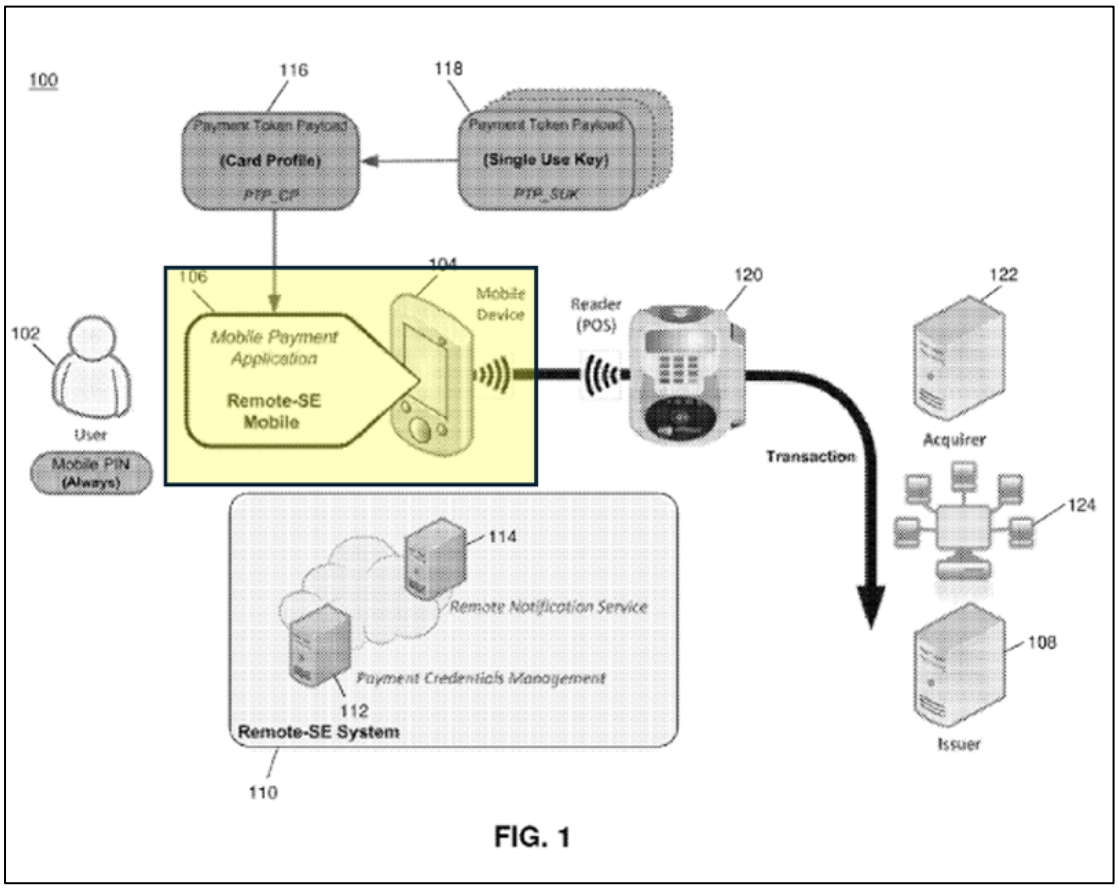


FIG. 1

Collinge, Fig. 1. (annotated)

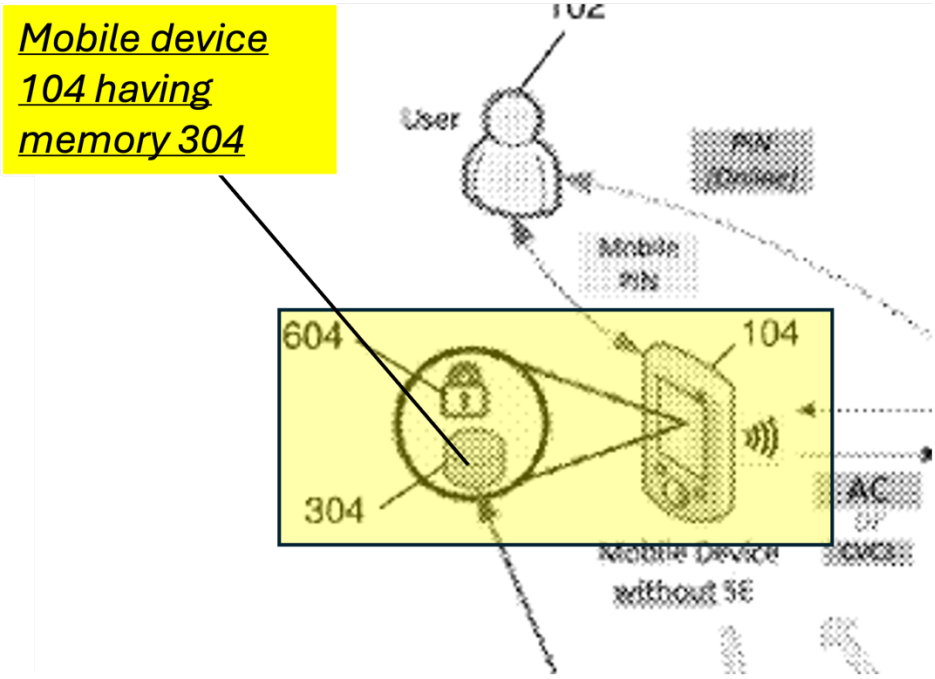
198. "The mobile payment application 106 may be configured to…conduct payment transactions via near field communication[.]" *Collinge* at [0041]. Collinge expressly teaches that mobile device 104 *complete[s] a payment transaction*. *Collinge* at [0070] ("In step 512, the mobile device 104 may conduct a contactless/NFC **payment transaction** using the mobile payment application 106 and the single use key 118.") (emphasis added). Therefore, Collinge teaches *an electronic device for completing a payment transaction*, where mobile device 104 is *an electronic device*.

28. 39(a): "a processor;"

199. As I discussed above at Claim 1(a)(1), Collinge teaches that mobile device 104 comprises *a processor*.

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

200. 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 (*electronic device*) 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*.

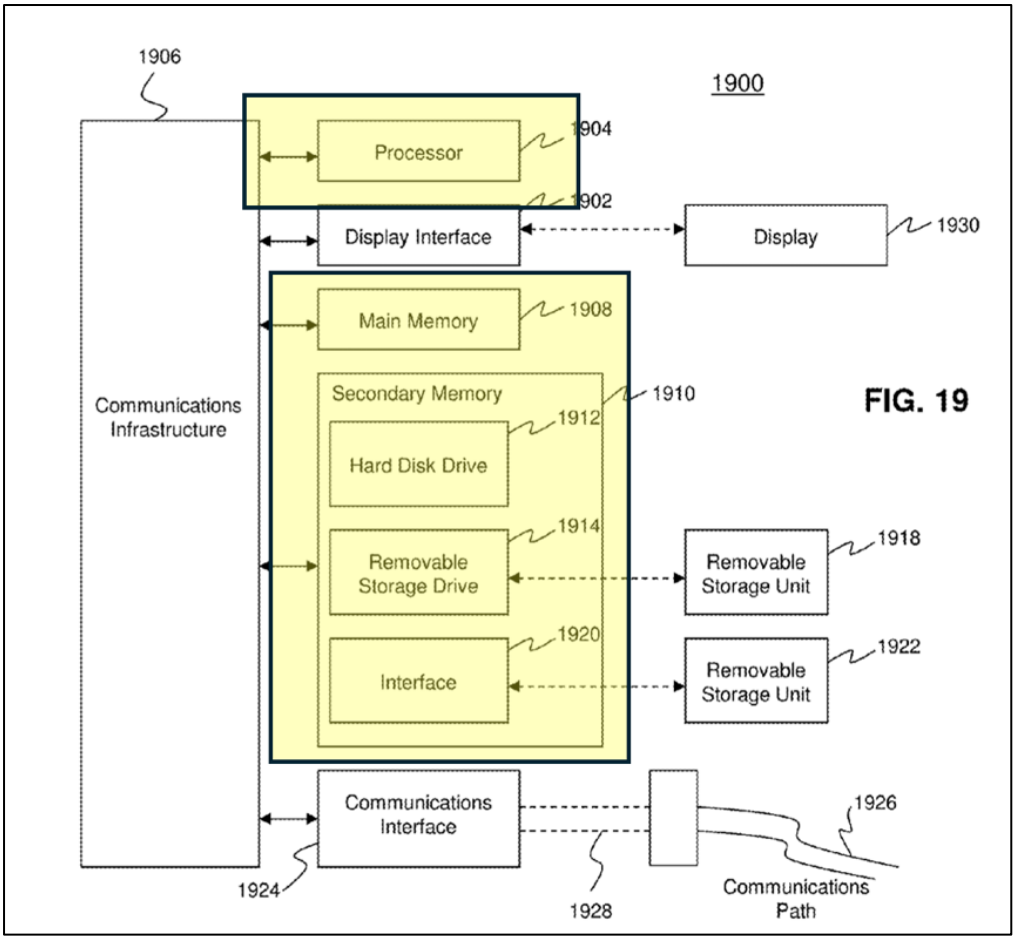


Collinge at Figure 6 (illustrating mobile device 104 having memory 304) (annotated excerpt).

201. 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*.

202. 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 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 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. 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]. Collinge teaches that the communications infrastructure may be a "bus[.]" *Collinge*, [0150].



Collinge at Figure 19 (annotated). For this additional reason, Collinge teaches that a memory is coupled to a processor.

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

203. Collinge teaches "the payment token payload provisioned to the mobile device 104." *Collinge* at [0047]. The payment token payload may include "card profile 116 and the single use key 118." *Collinge* at [0048]. Specifically, card profile 116 may include payment credentials 202/204 such as "payment account number, tracking data, and card layout" and "the number of digits in an application transaction counter and a bitmap for an unpredictable number and the application transaction counter." *Collinge* at [0049]. Single use key 118 "may be a payment token used one time to generate a payment cryptogram to be used in a payment transaction. The single use key may include an application transaction counter (ATC) and a generating key 208." *Collinge* at [0050]. Card profile 116 is *information associated with use an issued payment account* because it comprises information, including payment credentials, about the user's payment account. *Collinge* at [0043] ("The card profile 116 may include the payment credentials…"). Card profile 116 is stored in *the memory* (i.e., *the memory is operable to store information associated with use of an issued payment account*). *Collinge* at [0019] ("…**card profile 116** and single use key 118 **in the encrypted local storage 304**.") (emphasis added), [0074] ("The mobile payment application 106 may then store the received card profile 116 in the local encrypted database 304."); *'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.").

204. The *payment authority information* comprises at least the single use key 116. The single use key 116 is *payment authority information* because it is shared with the issuer (*payment authority*). *Collinge* at [0128] ("…the method 1500 may further include transmitting the generated single use key 118 to an issuer associated with the payment account.").

205. Additionally, Collinge teaches *the payment authority information comprises a secret information* because the single use key 118 is secret. Specifically, regarding single use key 118, Collinge teaches that "single use key 118 may be genuine if the mobile PIN is successfully authenticated" and may be "fake if the mobile PIN is unsuccessfully authenticated." *Collinge* at [0128]. Thus, single use key is *a secret information* because only a user who knows the correct PIN is able successfully utilize the authentic single use key 118.

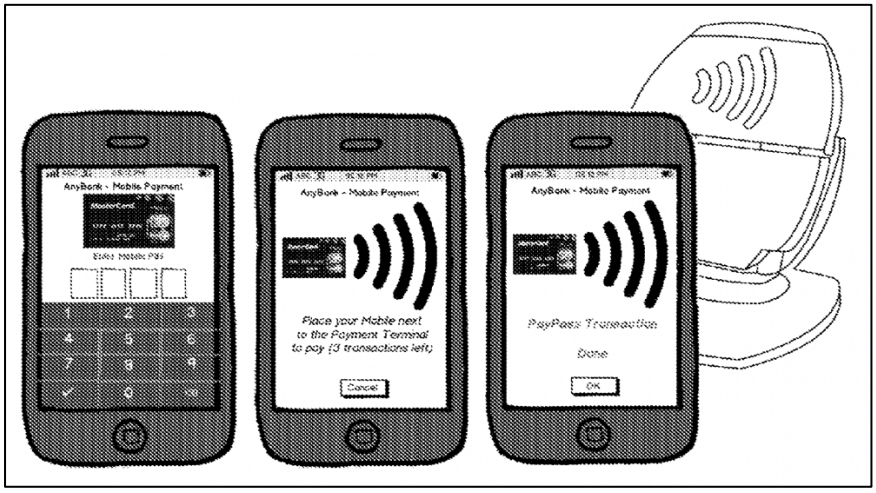
206. Further, *the payment authority information comprises a secret information* because the payment credentials (*payment authority information*) include the application transaction counter. *Collinge* at [0049] ("The mag stripe payment credentials 204 may include…the application transaction counter.").

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

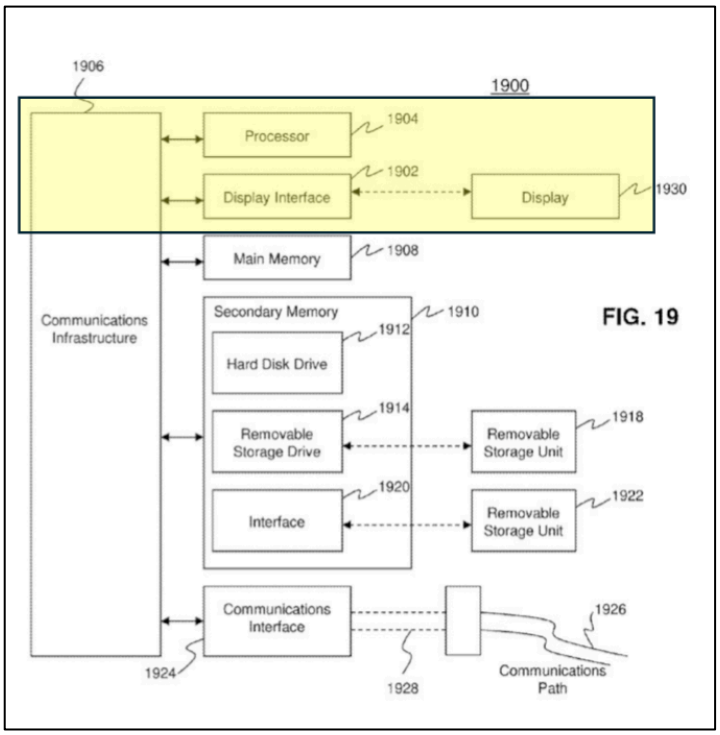
207. As I discussed above at Claim 1(a)(3), Collinge teaches that mobile device 104 has an NFC interface coupled to the processor. Additionally, as I discussed at Claim 1(c), Collinge in view of Lin renders obvious receiving a payment request via the NFC interface. Collinge in view of Lin teaches receiving a payment request via the NFC interface of mobile device 104, Collinge in view of Lin also teaches that the NFC interface is *operable to receive a payment request associated with the payment transaction*.

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

208. Collinge's mobile phone includes touch screen display that provides a graphical visual *user interface.* *Collinge*, [0133]. Collinge teaches a user interface that displays a notification to the user 102. *Collinge* at [0107] ("…the mobile payment application 106 may display a notification to the user 102 via a user interface[.]"), *see also* [0112], [0117].

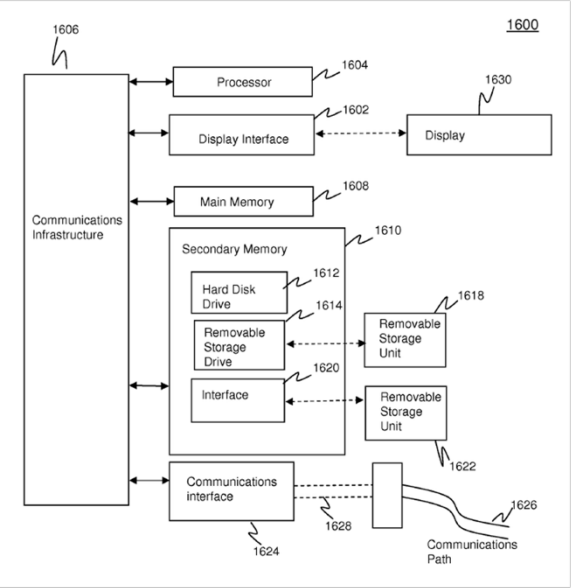


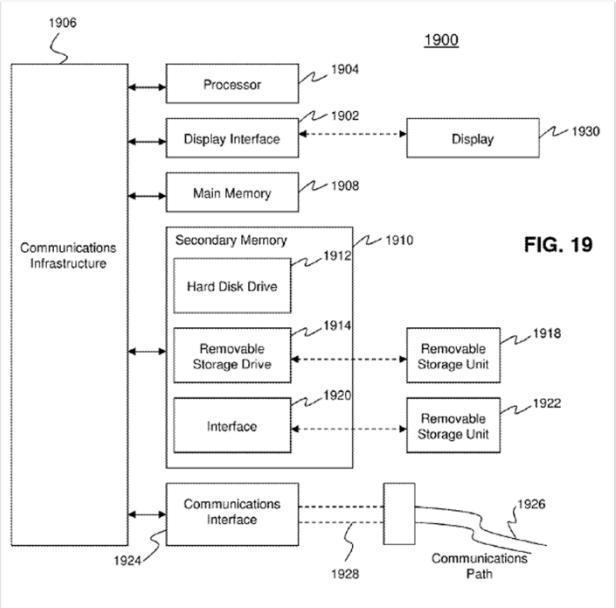
'098 Provisional (Ex.1008), 99; '248 Provisional (Ex.1006), Fig. 2B. The display of Collinge's mobile device is *coupled to the processor*. Collinge teaches that "at least one processor device" is used to implement Collinge's payment system. *Collinge,* [0147]. Collinge teaches and a POSITA would have understood that for the touch screen in Collinge's mobile device 104 to display information and receive and act on user input as taught by Collinge, the touch screen must necessarily be coupled to a processor. *Collinge,* [0147], Fig. 16. A POSITA would understand that Collinge's user interface is *coupled to the processor* because Collinge expressly teaches that mobile payment application 106, which is executed by *the processor* of mobile device 104, is what displays a notification on the user interface. *Collinge* at [0041], [0107], [0112], [0117]. Thus, the user interface is necessarily coupled the processor, because if the user interface were not coupled to the processor, then mobile payment application, which is executed by the processor, would not be able to display a notification on the user interface. Collinge teaches that the display interface is "coupled" to the processor via the communication interface:



Collinge, Fig. 19. (annotated). Collinge's communications infrastructure may be a "bus, message queue, network, multi-core message-passing scheme, etc." *Collinge*, [0150]. System 1900, shown in Figure 19 above, further confirms that the mobile device 104's touch screen (display interface) and display is "coupled" to the processor by the communications infrastructure 1906. 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]. 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). 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].

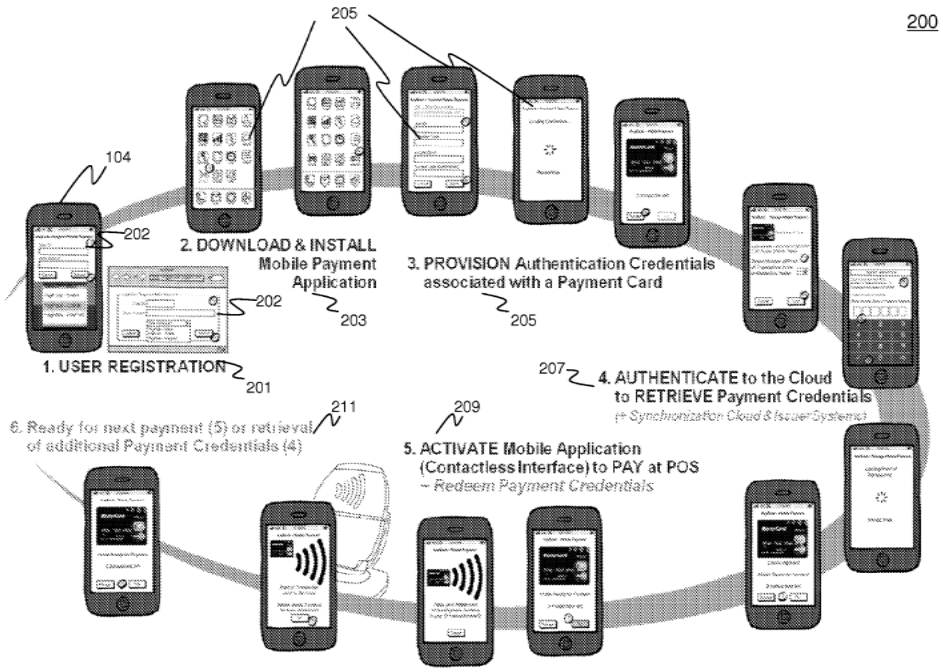


FIG. 2A

'248 Provisional (Ex.1006) at Figure 2A. 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 corresponds to a processor 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 applies to mobile device 104 (the *electronic device*). Additionally, a POSITA would have understood that in Figure 19, display interface 1902 is Collinge's touchscreen. It was well-known that a touch screens of a mobile device

was used for 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 allow 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. 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. Therefore, Collinge teaches a user interface (display) coupled to a processor.For this additional reason, Collinge's display interface (the touchscreen) is coupled to a processor. A POSITA would have understood that Collinge's display interface and display in Figure 19 is Collinge's touchscreen.

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

209. Collinge teaches a touchscreen (user input device) coupled to the processor. *See* Claim 1(a)(2).

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

210. As I discussed above at Claim 1(b), Collinge teaches a user of mobile device 104 inputting an activation code, such that card profile 116 and single use

key 118 are transmitted to mobile device 104, which *read[ies] the device to perform the payment transaction*.

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

211. As discussed above at Claim 1(c), College in view of Lin teaches mobile device 104 receiving a payment request and discussed above at claim 1(c), College in view of Lin teaches displaying information reflecting the payment request on mobile device 104. A POSITA would have understood that in the combination of Collinge and Lin, it is the *processor* that causes display of the payment request information on mobile device 104, because the mobile payment application 106 which is used to conduct payment transactions on mobile device 104 is executed by the processor of mobile device 104. *Collinge* at [0041].

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

212. As I discussed above at Claim 1(d), Collinge in view of Lin teaches displaying an image representing a selected issued payment account. The *issued payment account* is *user-selectable* because, as shown in Figure 14E of Lin, the user selects the account from a list of accounts.

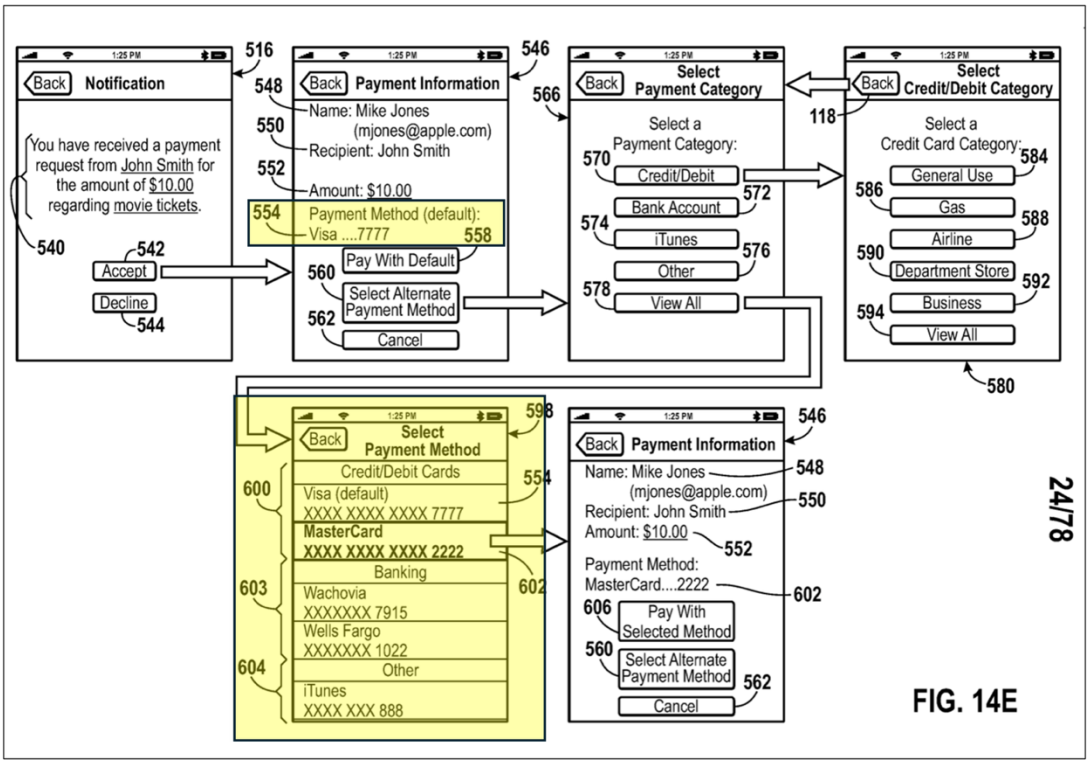


FIG. 14E

Lin at Figure 14E.

213. Like above at Claim 39(g), a POSITA would have recognized that it is the *processor* that causes display of the *image representing at least one user-selectable issued payment account* because the mobile payment application 106, which conducts payment transactions on mobile device 104, is executed by *the processor* of mobile device 104.

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

214. Collinge teaches generating a payment cryptogram/CVC3 (*limited-use payment information*) that is valid only for a single transaction by using the

"generating key" (part of single use key 118) and based on the application transaction counter (*based on a per-transaction sequential parameter*). Claim 1(e). Additionally, a POSITA would have found it obvious and been motivated to modify Collinge according to the teachings of Sahota such that mobile device 104 would maintain its own application transaction counter such that the peer-transaction sequential parameter used in generating the payment cryptogram would *originat[e] from the electronic device*. *See* Claim 1(f). Additionally because Collinge teaches generating the payment cryptogram (CVC3) based on the ATC and based on the "generating key" that is part of single use key 118 (the *secret information associated with a selected issued payment account*, see claim 39(b)(1). Collinge in view of Sahota teaches *dynamically generate a limited-use payment information based on a per-transaction sequential parameter originating from the electronic device, and secret information associated with a selected issued payment account*.

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

215. Collinge teaches that the payment credentials and payment cryptogram are transmitted to the point-of-sale terminal 120 (*NFC recipient*) via NFC. *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. 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)."), [0121] ("In step 1408, the point-of-sale terminal 120…may provide transaction data to the acquirer 122 including the payment credentials and payment cryptogram.").

216. As I discussed above at Claim 1(e), Collinge teaches the CVC3, a payment cryptogram is generated by combining multiple values one of which is the session key unpredictable number. As discussed above Collinge teaches the payments cryptogram may be "an application cryptogram or a dynamic card validation code (CVC3)." *Collinge*, [0077]. Because Collinge's CVC3 payment cryptogram is based on a combination of values including the session key unpredictable number (KS_{UN}) (*payment authority information*) and the payment cryptogram is sent to the point-of-sale terminal 120 (*NFC recipient*), Collinge teaches *cause the transmission, via said NFC interface, a payment information combination comprising the dynamically generated limited-use payment information and said payment authority information, for receipt by an NFC recipient*. *Collinge* 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.")

39. *39(k): "wherein the NFC interface is operable, in response to transmitting said payment information combination, to receive status information reflecting a transaction processing status of*

said payment transaction; and wherein the user interface is operable to provide an indication of the status information."

217. *See* Claim 1(i).

40. Claim 41: "The device of claim 39 wherein the payment authority information comprises a secret information shared by both the electronic device and a payment processing authority."

218. *See* Claim 5.

41. Claim 44: "The device of claim 39 wherein the processor is operable to cause the transmission of issued payment account information and in response thereto, to receive the processing authority information."

219. *See* claim 3.

42. Claim 45: "The device of claim 39 wherein the dynamically generated limited-use payment information comprises a cryptogram number, and further wherein the processor is operable to cause transmission, via said NFC interface, of a payment information combination comprising the dynamically generated limited-use payment information and at least a portion of said payment authority information in connection with the payment transaction in place of at least a portion of the payment information associated with said selected issued payment account."

220. As I discussed above at Claim 1(e), Collinge's payment cryptogram (CVC3) (*cryptogram number*) is generated based on part on the session key unpredictable number (KS_{UN}). The CVC3 payment cryptogram is transmitted to the point-of-sale terminal 120 via the *NFC interface* and the CVC3 payment cryptogram is used in place of the issuer provided CVC. *See* Claims 1(e) and 1(h).

43. Claim 46: "The device of claim 45 wherein the processor is operable to cause the transmission of issued payment account information and in response thereto, receive the processing authority information."

221. *See* Claim 3.

44. Claim 49: "The device of claim 39, wherein said user interface comprises a display and wherein said user input device comprises a touch panel disposed adjacent to said display and wherein further the processor is operable to identify an authorized user by validating a valid user passcode input to the touch panel."

222. As I discussed above at Claim 39(d), Collinge teaches mobile device 104 having a user interface that displays a notification to user 102. Collinge further teaches that the *user input device* is a touch screen (*wherein said user input device comprises a touch panel*). A POSITA would understand that the user interface comprises a display. The display is the glass screen of the mobile device that displays the user interface to the user. A POSITA would further understand that the touch screen of mobile device 104 is disposed adjacent to the display because the user 102 of mobile device 104 would view the user interface on the display and use the touch screen to interact with the user interface. In other words, the touch screen of mobile device 104 is adjacent to the display because in order to manually interact with the user interface displayed on the display, the user uses the touch screen. Thus, Collinge teaches *wherein said user interface comprises a display and wherein said user input device comprises a touch panel disposed adjacent to said display*.

223. Additionally, as I described above at Claim 1(a)(2), Collinge teaches a user may input a PIN using the touch screen. *Collinge* at [0133]. A POSITA would understand upon entering the PIN, the processor would operate to *identify an authorized user by validating a valid user passcode input to the touch panel*. Collinge expressly teaches that "the user 102 may provide a mobile PIN for authentication. 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* at [0051]. Thus, inputting the correct PIN into the touch screen constitutes *identify[ing] an authorized user by validating a valid user passcode input to the touch panel*. A POSITA would further understand that it is *the processor* of mobile device 104 that performs this function, because the mobile payment application 106, which is executed by *the processor*, is what receives the mobile PIN. Accordingly, Collinge teaches *wherein further the processor is operable to identify an authorized user by validating a valid user passcode input to the touch panel*.

> *45. Claim 50: "The device of claim 39, wherein said user interface comprises a display and wherein said user input device comprises a touch panel disposed adjacent to said display and wherein further the processor is operable to identify an authorized user by displaying a security challenge question presented on the display and receiving a correct user response thereto."*

224. *See* Claims 1(a) and 39(d).

46. Claim 55(a): "The device of claim 39, wherein the processor is operable to: receive a user-selection of an issued payment account presented on the user interface, received the user input device coupled to the processor, and"

225. See Claim 1(d).

47. Claim 55(b): "responsive thereto, select from the memory a specific processing authority information corresponding to the user-selected issued payment account information, and"

226. Collinge teaches that mobile payment application 106 (on mobile device 104) receives card profile 116 (<u>*payment authority information*</u>) which is stored "in the local encrypted database 304." *Collinge* at [0074]. Collinge's card profile includes payment credentials as well as the PAN. *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."); *Collinge*, [0048]("payment credentials included in the card profile 116 may include common payment credentials 202, magnetic stripe (mag stripe) payment credentials 204, and m/chip payment credentials 206.")

227. When performing a payment transaction, the payment credentials as well as the payment cryptogram (CVC3) are transmitted to the point-of-sale terminal 120. *Collinge* at [0070] ("…may transmit the generated cryptogram and payment credentials to a point-of-sale terminal 120."), [0077] ("The mobile payment

application 106 may transmit the payment cryptogram to the merchant point-of-sale terminal 120.")

228. Therefore, because the PAN is stored in the memory of mobile device 104 as part of the payment credentials, and because the PAN is sent to POS 120, the PAN must be selected from memory. Thus, Collinge teaches *responsive thereto, select from the memory a specific processing authority information corresponding to the user-selected issued payment account information*.

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

229. Collinge's payment cryptogram (CVC3) is generated based in part on the KS_{UN}, and the CVC3 is used in place of the issuer provided CVC. *See* Claim 1(e). As discussed above, the issuer provided CVC was well known. For example, 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].

49. Claim 56(Pre): "An electronic device for completing a payment transaction, the electronic device comprising:"

230. *See* Claim 39(Pre).

50. 56(a): "a processor;"

231. *See* Claim 39(a).

51. 56(b): "a memory coupled to the processor,"

232. *See* Claim 39(b).

52. 56(b)(1): "wherein the memory stores a payment authority information associated with a user-selectable issued payment account, and wherein the payment authority information includes a secret information;"

233. *See* Claim 39(b)(1).

53. 56(c): "a near field communications (NFC) interface coupled to the processor and operable to receive a payment request associated with the payment transaction;

234. *See* Claim 39(c).

54. 56(d): "a user interface coupled to the processor;"

235. *See* Claim 39(d).

55. 56(e): "a user input device coupled to the processor; and,"

236. *See* Claim 1(a)(2); 39(e).

56. 56(f):" wherein said processor is operable to: responsive to a priming operation, wherein the priming operation is operable to ready the device to perform the payment transaction,"

237. *See* Claim 1(b); 39(f).

57. 56(g): "cause the display of information associated with the payment request;"

238. *See* Claim 1(d); 39(g).

58. 56(h): "cause the display of an image representing the user-selectable issued payment account; and,"

239. *See* Claim 1(d); 39(h).

59. 56(i): "dynamically generate a limited-use payment information based on a per-transaction sequential parameter originating from the electronic device, and the secret information associated with the user-selectable issued payment account; and,"

240. *See* Claim 39(i).

60. 56(j): "cause the transmission, via said NFC interface, of a payment information combination comprising, the dynamically generated limited-use payment information and at least a portion of said payment authority information, for receipt by an NFC recipient;"

241. *See* Claim 39(j).

61. 56(k): "wherein the NFC interface is operable, in response to transmitting said payment information combination, to receive status information reflecting a transaction processing status of said payment transaction; and wherein the user interface is operable to provide an indication of the transaction status information."

242. *See* Claim 39(k).

62. Claim 60: "The device of claim 56, wherein the secret information is shared by both the electronic device and a payment processing authority."

243. *See* Claim 5.

63. Claim 61: "The device of claim 56, wherein the processor is operable to cause the transmission of issued payment account information and in response thereto, to receive the payment authority information."

244. *See* Claim 3.

64. Claim 62: "The device of claim 56, wherein the dynamically generated limited-use payment information comprises a cryptogram number, and further payment information

combination is used in place of at least a portion of fixed payment information associated with said user-selectable issued payment account."

245. Collinge's CVC3 is used in place of the issuer provided CVC. *See* Claim 1(e). As discussed above, the issuer provided CVC was well known. For example, 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].

65. Claim 63: "The device of claim 62, wherein the processor is operable to cause the transmission of issued payment account information and in response thereto, receive the payment authority information."

246. *See* Claim 3.

66. Claim 66: "The device of claim 56, wherein said user interface comprises a display and wherein said user input device comprises a touch screen interface of the display, and wherein further the processor is operable to identify an authorized user by validating a valid user passcode input to the touch screen interface."

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

67. Claim 67: "The device of claim 56, wherein said user interface comprises a display and wherein said user input device comprises a touch screen interface of the display, and wherein further the processor is operable to identify an authorized user by displaying a security challenge question presented on the display and receiving a correct user response via said touch screen interface of the display."

248. As I discussed above at Claims 39(d), Collinge teaches *wherein said user interface comprises a display and wherein said user input device comprises a touch screen interface of the display*. 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. *See* Claims 1(a), 11.

> *68. Claim 72(Pre): "The device of claim 56, wherein the processor is operable to receive, via the user input device, a user-selection of said user-selectable issued payment account presented on the user interface, and"*

249. *See* Claim 1(d).

> *69. Claim 72(a): "in response thereto, is further operable to select from memory the payment authority information corresponding to selected user-selectable issued payment account, and"*

250. *See* Claim 55(b).

> *70. Claim 72(b): "is further operable to use said payment information combination in place of at least a portion of fixed payment information associated with said selected user-selectable issued payment account."*

251. Collinge's CVC3 payment cryptogram is used in place of the issuer provided CVC. *See* Claim 1(e); 55(c). As discussed above, the issuer provided CVC was well known. For example, 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].

X. OPINIONS REGARDING GROUND 2: *COLLINGE IN VIEW OF LIN, SAHOTA, AND SMITH.*

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

252. Collinge teaches a "system 100 for the generating and provisioning of payment credentials to a mobile device lacking a secure element." *Collinge* at [0039], Figure 1. Collinge's system 100 is *a system for completing a payment transaction* because "the system 100 and the use of the payment token payment may enable user 102 to use mobile device 104 **to conduct NFC payment transactions**[.]" *Collinge* at [0046].

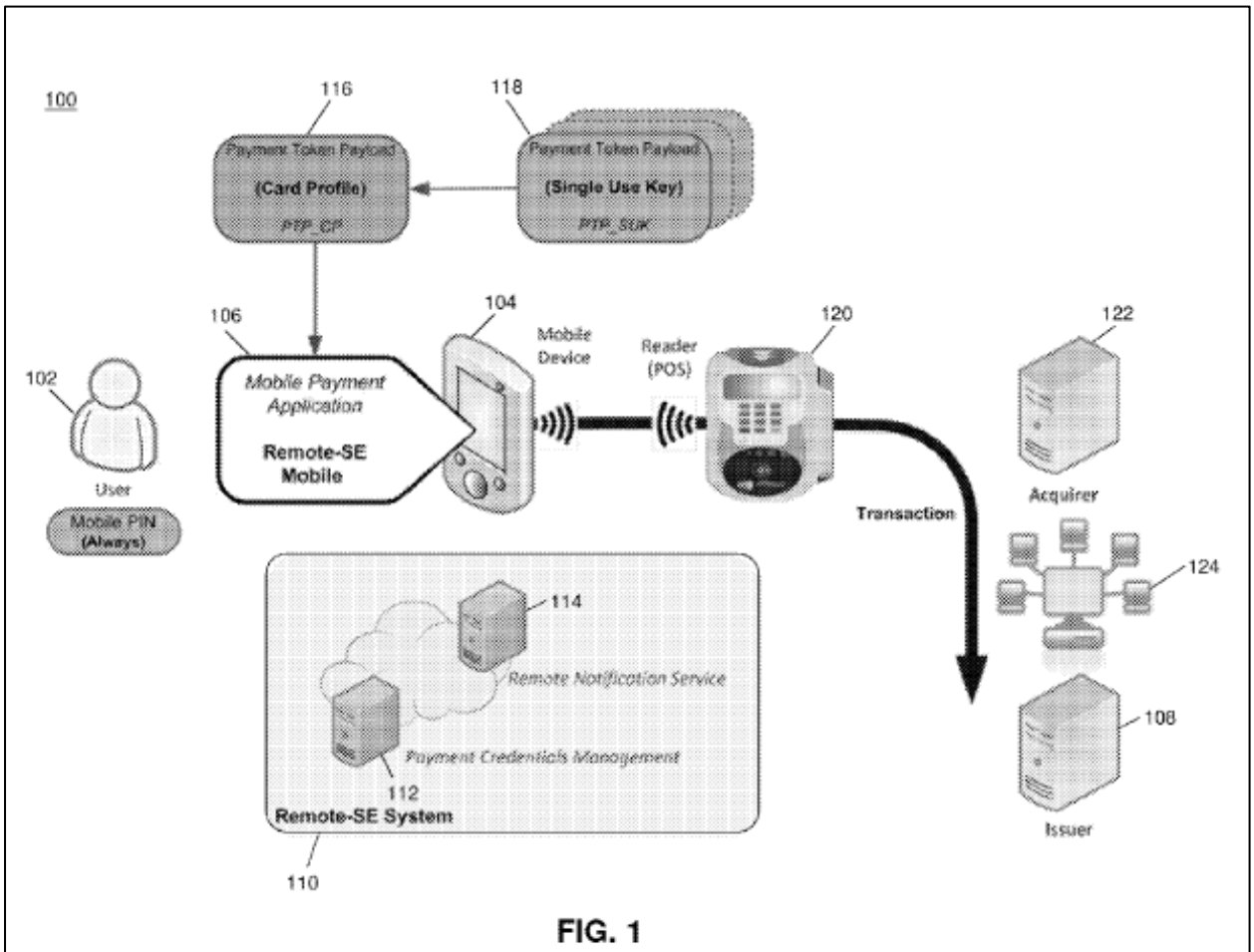


FIG. 1

Collinge at Figure 1 (illustrating system 100 that enables user 102 to conduct NFC payment transactions).

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

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

3. 29(b):" a processor;"

254. *See* Claim 1(a)(1).

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

255. *See* Claims 1(a)(3), 1(c).

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

256. *See* Claim 1(a)(2).

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

257. Collinge's mobile device 104 (*the electronic device*) is *operable to cause the display of information reflecting device-readiness, the payment request, and an image representing at least one selected issued payment account* when combined with the teachings of Lin. *See* Claim 1(d). Specifically, Collinge in view of Lin teaches displaying the payment request and an image representing at least one selected issued payment account.

258. Collinge additionally teaches that "mobile payment application 106 may display a notification to the user 102 via a user interface to indicate that the mobile payment application 106 is ready to conduct a contactless payment transaction." *Collinge* at [0112]. Therefore, Collinge also teaches that *the electronic device is operable to cause the display of information reflecting device-readiness*.

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

259. Collinge's mobile device 104 (*the electronic device*) is *operable to dynamically generate limited-use payment information based on a sequential counter count from the electronic device* when combined with Sahota. *See* Claims 1(e), 1(f).

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

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

a) Collinge's Teachings

261. 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], [0048]-[0049] ("common payment credentials 202 may include all data elements...data elements may include payment account number"); [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.") (emphasis added). A PAN is the unique identifier number found on the front of a credit, debit, or prepaid card or the like. *See, e.g., Brown (Ex.1043)* at 1:64–2:4. ("Several of the elements which are embossed and magnetically recorded on MasterCard, Visa, and other typical payment cards are there to uniquely identify

the account cardholder. A standardized personal account number (PAN) comprises four fields, e.g., a system number, a bank/product number, a user account number, and a check character. This PAN is typically sixteen digits but may be up to nineteen digits.")

262. 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)* at 159-160. Collinge teaches that using a Virtual PAN is safer and can "mitigate the risk of any misuse of a PAN value." *Id.*

263. 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:

500

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 at Figure 5.

264. 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)* at 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)* at [0078]. As another example, Roberts, a Mastercard patent teaches that "a PAN Sequence Number…in

combination with the PAN uniquely identifies the card." *Roberts (Ex.1044)* at [0074].

b) Smith's Teachings

265. Smith teaches a "mobile device" that "may…be used…with a near field communications enabled purchasing transaction." *Smith* at 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* at [0026].

266. This "temporary PAN is mapped to a **mobile PAN (e.g., such as a PayPass® PAN, or PPAN)**." *Smith* at [0026] (emphasis added). The PPAN (*device-specific user account information*) is "assigned to the mobile device 104." *Smith* at [0016]. The PPAN is "stored in the mobile device 204." *Smith* at [0022].

267. Once an actual PAN is issued, the temporary PAN is swapped with the actual PAN. *Smith* at [0026], [0040]. The PPAN (*device-specific user account information*) is then associated with a "related PAN[.]" *Smith* at [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* at [0040]. The PPAN is a different number from the actual PAN as depicted below.

600

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

FIG. 6

Smith at Fig. 6.

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

269. Smith teaches during a registration process the consumer will "access a web site operated by issuer 420 and enter details, including his or her personal information, a model number of the mobile telephone 410, a phone number of the mobile telephone 410, and/or an indication of a mobile network operator

associated with the telephone 410." *Smith*, [0028]. In response the card issuer transmits a response back to the mobile device that includes "a record identifier, an issuer code, a PPAN, an expiration date (e.g., an expiration month and year), a mobile phone number and carrier identifier, a verification code (e.g., selected by the consumer during the registration process), and/or an encryption key for security purposes." *Smith*, [0029]-[0030].

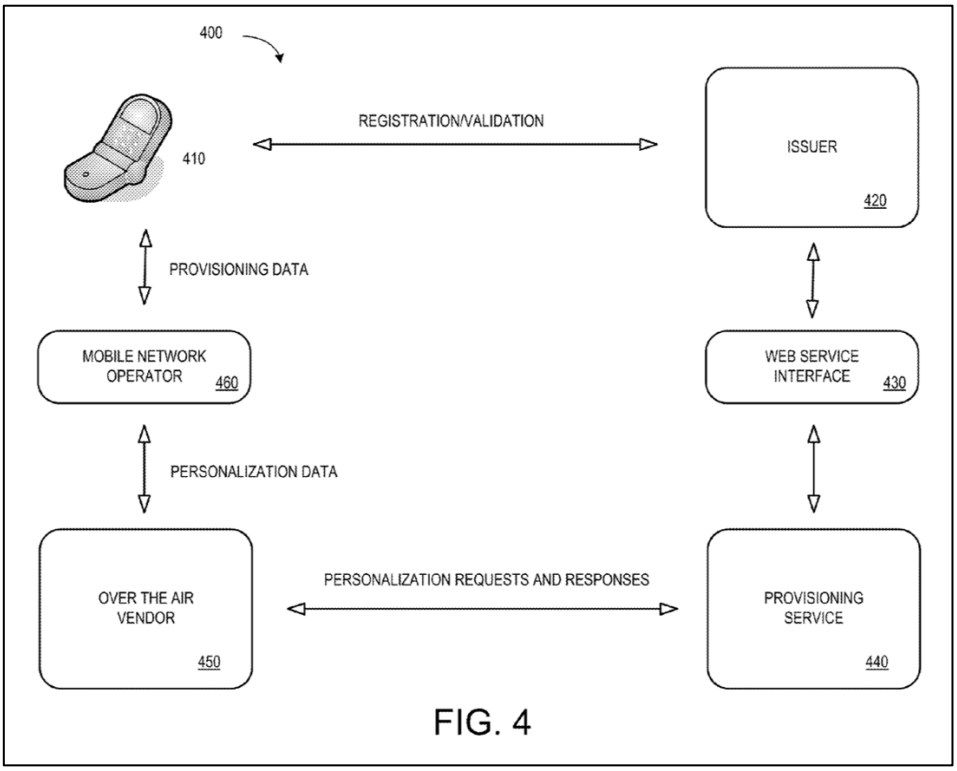


FIG. 4

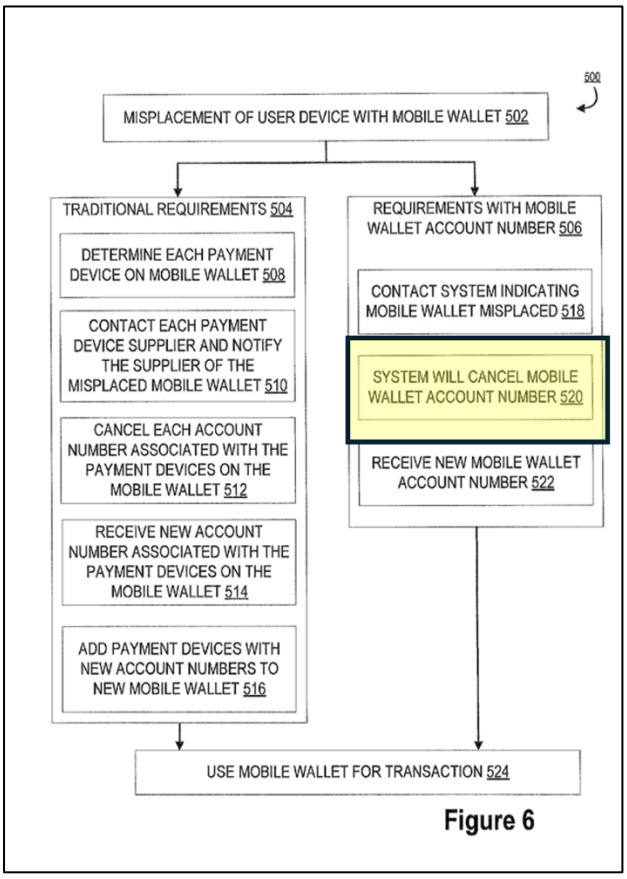
Smith, Fig. 4. During a transaction "the point of sale device is provided with information including the PPAN stored in the mobile device 204" by using NFC. *Smith* at [0024]. Once the PPAN is sent the "payment network 218 identifies the PPAN and requests a look up of the related PAN from the PAN mapping/account

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

270. The issuer can "implement dual account number structures" for "multiple NFC-enabled handsets may be managed for a single account." *Smith* at [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)* at [0035]. Accordingly, a POSITA would have understood Smith's PPAN is a distinct *device-specific user account information* for a payment account on a particular "mobile device."

271. 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* at [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.

272. 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. *See* '634 Patent, Claim 3. 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)* at [0074], Fig. 6.



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

273. A POSITA would have appreciated that such a modification would have improved card management, allowing the PPAN to be canceled if Collinge's mobile device is lost or compromised without affecting other devices using the same underlying PAN.

c) Motivation to Combine

274. 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)* at 159-160.

275. 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-specific user account information*) that is used in place of the PAN/account number. *Smith* at [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.

276. 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* at [0022]. Smith also teaches the issuer has to "request[] a look up of the related PAN from the PAN mapping/account generation service 210." *Smith* at [0023]. Both supporting that the PAN does not need to be stored in Smith's device.

277. 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)* at 51. ("Without a secure infrastructure for computing on the device, achieving secure m-commerce may not be possible."); *Collinge* at [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 an 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). For example, Vizzari 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)* at 5.

278. 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)* at 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* at [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* at [0024].

279. 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."); *Smith*, [0029]-[0030].

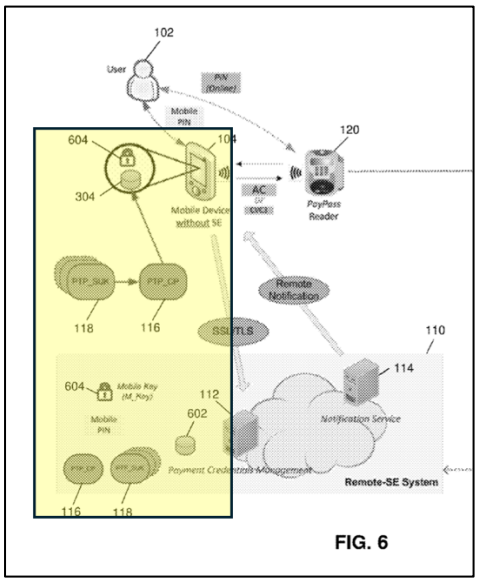


FIG. 6

Collinge, Fig. 6. (annotated excerpt).

280. 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 at 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."

500

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.

281. 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* at [0068]; *Smith* at [0022]. (The PPAN is "stored in the mobile device 204."). The PPAN would also be at least transitorily stored by Collinge's processor when received by Collinge's mobile device and when it is used by Collinge's mobile device to make a payment. *Collinge* at [0048]-[0049], [0063].

282. 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)* at 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)* at 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)* at 159-160.

283. Likewise, a POSITA would have substituted Smith's PPAN for Collinge's PAN when making payment transactions, as taught by Smith. *Smith* at [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* at [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.

284. 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. Likewise, the same simple substitution would have predictably allowed the POSITA to provision Smith's PPAN to Colline's mobile device 104 in place of the PAN to better protect sensitive financial information.

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

285. As I discussed above at Claim 1(h), Collinge teaches transmitting the generated payment cryptogram (*dynamically generated limited-use payment information*) and payment credentials to the point-of-sale terminal 20 (*NFC recipient*) via the *NFC interface* for conducting a payment transaction (*for use in connection with payment transaction*). Collinge teaches generating limited-use payment information (payment cryptogram). *See* Claim 1(e).

286. Collinge, in view of Smith, renders obvious transmitting *a combination of said dynamically generated limited-use payment information and said static device-specific user account information*, including a CVC3 (*limited-use payment information*) and PPAN (*static device-specific user account information*) when sending complete payment information to a POS terminal via Collinge's NFC interface, in place of the static CVC and PAN (*information associated with said selected issued payment account*). Smith's PPAN is part of the payment credentials instead of the PAN.

287. 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.")

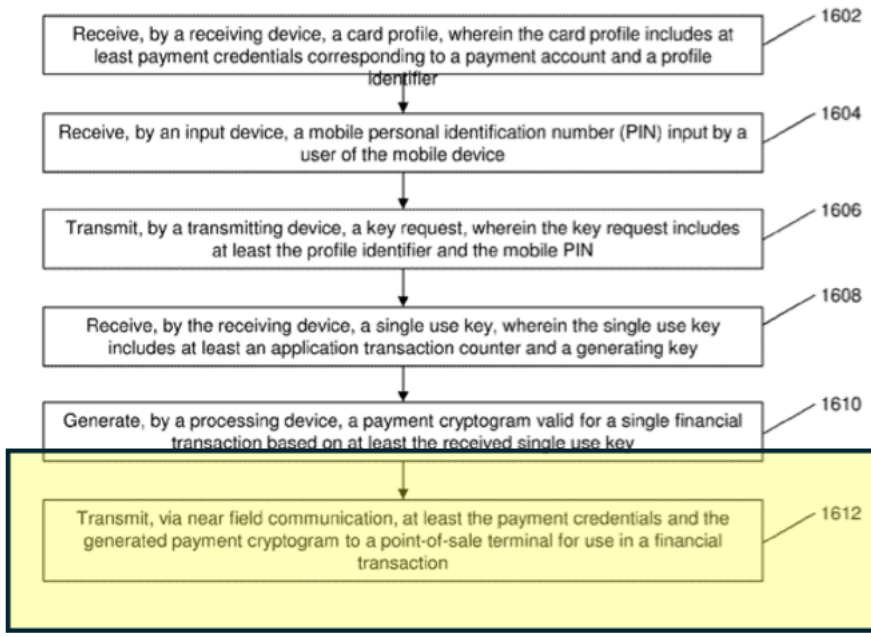


FIG. 16

Collinge, Fig. 16. (annotated); *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.").

288. As shown above, Collinge's card profile includes the PAN. Collinge's card profile is included in the payment credentials A POSITA would have substituted Smith's PPAN for Collinge's PAN when making payment transactions, as taught by Smith. *Smith,* [0018] ("the process of personalizing the mobile device 104 with the software (including the PPAN…[o]nce the personalization or

loading of the payment application is complete, the customer 102 may use the mobile device **104** to complete payment transactions."). A POSITA would again have recognized that substitution of a 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.

289. Because the payment credentials include the static PPAN (*said device-specific user account information*), and because both the CVC3 payment cryptogram and the PPAN are transmitted to the point-of-sale terminal 120, Collinge in view of Smith teaches *wherein the electronic device is operable to transmit a combination of said dynamically generated limited-use payment information and said static device-specific user account information to an NFC recipient via, said NFC interface for use in connection with payment transaction in place of information associated with said selected issued payment account*.

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

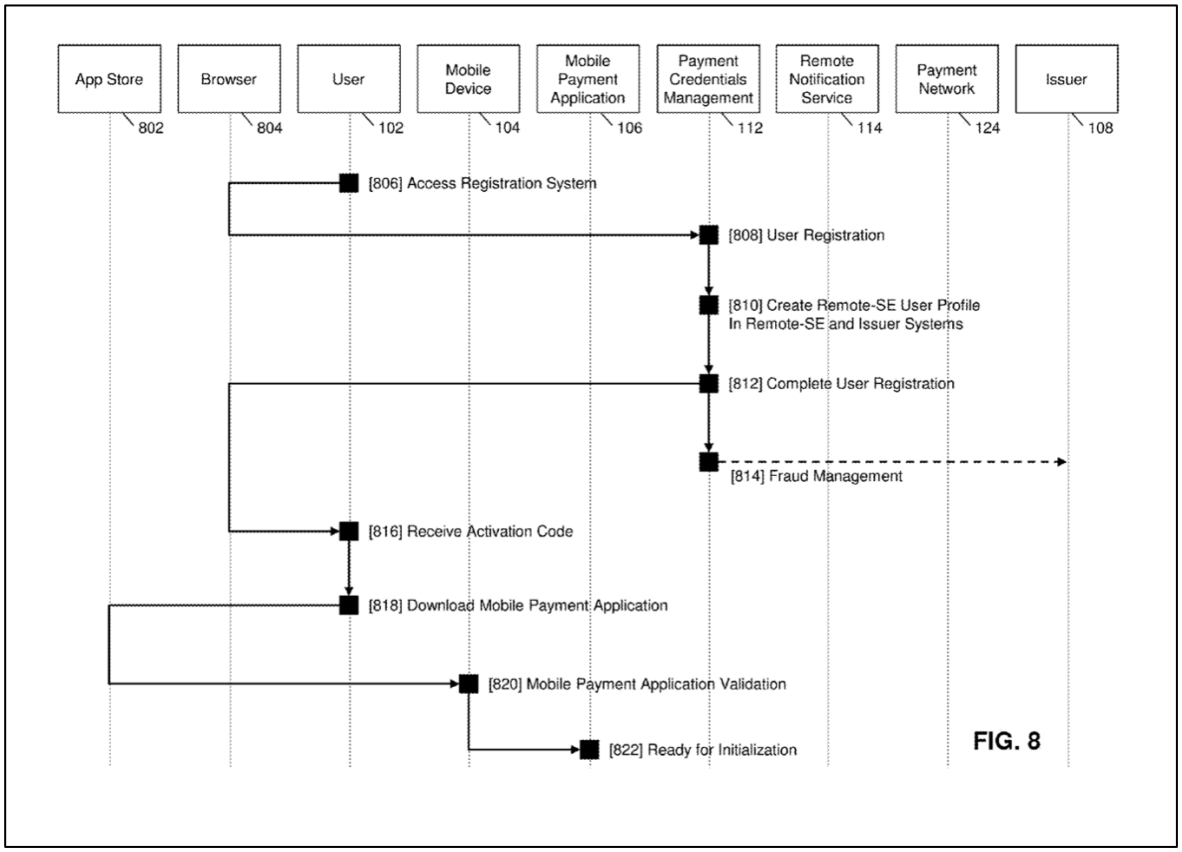
290. As I discussed above at Claim 1(i), Collinge teaches receiving and displaying a status information (such as "done") reflecting a status of the payment transaction after the payment cryptogram and the payment credentials are transmitted because transmission of that initiates a payment transaction. Thus, Collinge teaches *wherein the electronic device is operable, subsequent to transmission of said combination, to receive a status information reflecting a status of said payment transaction; and, wherein the touch-screen display is operable to display as indication of said status information*.

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

291. Prior to Collinge's *priming operation* (which may include inputting a PIN; bringing Collinge's mobile device within proximity of an NFC recipient, *see* Claim 1(a)), Collinge teaches a user inputting an activation code or bringing Collinge's mobile device 104 near an NFC recipient, *See* Claim 1 (a), Collinge's payment system transmits the user-provided issued payment account information from Collinge's mobile phone to the issuer (*payment processing authority)* during the registration process.

292. Collinge teaches in step 806 "[a]s part of the registration, the user 102 may provide account details for a payment account, and the payment credentials management service 112 may ensure the payment account is

eligible for remote payment transactions." *Collinge*, [0089]. In the first step of method 500, step 502, "the user may register with the remote-SE system 110 to use the mobile device 104 for contactless payment transactions." *Collinge* at [0065]. 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" is taught by Collinge with respect to Figure 8. *Collinge* at [0088].



Collinge, Fig. 8.

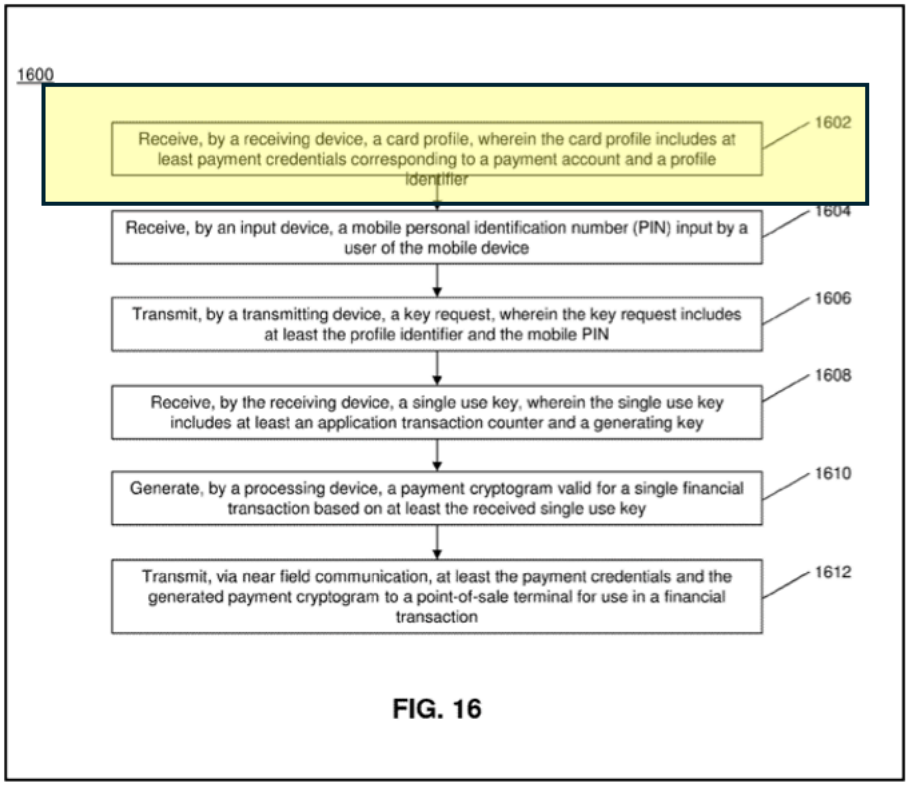
293. "At step 808, the user 102 may register with the payment credentials management service 112 via the browser 804. As part of the registration, the user

102 may provide account details for a payment account[.]" *Collinge* at [0089]. The payment credentials management service 112 may then "create a user profile for the user 102 in the remote-SE system 110." *Collinge* at [0090]. At step 814, "the payment credentials management service 112 may synchronize information (e.g., the user profile, activation code status, etc.) with the issuer 108 for fraud management." *Collinge* at [0090].

294. A POSITA would have understood that by synchronizing information with the issuer 108, including payment account information (*issued payment information*) in the user profile, Collinge thereby teaches *prior to the priming operation, transmitting the issued payment information for receipt by a payment processing authority*.

12. Claim 3(b): "in response to said transmitting issued payment information, receiving a static device account information that is unique to the electronic device."

295. As I discussed above at Claim 29(g), Collinge in view of Smith teaches a PPAN that is *static* and *unique to the electronic device*. *See* Claim 29(g); *Smith*, Fig. 4; [0029]-[0030]. In the combination of Collinge and Smith, the PPAN is received in place of the PAN information in Collinge's payment credentials/card profile 116, as I discussed above at Claim 29(g). Provisioning of the card profile 116 to mobile device 104 occurs after registration (when issued payment information is transmitted). *See* Claim 29(g). *Collinge*, Figs. 11, 15-16, [0104].



Collinge, Fig. 16. (annotated)

296. Thus, Collinge in view of Smith teaches *in response to said transmitting issued payment information, receiving a static device account information that is unique to the electronic device*.

> *13. Claim 4(a): "The method of claim 3 further comprising: combining said limited-use payment information and said static device account information, to [produce] a combined payment information;"*

297. *See* Claim 29(h).

> *14. Claim 4(b): "transmitting said combined payment information, in place of the issued payment account information, via said NFC [interface] for receipt by an NFC recipient; and"*

298. *See* Claim 29(h).

15. Claim 4(c): "receiving, via the NFC interface, and in response to transmitting said combined payment information, transaction processing information reflecting a status of said payment transaction."

299. *See* Claim 1(i).

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

300. As I discussed above at Claim 1(e), Collinge teaches that the CVC3 payment cryptogram is *dynamically generat[ed]*.

301. Collinge teaches wherein the dynamically generating further comprised dynamically generating the CVC3 payment cryptogram (*limited-use payment information*) based on secrets (session key unpredictable number, single use key) shared with the issuer (payment processing authority information).

302. Collinge teaches that the CVC3 payment cryptogram (*limited-use payment information*) is generated using the generating key within the single use key based on "the supplied CVC3 value, the session key unpredictable number, the application transaction counter, and the reader unpredictable number." *Collinge* at [0145]; *Collinge*, [0050] ("[t]he single use key 118 may be a payment token used one time to generate a payment cryptogram to be used in a payment

transaction...[t]he single use key may include an application transaction counter (ATC) and a generating key 208[.]")

303. The issuer 108 validates the generated CVC3 payment cryptogram. *Collinge,* [0141]. Specifically, the issuer receives "at least the K_{SUN},UN_{CLOUD}, and application transaction counter" (<u>*secrets*</u>) and the issuer 108 uses that information "in validating the generated CVC3 value used in the financial transaction." *Collinge*, [0141]. These values are therefore shared with the issuer 108 (<u>*payment processing authority*</u>). A POSITA would have been very familiar with methods of validating a CVC3 payment cryptogram, as recognized by Collinge. *Collinge,* [0077]. Typically, the issuer will recompute the payment cryptogram and compare the issuer-generated payment cryptogram to the cryptogram received from the merchant. When generating the cryptogram, the issuer will use the K_{SUN}, UN_{CLOUD}, and ATC. *Collinge,* [0141]; Claim 1(i). A POSITA would have understood that the K_{SUN} is secret information shared between two parties (<u>*secret*</u>). The issuer also computes $Cloud_CVC3_{TRACK1/2}$:

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

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

304. Collinge teaches generating a CVC3 payment cryptogram based on the following values: "the supplied CVC3 value, the session key unpredictable number, the application transaction counter, and the reader unpredictable number." *Collinge*, [0145]; '248 Provisional (Ex.1006), Table 1.

> The Mobile Payment Application use a specific process to generate the CVC3 using (KS_{UN}, Cloud_$CVC3_{TRACK1/2}$, ATC and UN_{READER})

305. 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 in 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 <u>*secret information*</u> 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. ("…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 processing authority*).

17. Claim 6: "The method of claim 5, wherein the limited-use payment information is based on at least one secret information shared by both the electronic device and the payment processing authority."

306. As I discussed above at Claim 5, Collinge teaches that the CVC3 payment cryptogram (*limited-use payment information*) is based on the session key unpredictable number and single use key. The session key unpredictable number and single use key 118 is *at least one secret information* because it is delivered to mobile device 104 as encrypted, thereby indicating it is a secret because if it were not a secret, it would not be encrypted. *Collinge* at [0144]. Additionally, the session key unpredictable number is shared by both mobile device 104 and issuer 108 and is thus *shared by both the electronic device and the payment processing authority*.

18. Claim 17(a): "The method of claim 1, further comprising: prior to the priming operation, transmitting the issued payment information for receipt by a payment processing authority; and,"

307. *See* Claim 3(a).

19. Claim 17(b): "in response to said transmitting issued payment information, receiving a static device account information that is unique to the electronic device."

308. *See* Claims 29(g) and 3(b).

20. Claim 18(a): "The method of claim 17 further comprising: combining said limited-use payment information and said static device account information, to produce a combined payment information;"

309. *See* Claim 29(h).

21. Claim 18(b): "transmitting said combined payment information, in place of the issued payment account information said NFC interface for receipt by an NFC recipient; and"

310. *See* Claim 29(h).

22. Claim 18(c): "receiving, via the NFC interface, and in response to transmitting said combined payment information, transaction processing information reflecting a status of said payment transaction."

311. *See* Claim 1(i).

23. Claim 19: "The method of claim 18, wherein the dynamically generating further comprises dynamically generating the limited-use payment information based on payment processing authority secret information."

312. *See* Claim 5.

24. Claim 20: "The method of claim 19, wherein the limited-use payment information is based on at least one secret information shared by both the electronic device and the payment processing authority."

313. *See* Claim 5.

25. Claim 21: "The method of claim 17, wherein the dynamically generating further comprises dynamically generating the limited-use payment information based on payment processing authority secret information."

314. *See* Claim 5.

26. Claim 22: "The method of claim 21, wherein the limited-use payment information is based on at least one secret information shared by both the electronic device and the payment processing authority."

315. *See* Claim 5.

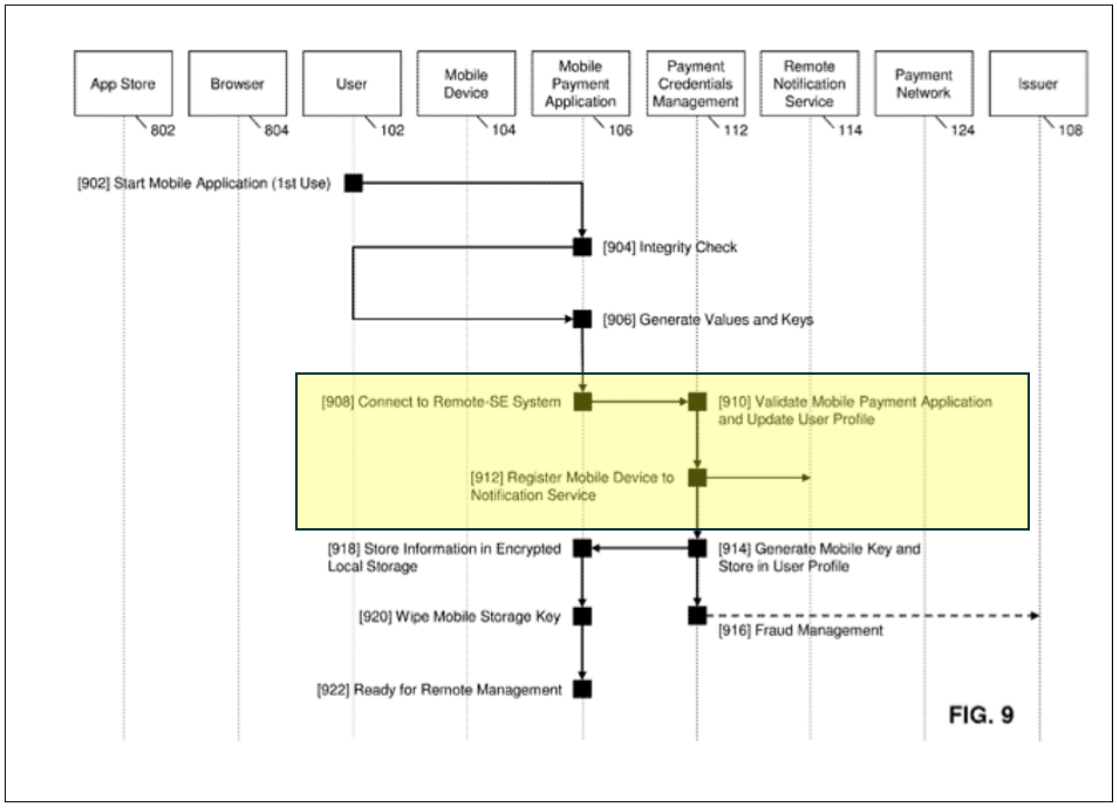
27. Claim 23(a): "The method of claim 1, further comprising: prior to the priming operation, transmitting the issued payment information, user information and device-specific information; and,"

316. As discussed above, Collinge teaches prior to the priming operation, transmitting the issued payment information for receipt by a payment processing authority. *See* Claim 3(a). As discussed in Claim 29(g), Collinge in view of Smith teaches a static device account number (PPAN).

a) Collinge's Teachings

317. Collinge's payment system transmits the user-provided issued payment account information from Collinge's mobile phone to the issuer (*payment processing authority)* during the registration process. *See* Claim 3(a). Collinge already teaches a device identifier such as the unique identifier. Specifically, Collinge teaches "the authentication code may be computed over a unique identifier defined by the remote-SE system 110 to uniquely identify the mobile device 104, which may be provided to the mobile payment application." *Collinge*, [0062]. This unique identifier as shown in step 910 is used to "validate the mobile payment application 106[.]" *Collinge*, [0095]. Collinge teaches "the payment credentials management

service 112 may also register the mobile device 104 with the remote notification service 114 using the unique identifier." *Collinge*, [0095].



Collinge, Fig. 9. (annotated)

b) Smith's Teachings

318. Smith teaches a PPAN that is used in place of a PAN. *See* Claim 29(g).

600

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

FIG. 6

Smith, Fig. 6.

319. Smith teaches during a registration process "the consumer might access a web site operated by issuer 420 and enter details, including his or her personal information, a model number of the mobile telephone 410, a phone number of the mobile telephone 410, and/or an indication of a mobile network operator associated with the telephone 410. According to some embodiments, a one-time PIN or verification code may be established for the consumer during the registration process." *Smith*, [0028].

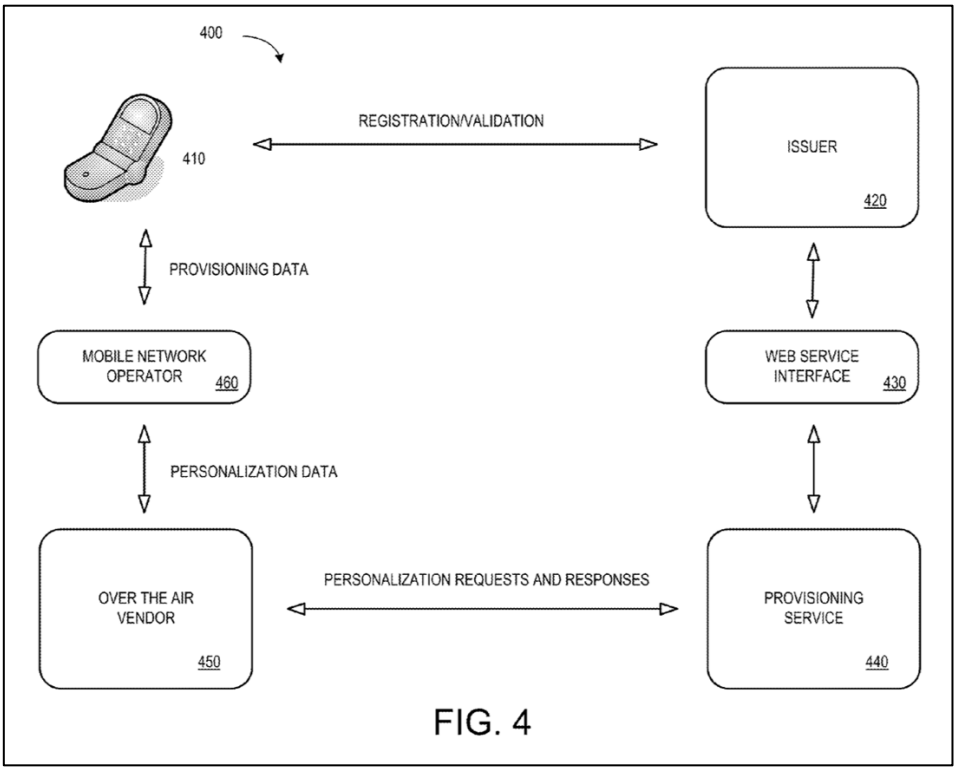


FIG. 4

Smith, Fig. 4.

320. Smith teaches "[t]he card issuer 420 may validate the application may by the consumer, determine the validity of the request, and ensure that sufficient details about the application have been provided. The card issuer 420may then send a personalization request to a provisioning service 440 (e.g., an over-the-air provisioning service associated with MasterCard) via a web service interface 430. ,…The request transmitted from the provisioning service 440 to the over-the-air vendor 450 might include, for example, a record identifier, an issuer code, a PPAN, an expiration date (e.g., an expiration month and year), a mobile phone number and carrier identifier, a verification code (e.g., selected by the consumer during the

registration process), and/or an encryption key for security purposes…The over-the-air vendor 450 may initiate a Wireless Application Protocol (WAP) session via WAP push to the NFC handset 410 via the mobile network operator 460 using the mobile number that was registered by the consumer during the initial phase of the registration process. Note that the WAP push may allow WAP content to be pushed to the mobile handset 410 with minimal user intervention (e.g., the WAP push may be a specially encoded message that includes a link to a WAP address)." *Smith*, [0029]-[0030]. Therefore, Smith teaches that the mobile network operator 460 provisions *a payment processing authority supplied secret information*, such as the PPAN to Smith's mobile device.

c) Motivation to Combine

321. It would have been obvious, and a POSITA would have been motivated to transmit "his or her personal information, a model number of the mobile telephone 410, a phone number of the mobile telephone 410[.]" as taught by Smith with Collinge's card information as discussed in Claim 3(a) prior to the priming operation. *Smith*, [0028]. Collinge already teaches that "the payment credentials management service 112 may also register the mobile device 104 with the remote notification service 114 using the unique identifier" that is used to "uniquely identify the mobile device 104[.]" *Collinge*, [0062], [0095]. A POSITA would have been motivated to transmit identifying device information in Collinge's registration

process as taught by Smith so that the issuer can correctly identify the device when it generates and transmits Smith's device-specific PPAN and would have had a reasonable expectation of success in doing so. A POSITA would have realized that this would have been a use of a known technique (sending device identifying information during registration) to improve Collinge's mobile payment system in the same way.

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

322. Collinge-Smith teaches receiving a device specific PPAN from an issuer which is a payment processing authority supplied secret user information. *See* Claim 3(b); 29(g).

29. Claim 24: "The method of claim 23 wherein said payment processing authority supplied secret information comprises static device account information."

323. *See* Claim 3.

30. Claim 30: "The system of claim 29, wherein the dynamically generated limited-use payment information comprises a cryptogram number."

324. *See* Claim 2.

31. Claim 31: "The system of claim 29, wherein the device-specific user account information comprises static device account information."

325. *See* Claim 29(g).

32. Claim 32: "The system of claim 31, wherein the static device account information comprises a static device account number that is unique to the electronic device."

326. *See* Claims 29(g) and 3(b).

33. Claim 34: "The system of claim 32 wherein the sequential counter count is changed per payment transaction."

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

34. Claim 35: "The system of claim 34 wherein the electronic device is operable to transmit issued payment account information and in response thereto, to receive the static device account information."

328. *See* Claim 3.

35. Claim 36(Pre): "The system of claim 29 wherein the electronic device is further operable to dynamically generate the limited-use payment information based on a shared information: from said user, information associated with said electronic device, information associated with said selected, issued payment account, and at least one secret; and,"

329. *See* Claims 5, 29(h).

36. Claim 36(a): "wherein said shared information is shared by both the electronic device and a payment processing authority."

330. *See* Claim 5.

37. Claim 37: "The system of claim 36 wherein the electronic device is further operable to dynamically generate the limited-use payment information based on payment processing authority secrets."

331. *See* Claim 5.

38. Claim 38: "The system of claim 29 wherein the electronic device is further operable to dynamically generate the limited-use

payment information based on payment processing authority secrets."

332. *See* Claim 5.

39. Claim 40: "The device of claim 39 wherein the payment authority information comprises information that is unique to the electronic device."

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

40. Claim 42: "The device of claim 41 wherein the processing authority information comprises a static device account number."

334. *See* Claims 24; 29(g).

41. Claim 47: "The device of claim 46 wherein the processing authority information comprises a static device account number."

335. *See* Claims 24; 29(g).

42. Claim 57: "The device of claim 56, wherein the payment authority information comprises information that is unique to the electronic device."

336. *See* Claims 5; 29(g).

43. Claim 58: "The device of claim 57, wherein the payment authority information comprises a static device account number."

337. *See* Claims 24; 29(g).

44. Claim 64: "The device of claim 63, wherein the payment authority information comprises a static device account number."

338. *See* Claims 24; 29(g).

XI. OPINIONS REGARDING GROUND 3: *COLLINGE IN VIEW OF LIN, SAHOTA, SMITH, AND KRANZLEY.*

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

339. Collinge in view of Lin, Sahota, and Smith teach *wherein said static device account information comprises a static device account number* (PPAN). Smith teaches an expiration date but is not specific as to if that is assigned to the PPAN. *Collinge* at [0133] ("…card profile 116 may be configured to utilize local data authentication, wherein the local data authentication includes swapping, in the payment credentials, the meaning of an expiration date…"), *Smith* at [0029] ("PPAN, an expiration date (e.g., an expiration month and year)").

340. A POSITA would have found it obvious and been motivated to modify Collinge-Lin-Sahota-Smith according to the teachings of Kranzley such that the PPAN would have *a static device-specific expiration date*.

a) Kranzley's Teachings

341. Kranzley teaches a "static VPAN" (virtual PAN) that may be stored by a "payment application of the mobile device[.]" *Kranzley* at [0036]. Kranzley further teaches that "the payment application also generates an expiration date associated with the static VPAN." *Kranzley* at [0039].

b) Motivation to Combine

342. A POSITA would have found it obvious and been motivated to include an *expiration date* for the PPAN as taught by Kranzley. Because the expiration date would be for the PPAN, which is a static device-specific account number (See Claim 29(g)) the expiration date would be a *static device-specific expiration date*. 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)”); *Caviles* at 2:39-41 (“The customer enters his or her credit card number, **the expiration date of the card**…”) (emphasis added). 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 PAN is decreased. The modification is nothing more than the application of a known technique (assigning an expiration date) to a known device ready for improvement to yield predictable results of increased security. 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. Thus, the modification would have had a reasonable expectation of success.

2. Claim 26: "The method of claim 25 wherein the static device account number is associated with the selected issued payment account on said electronic device."

343. *See* Claims 3 and 29(g).

3. Claim 33: "The system of claim 32 wherein the static device account information further comprises a static device account expiration date."

344. *See* Claim 25.

4. Claim 43: "The device of claim 42 wherein the processing authority information further comprises a static device account expiration date."

345. *See* Claim 25.

5. Claim 48: "The device of claim 47 wherein the processing authority information further comprises a static device account expiration date."

346. *See* Claim 25.

6. Claim 59: "The device of claim 58, wherein the payment authority information further comprises a static device account expiration date."

347. *See* Claim 25.

7. Claim 65: "The device of claim 64, wherein the payment authority information further comprises a static device account expiration date."

348. *See* Claim 25.

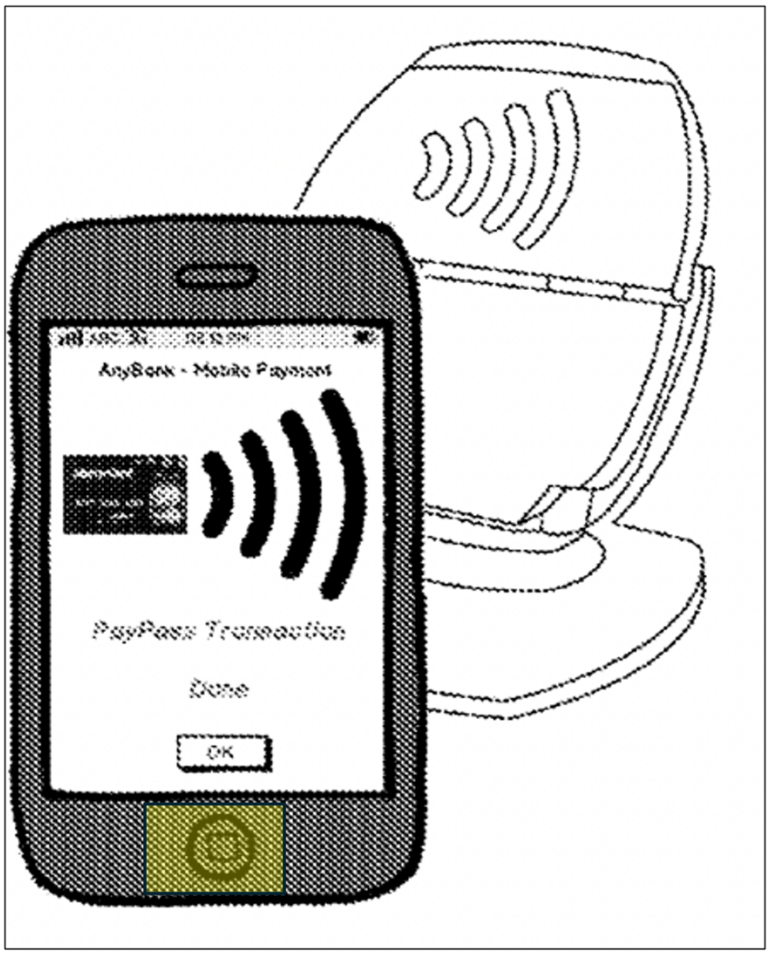
XII. OPINIONS REGARDING GROUND 4: *COLLINGE IN VIEW OF LIN, SAHOTA, AND FADELL.*

1. Claim 10.2: "The method of claim 8, wherein said successfully validating the identified user comprises the processor

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

a) Collinge's Teachings

349. Collinge teaches a touch screen included in mobile device 104, which is a *user input sensor*. *See* claim 1(a). Collinge teaches that a user 102 "may supply additional authentication credentials, such as…a biometric identifier." *Collinge* at [0143]. Collinge further teaches, in the '098 Provisional, 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.

350. Detecting fingerprints on mobile devices were common practice before the priority date as demonstrated by Fadell.

b) Fadell's Teachings

351. Fadell teaches an electronic device with "sensors operative to detect biometric information of a user." *Fadell,* Abstract. The sensors "may include a capacitive sensor operative to detect features of a user's skin." *Fadell,* [0056]. Specifically, Fadell teaches sensor 620 which is "operative to detect features of the

user's skin when the skin is held immobile over the sensor." *Fadell,* [0059]. "[S]ensor 620 may include an existing component of…the display stack for a touch screen display" which "may include a capacitance sensor." In that case, "the authentication system may use the detected output of a capacitance sensing component of the display stack (e.g., in a touch screen display) that has a sufficient resolution for distinguishing ridges and valleys of a user's skin." *Fadell,* [0061].

352. "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].

353. Because Fadell teaches that sensor 620 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 *wherein said 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 620 detecting the features of a user's finger is *a user input received via at least one of a set of user input sensor* because the user input is the fingerprint and it is received via the fingerprint sensor 620. 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. Fadell requires the user to hold their finder on the fingerprint sensor until they are authenticated.

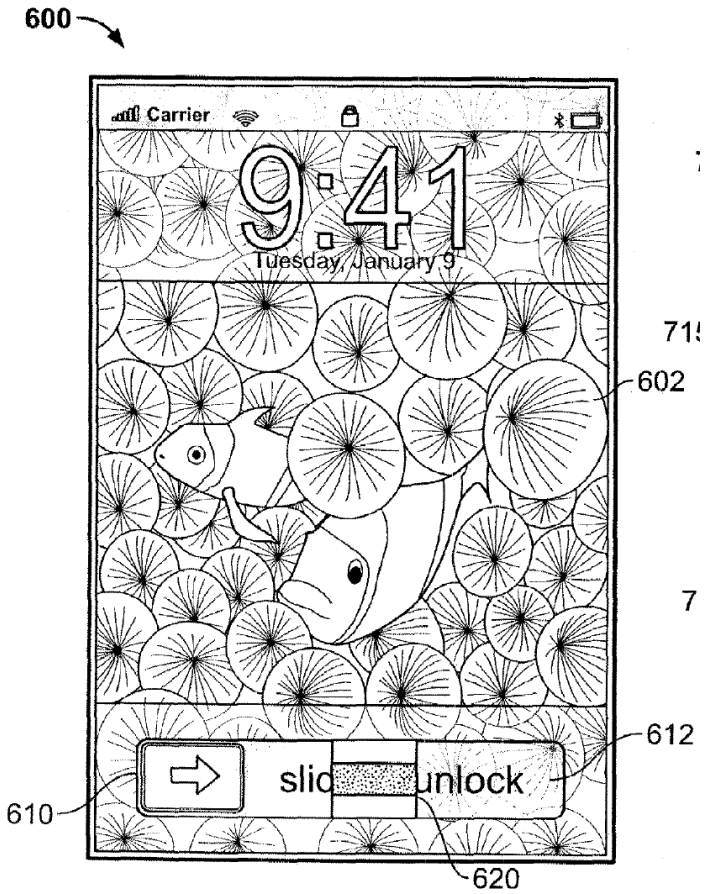


FIG. 6

Fadell at Figure 6.

c) Motivation to Combine

354. 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 includes a fingerprint sensor under the display, which is one of a <u>*set of user input sensors*</u> alongside Collinge's touch screen. In the combination, 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 [0143]. 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. When combined with Collinge's mobile device Faddell's fingerprint sensor and library would function the same way as it does on Faddell's phone.

355. The modification is straightforward particularly since Collinge already discloses being able to accept a "biometric identifier." A POSITA would have recognized that a fingerprint, unlike a pin or password, cannot be simply guessed. 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, many commercially available mobile devices employing fingerprint sensors, such as the Fujitsu F-01A, and Motorola Atrix, were known before the priority date of the '634 Patent. *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.

2. Claim 12: "The method of claim 10, wherein said predetermined user characteristics stored within the electronic device comprise known user biometric touch characteristics."

356. *See* Claim 10.2.

3. Claim 13: "The method of claim 10, wherein said predetermined user characteristics stored within the electronic device comprise a known user touch gesture."

357. As I discussed above at claim 11, Collinge teaches that user may input a PIN and/or activation code using Collinge's mobile device touch screen sensor. The user inputting a PIN/code is a <u>*known user touch gesture*</u>. *See also* Claim 10.1 Alternatively, Fadell teaches that a sensor may "detect features of a user's finger as it slides or rolls over the sensor" which is likewise a <u>*known user touch gesture*</u>. *Fadell,* [0058]; Claim 10.2.

4. Claim 16(Pre): "The method of claim 15, wherein said readying said device to perform a payment transaction comprises:"

358. *See* Claim 1(b).

5. Claim 16(a): "successfully identifying said identified user from said user input; and,"

See claims 1(a) and 1(b). As I described above, Collinge teaches that a user inputs a PIN to be identified as an authenticated user of mobile device 104 (<u>*successfully identifying said identified user*</u>). *Collinge,* [0133]; *'098 Provisional (Ex.1008)* at p. 99; *'248 Provisional (Ex.1006)* at Figures 2A-2B.

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

359. *See* Claim 8(b).

7. Claim 16(c): "wherein said successfully identifying further comprises said electronic device validating an authorized user

of said electronic device by comparing a user-touch input received via a touch input sensor on the electronic device with a recognized valid user-touch, stored in a memory of the electronic device; and,"

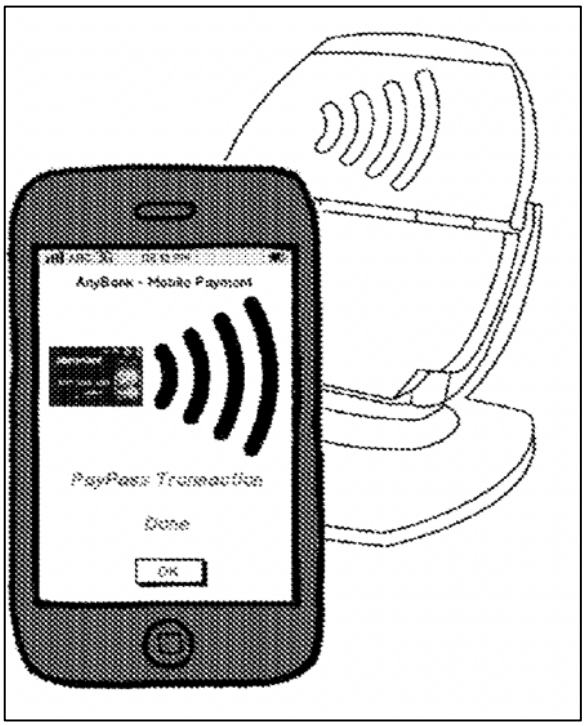
360. *See* Claim 10.1, 10.2.

8. Claim 16(d): "wherein said user approval for performing the payment transaction further comprises:"

361. See Claim 8(b).

9. Claim 16(e): "visually presenting information of the payment transaction on the touch screen display of said electronic device;"

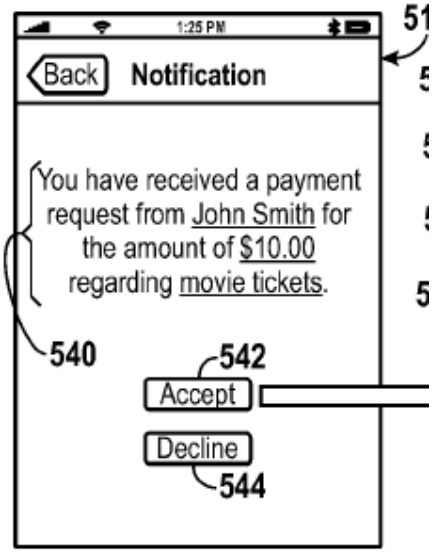
362. In the '098 Provisional (Ex.1008), which I understand is incorporated by reference into Collinge, Collinge teaches visually presenting, on the touch screen (*touch screen display*) of mobile device 104 (*said electronic device*), a notification of the status of the payment transaction (*information of the payment transaction*). For example, the touch screen displays a notification reading "PayPass Transaction Done[.]" *'098 Provisional (Ex.1008)* at p. 99. Thus, Collinge teaches displaying information to the user of mobile device 104.



'098 Provisional (Ex.1008), p. 99. (excerpt)

a) Lin's Teachings

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



Lin at Figure 14E (excerpt).

b) Motivation to Combine

364. A POSITA would have found it obvious and been motivated to modify Collinge's mobile device 104 to display details 540 of a payment request as taught by Lin. In the combination, Lin's details 540 would be displayed on the display/touch screen of Collinge's mobile device 104 (*visually presenting information of the payment transaction on the touch screen display of said electronic device*).

365. A POSITA would have been motivated to make this modification to increase accessibility and simplify user experience of using Collinge's mobile payment application 106 on mobile device 104 to conduct a payment transaction. The modification would have simplified user experience because a user of mobile

device 104 would quickly and easily view payment transaction details such as the amount requested by point-of-sale terminal 120 and the account information from which a payment will be made. A POSITA would have been motivated to combine prior art elements (mobile devices for conducting payment transactions, touch screens displaying payment transaction information) to yield the predictable result of a touch screen of a mobile device display payment information during a payment transaction. The combination is nothing more than the use of a known technique (displaying payment transaction information) to improve similar devices (mobile devices for conducting payment transactions) in the same way.

10. Claim 16(f): "visually presenting a request for user approval of the payment transaction via touch input at said electronic device; and,"

366. As discussed in Claim 8(b), a POSITA would have understood Collinge's teachings that after the user of mobile device clicks "pay" on the payment request that the payment transaction would be approved to be carried out by mobile device 104. *See* Claim 8(b). As shown below this "approve" selection option by Collinge is *visually presenting a request for user approval of the payment transaction via touch input at said electronic device*.

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

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

367. As I discussed above at Claim 8(b), a POSITA would have understood Collinge's teachings that after the user of mobile device clicks "pay" on the payment request that the payment transaction would be approved to be carried out by mobile device 104 (*subsequent to receiving a user-touch input from an identified user, approving performance of said payment transaction via said electronic device*).

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

> 12. *Claim 51: "The device of claim 39, wherein said user input device comprises a biometric sensor operable to detect a user touch of said electronic device and wherein further the processor is operable to identify an authorized user by biometric sensing of a continuous user touch."*

368. *See* Claim 10.2.

> 13. *Claim 52: "The device of claim 39, wherein said user interface comprises a display and wherein said user input device comprises a touch panel disposed adjacent to said display and wherein further the processor is operable to identify an authorized user by biometric sensing of a user touch at the touch panel."*

369. *See* Claims 10.2; 49.

14. Claim 53: "The device of claim 39, wherein said user interface comprises a display and wherein said user input device comprises a touch panel disposed adjacent to said display and wherein further the processor is operable to identify an authorized user by biometric recognition of a valid user identification."

370. *See* Claims 10.2; 49.

15. Claim 68: "The device of claim 56, wherein said user input device comprises a biometric sensor operable to detect a user touch of said electronic device and wherein further the processor is operable to identify an authorized user by biometric sensing of said user touch."

371. *See* Claim 10.2.

16. Claim 69: "The device of claim 56, wherein said user interface comprises a display and wherein said user input device comprises a touch screen interface of the display and wherein further the processor is operable to identify an authorized user by biometric sensing of a user touch at the touch screen interface."

372. *See* Claims 10.2;39(d).

17. Claim 70: "The device of claim 56, wherein said user interface comprises a display and wherein said user input device comprises a touch input of the electronic device and wherein further the processor is operable to identify an authorized user by biometric recognition of a valid user identification via the touch input."

373. *See* Claims 10.2; 39(d).

XIII. OPINIONS REGARDING GROUND 5: COLLINGE *IN VIEW OF LIN, SAHOTA, AND YU.*

1. Claim 10.3: "The method of claim 8, wherein said successfully validating the identified user comprises the processor successfully determining a match between: firstly, a user input received via at least one of a set of user input sensors of the electronic device; and, secondly, at least one of the set consisting of: predetermined user characteristics, and challenge-responses of an authorized user, as stored in the electronic device."

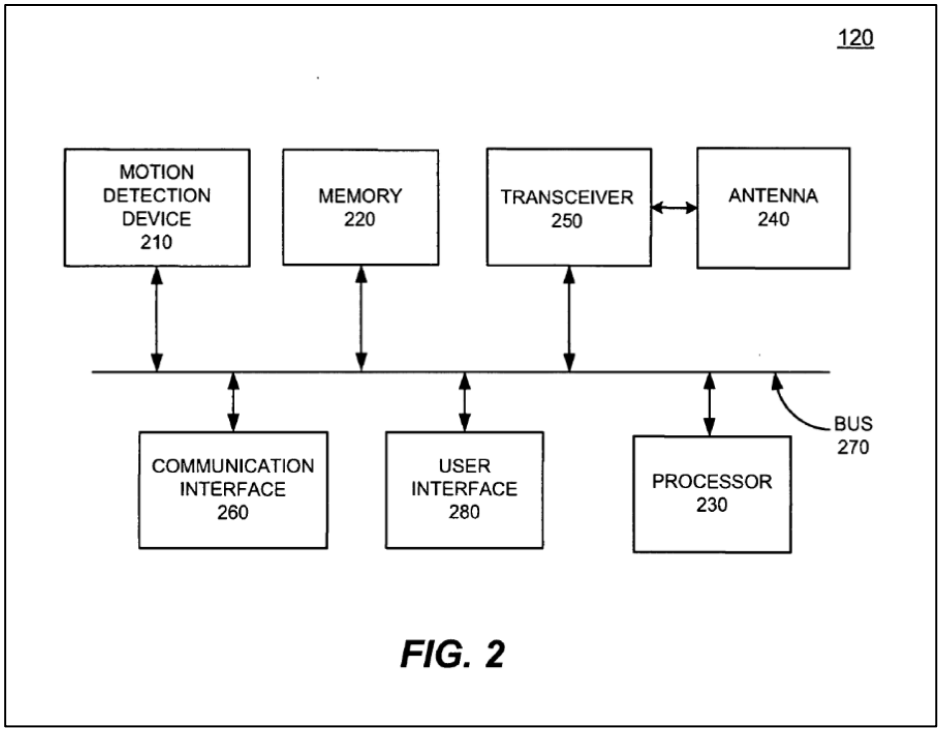
a) Collinge's Teachings

374. As I discussed above at Claim 8(a), Collinge teaches that a user of mobile device 104 provides a PIN to be identified as an authorized user. Collinge additionally teaches that the "user 102 may supply additional authentication credentials, such as a gesture[.]" *Collinge* at [0081]. As I will detail below, a POSITA would have found it obvious and been motivated to modify Collinges user authorization method according to the teachings of Yu.

b) Yu's Teachings

375. Yu teaches a "method and apparatus…that authenticate a user of a mobile device with motion sensors." *Yu* at Abstract. As illustrated in Figure 2 below, Yu teaches "a mobile communication device 120" comprising a "motion detection device 210." *Yu* at [0027]. Yu teaches an array of motion sensors, for example "[m]otion detection device 210 can comprise one or more accelerometers, gyros, inclinometers, cameras, tilt sensors, or any other sensors that can determine the motion of the device within N degrees of freedom…" *Yu* at [0028]. "The output of

motion detection device 210 can be processed by processor 230 with instructions from the movement of the mobile device to verify both the identity and presence of a mobile user." *Yu* at [0028].



Yu at Figure 2.

376. As explained with reference to Figure 3, in "action 310, a user subjects a device such as mobile communication device 120 to a series of movements so as to provide a movement sample." *Yu* at [0033]. The series of movements is analyzed, then in "action 360, verification is made to determine if the motion password matches the motion password for the user of the mobile communication device." *Yu* at [0037]. "The motion password for the user of the mobile communication device is maintained as a motion password shadow 370" that is a "one-way summary of the

motion password from motion captured in a learning session. The constructed motion password from action 350 is verified against the motion password shadow 370." *Yu* at [0037]. If the motion password does not match the motion password shadow 370, the method returns to 310. *Yu* at [0037]. If the "verification indicates a match control is passed to an action for further processing[,]" such as action 410, where "access to the service or device is granted." *Yu* at [0037]-[0038].

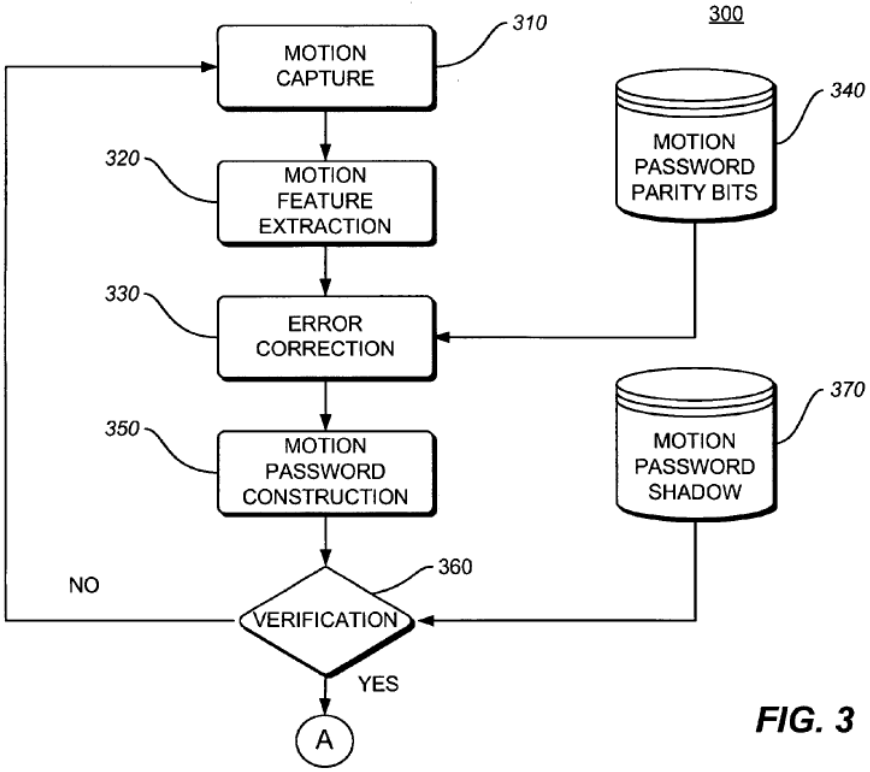


FIG. 3

Yu at Figure 3. Yu teaches that the "extracted motion features are used to construct a motion password. The "motion password shadow 370 is stored so it can later be used to authenticate a user. *Yu*, [0040].

377. Because Yu teaches that the processor processes the output of motion detection device 210 and the output of motion detection device 210 is compared to the motion password shadow for user verification, Yu teaches *successfully validating the identified user comprises the processor successfully determining a match*. The motion performed by the user of the mobile device is *a user input received via at least one of a set of user input sensors* because it is a motion performed by the user that is sensed via the motion detection unit 210 (which may "one or more accelerometers, gryos…"). *Yu* at [0028]. The motion password shadow 370 is *predetermined user characteristics* because it is a motion password from motion captured during a learning session (i.e., a predetermined motion). *Yu* at [0037].

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

c) Motivation to Combine

379. A POSITA would have found it obvious and been motivated to modify Collinge's mobile device 104 to include an array of motion sensors and to use those

motion sensors to identify an authorized user by detecting a recognized user displacement of the array of motion sensors as taught by Yu. Collinge already recognizes that "a gesture" as an authentication "credential" and motion detection hardware was already commonly found in mobile devices at the time as demonstrated by Yu. *Collinge* at [0143]. A POSITA would have been motivated to modify Collinge to identify a user via a known user's motion to increase accessibility and security of Collinge's mobile payment application. In the combination, a POSITA would have been motivated to modify Collinge so that Collinge's mobile device 104 comprises "one or more accelerometers…" (*a set of user input sensors*) and the user would establish a motion password that would be sensed by the *set of user input sensors*. A POSITA would have been motivated to store a known user's motion in the memory (304) of mobile device 104 to quickly authenticate a suer as taught by Yu. *Yu*, [0040]. A POSITA would have been motivated to modify Collinge to identify a user via a known user's motion to increase accessibility and security of Collinge's mobile payment application

380. The modification is expressly motivated by Yu, who teaches traditional verification or authentication methods using passwords or PINs "present many drawbacks," including "perpetrators intent on committing fraud can usually decipher user selected passwords and PINs fairly easily[,]" and "advances in technology have made it easier for a perpetrator to fraudulently obtain a password or PIN." *Yu* at

[0006]. A POSITA would have recognized that Yu's motion-based authentication was a known technique that could improve Collinge's mobile device in the same way, and it would have predictably resulted in the ability to use a motion or gesture to authenticate a user, increasing security. A POSITA would have had a reasonable expectation of success in making this modification, including because motion sensor arrays were already standard in mobile devices and because Collinge already teaches gesture-based authentication.

381. The modification would have been straightforward and merely required including Yu's motion detection unit into Collinge's display in Collinge's mobile device 104, configuring the memory to store the known user's motion, and configuring the processor to verify the user's motion by the known user's motion, which were all well-known techniques as demonstrated by Yu. A POSITA would have possessed the necessary skillset to implement such a feature in mobile device 104 without any undue experimentation and thus, the modification would have had a reasonable expectation of success.

2. Claim 14: "The method of claim 10, wherein said predetermined user characteristics stored within the electronic device comprise a known user motion of the device."

382. *See* Claim 10.3.

3. Claim 54: "The device of claim 39, wherein said user input device comprises an army of motion sensors and wherein further the processor is operable to identify an authorized user by

detecting a recognized user displacement of the array of motion sensors."

383. *See* Claim 10.3.

4. *Claim 71: "The device of claim 56, wherein said user input device comprises an array of motion sensors and wherein further the processor is operable to identify an authorized user by detecting a recognized user displacement of the array of motion sensors."*

384. *See* Claims 54; 10.3.

XIV. CONCLUSION

385. 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.

- 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.

- 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.

- 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.

- 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.

- 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

- 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)

- 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

IPR2025-01152
Apple EX1003 Page 300

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

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

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)

- 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.

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

- 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.