

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,

Petitioner

v.

CARDWARE INC.,

Patent Owner

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

DECLARATION OF DR. CLIFFORD NEUMAN

TABLE OF CONTENTS

I.	INTRODUCTION.....	21
A.	Educational Background and Professional Experience	21
II.	MATERIALS CONSIDERED	24
III.	OVERVIEW AND LEGAL STANDARDS	28
A.	Person of Ordinary Skill in the Art.....	29
B.	Obviousness	30
C.	Claim Construction	35
IV.	PRINTED SUBJECT MATTER	36
V.	LEVEL OF A PERSON OF ORDINARY SKILL.....	36
VI.	OVERVIEW OF THE '286 PATENT.....	37
D.	Summary of the '286 Patent	37
E.	Field of Endeavor.....	37
F.	Problem Solved by the Inventors of the '286 Patent	38
G.	File History of the '286 Patent.....	39
VII.	BACKGROUND OF TECHNOLOGY.....	39
A.	The Evolution of Payment Cards	41
1.	<i>Magnetic Stripe Cards.....</i>	<i>41</i>
2.	<i>Smart/Chip Cards</i>	<i>43</i>
3.	<i>Europay, MasterCard, and Visa (EMV) Standard</i>	<i>44</i>
B.	Contactless Payments.....	45
1.	<i>Near Field Communications.....</i>	<i>45</i>
1.	<i>Active Mode</i>	<i>47</i>
2.	<i>Passive Mode</i>	<i>49</i>
2.	<i>The Development of Near Field Communications</i>	<i>50</i>
3.	<i>Contactless EMV Payment Cards.....</i>	<i>50</i>
4.	<i>Mobile Devices and Mobile Wallets.....</i>	<i>51</i>

5.	<i>Card Emulation Mode</i>	55
C.	Payment Credential Security Features	57
1.	<i>Alternatives to a Payment Account Number (PAN)</i>	57
6.	<i>Alternatives to Static Card Verification Values</i>	60
VIII.	SUMMARY OF PRIOR ART REFERENCES	63
D.	Collinge.....	63
1.	<i>Collinge is Analogous Art</i>	66
2.	<i>Collinge is Prior Art</i>	68
3.	<i>Support for Collinge in Collinge Provisionals</i>	95
E.	Bona	99
4.	<i>Bona is Analogous</i>	101
F.	Smith	102
1.	<i>Smith is Analogous</i>	103
G.	Lin	105
1.	<i>Lin is Analogous</i>	106
H.	Patterson.....	107
1.	<i>Patterson is Analogous</i>	109
I.	Kranzley	110
1.	<i>Kranzley is Analogous</i>	111
J.	Eng	112
1.	<i>Eng is Analogous</i>	113
K.	Chin.....	114
1.	<i>Chin is Analogous</i>	115
L.	Fisher.....	116
1.	<i>Fisher is Analogous</i>	116
M.	Hammad	118
1.	<i>Hammad is Analogous</i>	119
IX.	SUMMARY OF UNPATENTABILITY	121

X.	OPINIONS REGARDING GROUND 1: CLAIMS 15 AND 17-18 ARE OBVIOUS OVER COLLINGE AND BONA.....	122
A.	Claim 15(Pre): A payment system comprising:.....	122
B.	15(a): a payment card device that is free of any fixed payment numbers disposed thereon and wherein said payment card device is operable for use in a merchant card-reader equipment; and.....	123
	1. <i>Patentable Weight</i>	123
	2. <i>Collinge's Teachings</i>	127
	3. <i>Bona's Teachings</i>	127
	4. <i>Motivation to Combine</i>	135
C.	15(b): a card-users personal computing device operable for completing a payment transaction and comprising:.....	143
D.	15(b)(1): a processor:	143
E.	15(b)(2): a touch-screen display interface;	145
F.	15(b)(3): a user-interface;	148
G.	15(b)(4): a wireless interface;	148
H.	15(b)(5): and a memory for storing a payment information accessible to the processor, ...	152
I.	15(c): wherein the computing device is configured to dynamically generate limited-use payment information, and.....	154
	1. <i>authenticated card user</i>	160
J.	15(d): wherein the computing device is configured to convey the limited-use payment information on a computing device interface upon the authorization of a valid user, and.....	162
	5. <i>Authorization of a payment transaction by a valid user</i>	165
K.	15(e): wherein a merchant is operable to receive a payment information provided by a personal computing device, and.....	167
L.	15(f): wherein the limited-use payment information provided by at least one or both of: the payment card device, and the computing device, is validated by a card issuing authority when used in merchant in-store facility transactions, and.....	168

M.	15(g): wherein a card issuing authority is operable to reject as invalid, a payment information used outside of its valid limitations of use, and.....	173
N.	15(h): wherein a card issuing authority is operable to validate generated limited-use payment information provided by the computing device in an authorized transaction completed by the computing device.	175
O.	Claim 17(a): The system of claim 15, wherein the touch-screen display interface is operable to display a merchant facility transaction, and wherein the touch-screen display interface is operable to accept a user approval and denial of a payment transaction, ...	175
P.	17(b): and wherein a card issuer authority is further operable to deny a card payment transaction from a user-denied merchant facility transaction, and to approve as authentic a card payment transaction from a user-approved facility transaction.....	177
Q.	Claim 18 (a): The system of claim 15, wherein a plurality of issuer-provided payment information is wirelessly downloaded into the personal computing device, and.....	177
R.	18 (b): wherein the user-interface is operable for a user selection, of at least one of issuer-provided payment methods via the touch-screen display interface, and.....	181
S.	18 (c): wherein the payment card device is operable for a transaction with a user-selected payment method.	181
XI.	OPINIONS REGARDING GROUND 2: CLAIMS 1, 5-8, 11, 20-27 ARE OBVIOUS OVER <i>COLLINGE, BONA, AND SMITH</i>.	181
A.	Claim 1 (Pre): A payment system comprising:.....	181
B.	1(a): a payment card device free of any fixed payment numbers visible thereon and wherein said payment card device is operable for use in payment card reader equipment; and”	181
C.	1(b): a computing device comprising: a processor;	181
D.	1(b)(1): a memory;.....	181
E.	1(b)(2): a wireless interface;	181

F.	1(b)(3): a touch-screen user interface operable to provide a visual user-interface for user payment interactions; and	181
G.	1(c): a user-input device coupled to the processor, and.....	182
H.	1(d): wherein the processor is operable to store a transaction sequence count,.....	189
I.	1(d)(1): a device account number and	192
	1. <i>Collinge's Teachings</i>	194
	2. <i>Smith's Teachings</i>	197
	3. <i>Motivation To Combine</i>	202
J.	1(d)(2) secrets limited to the computing device, and.....	210
	1. <i>local storage encryption key</i>	210
	2. <i>unique identifier</i>	211
	4. <i>key request</i>	212
	5. <i>single use key</i>	213
K.	1(e): wherein the computing device is operable to receive, store and transmit a card payment information not visible on the payment card device, and.....	214
	1. <i>Bona's Teachings</i>	215
	2. <i>Collinge's Teachings</i>	215
	3. <i>Motivation to Combine</i>	217
L.	1(f): wherein the processor is operable to generate at least a portion of a limited-use card payment information for use by an authenticated card user, and.....	217
M.	1(g): wherein the computing device is operable to convey said limited-use card payment information via an interface of the computing device, and	217
N.	1(h): wherein a card issuer authority is operable to reject as invalid a transaction attempt outside of its limitations of use,.....	217
O.	1(i): wherein a card issuer authority is operable to validate a card payment information as authentic when received from at	

	least one of: an authenticated users payment card; and an authenticated users computing device, and.....	217
P.	1(j): wherein the card issuer authority is operable to permit the authentic transactions to complete.....	218
Q.	Claim 5: The system of claim 1, wherein the payment card device is absent a payment number information necessary for completing an online transaction, and wherein the information presented on an interface of said card device, are limited to an in-store merchant card reader facility use only.....	219
R.	Claim 8: The system of claim 1, wherein the computing device is further operable to transceive the limited-use card payment information via an NFC interface of the computing device in an in-store NFC reader facility transaction.....	223
S.	Claim 11(a): The system of claim 1, further comprising a touch- screen user interface control for a user approving and denying a transaction, ...	225
T.	11(b): and wherein a card issuer authority is further operable to deny as authentic, a card payment transaction from a user- denied transaction, and to approve as authentic a card payment transaction from a user-approved transaction.	228
U.	Claim 14: The system of claim 1, wherein a payment issuing authority is operable to decline transactions performed by the payment card device when a user fails at least one security challenge presented to a user by the computing device.....	228
	1. <i>Bona's Teachings</i>	228
	2. <i>Collinge's Teachings</i>	228
	3. <i>Motivation to Combine</i>	229
V.	Claim 20(Pre) A payment system comprising:.....	230
W.	20(a): a payment card device, free of any depictions of fixed payment numbers thereon, and operable for use in payment card reader equipment; and.....	230
X.	20(b): a computing device comprising:	231
Y.	20(b)(1): a processor;	231

Z.	20(b)(2): a memory;	231
AA.	20(b)(3): a wireless interface;	231
BB.	20(b)(4): a touch-screen user interface operable to provide a visual user-interface for user payment interactions; and	231
CC.	20(b)(5): a user-input device coupled to the processor; and	231
DD.	20(c): wherein the memory is operable to store a transaction sequence count, a static device account number and secrets limited to the computing device;	231
EE.	20(d): wherein the computing device is operable to receive, store, display and transmit issuer-provided payment information, associated with, but not depicted on, the payment card device;	231
FF.	20(e): wherein the processor is operable to dynamically generate at least a portion of a limited-use payment information for use by an authenticated card user, ...	232
GG.	20(f): and to combine said at least a portion of the limited-use payment information with at least said static device account number to create combined payment information;	232
	<i>1. Motivation to Combine</i>	234
HH.	20(g): wherein the computing device is operable to convey said combined payment information via an interface of the computing device; and	234
II.	20(h): wherein the computing device is operable to receive information, from an issuer, in response to the conveyed combined payment information, indicating that a payment transaction is valid.	234
JJ.	Claim 21: The system of claim 20 wherein the computing device is operable to wirelessly receive the static device account number.	234
KK.	Claim 22: The system of claim 20, wherein the processor is operable to dynamically generate the at least a portion of a limited-use payment information based on a transaction sequence counter count, and further wherein the generated limited-use payment information is valid for a single use.	235

LL.	Claim 23: The system of claim 22 wherein the processor is operable to dynamically generate the at least a portion of a limited-use payment information further based on payment processing authority secrets.	235
MM.	Claim 24: The system of claim 23 wherein the processor is operable to dynamically generate the at least a portion of a limited-use payment information further based on the static device account number.	236
NN.	Claim 25: The system of claim 24 wherein the computing device is operable to wirelessly receive the static device account number.	236
OO.	Claim 26: The system of claim 22 wherein the processor is operable to dynamically generate the at least a portion of a limited-use payment information further based on the static device account number.	236
PP.	Claim 27: The system of claim 26 wherein the computing device is operable to wirelessly receive the static device account number.	236
XII.	OPINIONS REGARDING GROUND 3: CLAIMS 2, 3, AND 14 ARE OBVIOUS OVER COLLINGE IN VIEW OF BONA, SMITH, AND PATTERSON.....	236
A.	Claim 2: The system of claim 1, wherein the touch-screen user interface is operable to control an access for payment transactions by the card device, and is operable to enable as authentic payment transactions by the card device.....	236
1.	<i>Collinge's Teachings</i>	237
2.	<i>Bona's Teachings</i>	238
3.	<i>Patterson's Teachings</i>	238
4.	<i>Motivation to Combine</i>	241
B.	Claim 3: The system of claim 1, wherein the touch-screen user interface is operable to control an access of the card device for payment transactions at an NFC Card Reader facility, and is operable to enable and disable NFC payment transactions by the card device.	244

- C. Claim 4: The system of claim 3, wherein the touch-screen user-interface is configurable for a locking and unlocking of payment transactions, and wherein a card issuer authority is further operable for denying a payment transaction from at least one of: a locked card device; and a locked card-users computing device, and wherein a card issuer authority is further operable to permit as authorized, a card payment transaction from an unlocked device. 244

XIII. OPINIONS REGARDING GROUND 4: CLAIM 9 IS OBVIOUS OVER COLLINGE IN VIEW OF BONA, SMITH AND LIN 246

- A. Claim 9: The system of claim 1, wherein the computing device is further operable to transceive the limited-use payment information wirelessly with another device via a wireless interface of the computing device, in a device-to-device transaction. 246
1. *Lin's Teachings*..... 246
2. *Motivation to Combine* 248

XIV. OPINIONS REGARDING GROUND 5: CLAIM 10 IS OBVIOUS OVER COLLINGE IN VIEW OF BONA, SMITH, AND KRANZLEY 249

- A. Claim 10: The system of claim 1, wherein the computing device is further operable to transmit a payment information visually, in alphanumeric, graphical and iconography via the touch screen user interface.....249
1. *Collinge* 249
2. *Kranzley*..... 249
3. *Motivation to Combine* 251

XV. OPINIONS REGARDING GROUND 6: CLAIM 16 IS OBVIOUS OVER COLLINGE IN VIEW OF BONA AND KRANZLEY 252

- A. Claim 16: The system of claim 15, wherein the touch-screen user interface is operable for displaying the limited-use payment information, and wherein a merchant is operable to accept the displayed payment card information in a transaction at a merchant facility.....252

**XVI. OPINIONS REGARDING GROUND 7: CLAIM 19 IS OBVIOUS
OVER COLLINGE IN VIEW OF BONA AND ENG.....253**

- A. Claim 19(a): The card device of claim 15, wherein the payment card device comprises fixed payment information disposed thereon, and wherein the fixed payment information comprises only: a card-holder name; a payment issuing logo; a card payment network logo, and a card reader interface icon, and 253
1. *Bona's Teachings* 253
2. *Eng's Teachings* 255
3. *Motivation to Combine* 256
- B. 19(b): wherein the payment card device is free of any account numbers, expiration dates, card security codes, or other fixed payment numbers, disposed thereon. 257

**XVII. OPINIONS REGARDING GROUND 8: CLAIM 12 IS OBVIOUS
OVER COLLINGE IN VIEW OF BONA, SMITH, AND CHIN.....258**

- A. Claim 12(a): The system of claim 1, wherein the computing device is further operable to present at least one challenge, of a set of security challenges comprising: ...a user touch-screen entry...a user gesture of a device, a user passcode entry...and a biometric sensing of a recognized user, and 258
- B. 12(b): wherein the computing device is operable to reject and accept a user authorization to use the device based on the security challenge response, and.....259
1. *Collinge's Teachings* 259
2. *Chin's Teachings* 260
3. *Motivation to Combine* 260
- C. 12(c): wherein the computing device is operable to decline performing a payment transaction in the possession of an unauthorized user, ...263
- D. 12(d): and wherein the computing device is operable to perform a payment transaction while in the possession of a user correctly passing the at least one challenge. 263

E.	Claim 13: The user computing device of claim 12, wherein a payment issuing authority is operable to decline transactions performed by the computing device when a user fails the at least one security challenge.	264
XVIII.	OPINIONS REGARDING GROUND 9: CLAIM 4 IS OBVIOUS OVER <i>COLLINGE</i> IN VIEW OF <i>BONA, SMITH, AND FISHER</i>	264
F.	Claim 7: The system of claim 1, wherein the computing device is further operable to transceive the card payment information via the wireless interface for completing an online transaction.....	264
1.	<i>Collinge's Teachings</i>	264
2.	<i>Fisher's Teachings</i>	265
3.	<i>Motivation to Combine</i>	265
XIX.	OPINONS ON GROUND 10: <i>COLLINGE, BONA, SMITH, AND HAMMAD</i>	266
G.	Claim 6(a): A system of claim 1, wherein: the card issuer authority is operable to receive said transacted payment information, and wherein a card issuer authority is operable to compute a limited-use payment information from a transaction information, a merchant, a facility information, a sequence counter, a payment card account information, secrets and an information limited to said card device and to said computing device, ...	266
2.	<i>Collinge's Teachings</i>	268
1.	<i>Secrets</i>	271
2.	<i>Motivation to Combine</i>	272
H.	6(b): and wherein a card issuer authority is operable to compare said computed payment information to said device transacted information,.....	274
I.	6(c): and wherein a card issuer authority is operable to reject as invalid a device transaction used outside of a valid range of device limitations, ...	274

J. 6(d): and wherein a card issuer authority is operable to
authenticate as valid, a device transaction use within valid range
of device limitations.....274

XX. CONCLUSION.....275

CLAIM LISTING

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

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

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

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

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

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

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

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 opinions regarding the IPR petition with respect to U.S. Patent No. 11,328,286 (the “’286 Patent”). I understand that the Challenged Claims are 1-22, and my opinions herein are limited to those claims. A true and correct copy of my Curriculum Vitae, which provides further details about my background and experience, is appended to this Declaration.

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. 11,328,286 (“’286 Patent”)
1002	File History of the ’286 Patent (“’286 File History”)

1004	U.S. Patent Publication No. 2013/0262317 to Collinge et al. (“ <i>Collinge</i> ”)
1005	U.S. Provisional Patent Application No 61/619,095 to Collinge et al. (“’095 <i>Provisional</i> ”)
1006	U.S. Provisional Patent Application No 61/635,248 to Collinge et al. (“’248 <i>Provisional</i> ”)
1007	U.S. Provisional Patent Application No 61/735,383 to Collinge et al. (“’383 <i>Provisional</i> ”)
1008	U.S. Provisional Patent Application No 61/762,098 to Collinge et al. (“’098 <i>Provisional</i> ”)
1009	U.S. Patent Publication No. 2011/0140841 to Bona et al. (“ <i>Bona</i> ”)
1010	U.S. Patent Publication No. 2010/0125508 to Smith (“ <i>Smith</i> ”)
1011	US. Patent No. 8,103,588 to Patterson (“ <i>Patterson</i> ”)
1012	WIPO International Publication No. WO 2010/039337 to Lin et al. (“ <i>Lin</i> ”)
1013	U.S. Patent Publication No. 2010/0125509 to Kranzley et al. (“ <i>Kranzley</i> ”)
1014	U.S. Patent Publication No. 2013/0068366 to Eng (“ <i>Eng</i> ”)
1015	U.S. Patent Publication No. 2011/0282785 to Chin (“ <i>Chin</i> ”)
1016	U.S. Patent Publication No. 2013/0097040 to Fisher (“ <i>Fisher</i> ”)
1017	U.S. Patent No. 7,740,168 (“ <i>Hammad</i> ”)
1018	Intentionally Left Blank
1019	Intentionally Left Blank
1020	IBM, <i>The Magnetic Stripe</i> , IBM, https://www.ibm.com/history/magnetic-stripe . (“ <i>IBM</i> ”)
1021	VEDAT COSKUN, NEAR FIELD COMMUNICATION: THEORY TO PRACTICE (John Wiley & Sons, 1st ed. 2012) (“ <i>Coskun</i> ”)
1022	MAGTEK, MAGNETIC STRIPE CARD STANDARDS, (MagTek Inc. eds., 2011) (“ <i>MagTek</i> ”)
1023	EMVCo, LLC, EMV INTEGRATED CIRCUIT CARD SPECIFICATIONS FOR PAYMENT SYSTEMS: BOOK 2 – SECURITY AND KEY MANAGEMENT (EMVCo, LLC eds., Version 4.3 2011) (“ <i>EMV</i> ”)
1024	KLAUS FINKENZELLER, RFID HANDBOOK (John Wiley & Sons, 3rd ed. 2010) (“ <i>Finkenzeller</i> ”)
1025	MasterCard, <i>MasterCard PayPass™ in Action</i> , MASTERCARD (Jun. 11, 5:35 PM), https://www.mastercard.com/us/company/en/ourbusiness/paypass_i

	n_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) (“ <i>Smart</i> ”)
1027	U.S. Patent Publication No. 2012/0011058 to Pitroda et al. (“ <i>Pitroda</i> ”)
1028	MasterCard, <i>MasterCard Approved Mobile Devices</i> , MASTERCARD (Aug. 3, 2012), http://www.mastercard-mobilepartner.com/docs/MasterCard_Aproved_Mobile_Devices.pdf , [https://web.archive.org/web/20120906234255/http://www.mastercard-mobilepartner.com:80/docs/MasterCard_Aproved_Mobile_Devices.pdf] (“ <i>MasterCard Mobile Partner</i> ”)
1029	U.S. Patent Publication No. 2013/0054474 to Yeager (“ <i>Yeager</i> ”)
1030	EMVCo, LLC, <i>EMV Chip At-a-Glance: Enabling Seamless and Secure Contact and Contactless Payments Around the World</i> , EMVCo (2002), https://www.emvco.com/wp-content/uploads/2022/09/EMV%C2%AE-Chip-At-A-Glance-EMVCo-eBook.pdf (“ <i>EMVCo</i> ”)
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) (“ <i>PCI SSC</i> ”)
1032	ALESSANDRO VIZZARRI ET AL., SECURITY IN MOBILE PAYMENTS (2013) (“ <i>Vizzarri</i> ”)
1033	U.S. Patent Publication No. 2008/00110983 to Ashfield (“ <i>Ashfield</i> ”)
1034	Intentionally Left Blank
1035	WIPO International Publication No. WO 1994/17498 to Labaton et al. (“ <i>Labaton</i> ”)
1036	GEOFFREY R. GERDES ET AL., THE 2013 FEDERAL RESERVE PAYMENT STUDY – RECENT AND LONG-TERM TRENDS IN THE UNITED STATES:

	2003-2012 (Federal Reserve System, Rev. 2014) (“ <i>Study Summary</i> ”)
1037	GEOFFREY R. GERDES ET AL., THE 2013 FEDERAL RESERVE PAYMENT STUDY – RECENT AND LONG-TERM TRENDS IN THE UNITED STATES: 2000-2012 (Federal Reserve System, 2014) (“ <i>Study</i> ”)
1038	ConsumerWorld, <i>Two Months After the Deadline, Most Major Retailers Still Can't Read Chipped Credit Cards</i> , CONSUMERWORLD (Dec. 7, 2015), https://www.consumerworld.org/pages/creditcardreaders.htm (“ <i>ConsumerWorld Survey</i> ”)
1039	Ann Cavoukian, <i>Mobile Near Field Communications (NFC) “Tap ‘n Go” Keep it Secure & Private</i> , IPC (2011), https://www.ipc.on.ca/sites/default/files/legacy/Resources/mobile-nfc.pdf (“ <i>Cavoukian</i> ”)
1040	ANNIKA PAUS, NEAR FIELD COMMUNICATION IN CELL PHONES (2017) (“ <i>Paus</i> ”)
1041	Ashis K. Mahapatra, <i>Touch Screen Systems</i> , ORISSA REVIEW (2005), https://magazines.odisha.gov.in/orissareview/jun2005/engpdf/touch_screen_system.pdf (“ <i>Mahapatra</i> ”)
1042	U.S. Patent Publication No. 2006/0097991 to Hotelling et al. (“ <i>Hotelling</i> ”)
1043	U.S. Patent Publication No. 2008/0122796 to Jobs et al. (“ <i>Jobs</i> ”)
1044	U.S. Patent No. 10,181,121 (“ <i>Roberts</i> ”)
1045	U.S. Patent Publication No. 2013/0151292 to Van Deloo et al. (“ <i>Deloo</i> ”)
1046	U.S. Patent Publication No. 2006/0186195 to Gray (“ <i>Gray</i> ”)
1047	U.S. Patent Publication No. 2014/0006276 to Grigg et al. (“ <i>Grigg</i> ”)
1048	Anup K. Ghosh & Tara M. Swaminatha, <i>Software Security and Privacy Risks in Mobile E-Commerce</i> , 44 CACM 51 (2001) (“ <i>Ghosh</i> ”)
1049	Josh Constine, <i>Bump Pay Lets You PayPal Someone With A Tap, But Only In-Person</i> , TECHCRUNCH (Mar. 29, 2012, 5:01 AM), https://techcrunch.com/2012/03/29/bump-pay/#:~:text=Now%20it's%20as%20easy%20as,to%20anyone%20in%20arm's%20reach. (“ <i>Tech</i> ”)
1050	U.S. Patent Publication No. 2009/0083850 to Fadell et al. (“ <i>Fadell</i> ”)

11. I have considered these materials from the viewpoint of a POSITA as of the priority date of the '286 Patent. For the purposes of this declaration, I have been asked to assume that the earliest priority date of the '286 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 '286 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 '286 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 '286 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 Petitioner does not assert that any claim terms require express construction for purposes of this IPR.

IV. 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.

V. LEVEL OF A PERSON OF ORDINARY SKILL

28. Based on my review and analysis of the '286 Patent, the cited prior art, and the ordinary skill factors described in this section, a POSITA in the field of the '286 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.

VI. OVERVIEW OF THE '286 PATENT

D. Summary of the '286 Patent

31. The '286 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.” *'286 Patent (Ex. 1001)*, 2:22-28. The '286 Patent also describes “generating a limited-duration credit card number...which is limited in scope to a predetermined number of authorized transactions.” *Id.* at 2:33-37.

E. 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 '286 Patent defines the “Field of the Invention” as relating to “electronic or smart multi-function electronic devices and, more specifically, to

more secure, smart multi-function electronic payment card and device systems and transaction processing thereof.” ’286 Patent (*Ex.1001*), 1:31-35. After reviewing the ’286 Patent, it is my option that a POSITA would understand that the field of endeavor of the ’286 Patent includes more secure payment cards, devices and systems.

34. The ’286 Patent’s specification criticizes existing systems due to being “susceptible to theft and/or compromise.” 2:4-12. For these reasons, a POSITA would have understood that the ’286 Patent is trying to solve the problem of providing payment solutions that limit opportunities for theft or compromise of payment credentials.

F. Problem Solved by the Inventors of the ’286 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 ’286 Patent and determine the problem that the inventors were trying to solve.

36. The ’286 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.” ’286 Patent (*Ex.1001*), 2:4-8. The ’286 Patent also noted that “cards employing smart integrated

circuit chips and RF technology are not in wide use at present because they are incompatible with existing credit card infrastructure, which still predominantly supports conventional plastic credit cards.” ’286 Patent (*Ex.1001*), 2:8-12. 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.” ’286 Patent (*Ex.1001*), 2:22-26. The “Summary of the Invention” further describes a method of performing a transaction that includes “generating...a limited duration credit card number.” ’286 Patent (*Ex.1001*), 3:6-15. Thus, a POSITA would understand that the ’286 Patent is directed to solving the problem of providing payment solutions that limit opportunities for theft or compromise of payment credentials.

G. File History of the ’286 Patent

37. I have reviewed the prosecution history for the ’286 Patent. The ’286 Patent claims priority to Provisional Application No. 61/794,891, filed March 15, 2013. The ’286 Patent did not face any prior art rejections during prosecution. ’286 *File History* (*Ex. 1002*).

VII. 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 '286 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 '286 Patent.

39. As described below, all of the hardware components and functionalities encompassed by the Challenged Claims were well-known to a POSITA in the industry prior to the invention of the '286 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.

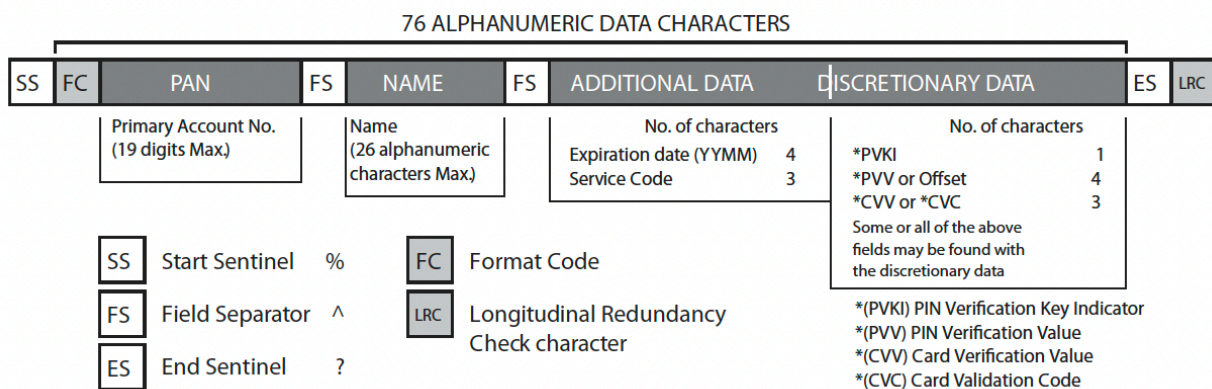
A. The Evolution of Payment Cards

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 (Ex. 1021)*, 59. “A magnetic stripe card is one that contains a digital storage space where the data are loaded during the manufacturing phase. The stripe is made up of tiny magnetic particles in a resin. It is traditionally a read-only item. It is read by physical contact by swiping the card past a device with a magnetic reading head.” *Coskun (Ex. 1021)*, 6.

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

Card Data Format - Track 1



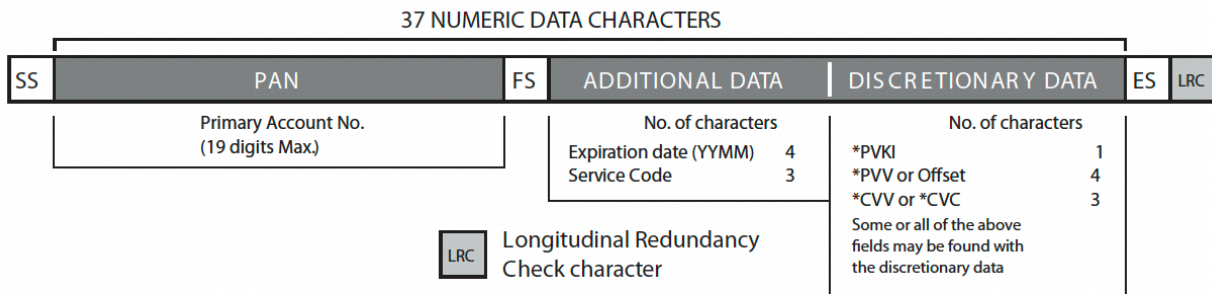
MagTek (Ex. 1022), 1. On a card’s track:

“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. 1009), [0102]. Track 2 data includes the following data:

Card Data Format - Track 2



MagTek (Ex. 1022), 1.

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



Figure 2.15 Magnetic stripe card.

Coskun (Ex. 1021), Figure 2.15.

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

2. *Smart/Chip Cards*

45. Smart cards were well known in the art all the way back to the “1970s.” *Coskun (Ex. 1021)*, 60. “The first mass use of the cards was for telephone

payments in the 1980s. In the meantime, microprocessor smart cards were introduced. Microchips were integrated into debit cards in the 1990s. Smart card based electronic purse systems which store values on a card and do not need network connectivity, began to be used in Europe from the mid 1990s.” *Coskun (Ex. 1021)*, 60.

46. One major improvement “in smart card technology occurred in the 1990s; smart card based SIMs were introduced and started to be used in GSM based mobile phone environments in Europe. The use of smart cards increased with the ubiquity of mobile phones in Europe. In 1993, the international payment brands Europay, MasterCard, and Visa (EMV) collaborated to develop new specifications for smart cards in order to use them in payments both as a debit and a credit card.” *Coskun (Ex. 1021)*, 60.

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

47. The EMV standard established a global framework for secure, chip-based payment card transactions. It introduced dynamic data generation, such as cryptograms to prevent replay attacks and authenticate transactions securely. *EMV (Ex. 1023)*, 71-74 (“generation of the combined dynamic signature and Application Cryptogram”); *EMV (Ex. 1023)*, 74-77 (“Dynamic Signature Verification”); *EMV (Ex. 1023)*, 87-91 “generation of the Application Cryptograms (TC, ARQC, or

AAC) generated by the ICC and the Authorisation Response Cryptogram (ARPC) generated by the issuer and verified by the ICC.”) The EMV standard defined clear steps in the transaction process, including cardholder verification (e.g., PIN or signature). *See EMV (Ex. 1023)*, 81-86. The EMV standard laid the foundation for modern secure payments, including contactless and mobile EMV solutions.

B. Contactless Payments

1. 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 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.

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.” *Finkenzeller (Ex. 1024)*, 57.

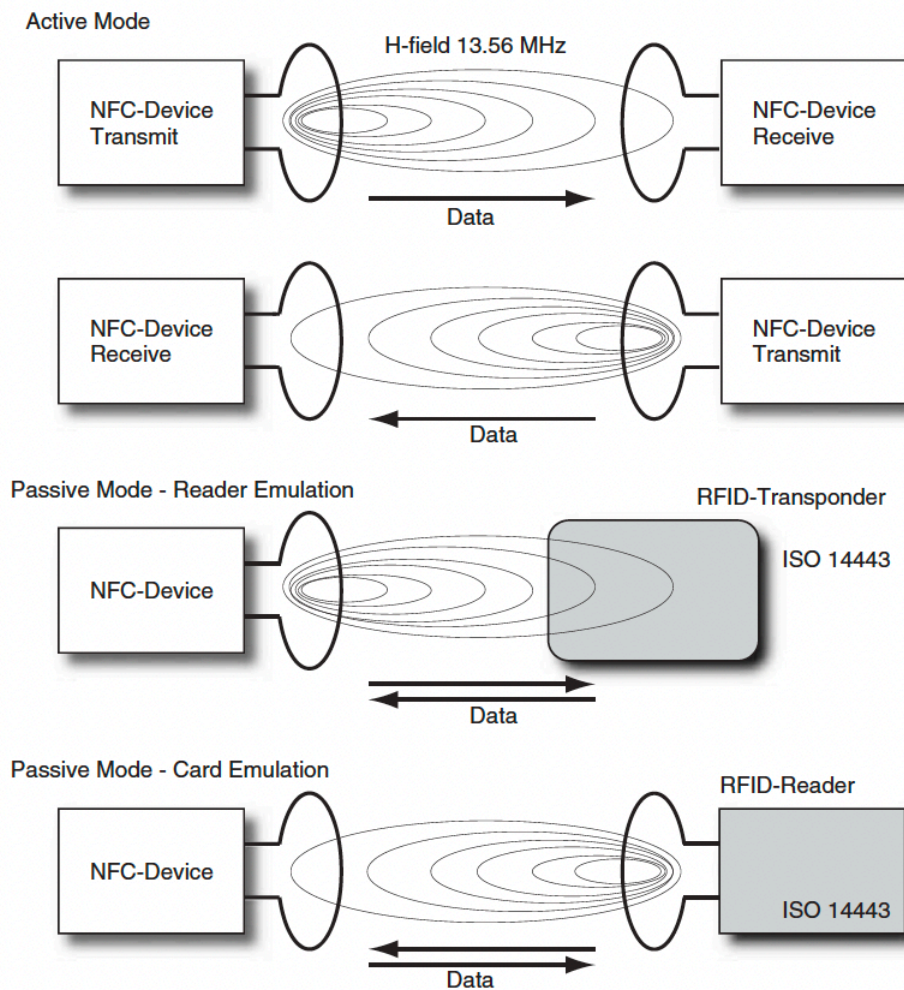


Figure 3.33 NFC distinguishes between three different operating modes: active mode (i); and passive mode in the operating modes reader emulation (ii); and card emulation (iii)

Finkenzeller (Ex. 1024), 58.

1. 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.” *Finkenzeller (Ex. 1024), 57.*

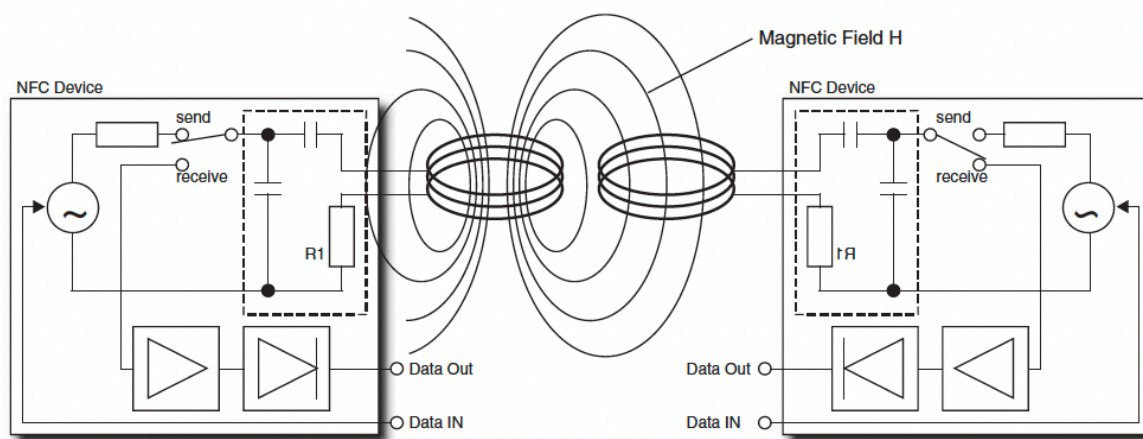


Figure 3.32 In active mode, the NFC interfaces alternately emit magnetic fields for data transmission

Finkenzeller (Ex. 1024), 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.” *Finkenzeller (Ex. 1024)*, 59.

2. *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.” *Finkenzeller (Ex. 1024)*, 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*’.” *Finkenzeller (Ex. 1024)*, 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*’.” *Finkenzeller (Ex. 1024)*, 59.

2. 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.

3. 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.

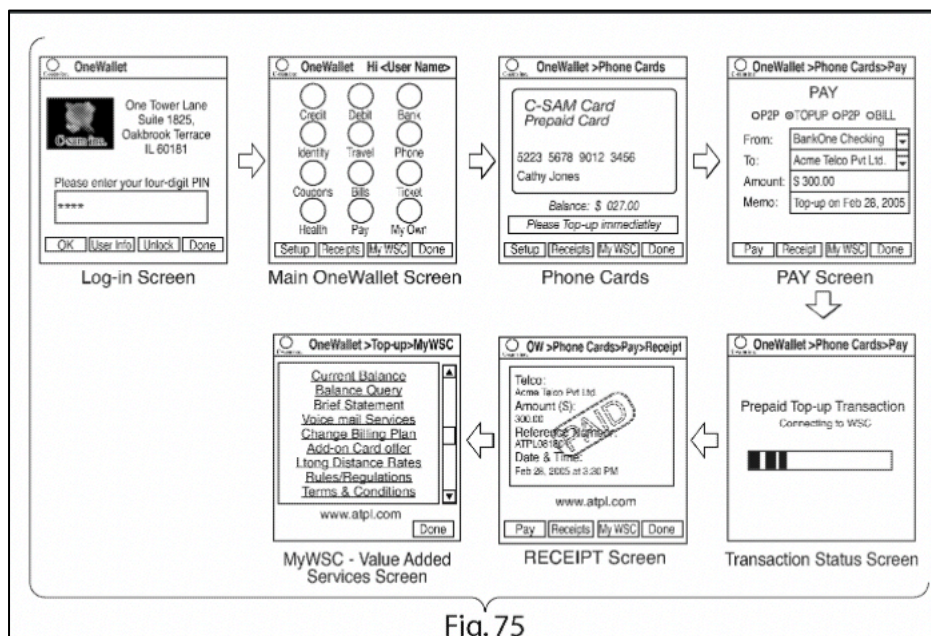
4. *Mobile Devices and Mobile Wallets*

60. Mobile devices performing contactless payments were well known before the '286 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].



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].” *Coskun (Ex. 1021)*, 345. Turkcell’s mobile wallet software is preloaded and “supports more than one bank-issued application.” *Id.*

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.

5. *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.”)

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.

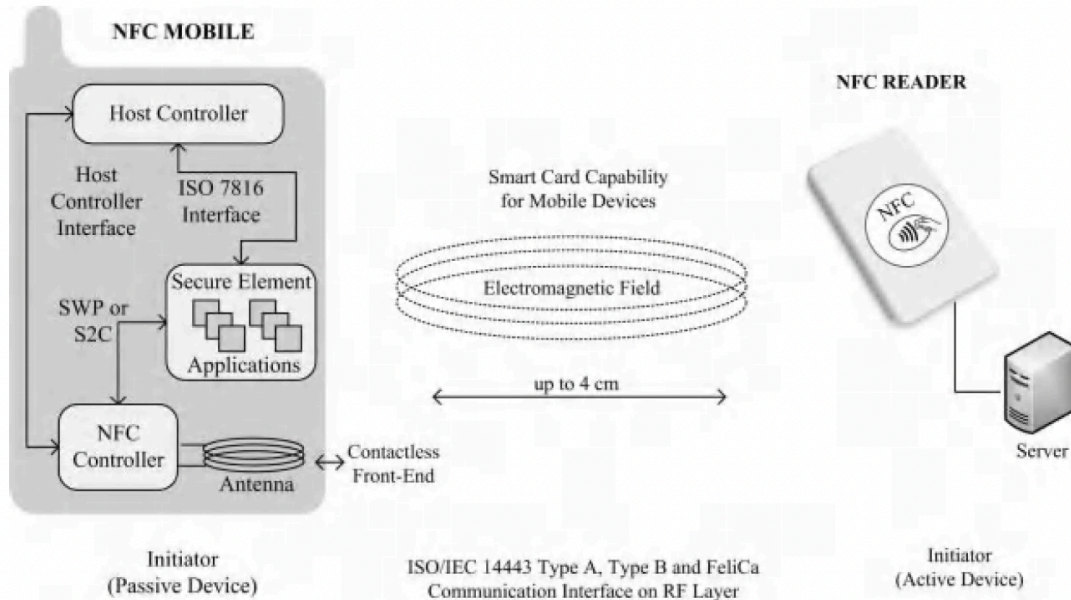


Figure 3.32 Communication architecture of card emulation operating mode.

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 by 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 763 successfully 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].

C. Payment Credential Security Features

69. With the increase in contactless payment transactions came additional opportunities for malicious intent 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 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 (Ex. 1013)*, [0066]. Each VPAN is also “associated with the static card verification code 506 from the payment account.” *Kranzley (Ex. 1013)*, [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 (Ex. 1013), 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 (Ex. 1013)*, [0065]. 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. *Vizzarri (Ex. 1032)*, 1-6. Classical methods are end-to-end encryption and tokenization. With tokenization an encrypted or random value, called token, replaces the card number (PAN) or the magnetic stripe track data in an electronic transaction. The token then becomes the reference number representing the card number, so all

tokens can be referenced back to the original card number.” *Vizzarri (Ex. 1032)*, 5.

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

6. *Alternatives to Static Card Verification Values*

73. Another method to increase security in 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[.]” *Id.*

74. 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.” *Id.*

75. 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. 1009)*, [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 (Ex.1013)*, [0066]. Bona notes that “[t]hese one-time (i.e., dynamic) codes are generated by the smart card chip and are unique to each transaction.” *Bona (Ex. 1009)*, [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. 1009)*, [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

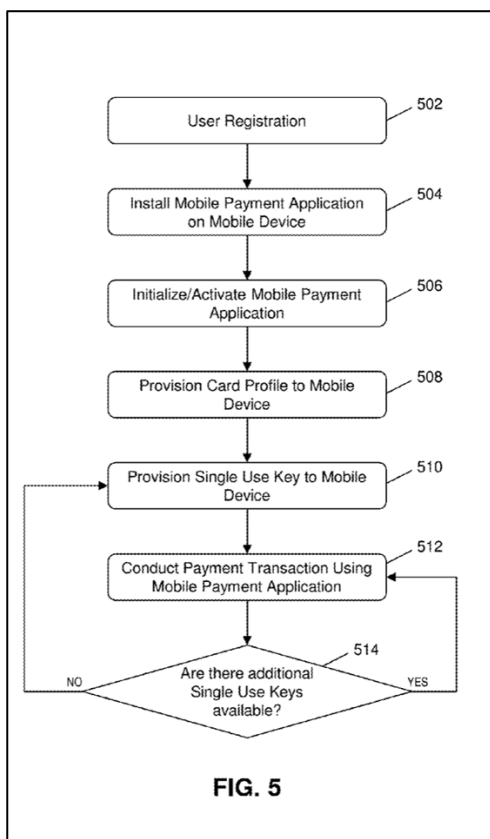
Card specification	Cryptogram Designator or Name
MasterCard PayPass MSD	CVC3
Visa Contactless MSD	dCVV
Discover ZIP MSD	dCVV
EMV, Visa QVSDC, VISA VSDC, MasterCard MCHIP	AC, TC, AAC, ARQC

Yeager, 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].

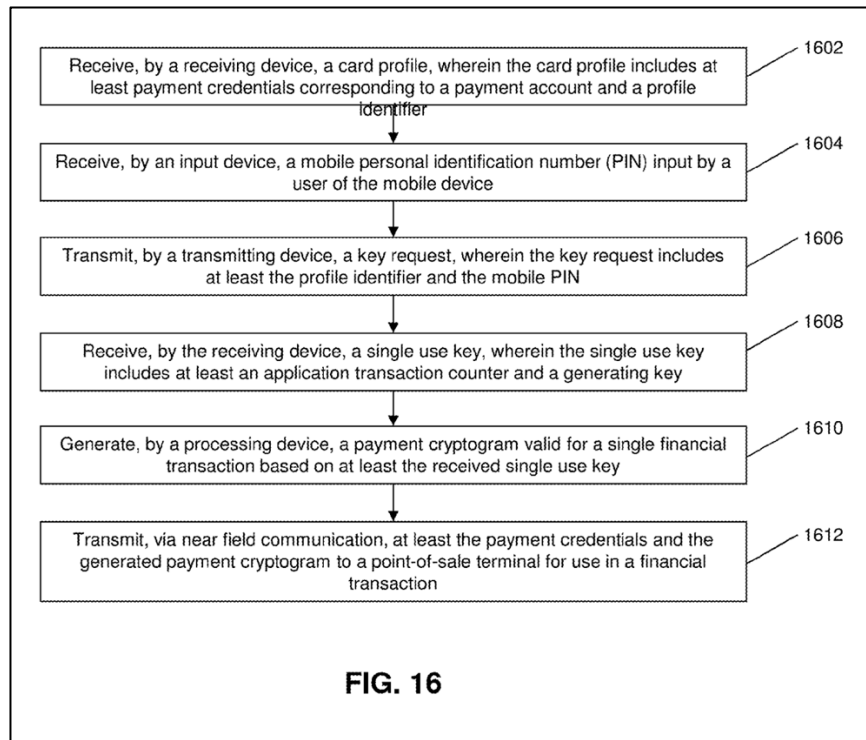
VIII. SUMMARY OF PRIOR ART REFERENCES

D. Collinge

76. 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 ’286 Patent. *’286 Patent (Ex. 1001)*, (56); *’286 File History (Ex. 1002)*. Collinge teaches “[a] method for generating and provisioning payment credentials to a mobile device lacking a secure element” which payment credentials may be used “in conducting a near field financial transaction.” *Collinge*, Abstract; [0002]. Collinge teaches that a user may register their mobile device for use in contactless payments and install a mobile payment application on the mobile device. *Collinge*, [0065]-[0066]. Collinge teaches that after registration, the mobile payment application of the mobile device is provisioned with a card profile and single use key from a remote secure element. *Collinge*, [0068]-[0069]; Fig. 5.



Using the provisioned single use key, the mobile payment application within Collinge’s mobile device generates a payment cryptogram valid for a single financial transaction. *Collinge*, [0069]. The 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. It is my understanding *Collinge* is entitled to a priority date of April 18, 2012 for the reasons discussed below. As I produced below, a table of key terminology used throughout *Collinge*.

<i>Abbreviation in Collinge</i>	<i>Meaning in Collinge</i>	<i>Mapping in Petition</i>
KS _{SUN} <i>Collinge</i> , Fig. 17, [0141], [0145].	session key unpredictable number	Secret used to generate and validate a payment cryptogram. Shared with issuer.
UN _{CLOUD} <i>Collinge</i> , Fig. 17, [0141].	cloud unpredictable number	Issuer secret used to validate a payment cryptogram.
single use key <i>Collinge</i> , [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 Collinge, Fig. 18, [0141], [0145].	Application transaction counter	Transaction counter, also shared with issuer
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

77. 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.

78. A POSITA would have classified Collinge within the same field of endeavor as the '286 Patent because both Collinge and the '286 Patent relate to conducting secure payment transactions. For example, Collinge describes

provisioning and storage of payment credentials for use in conducting near field financial transactions. *Collinge (Ex. 1004)*, [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 (Ex. 1004)*, [0043]. The mobile device can then use the single use key to generate a payment cryptogram for use in a financial transaction. *Collinge (Ex. 1004)*, [0070]. The '286 Patent similarly describes payment devices and transaction processing that can be utilized with near field communications. '286 *Patent (Ex. 1001)*, 1:31-36, 3:6-15. Similar to Collinge, the '286 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. '286 *Patent (Ex. 1001)*, 11:11-16.

79. Additionally, a POSITA would have found Collinge reasonably pertinent to the problem faced by the inventors of the '286 Patent because both Collinge and the '286 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 (Ex. 1004)*, [0003]-

[0007]. Likewise, the '286 Patent describes that its invention “address security concerns of a credit card owner” for use in RFID transactions. '286 Patent (*Ex. 1001*), 9:63-10:2, 12:33-37. Accordingly, a POSITA would have considered Collinge analogous art to the '286 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 '286 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 15, 2013 based on a showing of earlier conception and reduction to practice, it is additionally my understanding that Collinge is entitled to a prior date at least as early as April 18, 2012 based on Collinge's provisional application filed on and before that date (Provisional Nos. 61/619,095 (*Ex.1005*), filed April 2, 2012 (“’095 Provisional”), and 61/635,248 (*Ex.1006*) filed April 18, 2012 (“’248 Provisional”) (collectively, “Collinge's April 2012 Provisionals”).

82. I understand that for Collinge to be entitled to the April 18, 2012 filing date of the '248 Provisional, Collinge's April 2012 Provisional 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

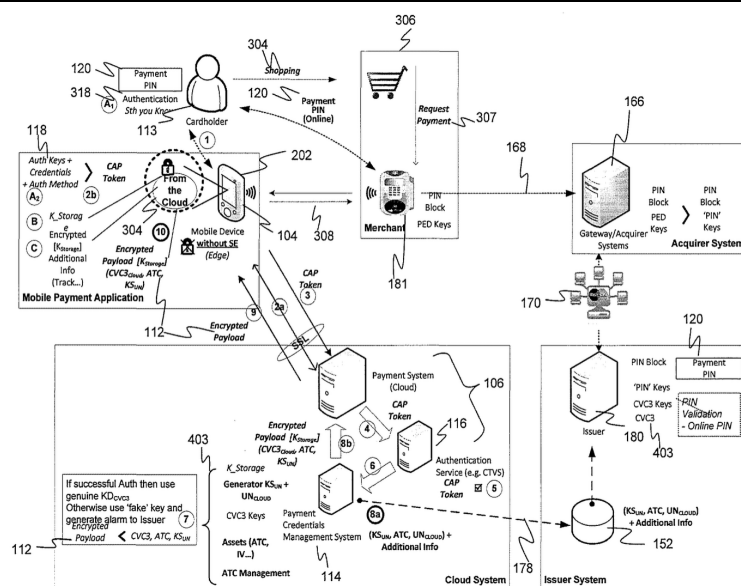
Provisional and it is my opinion Collinge's April 2012 Provisionals provide a detailed disclosure of the provisioning, storage and use of payment credentials for use in an NFC financial transaction disclosed and claimed in Collinge, including storing a storage key, a plurality of dynamic card validation codes ("DCV3"), and an application transaction counter ("ATC"); providing the storage key, an authentication component, and static payment credentials to a mobile device; validating a mobile device using a CAP token; generating a session key and cloud unpredictable number; identifying an encrypted payload, that includes a DCV3, the session key unpredictable number and ATC, based on a derived dynamic card validation code; transmitting the encrypted payload to the mobile device to generate a DCV3 for use in a financial transaction; and, transmitting the session key and cloud unpredictable number and ATC to an issuer for use in validating the DCV3 generated by the mobile device, which is similar to the level of disclosure in Collinge itself. In my opinion, Collinge's April 2012 Provisionals provide sufficient written description to enable a POSITA to practice the inventions claimed in at least claim 20 of Collinge.

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 mobile device lacking a secure element, comprising:	The Collinge Provisionals disclose methods for provisioning payment credentials to a mobile device lacking a secured element. “The present disclosure is directed to a method and system providing technical solutions for processing electronic payments initiated from a mobile device without requiring a secure element (SE) in the mobile device using in part a 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

¹ Unless otherwise noted, all emphasis is added.



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

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

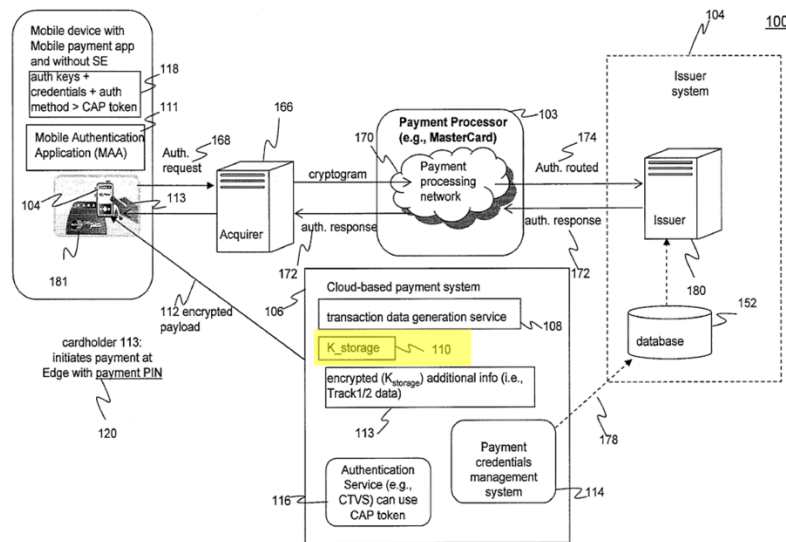
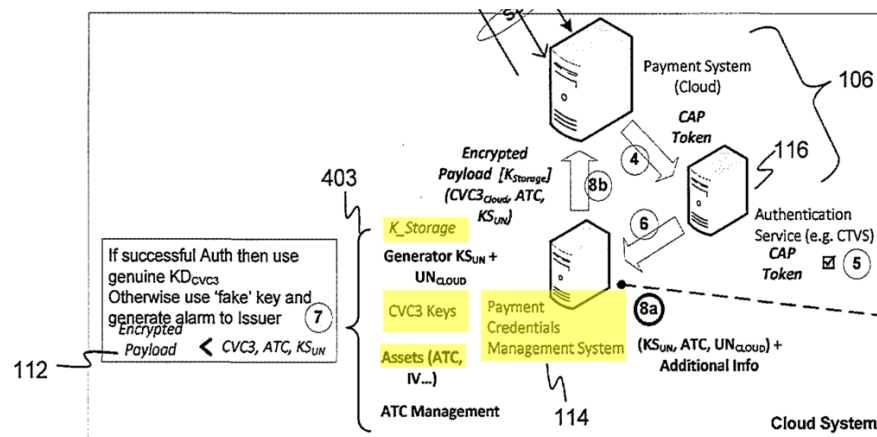


FIG. 1

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

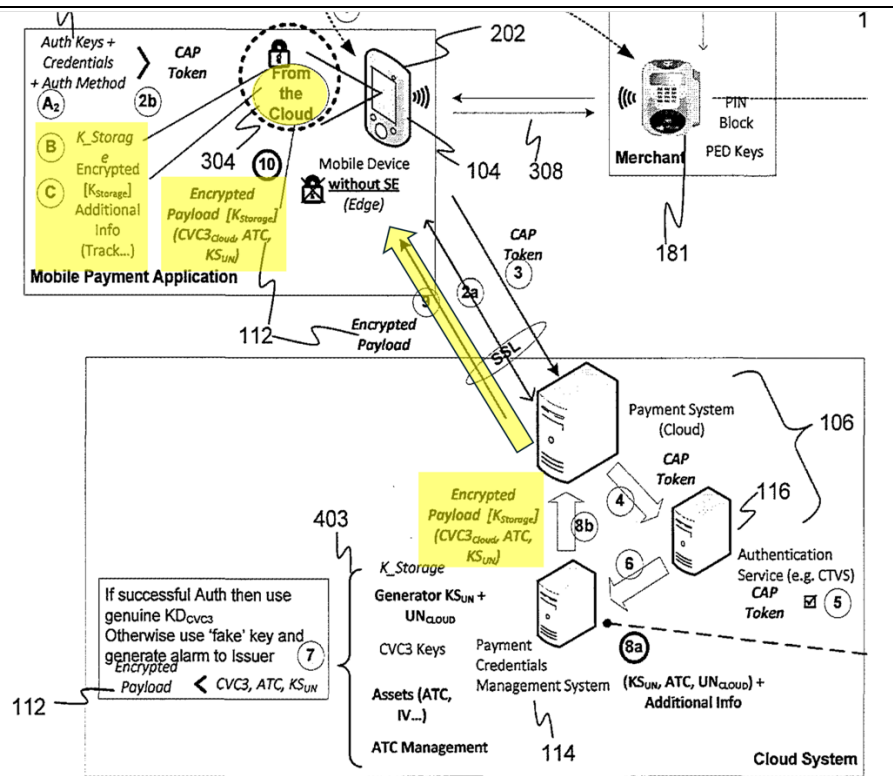


'095 Provisional (Ex. 1005), Fig. 5 (annotated excerpt);

see also '095 Provisional (Ex. 1005), Figs. 4, 6-8

provisioning, to the mobile device, at least the storage key, an authentication component, and static payment credentials, wherein the static payment credentials are associated with a payment account;	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 <table border="1"> <tr> <td data-bbox="509 594 678 751">B</td><td data-bbox="678 594 1377 751">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 data-bbox="509 751 678 835">C</td><td data-bbox="678 751 1377 835">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 $IVCVC3_{\text{Track1/2}}$ are static (if one considers a given PAN (and PSN) value, the values KD_{CVC3} and $IVCVC3_{\text{Track1/2}}$ 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}	B	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	C	At time of the authentication credentials provisioning, static payment credentials are also provisioned
B	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				
C	At time of the authentication credentials provisioning, static payment credentials are also provisioned				

	derivation process. This avoids mandating any change regarding the management of this value at issuer level even if the PSN may be used to identify a SE-less ‘virtual card’ defined for a given PAN. *** ► Delivery of Encrypted Payload [using K_{storage}] (K_{SUN}, 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

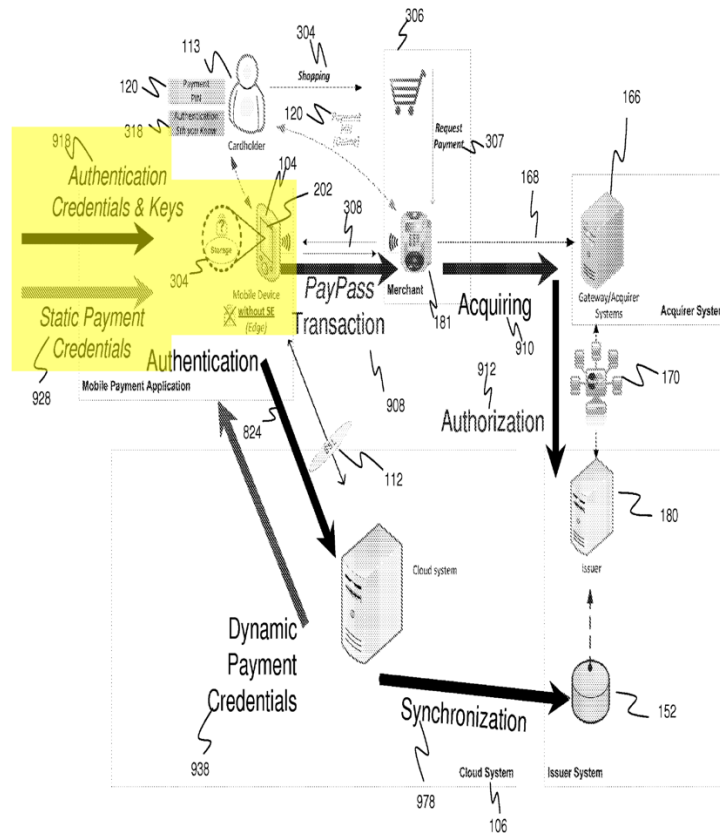


FIG. 9A

'248 Provisional (Ex. 1006), Fig. 9A

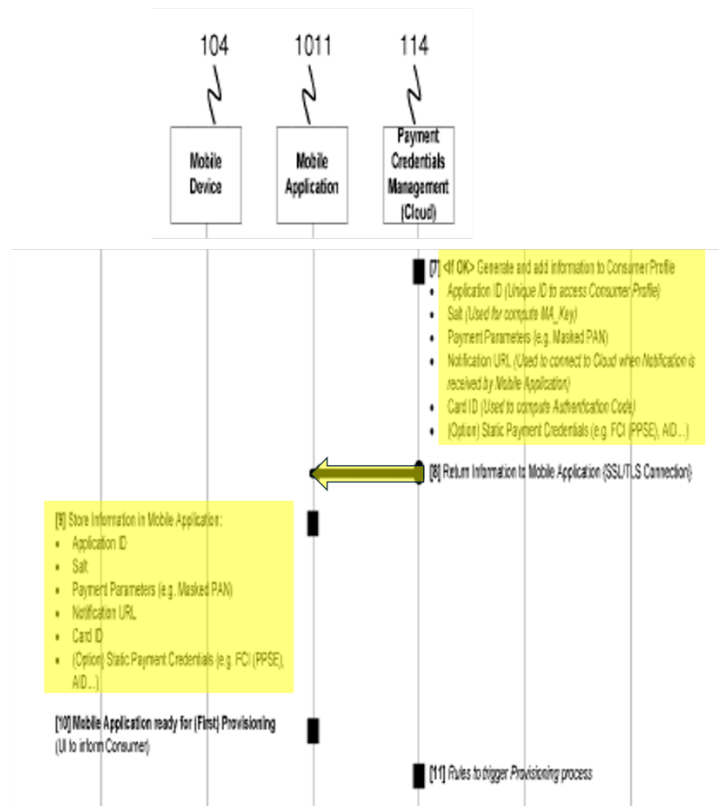
“The communications sequence depicted in Figure 11 encompasses pushing the following parameters/data to the mobile application 1011 as part of stage [7]: an application ID, which is a unique ID used to access the consumer profile (i.e., the profile for the user 113); a salt, which is a value used (in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

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

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

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

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



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

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

	depicted in Figures 9-15 and described above with reference to those Figures. Payment Token Payload According to an embodiment, the Payment Token Payload contains four parts: ◆ Length ◆ Proof Information ◆ Payment Data (Static - Non Sensitive, Static - Sensitive, Dynamic) ◆ [End Tag] The Payment Token Payload is transported and stored in encrypted form using a Mobile Application Key (MA_Key). The process to derive this key is defined in <i>Fn_MA_Key</i>. *** 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: ◆ <i>Length</i> ◆ <i>Proof Information</i> ○ Proof (Random - 5 bytes) ◆ <i>Static Payment Data</i> ○ FCI (PPSE) ○ AID ○ FCI (PayPass App) ○ AIP ○ APL ◆ <i>Static Payment Data (PayPass Transaction)</i> ○ PUNATC Track 1 ○ PUNATC Track 2 ○ PCVC3 Track 1 ○ PCVC3 Track 2 ○ NATC Track 1 ○ NATC Track 2 ○ UDOL ◆ <i>Static Payment Data (Sensitive Data)</i>
--	--

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

mobile device 104 where the cardholder 113 uses the Mobile Authentication Application (MAA) to generate a CAP Token.”

’095 Provisional (Ex. 1005), ¶0031

“The cloud-based transaction data generation system 106 also includes a payment credentials management system 114 and an authentication service 116. In the exemplary embodiment of Figure 1, the authentication service 116 is configured to perform CVTS CAP Token validation (CTVS) and can use a Chip Authentication Program (CAP) token for authentication.”

’095 Provisional (Ex. 1005), ¶0038

2b The Cardholder uses the MAA component of the Mobile Payment Application to generate a CAP Token for the authentication transaction. The Cardholder has to supply some credentials (e.g. A gesture, a password...)

3 Mobile Payment Application sends a CAP Token to the Cloud

’095 Provisional (Ex. 1005), Table 1 (p. 15)

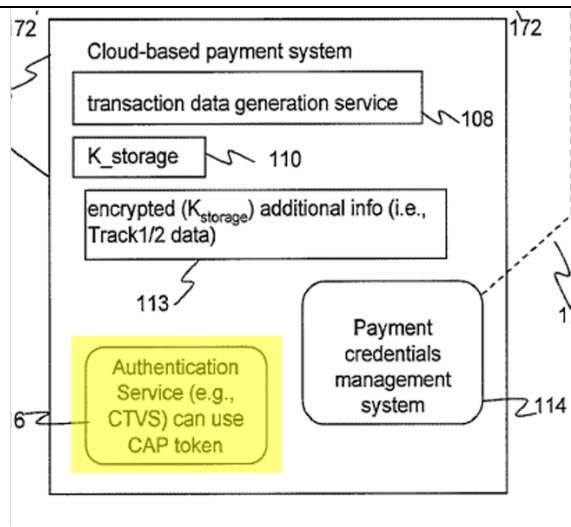
“forwarding payment credentials comprising at least one token from the Cloud to the mobile device;
receiving, at the Cloud, a token from a mobile authentication application (MAA) component of the mobile payment application;
validating the token based upon the authentication credentials and at least one additional credential received from the mobile device;”

’095 Provisional (Ex. 1005), Claim 1

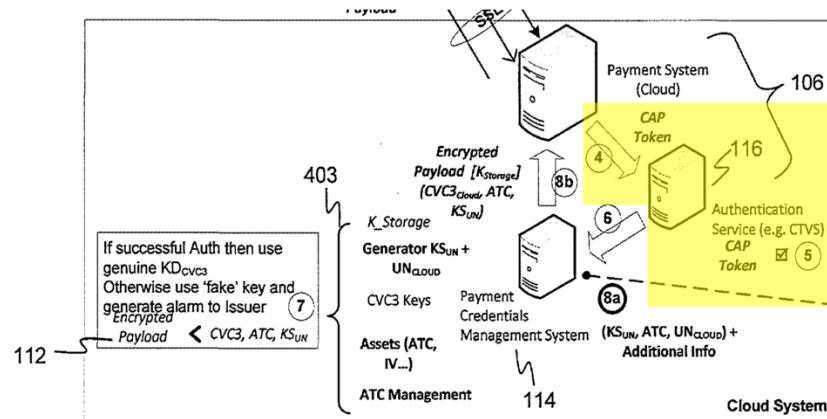
“9. The method of claim 1, wherein the token is a Chip Authentication Program (CAP) token indicating one or more controls on purchases.”

’095 Provisional (Ex. 1005), Claim 9

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



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



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

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

'095 Provisional (Ex. 1005), Claim 1

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

'095 Provisional (Ex. 1005), Claim 9

generating, by a processing device, a session key unpredictable number (KS_{UN});

The Collinge Provisionals disclose a cloud-based payment system generating a session key unpredictable number (KS_{UN}).

“Exemplary data flow stages depicted in Figures 5-7 are described in Table 1 below.

7	Upon successful authentication, a genuine KD_{CVC3} is used and (KS_{UN} , $Cloud_CVC3_{TRACK1/2}$, ATC) is returned.	”
---	--	---

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

“Exemplary solutions and embodiments disclosed herein can incorporate several core principles outlined below:

► Session key generation (KS_{UN}) in the Cloud to bind (ATC, UN_{CLOUD} , PAN and PSN) at the Edge (Mobile Payment Application)”

’095 Provisional (Ex. 1005), ¶0068

“A Glossary of terms and acronyms described above and depicted in Figures 3-8 is provided in Table 2 below:

Table 2	
Stage	Description

UN	Unpredictable Number
----	----------------------

’095 Provisional (Ex. 1005), Table 2 (p. 26)

“According to an embodiment, the principles for the synchronization process (between the Cloud-based transaction data generation system 106 to issuer 180) are as follows:

	1. The Cloud_CVC3_{TRACK1/2} generation is managed in the Cloud-based transaction data generation system 106 (“the Cloud). This encompasses the generation of KS_{UN} and UN_{CLOUD}, and the application transaction counter (ATC) management.” ’248 Provisional (Ex. 1006), ¶0077; ’095 Provisional (Ex. 1005), ¶0056 (p.13) ’095 Provisional (Ex. 1005), Fig. 1 (annotated excerpt); <i>see also</i> ’095 Provisional (Ex. 1005), Fig. 7
generating, by the processing device, a cloud unpredictable number (UN_{CLOUD});	The Collinge Provisionals disclose a cloud-based payment system generating a cloud unpredictable number (UN_{CLOUD}). “According to an embodiment, the principles for the synchronization process (between the Cloud-based transaction data generation system 106 to issuer 180) are as follows: 1. The Cloud_CVC3_{TRACK1/2} generation is managed in the Cloud-based transaction data generation system 106 (“the Cloud). This encompasses the generation of KS_{UN} and UN_{CLOUD}, and the application transaction counter (ATC) management.” ’248 Provisional (Ex. 1006), ¶0077; ’095 Provisional (Ex. 1005), ¶0056 (p.13) “A Glossary of terms and acronyms described above and depicted in Figures 3-8 is provided in Table 2 below:

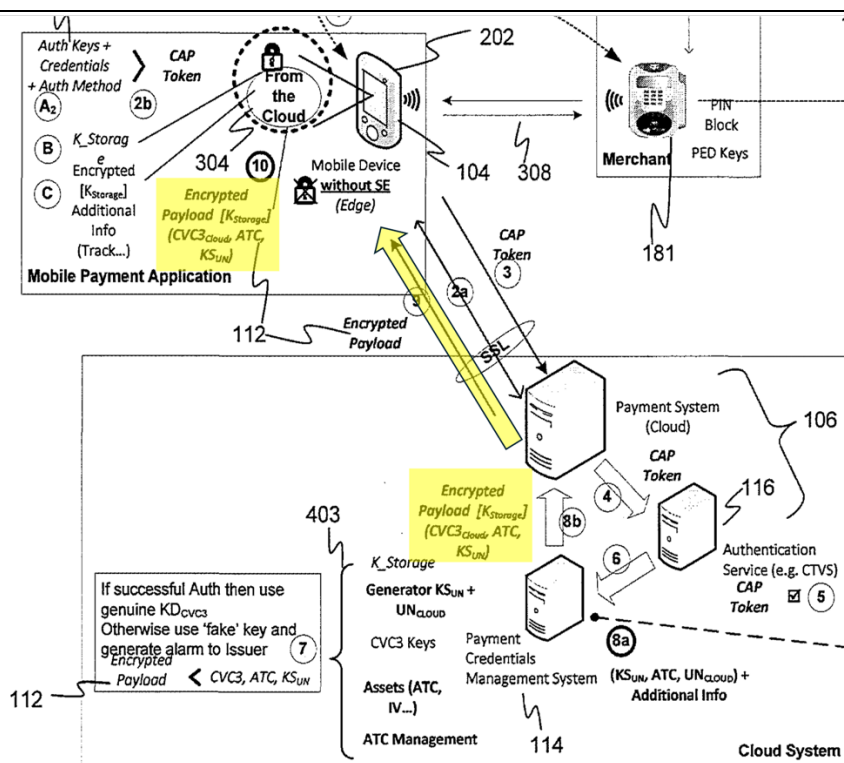
Table 2	
Stage	Description

UN	Unpredictable Number
	'095 Provisional (Ex. 1005), Table 2 (p. 25)
	The diagram illustrates a cloud-based transaction data generation system (106). It includes a Payment System (Cloud) and an Authentication Service (e.g., CTVS). A CAP Token is generated by the Authentication Service. A Generator (KS_UN + UN_CLOUD) and a Payment Credentials Management System (114) are involved in generating an encrypted payload (CVC3, ATC, KS_UN). The payload is then sent to the Payment System (Cloud) via an Encrypted Payload (K_STORAGE). The system also includes Assets (ATC, IV...) and ATC Management. A box labeled 112 contains a decision logic: 'If successful Auth then use genuine KD_CVC3. Otherwise use 'fake' key and generate alarm to issuer.' The diagram is annotated with various labels and numbers, including 403, 4, 6, 8a, 8b, 116, and 114.
	'095 Provisional (Ex. 1005), Fig. 5 (annotated excerpt); '095 Provisional (Ex. 1005), Fig. 4, 6-7
identifying, by the processing device, an encrypted payload based on a derived dynamic card validation code key (KD _{CVC3}), wherein the encrypted payload includes at least a dynamic card validation code key of the	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)

financial transaction; and	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 turn 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_{TRACK1/2} ◇ 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_{TRACK1/2} Mobile Payment Application to perform CVC3 generation using: ◇ Information from the Reader ◇ Stored Information ◇ Credentials previously retrieved from the Cloud
--	--

	CVC3 value to be included in Payment Authorization message (Track 2 (and Track 1) information). '095 Provisional (Ex. 1005), p. 23 “Issuer Validation Process An exemplary validation process is described below wherein the Issuer 180 uses the information provided in the payment transaction: • Identifier - e.g. PAN Information • UN_{READER} (4 bytes) - Partial Information retrieved from Track data (Discretionary Information) • ATC (2 bytes)-Partial Information retrieved from Track data (Discretionary Information) • CVC3_{TRACK1/2} Partial Information retrieved from Track data (Discretionary Information) *** The Issuer can validate the CVC3_{TRACK1/2}.” '095 Provisional (Ex. 1005), ¶¶0072-0074 “The dynamic values (CVC3 and ATC) are used as a first form factor to authenticate the payment transaction. The Online PIN can be used as a second form factor. This dynamic CVC3 value is generated by the mobile payment application using information from the payload provided by the cloud-based transaction data generation system 106 (‘the Cloud’).” '095 Provisional (Ex. 1005), ¶0112
--	--



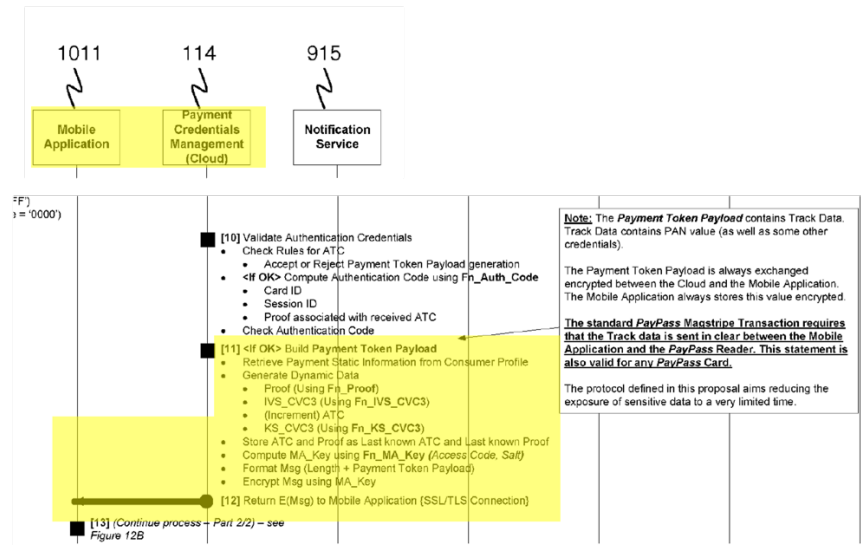
'095 Provisional (Ex. 1005), Fig. 5 (annotated excerpt);
'095 Provisional (Ex. 1005), Figs. 1, 6-8

“In stage [11], the payment token payload is built. In the exemplary embodiment of Figure 12A this stage includes retrieving payment static information from the consumer profile and generating dynamic data. Such dynamic data generation includes: the proof (using Fn_Proof), the IVS_CVC3 (using Fn_IVS_CVC3), incrementing the ATC, and the KS CVC3 (Using Fn_KS_CVC3).”

'248 Provisional (Ex. 1006), ¶0161

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

'248 Provisional (Ex. 1006), ¶¶166



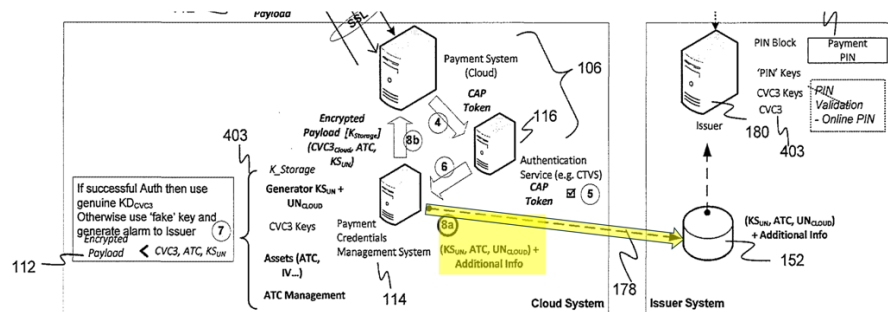
'248 Provisional (Ex. 1006), Fig. 12A (annotated excerpt)

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

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

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

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



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

'095 Provisional (Ex. 1005), Figs. 6-7

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

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

“Payload sent to the Issuer

◇ Identifier (PAN ...)
◇ UN_{CLOUD}
◇ ATC
◇ Authentication Status Info+ Additional Generation Information (e.g. Validity)”

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

“Issuer Validation Process

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

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

The Issuer system is able to compute Cloud_CVC3_{TRACK1/2} using:

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

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

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

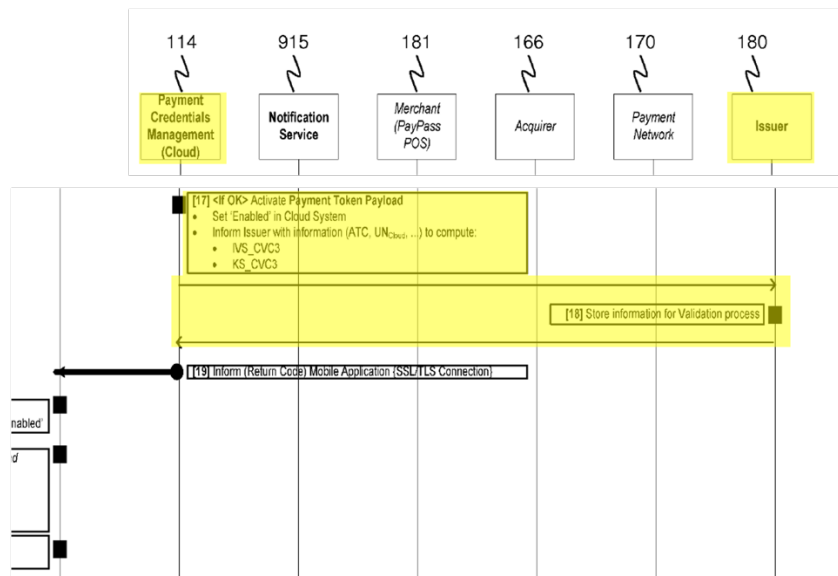
The Issuer can validate the CVC3_{TRACK1/2}”

’095 Provisional (Ex. 1005), ¶¶0072-0074;

’248 Provisional (Ex. 1006), ¶0226 (p. 54)

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

’248 Provisional (Ex. 1006), ¶0172



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

	“CVC3 Validation process (<i>Fn_ValCVC3</i>) 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 <i>Fn_ValCVC3</i> 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 <i>“UN_{CLOUD} is part of the payload exchanged between the Cloud and the Issuer during the Synchronization process.”</i> ’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 ground below appear substantially identically in Collinge Provisionals. I have endeavored to include citations to corresponding disclosures in the Collinge Provisionals in the charts above. Accordingly, the disclosure relied on to meet challenged claim limitations is entitled to Collinge Provisionals’ filing date. Further, Collinge’s provisional applications are directed to the same invention. Figures, invention elements numbering, and invention descriptions substantially overlap, and a POSITA would recognize that the Provisionals provide additional implementation details relevant to Collinge’s payment system. *Compare ’098 Provisional (Ex. 1008), Fig. 19 with*

Collinge (Ex. 1004), Fig. 6; '095 Provisional (Ex. 1005), Fig. 9 with Collinge (Ex. 1004), Fig. 19 and '248 Provisional (Ex.1006), Fig. 16.

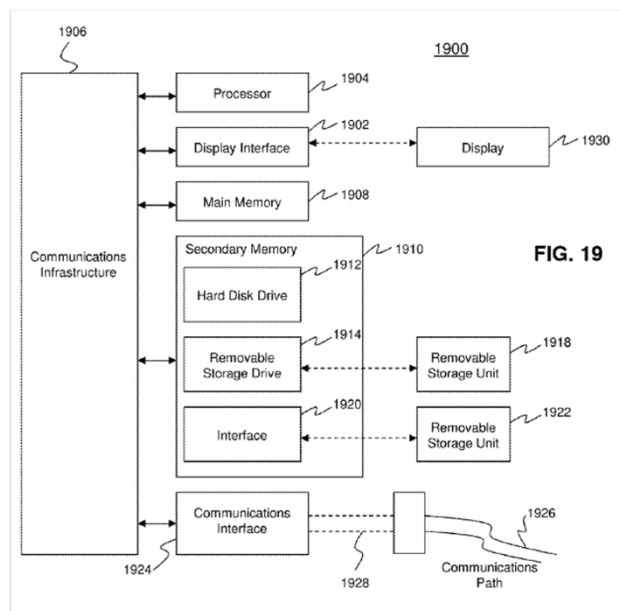


FIG. 19

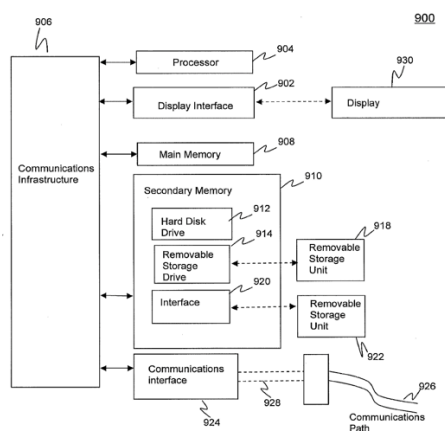


FIG. 9

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

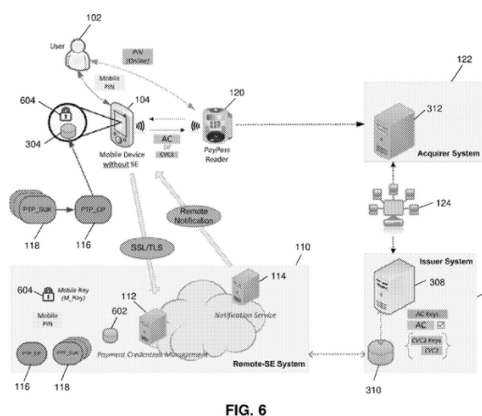


FIG. 6

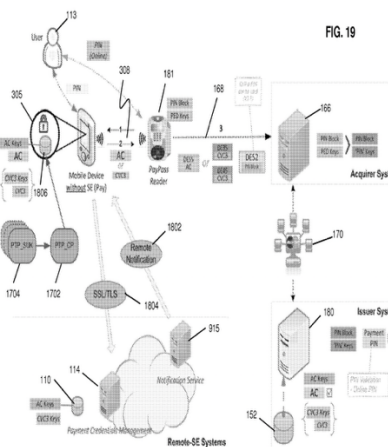
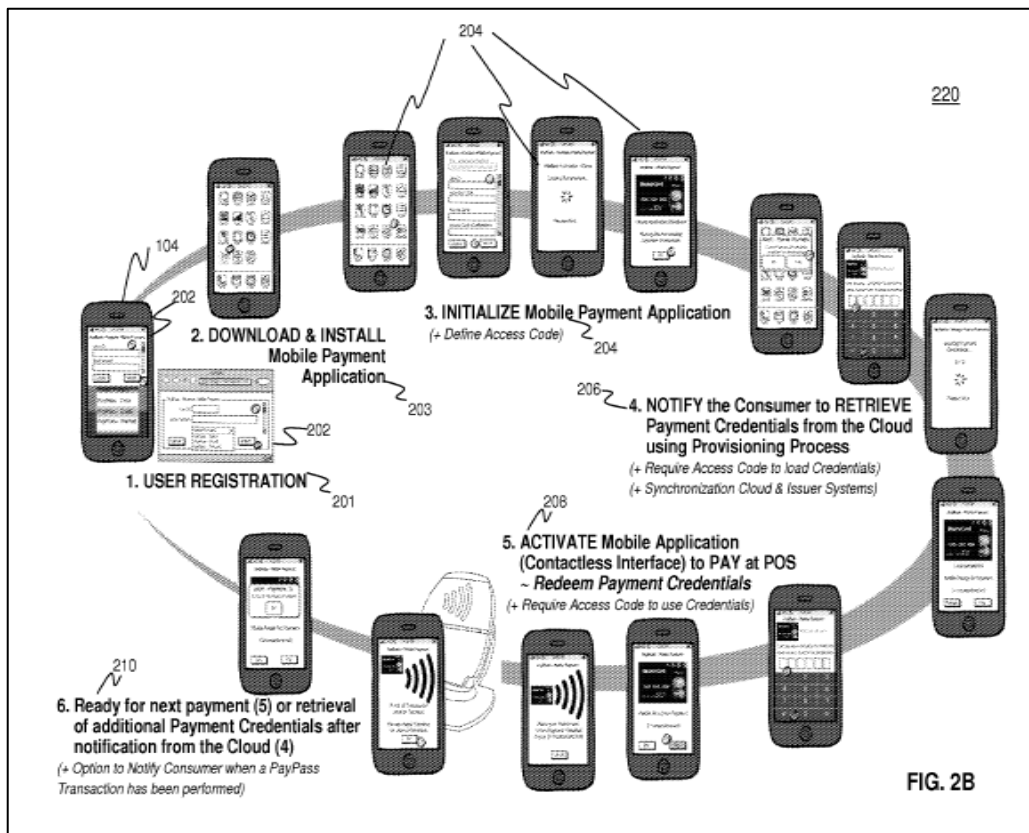


FIG. 19

Collinge at Figure 6 (left); *'095 Provisional (Ex. 1005)*, Figure 19 (right). Even if *Collinge's* Provisionals were directed to different payment system embodiments, it would have been obvious, and a POSITA would have been motivated to apply the

teachings in Collinge's Provisionals in Collinge's payment system. For example, Collinge's provisional applications provide additional detail about what is shown on the graphical user interface of Collinge's mobile device during user registration, user selection of a payment option, and an NFC transaction. *See e.g., '248 Provisional (Ex. 1006), Fig. 2A, 2B; '098 Provisional (Ex. 1008), p. 96-100; Collinge (Ex. 1004), [0133].*

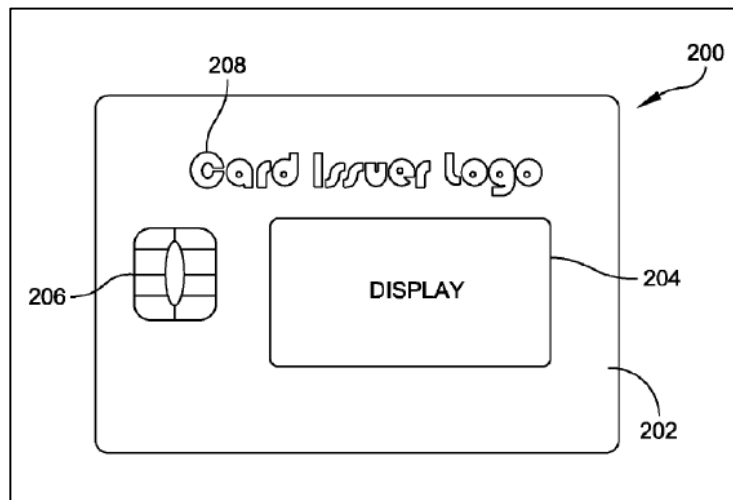


'248 Provisional (Ex. 1006), Fig. 2B. A POSITA would have found it obvious and would have been motivated to incorporate these disclosures into Collinge's payment system as examples of selectable softbuttons that could be used to implement the

invention. As another example, Collinge teaches use of a “CAP token” (*Collinge (Ex. 1004)*, [0144]) and the provisional applications provide examples of what controls on purchases may be represented by the token. *See '095 Provisional (Ex. 1005)*, Claims 9-10 (day of week, time of day, etc.). A POSITA looking to implement a CAP token would have been motivated to implement one or more of the examples of a CAP token in Collinge’s Provisional application. In each case, a POSITA would have found a teaching, suggestion, or motivation in Collinge since the provisional was directed to the same mobile device used in Colline, that would have led them to apply the additional details in Collinge’s Provisionals to Collinge’s payment system and would have had a reasonable expectation of success.

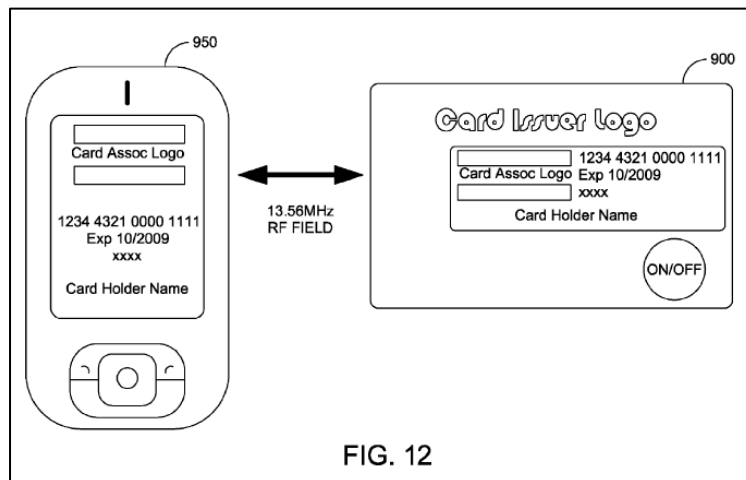
E. Bona

87. I understand Bona teaches an NFC enabled companion card that “includes an on/off button 906 for powering the smart card on/off and a display 904 for displaying information to the user.” *Bona (Ex. 1009)*, [0110].



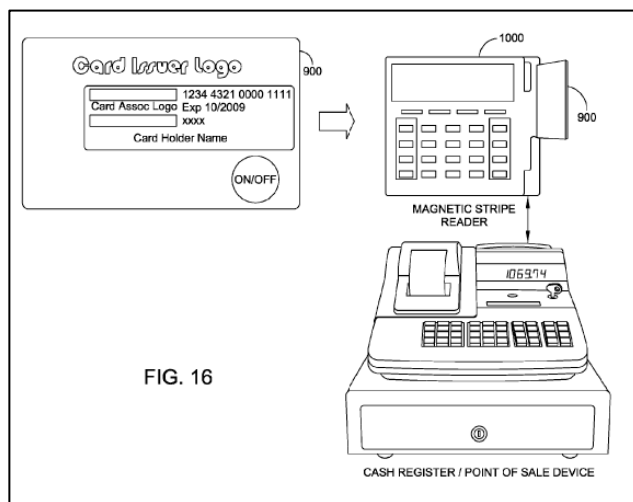
Bona (Ex. 1009), Fig. 2A.

88. Bona teaches using its NFC enabled companion card in connection with a cell phone for transactions. *Bona (Ex. 1009), [0119].*



Bona (Ex. 1009), Fig. 12.

89. Bona's payment card device is operable for use in a payment card reader equipment, such as "contact smart card readers, contactless smart card readers and magnetic stripe readers[.]" *Bona (Ex. 1009), 0036.*



Bona (Ex. 1009), Fig. 16.

90. 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.

4. *Bona is Analogous*

91. A POSITA would have classified Bona within the same field of endeavor as the '286 Patent because both Bona and the '286 Patent relate to the generation and use of credentials for smart payment devices. For example, *Bona*, like the '286 Patent discloses conducting secure payment transactions. *Compare*

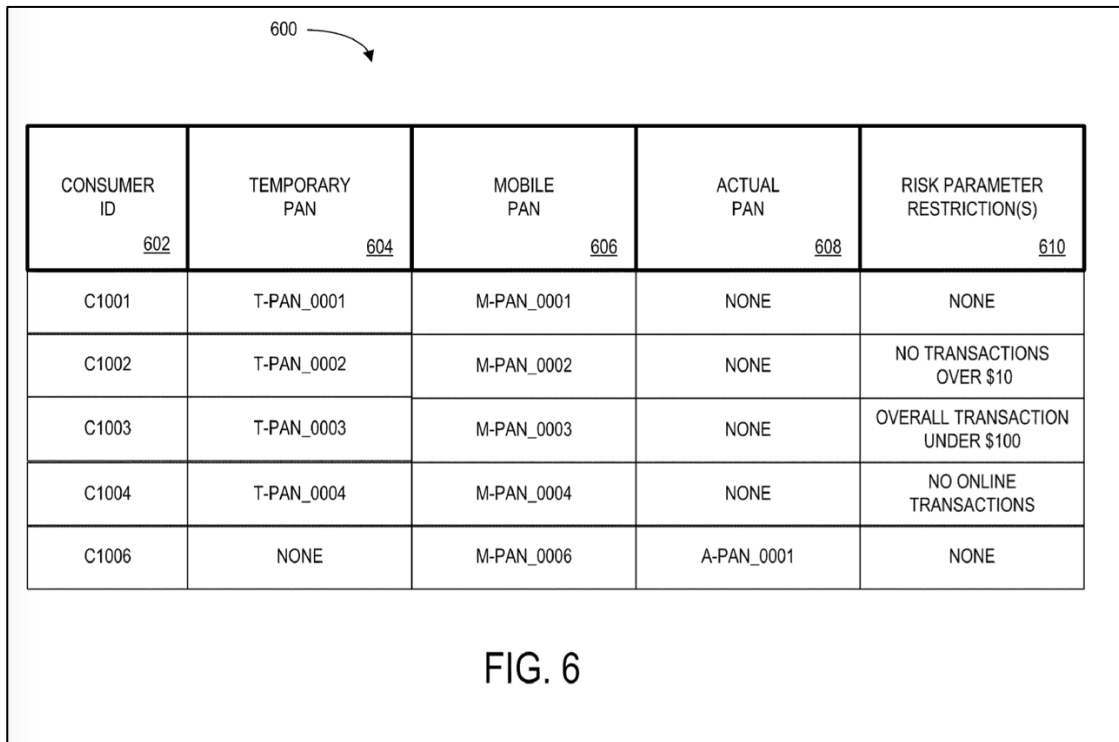
'286 Patent (*Ex. 1001*), Abstract, 1:31-35, Fig. 1 with *Bona* (*Ex. 1009*), Abstract, 0036-0037, Fig. 16. Thus, *Bona* is in the same field of endeavor as the '286 Patent.

92. Additionally, a POSITA would have found *Bona* reasonably pertinent to the problem faced by the inventors of the '286 Patent because both *Bona* and the '286 Patent describe the need for increased security in financial transactions using smart card or mobile devices to prevent fraudulent or unauthorized transactions. *See* '286 Patent (*Ex. 1001*), 1:31-35, 2:4-12, 9:63-10:2. For example, *Bona*'s invention "make[s] it possible to implement some dynamic data in transactions utilizing magnetic stripe readers" to "serve as an effective safeguard for secured static credit card (or other) information and thus act as a significant tool against fraudulent transactions." *Bona* (*Ex. 1009*), [0036]; *compare* *Bona* (*Ex. 1009*), [0008]-[0010]. *Bona* is also reasonably pertinent to problems addressed by the '286 Patent such as increasing security of payment transactions. *Compare* '286 Patent (*Ex. 1001*), 1:31-35, 2:4-12, 9:63-10:2 with *Bona* (*Ex. 1009*), [0008]-[0010]. Therefore, a POSITA would have considered *Bona* analogous art to the '286 Patent.

F. Smith

93. I understand *Smith* teaches a "mobile PAN" for a "mobile device" that "may...be used...with a near field communications enabled purchasing transaction." *Smith* (*Ex. 1010*), Abstract.

94. I understand Smith teaches a “mobile PAN” is used in place of the actual PAN. *Smith* (Ex. 1010), [0023] (the PPAN is associated with a “related PAN[.]”); *see also Smith* (Ex. 1010), [0026].



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

FIG. 6

Smith (Ex. 1010), Fig. 6. The mobile PAN is “stored in the mobile device 204.” *Smith* (Ex. 1010), [0022].

1. Smith is Analogous

95. Smith is analogous art to the '286 Patent because it is from the same field of endeavor because both Smith and the '286 Patent are directed towards conducting secure payment transactions. Like the '286 Patent, Smith is concerned with conducting secure payment transactions. *See, e.g., Smith* (Ex. 1010), [0021]

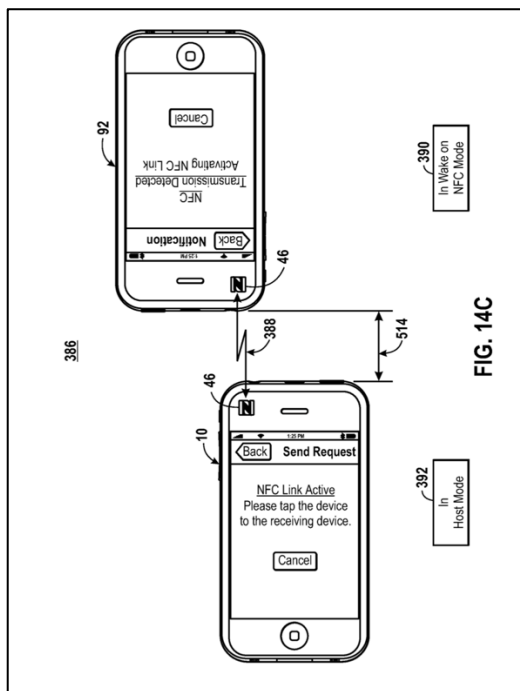
(“ a mobile device 204 to be used to conduct a payment transaction using a payment application stored in the mobile device[.]”); [0022] (“a transaction may be initiated by the customer presenting their mobile device 204 at a merchant 214 to complete a purchase.”); [0022] (“the mobile device 204 may be presented within range of a point of sale device having NFC capabilities.”); [0024] (“a series of messages (defined by the PayPass® standard) occur, and the point of sale device is provided with information including the PPAN stored in the mobile device 204.”) *Compare* ’286 Patent (*Ex. 1001*), Abstract, 1:31-35, Fig. 1 *with Smith (Ex. 1010)*, Abstract, [0021]-[0023].

96. Additionally, a POSITA would have found Smith reasonably pertinent to the problem faced by the inventors of the ’286 Patent because both Smith and the ’286 Patent describe the need for increased security in financial transactions using smart card or mobile devices to prevent fraudulent or unauthorized transactions. *See, e.g., Smith (Ex. 1010)*, [0002] (“One approach, introduced by MasterCard International Incorporated, the assignee of the present application, is to securely install a payment application in mobile phones that are Near Field Communications (NFC)-enabled, allowing the phones to be used as a payment device in contactless payment transactions.”) [0015] (“the data elements are transmitted using a secure web service or other data protocol, such as a Simple Object Access Protocol

(“SOAP”) service.”); [0020] (“a cost effective and secure method may be provided for issuers to extend NFC products by issuing and enabling over-the-air personalization of approved NFC-enabled mobile phones...The cardholder may then use his or her mobile phone as a standalone NFC payment device.”). *Compare* ’286 Patent (Ex. 1001), 1:31-35, 2:4-12, 9:63-10:2 with Smith (Ex. 1010), [0002], [0015], [0020].

G. Lin

97. I understand Lin teaches “the establishment of an NFC connection 388 between two devices, namely the payee device 10 and the payor device 92, by way of the tap operation 386 [.]” *Lin* (Ex. 1012), 68:10-13.



Lin (Ex. 1012), Fig. 14C.

98. Once “active device 10 is placed within an acceptable distance 514 (e.g., 2-4 cm) from the payor device 92” the devices establish an “NFC connection 388...through which the payment request may be transmitted.” *Lin (Ex. 1012)*, 68:13-25.

1. Lin is Analogous

99. Lin is analogous art to the '286 Patent because it is from the same field of endeavor because both Lin and the '286 Patent are directed towards conducting secure payment transactions. *See, e.g., Lin (Ex. 1012)* 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 '286 Patent (Ex. 1001)*, Abstract, 1:31-35, Fig. 1 *with Lin (Ex. 1012)*, Abstract, 68:13-25, Fig. 14C.

100. Lin is also reasonably pertinent to at least one problem addressed by the '286 Patent. Like the '286 Patent, Lin is concerned with increasing security of payment transactions. *See, e.g., Lin (Ex. 1012)*, 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 (Ex. 1012)* at 27:8–28:15; *compare '286 Patent (Ex. 1001)*, 1:31–35, 2:4–12, 9:63–10:2 *with Lin (Ex. 1012)*, 26:26–28–15.

H. Patterson

101. Patterson teaches “a consumer 10 may be presented with a webpage via a client computer 16 to register for account level blocking, as shown in FIG. 7 and in step 405 of FIG. 4. This webpage or web application may be hosted at the payment processing network 40 or the issuer 50. A consumer may also register in other manners such as by phone, email, SMS, etc.” *Patterson (Ex. 1011)*, 6:12–16.

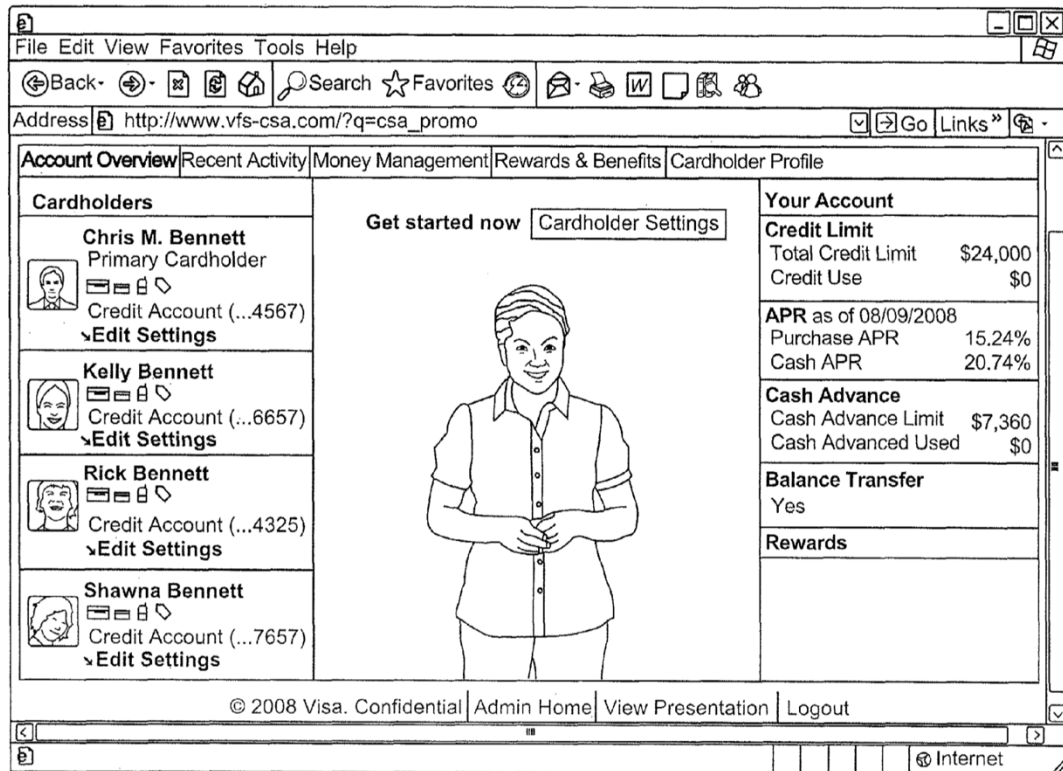


FIG. 7

Patterson (Ex. 1011), Fig. 7.

102. “As part of the registration, the consumer may be asked to provide identifying information to the registration web server, in order to authenticate to the server that the consumer is in fact who he claims to be. Once the consumer has been authenticated, he may then specify blocking criteria to be associated with one or more accounts. The use of such blocking criteria may allow the consumer 10 to place restrictions on his account that are more specific than restrictions that may be placed by the issuer 50 of the account.” *Patterson (Ex. 1011)*, 6:17-27.

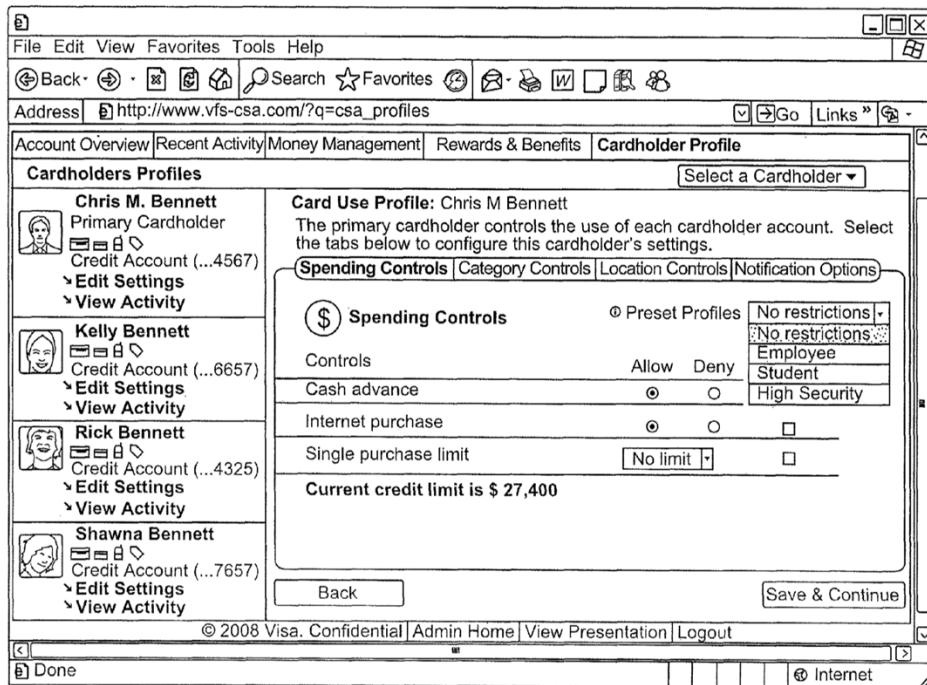


FIG. 8

Patterson (Ex. 1011), Fig. 8.

1. *Patterson is Analogous*

103. Patterson is analogous art to the '286 Patent because it is from the same field of endeavor. Like the '286 Patent, Patterson is concerned with conducting secure payment transactions. *See, e.g., Patterson (Ex. 1011)*, Abstract (“The method includes receiving, at a server computer, a transaction clearing request for a transaction, and then determining, using the server computer, if the transaction satisfies a stored blocking parameter. The method further includes allowing, using the server computer, the transaction clearing request if the transaction does not satisfy the stored blocking parameter, and denying, using the server computer, the

transaction clearing request if the transaction satisfies the stored blocking parameter.”); 1:15-17. (“In some cases, a consumer may want to restrict his usage of his account so that certain transactions are authorized and some are not.”) *Compare* ’286 Patent (Ex. 1001), Abstract, 1:31-35, Fig. 1 with Patterson (Ex. 1011), Abstract, 1:15-17, Fig. 1.

104. Patterson is also reasonably pertinent to at least one problem addressed by the ’286 Patent. Like the ’286 Patent, Patterson is concerned with increasing security of payment transactions. *See, e.g., Patterson* (Ex. 1011), Abstract (“... denying, using the server computer, the transaction clearing request if the transaction satisfies the stored blocking parameter.”); 6:18-46 (“Blocking criteria may include... lost or stolen card (e.g., a “hotcard” list which will block all transactions from that card from being authorized)”; 11:22-25 (“The blocking system 41 would also compare the list of lost or stolen cards (not shown) and determine whether or not the account number matched a lost or stolen card.”) *Compare* ’286 Patent (Ex. 1001), 1:31-35, 2:4-12, 9:63-10:2 with Patterson (Ex. 1011), 5:18-46, 11:22-25.

I. Kranzley

105. Kranzley teaches that “[t]he payment application of the mobile device 12 converts the data (including the PAN, expiry, and dynamic data) into a bar

code image 13.” *Kranzley (Ex. 1013)*, [0028]. *Kranzley* teaches displaying “the static VPAN...in plain text on a display device 14 of the mobile device 12 along with an expiry date and dynamic data.” *Kranzley (Ex. 1013)*, [0035]; [0033]-[0036].

1. Kranzley is Analogous

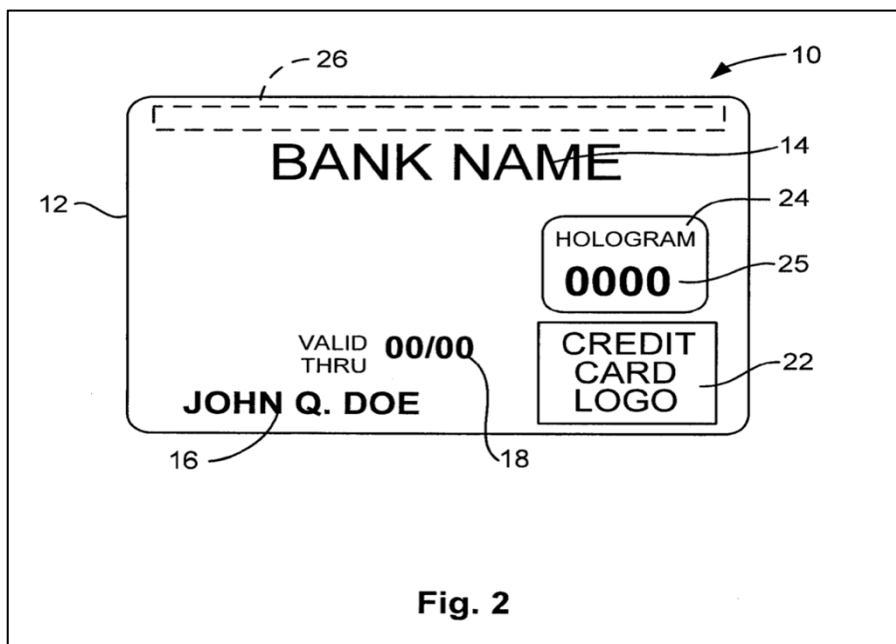
106. *Kranzley* is analogous art to the ’286 Patent because it is from the same field of endeavor. Like the ’286 Patent, *Kranzley* is concerned with conducting secure payment transactions. *See, e.g., Kranzley* at Abstract (“Systems, methods processes, computer program code and means for conducting 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 ’286 Patent (Ex. 1001)*, Abstract, 1:31-35, Fig. 1 with *Kranzley (Ex. 1013)*, Abstract, [0010], Fig. 1.

107. *Kranzley* is also reasonably pertinent to at least one problem addressed by the ’286 Patent. Like the ’286 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 '286 Patent (Ex. 1001), 1:31-35, 2:4-12, 9:63-10:2 with Kranzley (Ex. 1013), [0003], [0065].*

J. Eng

108. Eng teaches a card that has the following fixed payment information: (1) *a card-holder name*, (2) bank name (*a payment issuing logo*) among other items. *See Eng (Ex. 1014), [0020]-[0021].*



Eng (Ex. 1014), Fig. 2.

1. Eng is Analogous

109. Eng is analogous art to the '286 Patent because it is from the same field of endeavor. Like the '286 Patent, Eng is concerned with conducting secure payment transactions. *See, e.g., Eng (Ex. 1014), [0023]* (“cards containing only partial credit card account information herein provides added security.”); *[0024]* (“the partial account information appearing on the credit card is plainly visible and can be compared by a merchant to an authorization receipt or document.”); Abstract (“systems and methods for protecting information related to credit card accounts and other kinds of information displayed on personal and identification cards.”). *Compare '286 Patent (Ex. 1001), Abstract, 1:31-35, Fig. 1 with Eng (Ex. 1014), Abstract, [0024]-[0024], Fig. 2.*

110. Eng is also reasonably pertinent to at least one problem addressed by the '286 Patent. Like the '286 Patent, Eng is concerned with increasing security of payment transactions. *See, e.g., Eng (Ex. 1014)*, [0023] (“cards containing only partial credit card account information herein provides added security.”), Abstract (“systems and methods for protecting information related to credit card accounts and other kinds of information displayed on personal and identification cards.”); *compare '286 Patent (Ex. 1001)*, 1:31-35, 2:4-12, 9:63-10:2 *with Eng (Ex. 1014)*, Abstract, [0023], Fig. 2.

K. Chin

111. Chin discloses “gesture based authentication for wireless payment by a mobile electronic device.” *Chin (Ex. 1015)*, [0008]. Specifically, Chin teaches accepting a gesture on “the touch receptive input area (e.g., a touchscreen)” and “comparing the applied gesture” with a user-defined payment gesture stored locally within the device, which may be a “mobile electronic device equipped with NFC payment capabilities.” *Chin (Ex. 1015)*, [0009]. If the gesture input by the user “matches the user-defined payment gesture stored locally within the target device, the method may include permitting the wireless transmission (e.g., using NFC technology) of protected payment data resident on the target device to an

initiator device (e.g., an NFC reader, a contactless smart card reader based on RFID technology, an NFC scanner, etc.).” *Chin (Ex. 1015)*, [0009].

1. Chin is Analogous

112. Chin is analogous art to the '286 Patent because it is from the same field of endeavor. Like the '286 Patent, Chin is concerned with conducting secure payment transactions. *See, e.g., Chin (Ex. 1015)*, [0009] (“the method may include permitting the wireless transmission (e.g., using NFC technology) of protected payment data resident on the target device to an initiator device (e.g., an NFC reader, a contactless smart card reader based on RFID technology, an NFC scanner, etc.). However, if the applied gesture on the touch receptive input area of the target device does not match the user-defined payment gesture stored locally within the target device, the method may include denying the wireless transmission of the protected payment data resident on the target device to the initiator device.”). *Compare '286 Patent (Ex. 1001)*, Abstract, 1:31-35, Fig. 1 *with Chin (Ex. 1015)*, [0009], [0030].

113. Chin is also reasonably pertinent to at least one problem addressed by the '286 Patent. Like the '286 Patent, Chin is concerned with increasing security of payment transactions. *See, e.g., Chin (Ex. 1015)*, [0004] (“A potential problem with wireless transmission of payment information may be data security.”), [0005] (“A mobile electronic device may employ security measures to guard against

unauthorized access to or use of sensitive information stored within it”), [0007] “(What is needed is a security method enabling a user of an NFC-equipped mobile electronic device to quickly and conveniently authorize wireless transmission of protected payment information stored locally within the mobile device to an NFC-capable reader for touchless payment.”), [0054] (“prompt the user to enter the user-defined payment gesture **110** prior to enabling wireless transmission of a signal”); *compare* ’286 Patent (*Ex. 1001*), 1:31-35, 2:4-12, 9:63-10:2 with *Chin (Ex. 1015)*, [0054], [0004]-[0007].

L. Fisher

114. I understand Fisher teaches a “mobile communication device” with a “mobile wallet application that executes PayPass[.]” *Fisher (Ex. 1016)*, [0024]. When “a consumer (or user) is shopping online and they are ready to pay for their products, the consumer opens his mobile wallet and selects one of the payment methods (e.g., credit card, debit card, prepaid card, etc.) from their mobile wallet.” *Fisher (Ex. 1016)*, [0018]. The user “waves their phone over the NFC reader present on the PC 404.” *Fisher (Ex. 1016)*, [0018]. The user’s “payment credentials are transferred from the phone to the merchant website (e.g., online store application 410)” *Fisher (Ex. 1016)*, [0018].

1. Fisher is Analogous

115. Fisher is analogous art to the '286 Patent because it is from the same field of endeavor. Like the '286 Patent, Fisher is concerned with conducting secure payment transactions *See, e.g., Fisher (Ex. 1016)*, [0018] (“After the consumer enters any necessary validation information (e.g., pin) to provide a multi-factor authentication and confirms the transaction, the online purchase is processed as normal by the merchant's online processor.”), [0023] (“When it comes time to authorize the purchase, (in one implementation) the user is given an option to purchase with the mobile communication device 402.”); *compare '286 Patent (Ex. 1001)*, Abstract, 1:31-35, Fig. 1 *with Fisher (Ex. 1016)*, [0018], [0023]-[0025].

116. Fisher is also reasonably pertinent to at least one problem addressed by the '286 Patent. Like the '286 Patent, Fisher is concerned with increasing security of payment transactions. *See, e.g., Fisher (Ex. 1016)*, [0004] (“sending payment authorization for the total purchase amount from the point of sale device to a payment entity, in which the payment authorization is sent to the payment entity via a mobile communication device of the user. The method further includes receiving a result of the payment authorization from the payment entity through the mobile communication device; and completing the payment transaction based on the result of the payment authorization.”), [0005] (“The payment authorization can be an authorization for payment with a credit card, a debit card, or a prepaid card.”);

compare '286 Patent (Ex. 1001), 1:31-35, 2:4-12, 9:63-10:2 with Fisher (Ex. 1016), [0003]-[0006].

M. Hammad

117. Hammad generally teaches methods and system for generating verification values on a portable consumer device for use in payment transaction. *Hammad (Ex. 1017), 2:10-20, 2:65-3:11.* The dynamically generated verification values, which are embedded in payment data sent to a service provider, are generated using two or more dynamic data elements and static data elements. *Id.*, 4:21-6:42.

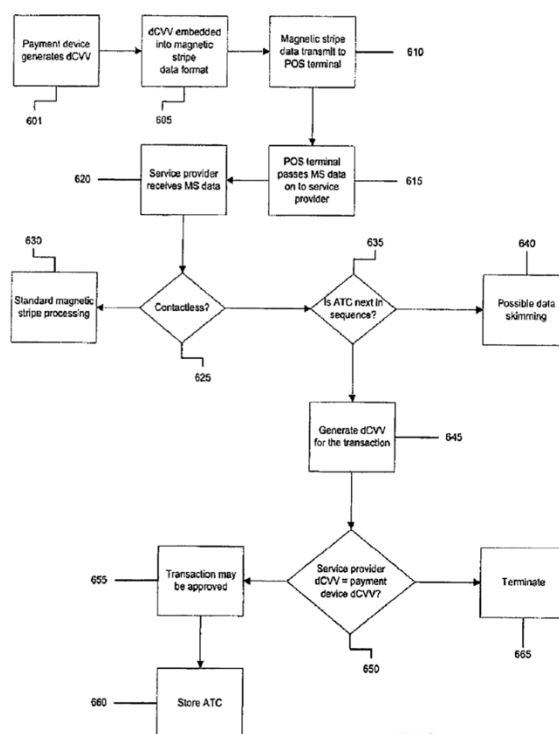


FIG. 6

Hammad (Ex. 1017), Fig. 6.

1. Hammad is Analogous

118. Hammad is analogous art to the '286 Patent because it is from the same field of endeavor. Like the '286 Patent, Hammad is concerned with increasing security of payment transactions. *See, e.g., Hammad (Ex. 1017)*, Abstract (“The method includes generating a verification value in response to a transaction involving a portable consumer device, where the verification value is generated using a first dynamic data element and a second dynamic data element. The verification value is sent to a service provider associated with the portable consumer device so that the service provider can verify the transaction.”); *compare '286 Patent (Ex. 1001)*, Abstract, 1:31-35, Fig. 1 *with Hammad (Ex. 1017)*, Abstract, 2:12-20, Fig. 6.

119. Hammad is also reasonably pertinent to at least one problem addressed by the '286 Patent. Like the '286 Patent, Hammad is concerned with increasing security of payment transactions. *See, e.g., Hammad (Ex. 1017)*, 1:20-23 (“One of the primary sources of fraud, which is prevalent in the credit card industry is skimming. Skimming refers to the electronic copying of a card's magnetic stripe data to create counterfeit cards.”), 1:45-65 (“To address the above problems, a dCVV or a dynamic card verification value can be used. The dCVV can be generated using an algorithm which uses at least a counter and input data such as an account number,

expiration date, and other information. The counter can increase by one each time a transaction is conducted. The dCVV can be independently generated by either a portable consumer device or POS terminal at the front end of a transaction and can be sent to a back end computer. The counter may be sent from the merchant to the back end computer so that it knows the current counter value associated with the portable consumer device. In other cases, the counter may simply be present at the back end computer. In the latter case, the counter increments every time the back end computer sees a transaction. The back end computer, using a similar algorithm to the one that generated the dCVV at the front end, the counter value, and input data, can independently generate a second dCVV. If the received dCVV and the generated dCVV match, the transaction can be considered authentic. If the dCVVs do not match, this may indicate that the transaction is fraudulent.”); *compare* ’286 *Patent* (Ex. 1001), 1:31-35, 2:4-12, 9:63-10:2 with *Hammad* (Ex. 1017), 1:20-23; 1:45-65.

IX. SUMMARY OF UNPATENTABILITY

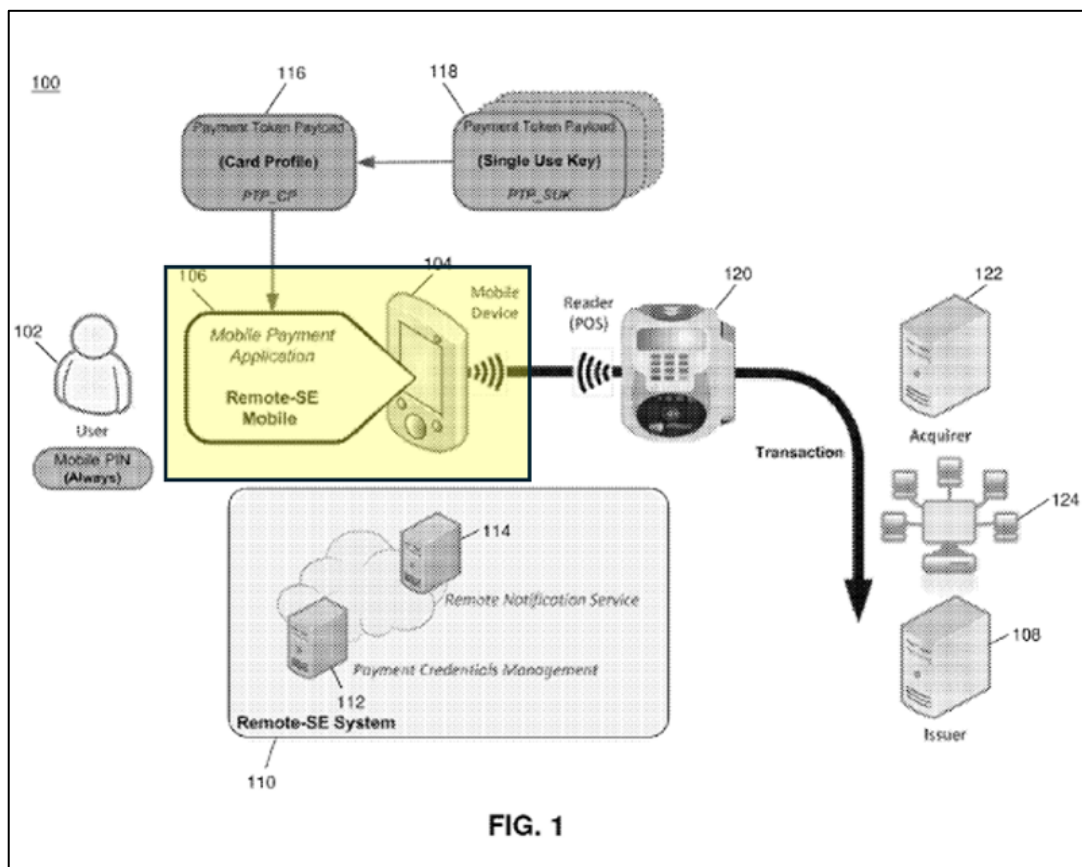
120. I have reproduced the Proposed Grounds of Unpatentability from the Petition for ease of reference:

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

X. OPINIONS REGARDING GROUND 1: CLAIMS 15 AND 17-18 ARE OBVIOUS OVER COLLINGE AND BONA.

A. Claim 15(Pre): A payment system comprising:

121. Collinge teaches a payment system.² Collinge teaches “generating and provisioning payment credentials to a mobile device” for “use in mobile payment transactions.” *Collinge* (Ex. 1004), [0005]-[0006], [0039]. An exemplary embodiment of Collinge’s payment system is shown in Fig. 1 below.



² I emphasize the claim language throughout with italics and underline for clarity.

Collinge (Ex. 1004), Fig. 1 (annotated).

122. The payment credentials provisioned to Collinge’s mobile device in Collinge’s payment system are used by the mobile device to generate a payment cryptogram which is then used “in conducting a near field financial transaction” at a point-of-sale terminal. *Collinge (Ex. 1004)*, Abstract, [0002]. For these reasons, Collinge teaches a payment system.

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

1. Patentable Weight

123. The limitation “free of any fixed payment numbers visible thereon” is directed to printed matter which I understand has no patentable weight if it has no functional or structural relationship to the claimed card device.

124. A POSITA would have understood that, at the time, it was common for a payment card (such as a credit or debit card) to have fixed payment numbers such as a PAN (primary account number), expiration date, and CVC numbers as shown in the image below in an article titled “MasterCard *PayPass*TM in Action” (“PayPass”):

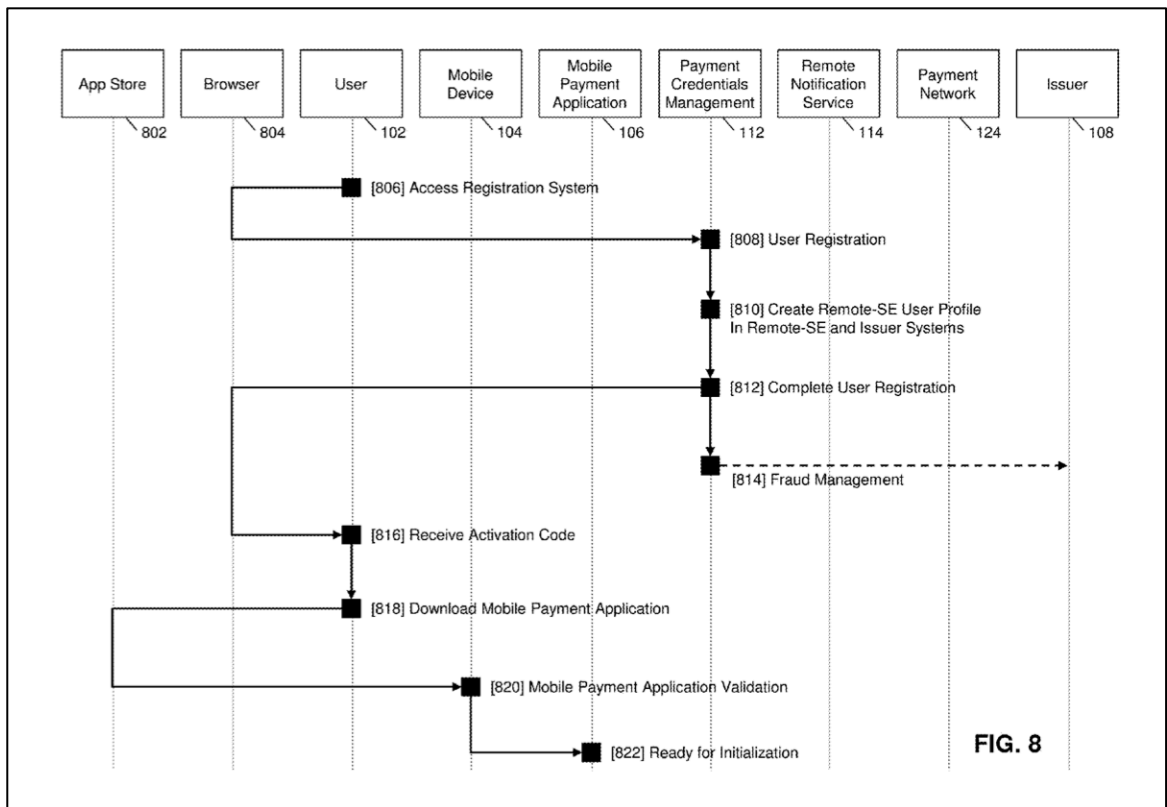


PayPass (Ex. 1025), 1.

125. The PAN, expiration date, and CVC/CVV shown on the face(s) of a traditional payment card are useful to the card-holder because they provide the card-holder with information that may be used to make payments online, by mail, over the phone, or in other circumstances where card-reader equipment such as a magnetic stripe reader or smart card reader is unavailable. In such cases for online, by mail, or over the phone payments, the medium that the payment information is provided on—for example, the plastic of the payment card itself—is irrelevant to conducting the payment transaction. The plastic card is merely how the payment information is stored for later reference by the user. I was asked to consider whether a POSITA at the time of the '286 Patent would have understood the PAN, expiration date, CVC, and other payment information on the face of a common payment card to have a functional relationship with the material (e.g., plastic) of the payment card

itself. I was unable to identify any such functional relationship. The physical payment card simply serves as the medium on which the information is attached, the same way paper may serve as the medium when a payment card number is printed on a receipt.

126. I was also asked to consider whether the limitation “free of any fixed payment numbers visible thereon” has any relationship to any other element of the claims that might impact my opinion. I observed that Claim 1 also has the requirement: “wherein the computing device is operable to receive, store and transmit a card payment information not visible on the payment card device.” *See* Claim 1. It was well-known at the time that in order to use a mobile device to make payments, the device must first be provided with payment information, often through a registration process, such as the one Collinge teaches.



Collinge (Ex. 1004), Fig. 8. It is worth noting there are several ways for a user to provide payment information. Accordingly, the ability of a computing device to receive, store, and transmit card payment information is not functionally related to whether card payment information is visible on an associated payment card. None of the other limitations of the claims of the '286 Patent impact my opinion that payment numbers do not have a functional relationship to physical (e.g., plastic or metal) payment cards.

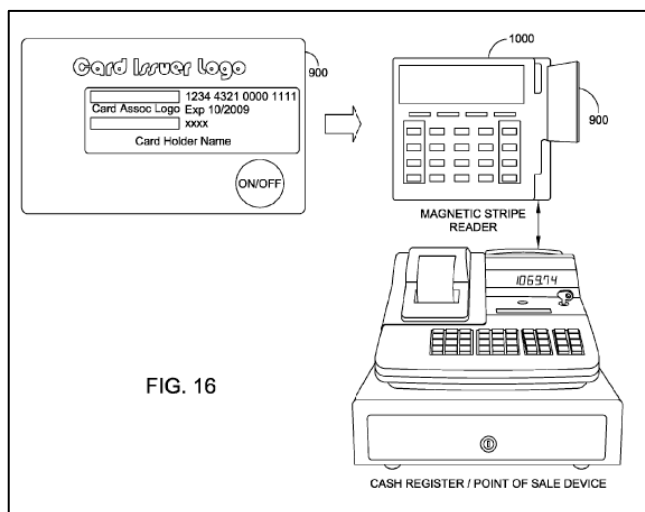
127. Nevertheless, a POSITA would have understood that the combination of *Collinge* and *Bona* renders this limitation obvious.

2. *Collinge's Teachings*

128. Collinge notes that a “payment card may be a physical card that may be provided to a merchant, or may be data representing the associated payment account (e.g., as stored in a communication device, such as a smart phone or computer).” *Collinge (Ex. 1004)*, [0038].

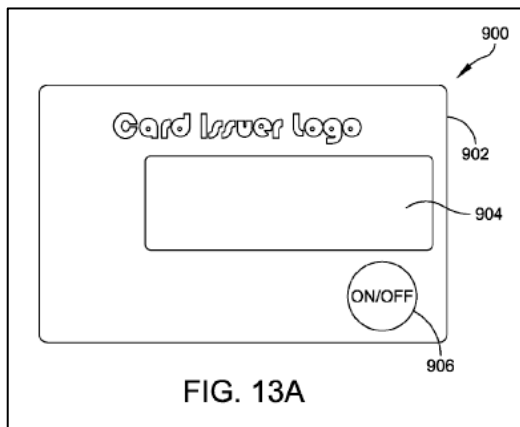
3. *Bona's Teachings*

129. Bona's NFC-enabled companion card 900 is a payment card device that is operable for use in payment card reader equipment. Bona's NFC-enabled companion card 900 “takes the shape of a standard plastic magnetic stripe card” and includes “display 204,” an “internal power source 212” a “smart card controller 216” and a “magnetic stripe emulator 214.” *Bona (Ex. 1009)*, [0045]-[0047], [0011]. Bona's companion card 900 is operable for use in payment card reader equipment, such as “a traditional magnetic stripe reader” *Bona (Ex. 1009)*, [0125].



Bona (Ex. 1009), Fig. 16.

130. Bona's payment card device is free of any fixed payment numbers visible thereon. *Bona (Ex. 1009), Fig. 13(a), [0108]*. When Bona's card is off, there is no information on the display of the payment card device as shown below in Figure 13A. *Bona (Ex. 1009), [0110]*. ("The smart card includes an on/off button 906 for powering the smart card on/off and a display 904 for displaying information to the user."). Because Bona's card shows no visible payment numbers when the device is off, it is free of any fixed payment numbers.

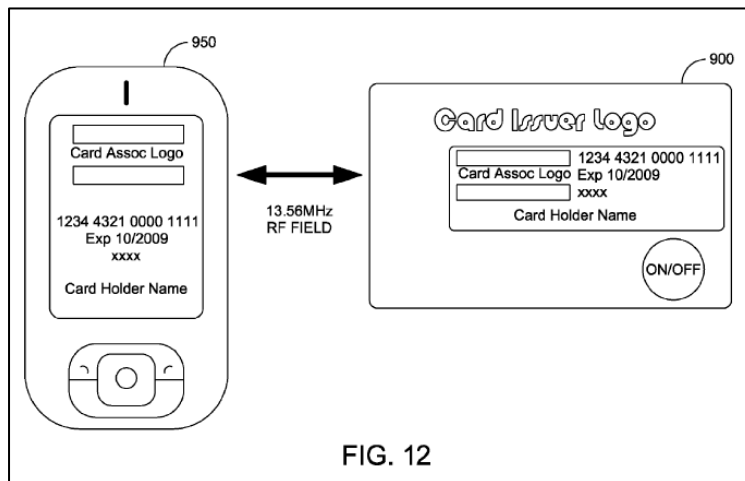


Bona (Ex. 1009), Fig. 13(a).

131. When Bona's companion card 900 is powered on, still it is free of any fixed payment numbers. Any payment numbers shown on Bona's screen are not fixed for at least three reasons.

132. **First**, Bona's companion card 900 may be provisioned with different payment numbers for use in different payment transactions. *Bona (Ex. 1009), [119]*.

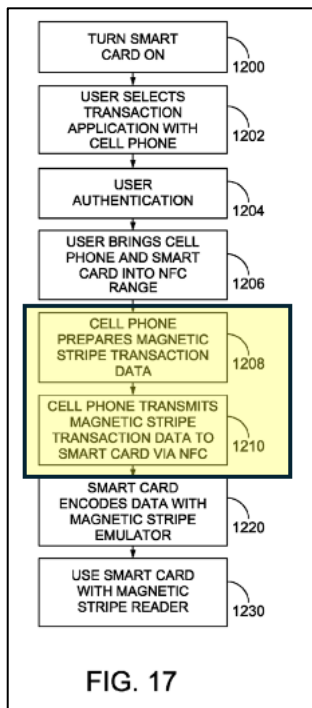
Accordingly, any provisioned payment numbers are not fixed. As shown in Fig. 12, Bona teaches that its NFC enabled companion card 900 may be used in connection with a cell phone 950 that “is configured for contactless transactions (e.g., contactless credit or debit transactions) using existing NFC techniques.” *Bona (Ex. 1009)*, [0108]-[0109], [0127]. Bona’s cell phone 950 “can be programmed with a mobile wallet application that allows the user to select from among the installed applications (credit, debit, others) and enable or activate one for use in the next transaction.” *Bona (Ex. 1009)*, [0119].



Bona (Ex. 1009), Fig. 12.

133. Bona teaches that when a user is ready to make a payment, the user turns on Bona’s companion card 900 and uses cell phone 950 to select from a “list of transaction applications (e.g., debit, VISA, Inc., MasterCard Inc., etc.) [.]” *Bona (Ex. 1009)*, [0119].

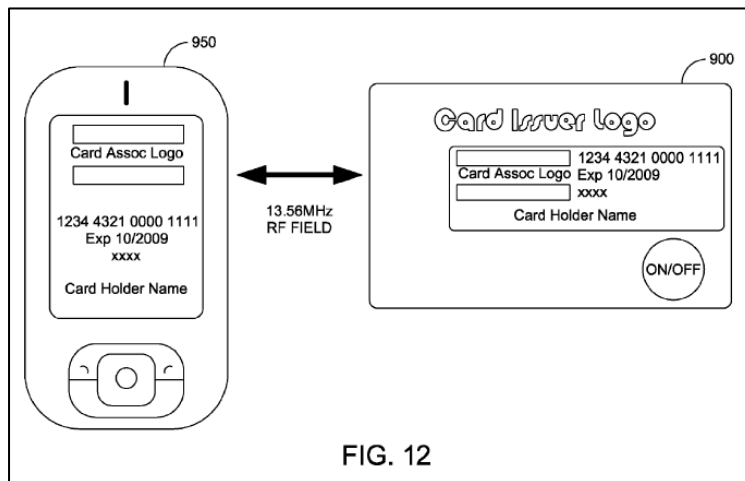
134. Once an application has been selected and the user is authenticated (*Bona (Ex. 1009)*, [0120]), and the user “brings the NFC enabled companion card 900 within NFC range of the cell phone 950 so that they can communicate with one another” in a “peer-to-peer session.” *Bona (Ex. 1009)*, [0121]. As shown in Fig. 17, once Bona’s companion card 900 and cell phone 950 are within NFC range of each other, Bona’s cell phone “prepares magnetic stripe transaction data for use by the NFC enabled companion card 900” and “transmits the magnetic stripe transaction data to the smart card using NFC communication instructions 972.” *Bona (Ex. 1009)*, [0122]-[0123].



Bona (Ex. 1009), Fig. 17 (annotated).

135. Once Bona's NFC enabled companion card receives the necessary magnetic stripe transaction data for a transaction and encodes the data, the user is notified that "the card is ready to use in a traditional magnetic stripe reader." *Bona* (Ex. 1009), [0125].

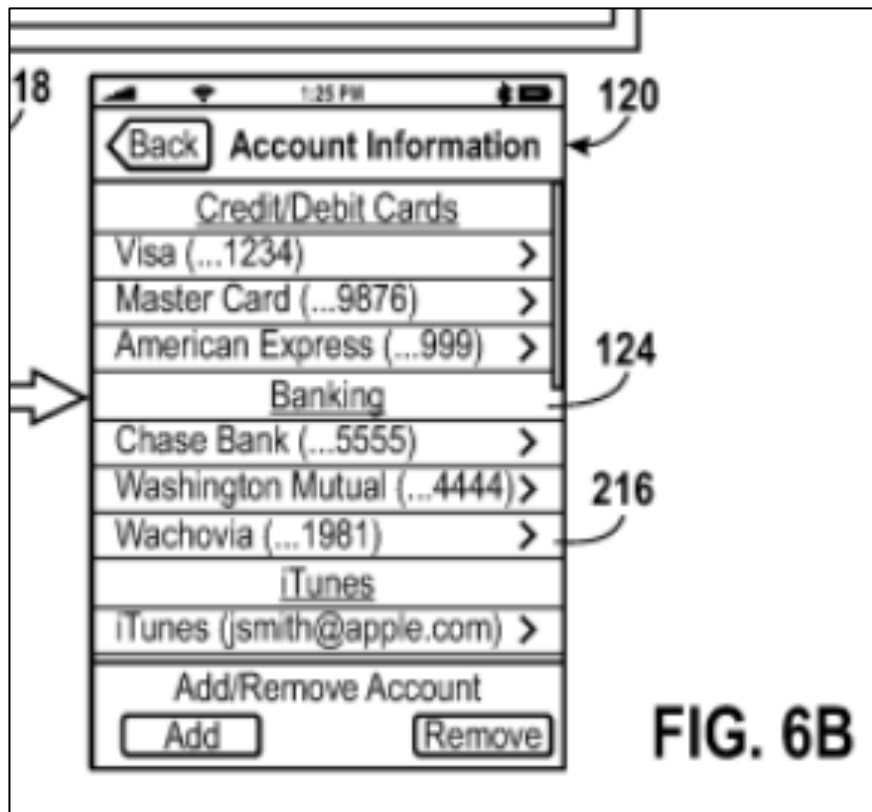
136. Bona teaches that "any necessary data for display on the NFC enabled companion card 900 for use in the transaction can also be transmitted." *Bona* (Ex. 1009), [0109]. As shown in Figure 12, the data displayed on Bona's NFC-enabled companion card may include payment numbers.



Bona (Ex. 1009), Fig. 12.

137. A POSITA at the time of the alleged information would have understood that the payment information associated with a VISA card would differ from the payment information associated with a MasterCard, as set forth in *ISO/IEC Standard 7811*. For example, the first digit of a credit card number is the Major Industry Identifier (MII), and each major credit card has its own number. *Id.*

MasterCard begins with a 5, Visa begins with a 4, and Discover Cards begin with a 6. *Id.* A POSITA would have understood that the payment information for VISA card and for MasterCard would remain different when payment information for both cards is loaded to a mobile wallet application. This concept was well known in the art. As an example as depicted in WO 2010/039337 to Lin. et. al. ("*Lin*"), a mobile wallet may include multiple credit/debit cards, each with its own associated payment number.

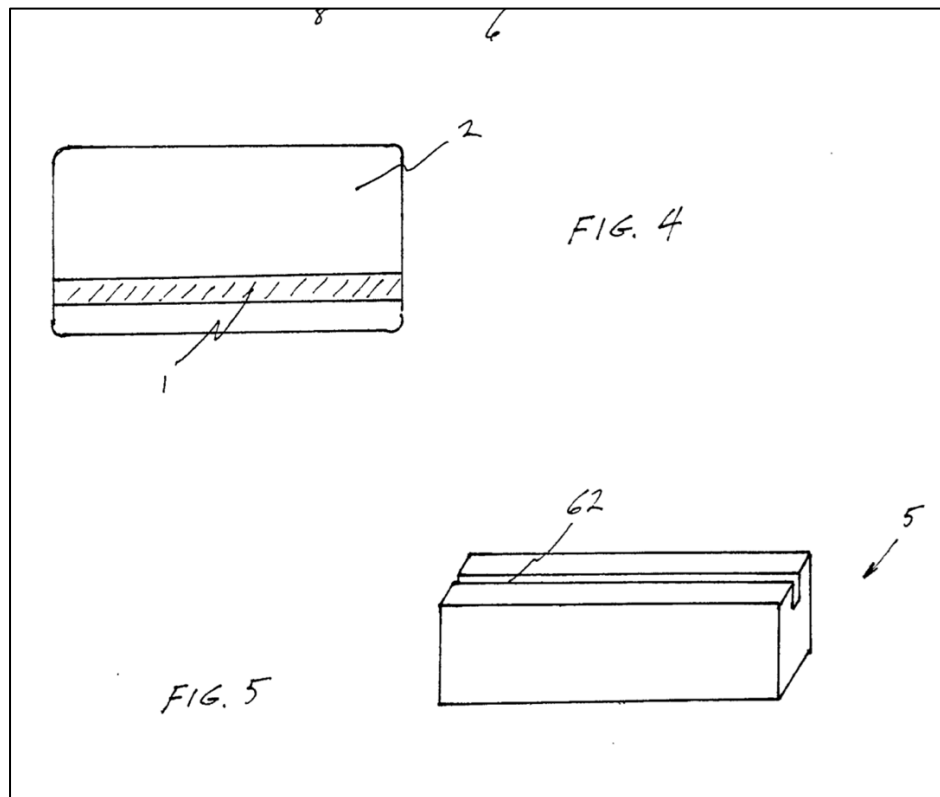


Lin (Ex. 1012), Fig. 6B. (excerpt).

138. Because Bona teaches that different payment numbers may be displayed on the NFC enabled companion card 900 associated with different credit or debit cards, any information displayed on companion card 900 is not fixed. Therefore, Bona's payment card is free of any fixed payment numbers.

139. **Second**, Bona teaches that any payment credentials provisioned to the companion card 900 are deleted completely "[a]fter a successful transaction, at a predetermined time limit or when the user presses the on-off button 906" so that "the NFC enabled companion card 900 retains no useful information related to the transaction." *Bona (Ex. 1009)*, [0126]. For this additional reason, Bona's payment card is free of any fixed payment numbers.

140. **Third**, a POSITA would have understood that payment information is not required to be shown on a payment card in order to perform a transaction via a magnetic stripe terminal at a POS reader. For example, WO 1994/017498 to Labaton et al. ("Labaton") describes a "blank credit card" that is for use in "Point of Sale (POS) transaction sites." *Labaton (Ex. 1035)*, 8:28-33; 5:2-21.



Labaton (Ex. 1035), Fig. 4-5. Bona teaches that “any **necessary data** for display on the NFC enabled companion card 900 **for use in the transaction** can also be transmitted.” *Bona (Ex. 1009)*, [0109]. A POSITA would have understood that because the point-of-sale reader reads and processes the magnetic stripe information in order to process the transaction, it often would not be necessary to display any data on the NFC enabled companion card 900 as shown by Labaton above. A POSITA would further have understood that the magnetic stripe terminal at the POS reader would not read any payment numbers (e.g., a PAN, expiration date) displayed on the face of the card, as a magnetic stripe reader does not read displayed data. Therefore, A POSITA would have understood that no payment information would

need to be shown on the face of Bona's card in order to perform a payment transaction, and for this additional reason, Bona's payment card is free of any fixed payment numbers.

4. *Motivation to Combine*

141. As discussed above, Collinge teaches a payment system including a mobile device provisioned with payment credentials and operable to conduct a near field payment transaction at a point of sale terminal. Bona teaches a NFC-enabled companion card 900 free of any fixed payment numbers visible thereon that includes a magnetic stripe emulator and is operable for use in a payment card reader equipment including a traditional magnetic stripe reader. Thus, Collinge modified by Bona teaches a payment system including a payment card device that is (1) free of any fixed payment numbers visible thereon and (2) operable for use in payment card reader equipment. A POSITA would have found it obvious and would have been motivated to use Bona's payment card device free of any fixed payment numbers visible thereon and operable for use in payment card reader equipment with Collinge's NFC-enabled computing device (i.e. cell phone) and payment system.

142. It was well-known that many point-of-sale terminals only accepted a physical magstripe payment method. A POSITA would have understood, and Bona expressly recognizes, that at the time "the predominate point of sale reader

technology deployed worldwide” continued to be “magnetic stripe.” *Bona (Ex. 1009)*, [0008]. Bona estimated that there were “20,000,000 magnetic stripe readers in the field.” *Bona (Ex. 1009)*, [0036], [0080]. A 2013 study by the Federal Reserve confirmed the prevalence of magnetic stripe transactions, estimating that only 74 out of every 100,000 card-present credit card transactions were initiated with a chip while the remainder were initiated with a traditional swipe of a magnetic stripe. *Study Summary (Ex. 1036)*, 17. A POSITA would have understood that at the time of the alleged invention, there were tens of millions of magnetic stripe readers in use and magnetic stripe technology continued to be the “predominate point of sale reader technology deployed worldwide.” *Bona (Ex. 1009)*, [0008], [0036], [0080].

143. Further, at the time it was well-known that many point-of-sale terminals still **only** accepted a physical magstripe payment method. The same 2013 Federal Reserve study noted that chip cards and chip terminals were “not widely adopted” though their availability was “growing.” *Study (Ex. 1037)*, 63 n.46. Notably, in a further survey reported in December 2015, it was reported that three-quarters of the major retailers surveyed had installed checkout terminals able to read smart cards, but had not yet enabled the terminals to accept chip payments, meaning swipers were still required to swipe their card’s magnetic strip to make a payment. *ConsumerWorld Survey (Ex. 1038)*. A POSITA therefore would have been

motivated to modify Collinge's payment system to take advantage of Collinge's more secure payment system while also having the flexibility to make payments on point-of-sale terminals that only accepted magstripe transactions.

144. A POSITA would have understood that, as expressly recognized by Bona, "existing contactless transaction enabled cell phones cannot be used for magnetic stripe transactions, which is the dominant technology presently in use." *Bona (Ex. 1009)*, [0109]. A POSITA would have understood that Collinge's mobile phone does not have a physical magstripe that is able to be swiped in a reader, and therefore Collinge's mobile phone would not be suitable for performing magnetic stripe transactions where only a physical reader is available. A POSITA would have understood that providing the user with both payment options would expand the number of POS terminals where Collinge's payment credentials could be used, and provide the user with additional payment options if an NFC-enabled point-of-sale terminal was broken, not enabled, or not present.

145. A POSITA would have recognized that given the state of point-of-sale terminals at the time, a user would have found it valuable to have access to a variety of methods for completing a payment transaction. Bona expressly teaches that it is valuable when, in addition to Bona's companion card 900, the user's cell phone "can also be used in conventional contactless smart card transactions." *Bona (Ex. 1009)*,

[0127]. In addition, a user of Collinge's payment system would have benefited from having back-up payment options in the event that point-of-sale equipment (such as an NFC-enabled point of sale terminal) was broken, mobile payment features of the terminal were not enabled by the merchant, or a merchant was only able to accept magnetic stripe payments. A POSITA would have been motivated to combine Collinge with Bona to allow the flexibility to make contactless payments using Collinge's payment application on Collinge's cell phone, and also make payments at point-of-sale terminals that still only accepted a physical swipe of a magstripe card, as expressly taught by Bona. *Bona (Ex. 1009)*, [0127].

146. A POSITA would have had a reasonable expectation of success in making the proposed combination. Collinge and Bona describe compatible payment systems. Both Bona and Collinge discuss compliance with ISO/IEC 7813, an industry standard which a POSITA would have been familiar with. *Bona (Ex. 1009)*, [0102] ("magnetic stripe credit card transactions defined in ISO/IEC 7813"); '095 *Provisional (Ex. 1005)*, [0064] ("Track 2 Data (DE 35) comprises information encoded on track 2 of a payment card's magnetic stripe as defined in ISO 7813" and "Track 1 Data (DE 45) includes information encoded on track 1 of a bankcard's magnetic stripe as defined in ISO 7813."). ISO/IEC 7813 is an international standard

that defines the structure and content of magnetic tracks 1 and 2 on financial transaction cards. *See MagTek (Ex. 1022).*

147. Bona teaches that 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. 1009), [0102].

148. Collinge teaches that:

“authorization request 168 includes DExx CVC3 track data 610 to facilitate payment between the POS terminal 181 and the acquirer 166 or a bank. In an embodiment, the track data DExx CVC3 610 can be DE35/DE45 (CVC3) track 2 or track 1 data. According to an embodiment Track 2 Data (DE 35) comprises information encoded on track 2 of a payment card's magnetic stripe as defined in ISO 7813, including field separators, but excludes beginning and ending sentinels and Longitudinal Redundancy Check (LRC) characters. In an embodiment, Track 1 Data (DE 45) includes information encoded on track 1 of a bankcard's magnetic stripe as defined in ISO 7813, including field separators.”

'095 Provisional (Ex. 1005), [0064].

149. A POSITA would have had a reasonable expectation of success in combining Bona's companion card 900 with Collinge's payment system because Collinge's payment system already teaches including "magnetic stripe (mag stripe) payment credentials 204" in the card profile provisioned to the mobile device. *Collinge (Ex. 1004), [0048], [0049].* Collinge's mobile device is likewise operable to transmit magnetic track data (e.g., track 1, track 2 data compliant with ISO/IEC 7813) via NFC (*'095 Provisional (Ex. 1005), [0064]*) and Bona's companion card 900 is already operable to receive magnetic strip transaction data via NFC in a data format compliant with ISO/IEC 7813. *Bona (Ex. 1009), [0102].*

150. A POSITA would have had a reasonable expectation of success in combining Bona's NFC-enabled companion card with Collinge's payment system as a combination of known elements that would yield predictable results. Bona already teaches being able to receive, from a cell phone, via an NFC interface, "transaction data preferably include any necessary static secured data for performing the transaction as well as dynamic card verification data for use in authorizing the transaction." *Bona (Ex. 1009), [0109].* Bona further teaches that:

"card controller 216 controls the magnetic stripe emulator 214 for transmitting secure transaction data during a transaction, e.g., a credit card swipe transaction. Importantly, this data includes not only standard secured

data, such as the static transaction data called for by governing specifications (e.g., account holder name, account number, etc.) but also dynamic information. Using this dynamic information in authorizing transactions prevents fraudulent transactions since the static information alone cannot be used to perform a transaction.”

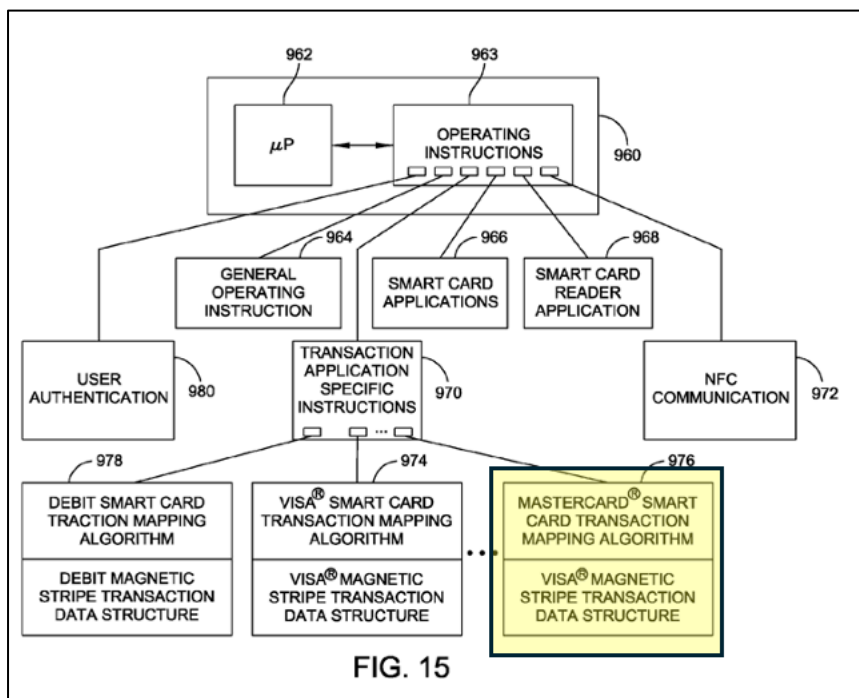
Bona (Ex. 1009), [0053].

151. Notably Collinge already teaches that Collinge’s mobile device is able to send payment credentials and dynamic data (payment cryptogram) via Collinge’s NFC interface. “The mobile payment application 106 may generate a payment cryptogram, discussed in more detail below, and may transmit the generated cryptogram and payment credentials to a point-of-sale terminal 120.” *Collinge (Ex. 1004)*, [0070].

152. A POSITA would have appreciated that modifying Collinge to send payment credentials and dynamic data (such as a payment cryptogram) to Bona’s payment card would not change the functionality of Bona and Collinge. This combination of Collinge and Bona would have allowed a POSITA to take advantage of the security features of Collinge’s payment system at point-of-sale locations having only a traditional magnetic stripe reader, such as Collinge’s single-use cryptogram. A POSITA would have understood that providing the user with the option to pay via Collinge’s mobile device 104 and Bona’s companion card would

have advantageously expanded the number of point-of-sale terminals where Collinge's payment credentials could be used.

153. A POSITA would have had a reasonable expectation of success in combining Bona's NFC-enabled companion card with Collinge's payment system which would have been a combination of known elements to yield predictable results. Bona teaches that its NFC enabled companion card 900 communicates with Bona's cell phone 950 using NFC communications. *Bona (Ex. 1009)*, [0109]. Collinge's mobile device 104 is already operable to communicate via near field communications (*Collinge (Ex. 1004)*, [0046]), and therefore already has the hardware necessary to communicate with Bona's companion card 900. In the resulting combination, Collinge transmits necessary transaction information (such as Collinge's dynamically generated single-use CVC3 and payment credentials) via NFC to Bona's companion card 900. Then the companion card 900's magnetic stripe emulator encodes the received transaction information in its magnetic field, as taught by Bona. *Bona (Ex. 1009)*, [0124]. Bona's companion card 900 would then be ready for use with a standard magnetic stripe reader. *Bona (Ex. 1009)*, [0125]. Bona already teaches being compatible with Mastercard data. *Bona (Ex. 1009)*, Fig. 15.



Bona (Ex. 1009), Fig. 15.

154. For these reasons, a POSITA would have been motivated to include Bona’s companion card 900 in Collinge’s payment system to yield the predictable result of a payment system including a payment card device free of any fixed payment numbers visible thereon and...operable for use in payment card reader equipment. Both Bona and Collinge are directed towards improved payment systems that reduce the risk of fraudulent transactions.

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

D. 15(b)(1): a processor:

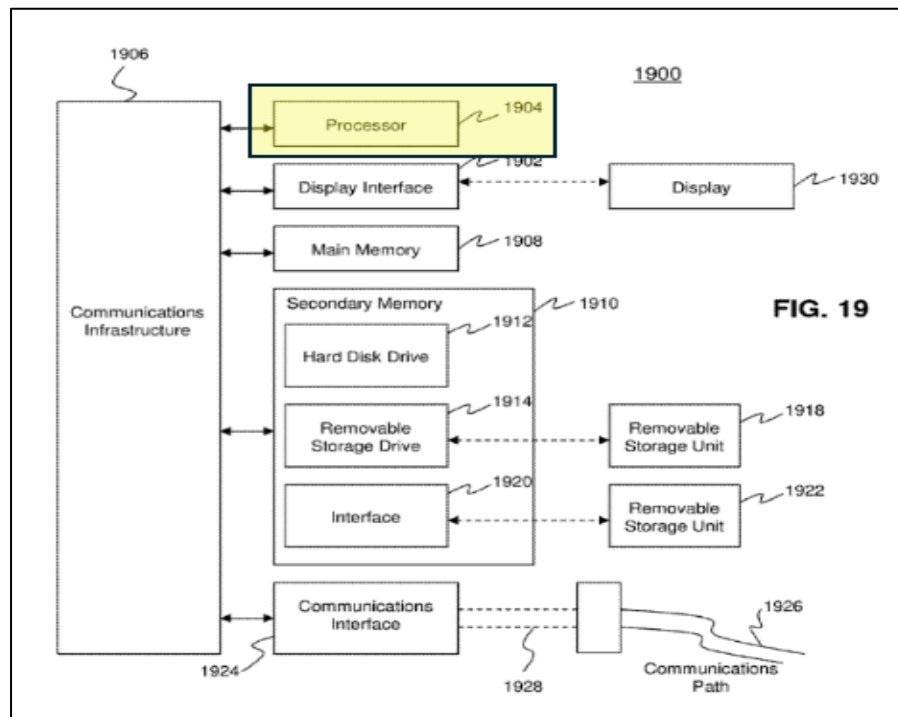
155. Collinge teaches a personal computing device (“mobile device”) that includes a processor. Collinge (Ex. 1004), [0042] (“The user 102 may desire to use

their mobile device 104 to conduct payment transactions”) (emphasis added).

Collinge specifically teaches “an application program stored in data storage of the mobile device” that is “executed by a processor included in the mobile device[.]”

Collinge (Ex. 1004), [0041]. Collinge also teaches that “at least one processor device and a memory may be used to implement the above described embodiments[.]”

Collinge (Ex. 1004), [0147].



Collinge (Ex. 1004), Fig. 19 (annotated). A POSITA would have understood Collinge’s mobile device comprises a processor. A POSITA would have understood Collinge’s mobile device in view of Bona’s teachings to teach a card-users personal computing device. See *Bona (Ex. 1009)*, [0117]-[0127] (describing the user cell

phone associated with Bona's companion card as accepting authentication from the user).

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

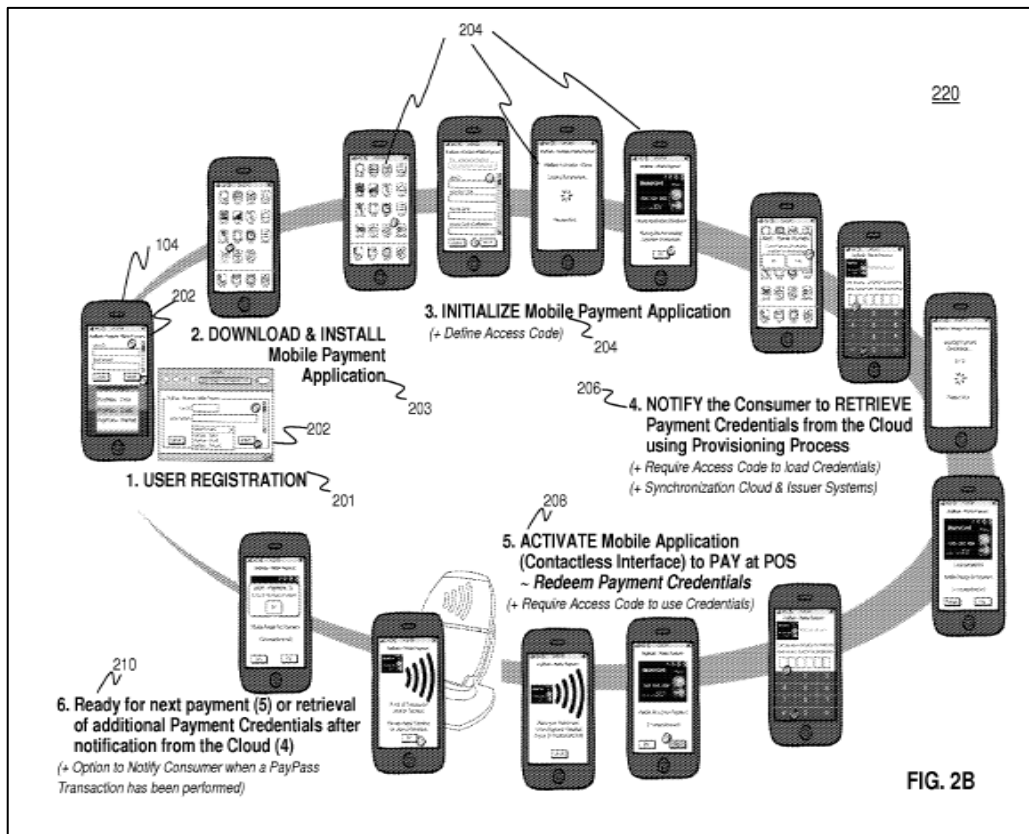
156. Collinge's mobile device includes a touch-screen user display interface. Collinge teaches that "a touch screen" is an "input device" of "the mobile device 104" *Collinge (Ex. 1004)*, [0133].

157. Collinge also teaches that the touch screen of the mobile device 104 provides a visual user-interface for user payment interactions. Collinge teaches that touch screen receives a user's input of a "mobile personal identification number (PIN)" prior to generation of a payment cryptogram. *Collinge (Ex. 1004)*, [0133].

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

159. Collinge's '248 *Provisional* application (which I understand is incorporated by reference into Collinge) provides further examples of user

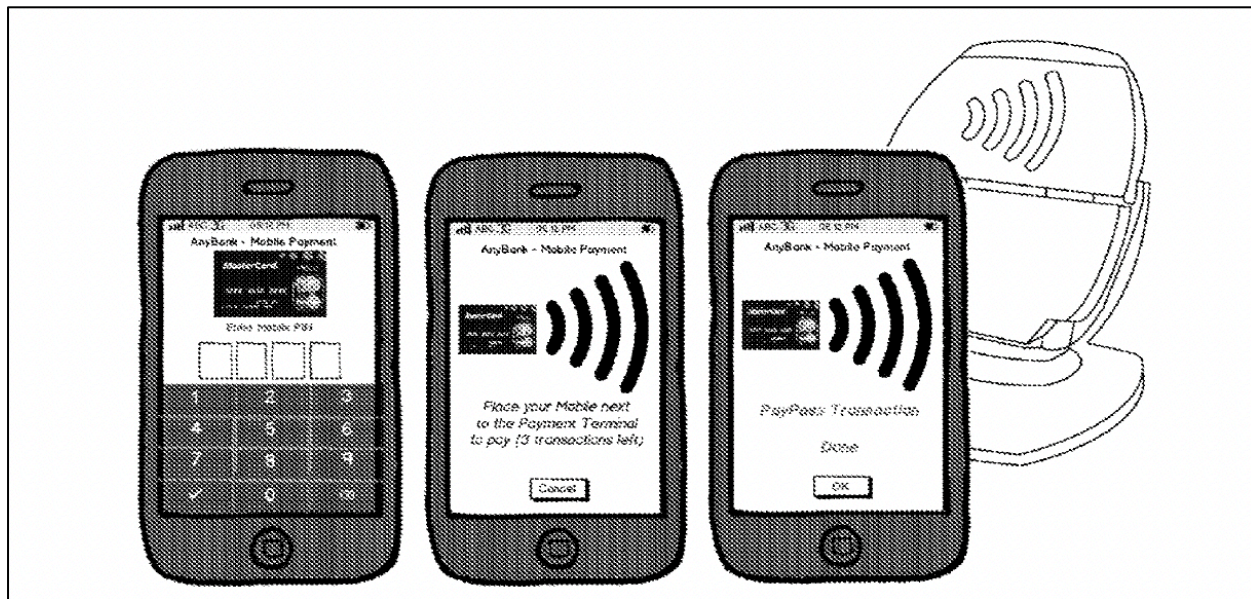
interaction with the touch screen during the user registration and payment process. In the below image, Collinge teaches that the user interacts with the user-interface on the touch screen of the device to download and install the mobile payment application, input access codes (e.g., PIN numbers), make selections, and receive status information throughout the transaction.



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

160. As shown below, Collinge teaches that the user interface may direct the user to input a PIN, direct the user to place the mobile device near a payment

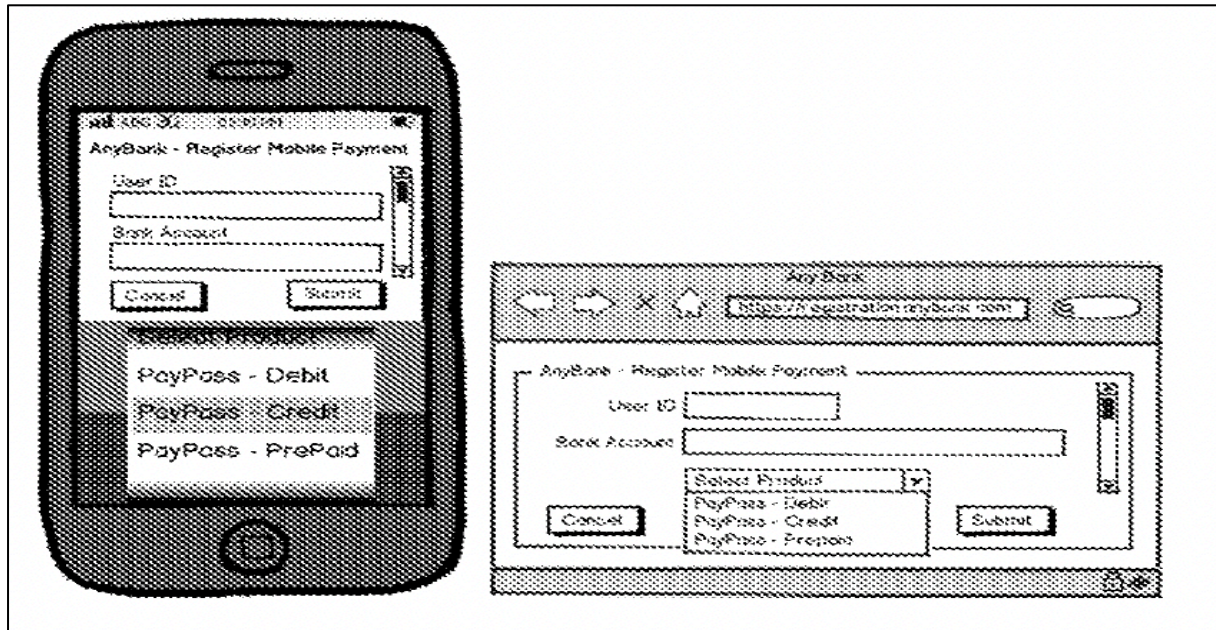
terminal, and provide an indication to the user when the payment transaction is complete. '098 Provisional (Ex. 1008), 99.



'098 Provisional (Ex. 1008), 99. Collinge further teaches that that registration process steps can also “be accomplished using input supplied by a cardholder or user” “via a GUI” of the mobile device 104. '098 Provisional (Ex. 1008), [0063]. A POSITA would understand that all of the interactions depicted above during Collinge’s registration and payment process are user payment interactions. In each instance, the user interacts with the visual user-interface on the touch screen of Collinge’s mobile device 104 which displays information relating to Collinge’s system for making payments using mobile device 104.

161. Collinge’s registration process steps can likewise “be accomplished using input supplied by a cardholder or user” “via a GUI” of the mobile device 104.

Id., [0063]. Collinge's user-interface is also operable for a user selection, of at least one of issuer-provided payment methods via the touch-screen display interface.



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

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

162. See Claim 15(b)(2).

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

163. Collinge's mobile device includes a wireless interface (NFC interface).

Collinge's mobile device can "conduct payment transactions via near field communication[.]" *Collinge* (Ex. 1004), [0041]. Collinge repeatedly recognizes that a POSITA would have been familiar with methods for performing contactless payments via NFC technology. *Collinge* (Ex. 1004), [0044] ("Suitable methods and protocols for the secure transmission of information via NFC will be apparent to

persons having skill in the relevant art.”). [0070] (“Methods for transmitting payment credentials and a payment cryptogram to a point-of-sale terminal 120 via NFC will be apparent to persons having skill in the relevant art.”); [0120] (“Methods for executing transmission of payment credentials from a mobile device to a point-of-sale terminal will be apparent to persons having skill in the relevant art.”).

164. 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.*

165. 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 (Ex. 1004)*, [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 (Ex. 1012)*, 19: 26-27.

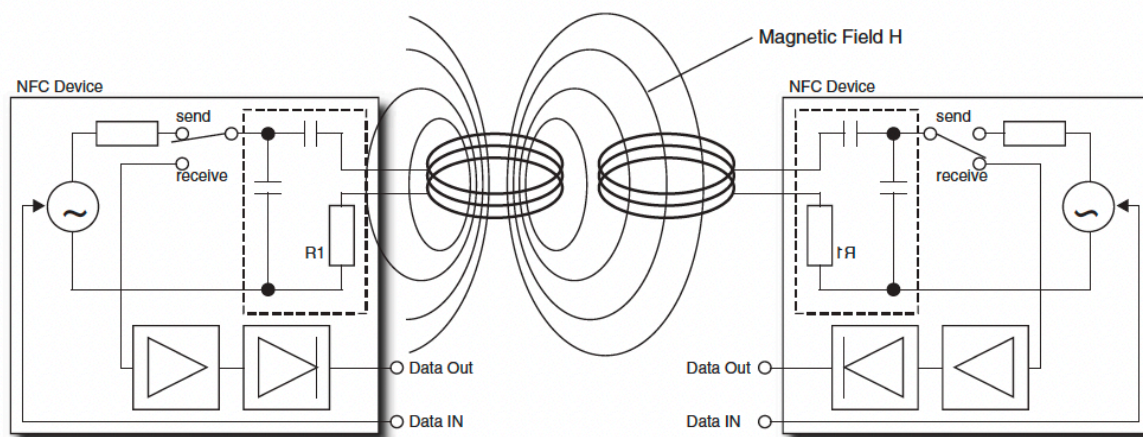
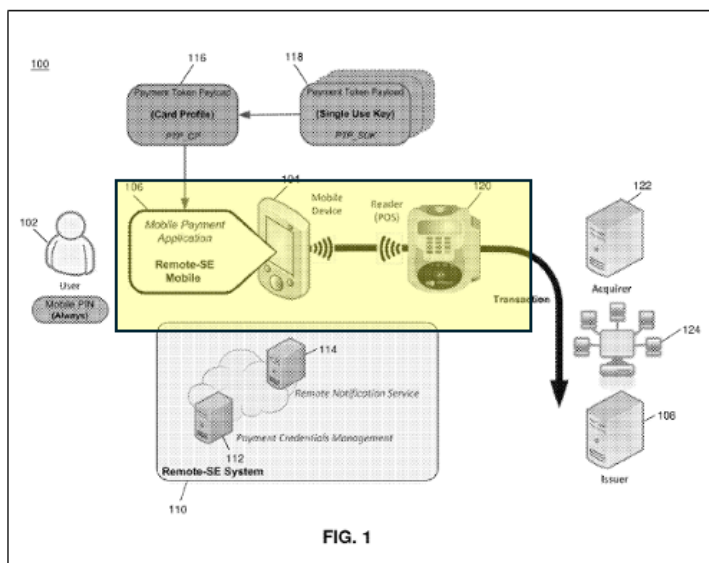


Figure 3.32 In active mode, the NFC interfaces alternately emit magnetic fields for data transmission

Finkenzeller (Ex. 1024), 58.

166. Collinge teaches an NFC interface, as shown in Fig. 1 below. In addition, a POSITA would recognize that an NFC interface is necessarily present in

Collinge's mobile device 104 because an NFC interface is required to “conduct payment transactions via near field communication[.]” *Collinge (Ex. 1004)*, [0041]; '248 *Provisional (Ex. 1005)*, [0067] (**NFC interface of the mobile device 104...**”), [0184]; Accordingly, a POSITA would have understood that Collinge teaches that mobile device 104 has an NFC interface that allows it to communicate with other NFC-enabled devices.



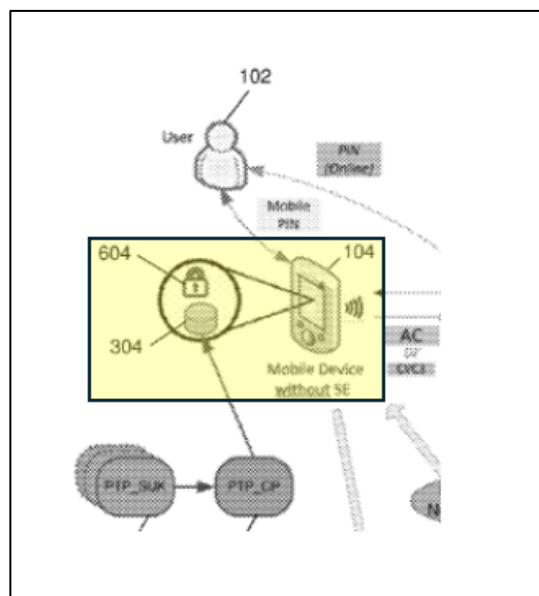
Collinge (Ex. 1004), Fig. 1 (annotated excerpt).

167. 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.

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

168. Collinge’s mobile device includes a memory for storing a payment information accessible to the processor. Collinge teaches “an application program stored in **data storage** of the mobile device[.]” *Collinge (Ex. 1004)*, [0041] (emphasis added). Collinge likewise teaches that its mobile device includes **storage 304**, which may include a “**local encrypted database.**” *Collinge (Ex. 1004)*, [0067] (emphasis added) (“The mobile payment application 106 may also generate the local storage encryption key and encrypt the storage 304 to create the local encrypted database”), [0119] (describing retrieval of information stored in “encrypted local storage 304”).



Collinge (Ex. 1004), Fig. 1 (annotated excerpt); *see also Collinge (Ex. 1004)*, [0147] (“at least one processor device and **a memory** may be used to implement the above-described embodiments”) (emphasis added). 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 (Ex. 1004)*, [0043], [0143], [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.”); *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).

169. Collinge’s “card profile” including payment credentials is stored in storage 304. *Collinge (Ex. 1004)*, [0063] (“The storage 304 may then store the shared mobile key, received payment credentials, and any additional information in the mobile device 104 to prevent unauthorized access.”).

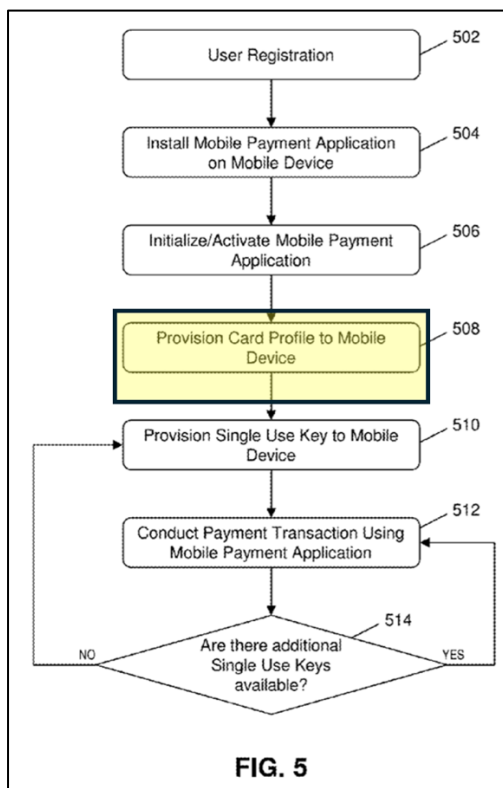
170. Collinge’s mobile device includes “an application program stored in data storage of the mobile device” that is “executed by a processor included in the mobile device[.]” *Collinge (Ex. 1004)*, [0041]. A POSITA would have

understood that Collinge therefore teaches a computing device comprising a memory.

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

171. Collinge's mobile device (computing device) has a processor operable to dynamically generate at least a portion of a limited-use card payment information (payment cryptogram) for use by an authenticated card user (user authenticated by a successfully entered PIN or passcode). Collinge's mobile device includes a mobile payment application that is "stored in data storage of the mobile device 104 and executed by a processor included in the mobile device 104." *Collinge (Ex. 1004)*, [0041].

172. After the user is registered and a mobile payment application is installed on Collinge's mobile device, a card profile and single use key is provisioned from a remote secure element to Collinge's mobile payment application on Collinge's mobile device. *Collinge (Ex. 1004)*, [0068]-[0069], Fig. 5; *see also* Figs. 6, 15.



Collinge (Ex. 1004), Fig. 5 (annotated). The card profile includes “at least payment credentials corresponding to the associated payment account and a profile identifier[.]” *Collinge (Ex. 1004)*, Abstract. Specifically, Collinge teaches that the “Payment Token Payload – Card Profile (PTP_CP_ contains **the Payment Credentials required to perform a [MasterCard] PayPass transaction**” including “data elements such as: **PAN**, PSN + Track Data.” *'098 Provisional (Ex. 1008)*, [0101] (emphasis added). As discussed in Claim 15(b), Collinge’s “card profile” including payment credentials is stored in storage 304. *Collinge (Ex. 1004)*, [0048], [0063] (“The storage 304 may then store the shared mobile key, received

payment credentials, and any additional information in the mobile device 104 to prevent unauthorized access.”).

173. Collinge’s single use key is generated based on at least “the profile identifier, an application transaction counter, and a generating key for use in generating a payment cryptogram valid for a single financial transaction.” *Collinge (Ex. 1004)*, [0011]. The generating key in the single use key is used by Collinge’s mobile payment application to “generate a dynamic card validation code (CVC3) or an application cryptogram (AC).” *Collinge (Ex. 1004)*, [0050].

174. Once the user “input[s] to the mobile payment application 106 that a payment transaction is to be conducted” the mobile payment application will then “generate a payment cryptogram using the generating key included in the single use key[.]” *Collinge (Ex. 1004)*, [0077]; *see also* [0043]. The payment cryptogram may be “a dynamic card validation code (CVC3) or an application cryptogram (AC).” *Collinge (Ex. 1004)*, [0050]. The payment cryptogram is “valid for a single financial transaction[.]” *Collinge (Ex. 1004)*, Abstract. Collinge teaches generating a CVC3 based on at least: “the supplied CVC3 value, the session key unpredictable number, the application transaction counter, and the reader unpredictable number.” *Collinge (Ex. 1004)*, [0145]; *’248 Provisional (Ex. 1006)*, Table 1.

20150001

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

175. A POSITA would recognize the benefits of a dynamic CVC3, which increases security and reduces the risk of fraud during a transaction as compared to the traditional static CVC value of a credit card. Notably, Bona teaches that use of 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. 1009)*, [0037].

176. A POSITA would have understood that Collinge’s CVC3 is used instead of the card issuer’s CVC in a transaction. For example, 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, 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]. Collinge teaches the CVC3 is generated based in part on track data, which is found in a traditional magstripe. See Section VII; *Collinge*, [0145].

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 at Table 1. Collinge teaches that a type of payment cryptogram may be a CVC3. *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 116 and 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. 1009)*, at [0037] On the other hand, “MasterCard Inc.’s PAYPASS® Magstripes smart card specification has a similar code designated the CVC3.” *Bona*

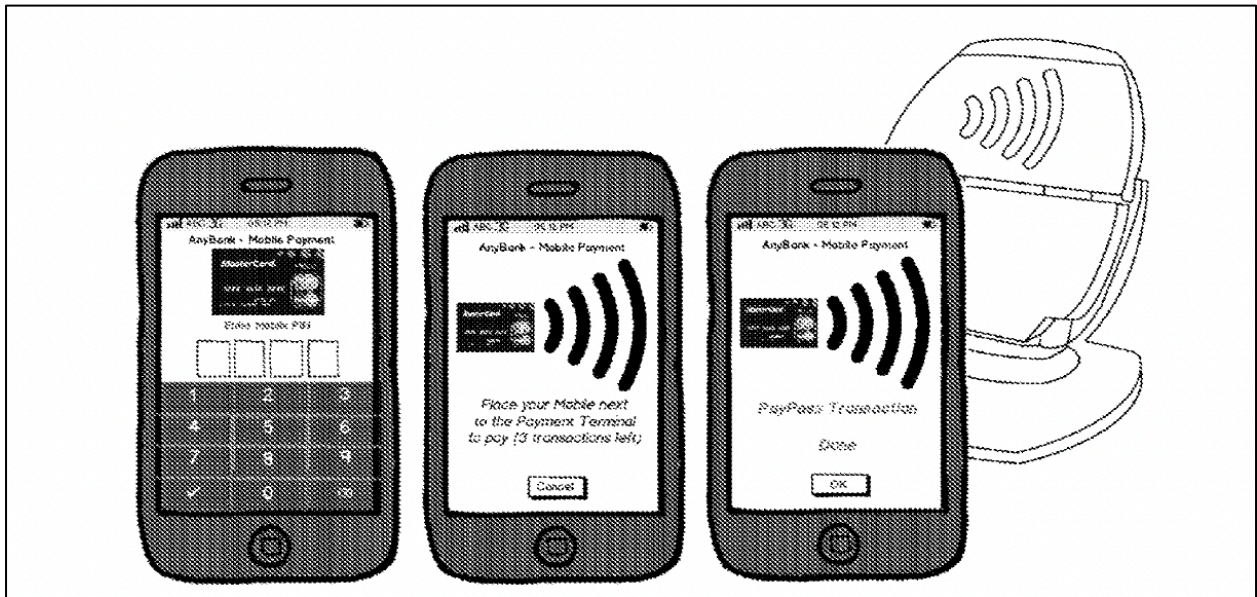
(*Ex. 1009*), at [0037] Both Visa's dCVV and Mastercard's CVC3 are a "one-time (i.e., dynamic) codes... unique to each transaction." *Bona (Ex. 1009)*, at [0037]. CVVs need to be present in a magstripe transaction. *Bona (Ex. 1009)*, at [0037]. ("magnetic stripe specifications for Track 1 and Track 2 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 CVV. 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 VII; *Bona* 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* 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.”)

1. authenticated card user

177. Collinge teaches that the generated limited-use payment information (e.g., payment cryptogram (for example CVC3)) is for use by a card user who has been successfully authenticated with a pin or passcode. *Collinge (Ex. 1004)*, [0051]. Specifically, Collinge teaches that the single use key used in generating the CVC3 “may be protected based on a mobile personal identification number (PIN) value.” *Collinge (Ex. 1004)*, [0051]. If the single use key is protected based on a PIN, the user “may provide a mobile PIN for authentication.” *Collinge (Ex. 1004)*, [0051]. If

the mobile PIN provided is incorrect, “an incorrect value of the single use key may be used by the mobile payment application 106” and “the issuer 108 will not authorize the payment transaction” resulting in “additional security for the user 102, the issuer 108, and the merchant involved in the payment transaction.” *Collinge (Ex. 1004)*, [0051]. Therefore, the CVC3 payment information can only be used by a user authenticated by a mobile PIN. An example of the PIN input screen is depicted below:

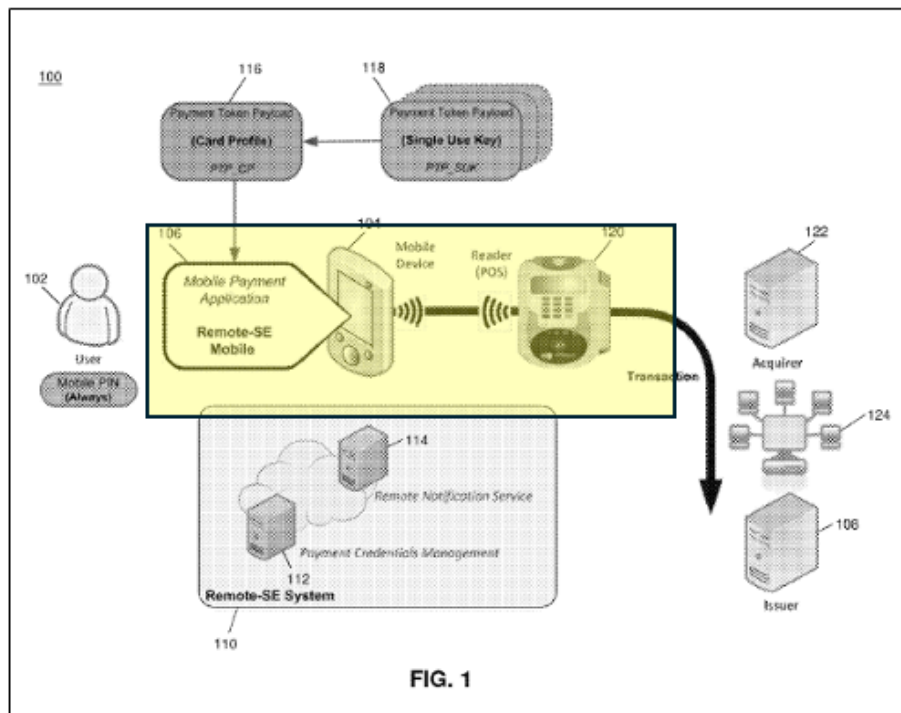


'098 Provisional (*Ex. 1008*), 99; '248 Provisional (*Ex. 1006*), Fig. 2B. A POSITA would have recognized and Bona teaches that requiring a correct PIN to perform a transaction was well known. *Bona (Ex. 1009)*, [0007] (“Once the card has been verified as authentic, the customer enters a 4-digit PIN, which is checked against the PIN stored on the card; if the two match, the transaction completes.”); [0120] (“the

user is authenticated, such as using biometrics if the cell phone (or smart card) has biometric capabilities or a PIN or password authentication scheme.”)

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

178. As discussed above at Claim 1(b)(2), Collinge teaches a wireless interface. Collinge’s mobile device conveys payment information, including a CVC3 payment cryptogram (*limited-use payment information*) via an NFC interface (*interface of the computing device*) to a point of sale terminal. As discussed in section VII, it was well known how wireless interfaces such as NFC sent data during a transaction.

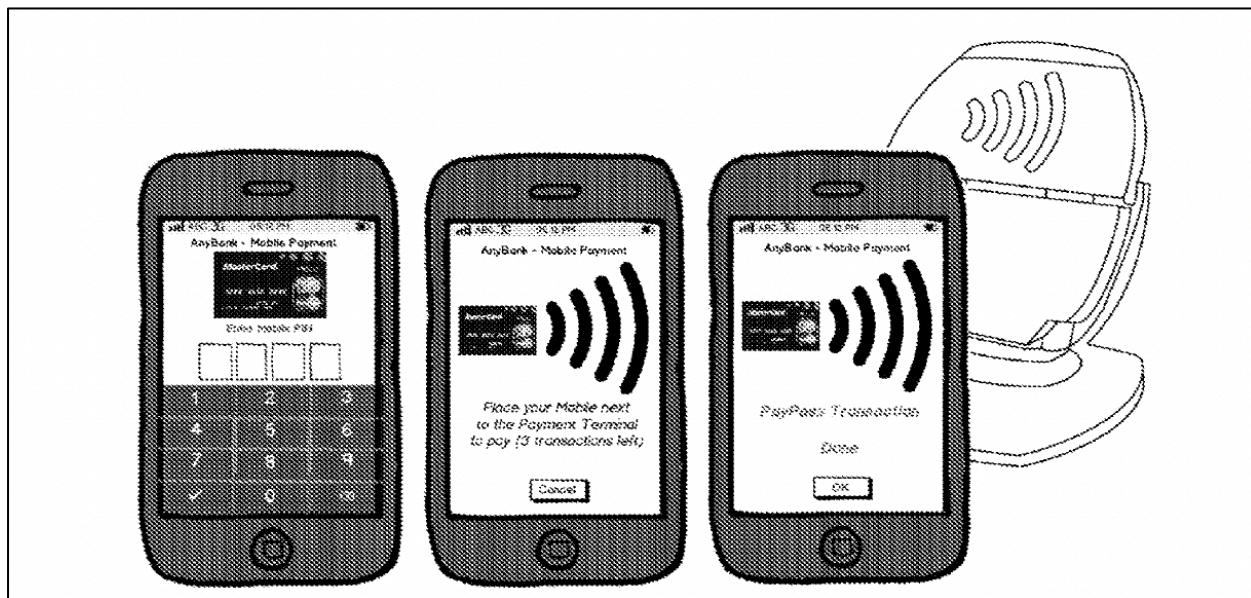


Collinge (Ex. 1004), Fig. 1 (annotated excerpt).

179. Collinge’s “mobile device 104 may conduct a **contactless/NFC payment transaction** using the mobile payment application 106.” *Collinge (Ex. 1004)*, [0070] (emphasis added). Collinge teaches in several instances that the mobile device transmits “generated cryptogram and payment credentials” “to a point of sale terminal 120 via NFC.” *Collinge (Ex. 1004)*, [0070]. As another example, Collinge also teaches that “the application transaction counter may be transmitted, via near field communication, to the point-of-sale terminal 120 for including in an authorization request in a financial transaction.” *Collinge (Ex. 1004)*, [0145]. As

another, Collinge teaches, “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 (Ex. 1004)*, [0120].

180. A POSITA would have understood that when Collinge’s mobile device transmits payment information via NFC it is transmitting the payment information via an interface of the computing device. Specifically, a POSITA would have understood that Collinge transmits payment information via NFC, a wireless interface of Collinge’s computing device.

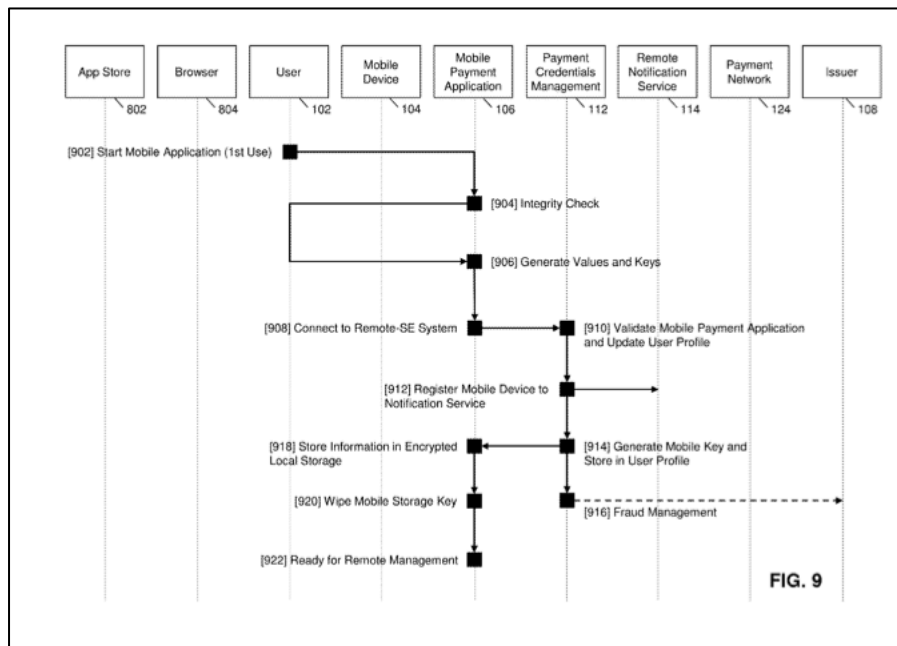


'098 Provisional (*Ex. 1008*), 99; '248 Provisional (*Ex. 1006*), Fig. 2B..

A valid user

181. Collinge further teaches conveying the limited-use card information upon the authorization of a valid user. *Collinge (Ex. 1004)*, [0093], [0123].

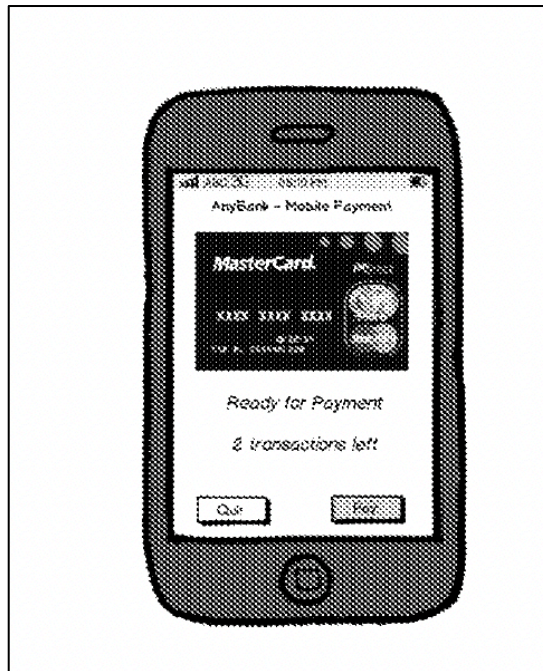
182. After the user starts the mobile payment application, “the mobile payment application 106 may perform an integrity check. As part of the integrity check, the mobile payment application 106 may authenticate the user 102 and request the activation code provided to the user 102 during the registration process (e.g., at step 812 in FIG. 8).” *Collinge (Ex. 1004)*, [0093], [0123] (describing “authentication by the user 102 at both the mobile device 104 (e.g., entering of the mobile PIN) and the point-of-sale terminal 120 (e.g., entering of an online PIN or signature).”).



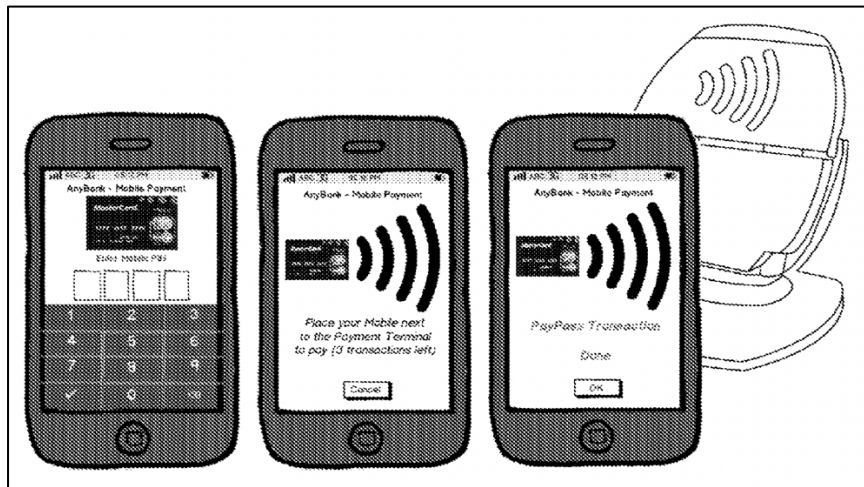
Collinge (Ex. 1004), Fig. 9. Therefore, Collinge identifies a user as a valid user via the correct input of an activation code.

5. *Authorization of a payment transaction by a valid user*

183. Collinge teaches a user may confirm or deny (authorize) a payment transaction after inputting the user's mobile PIN (*Collinge (Ex. 1004)*, [0093], [0123]; *'098 Provisional (Ex. 1008)*, 99) and then confirming a payment method (“quit” or “pay”):



'098 Provisional (Ex. 1008), 100; *'248 Provisional (Ex. 1006)*, Fig. 2B.. The user is then instructed to place Collinge's mobile device by a payment terminal:



'098 Provisional (Ex. 1008), 99; '248 Provisional (Ex. 1006), Fig. 2B. Once the mobile device is placed next to the payment terminal and Collinge's NFC interface is activated Collinge transmits payment credentials and a dynamic CVC3 to the payment terminal. *Collinge* (Ex. 1004), [0044], [0077]; '248 Provisional (Ex. 1006), [0073] ("For example, step 208 can comprise activating an NFC interface using the mobile payment application.")

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

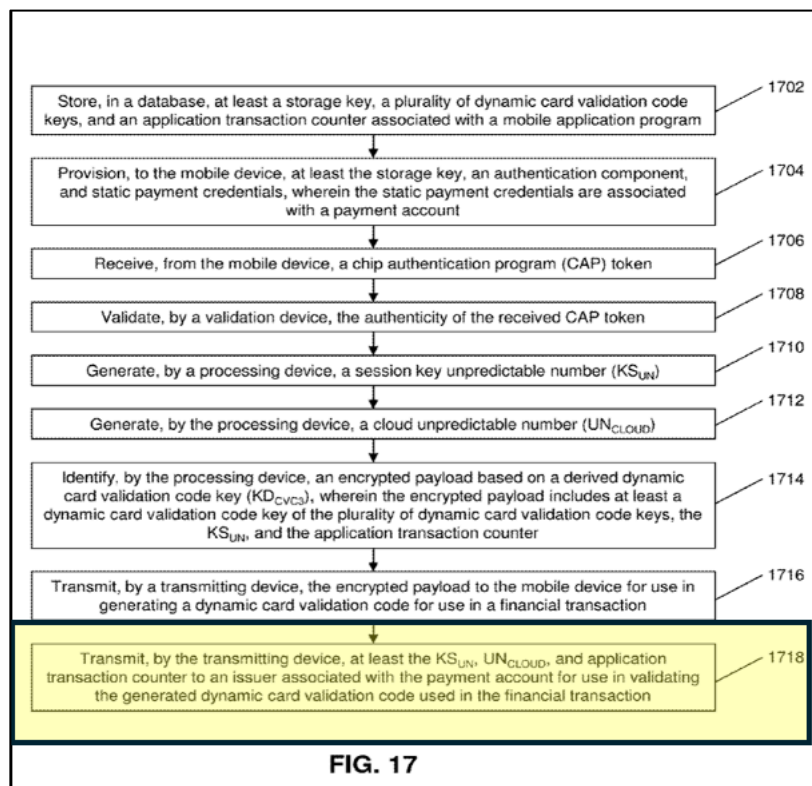
184. Collinge teaches "the user 102 may shop at a merchant 306 and select goods or services for purchase." *Collinge* (Ex. 1004), [0077] Then the user "may then input to the mobile payment application 106 that a payment transaction is to be conducted." *Collinge* (Ex. 1004), [0077]. A CVC3 payment cryptogram (payment information) is generated by the mobile payment application on Collinge's mobile device (personal computing device). See Claim 15(f). Then Collinge's mobile

payment application “may transmit the payment cryptogram to the merchant point-of-sale terminal 120.” *Id.* Therefore, a POSITA would have understood that since Collinge’s mobile application is able to transmit the payment cryptograph to the merchant point of sale terminal, the merchant point of sale terminal is operable to receive such information.

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

185. Collinge teaches an issuer 108 (card issuer authority) validates a CVC3 payment cryptogram (a card payment information) that has been provided by the computing device to a point of sale terminal as authentic when received from an authenticated user of Collinge’s mobile device (an authenticated user’s computing device). As described above, Collinge teaches authenticating the mobile device user through a pin or passcode. *See* Claim 15(d).

186. In Collinge, the issuer 108 validates the generated CVC3 payment cryptogram. *Collinge (Ex. 1004)*, [0141]. Specifically, the issuer receives “at least the K_{SUN} , UN_{CLOUD} , and application transaction counter” and the issuer 108 uses that information “in validating the generated CVC3 value used in the financial transaction.” *Collinge (Ex. 1004)*, [0141].



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

The issuer may then “authenticate the dynamic card validation code[.]” *Collinge (Ex. 1004)*, [0056]. *Collinge*’s provisional details how the issuer validates the CVC3 payment cryptogram. *Collinge* teaches generating a CVC3 payment cryptogram based on at least: “the supplied CVC3 value, the session key unpredictable number, the application transaction counter, and the reader unpredictable number.” *Collinge (Ex. 1004)*, [0145]; *'248 Provisional (Ex. 1006)*, Table 1.

2015000000

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

187. Specifically, based on the received information at the issuer above (K_{SUN} , UN_{CLOUD} , and ATC) the issuer will compute $Cloud_CVC3_{TRACK1/2}$. '095 Provisional (Ex. 1005), 24. The issuer also uses $IVCVC3_{TRACK1/2}$ which is a MAC calculated over track 1 and 2 data using KD_{CVC3} which is “kept in the Cloud/Issuer” '095 Provisional (Ex. 1005), 21.

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

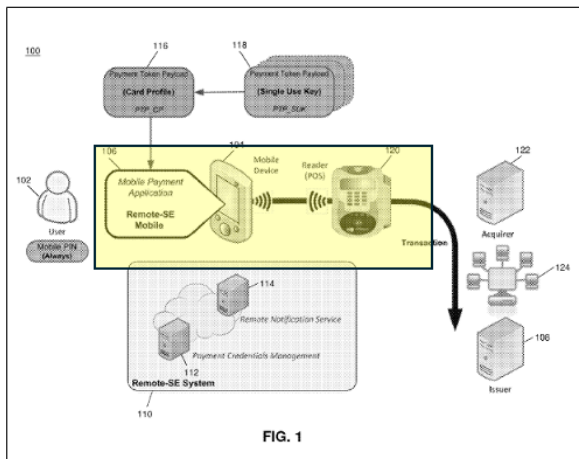
'095 Provisional (Ex. 1005), 24. After computing $Cloud_CVC3_{TRACK1/2}$, the issuer computes $CVC3_{TRACK1/2}$ which is directly used in generating the CVC3. '095 Provisional (Ex. 1005), 25.

The Issuer system is able to compute $CVC3_{TRACK1/2}$ using: ◇ $Cloud_CVC3_{TRACK1/2}$ (2 bytes) ◇ UN_{READER} (4 bytes) ◇ ATC (2 bytes) The Issuer can validate the $CVC3_{TRACK1/2}$.

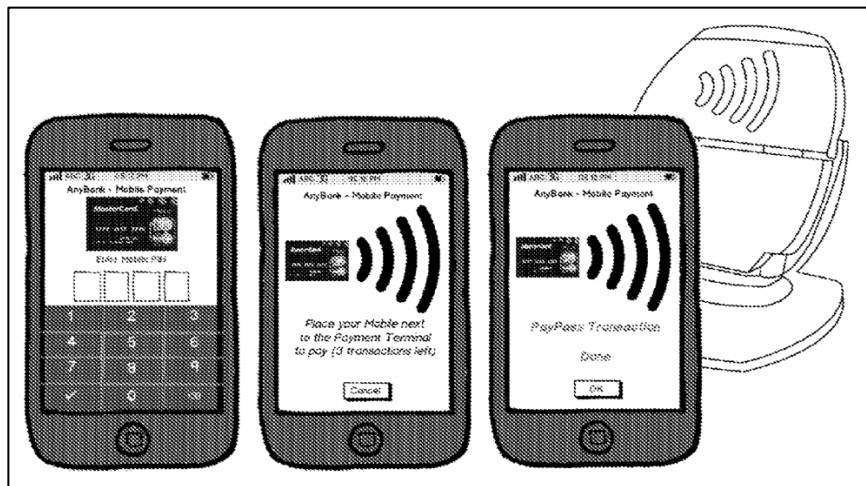
'095 Provisional (Ex. 1005), 25. The issuer already has the rest of the values used when generating the CVC3 (K_{SUN} , UN_{CLOUD} , and ATC). '095 Provisional (Ex. 1005), 24-25. Based on the result of the authentication, the issuer will “approve or deny the payment transaction.” Collinge (Ex. 1004), [0056]. It was well known that if an issuer successfully validates a payment transaction via validating a payment

cryptogram (in this instance a CVC3), the transaction is authentic since the PIN entered by the user in Collinge would be found valid. *Collinge*, [0128] (“the single use key 118 may be incorrect (e.g., fake, not genuine, etc.) if the key request includes a mobile PIN for which authentication is unsuccessful,,include transmitting the generated single use key 118 to an inssuer associated with the payment account.”); *Hammad*, 1:45-65. (“If the received dCVV and the generated dCVV match, the transaction can be considered authentic. If the dCVVs do not match, this may indicate that the transaction is fraudulent.”).

188. As depicted below, a POSITA would have understood Collinge teaches performing a transaction via NFC at a physical point-of-sale terminal, which a POSITA would have understood would be a merchant in-store facility transaction. *Collinge (Ex. 1004)*, [0044] (“transmit a generated payment cryptogram and payment credentials to a point-of-sale terminal¹²⁰ at a merchant.”) Collinge specifically discloses transmitting a generated CVC3 payment cryptogram and payment credentials to a point-of-sale terminal **at a merchant**. *Collinge (Ex. 1004)*, [0044], [007].



Collinge (Ex. 1004), Fig. 1 (excerpt); see also '098 Provisional (Ex. 1008), 99 (instructing the user to “[p]lace your Mobile next to the Payment Terminal to pay” at the physical terminal).



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

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

189. Collinge teaches that issuer 108 (*card issuing authority*) is operable to reject as invalid, a payment information based on for example, an invalid PIN, available credit, and control limits (*outside of its valid limitations of use*).

190. Collinge teaches that issuer 108 (*card issuer authority*) will “deny the payment transaction” (*reject as invalid*) when the received CVC3 value is unable to be authenticated because, for example, the single-use key is not genuine based on an unsuccessfully entered mobile PIN. (*outside of limitations of use*). *Collinge (Ex. 1004)*, [0056], [0076], Abstract.

191. Specifically, Collinge teaches that the single-use key is “protected based on a mobile personal identification number (PIN)[.]” *Collinge (Ex. 1004)*, [0051]. To use the single-use key to generate a payment cryptogram, “user 102 may provide a mobile PIN for authentication.” *Collinge (Ex. 1004)*, [0051]. If the “mobile PIN provided is incorrect, an incorrect value of the single use key may be used by the mobile payment application 106. In such an instance, the issuer 108 will not authorize the payment transaction.” *Collinge (Ex. 1004)*, [0051]. A POSITA would have understood that an incorrect value of the mobile PIN used when generating a payment cryptogram is outside of Collinge’s limitations of use.

192. As another example, Collinge teaches that the issuer will “deny the payment transaction” (reject as invalid) when the user’s “available credit in the payment account” does not support the “transaction amount” (outside of limitations of use). *Collinge (Ex. 1004)*, [0120], [0077]. A POSITA would have understood that the available credit in a payment account is a limitation of use. A POSITA would have understood that to use this specific payment account in a transaction successfully, the transaction amount must be under or at the available credit in a payment account. Otherwise, if the transaction amount exceeds the available credit, the purchase will be unsuccessful.

193. As another example, Collinge teaches that the issuer may deny (reject as invalid) the payment transaction based on “control limits” (outside of limitations of use) synchronized between mobile payment application 106 and issuer 108. *See ’095 Provisional (Ex. 1005)*, Claims 9-10. (“a day of week; a time of day; an expiration date associated with a CAP token; an expiration date associated with a payment account; a merchant category corresponding to a point-of-sale (POS) terminal; a geographic location of a merchant; a spending limit for a payment account; a spending limited for a specified merchant category; and a spending limit for a duration.”) *Collinge (Ex. 1004)*, [0143]-[0144] (“a chip authentication program (CAP) token may be generated by a processing device, wherein the CAP token is

based on at least the authentication component and the at least one additional credential.”). It was well-known that implementing a credit limit is one way to limit the amount that a bad actor can fraudulently obtain or to limit spend by a minor card or employees using a company card. *Patterson (Ex.1011)* at 12:18-49.

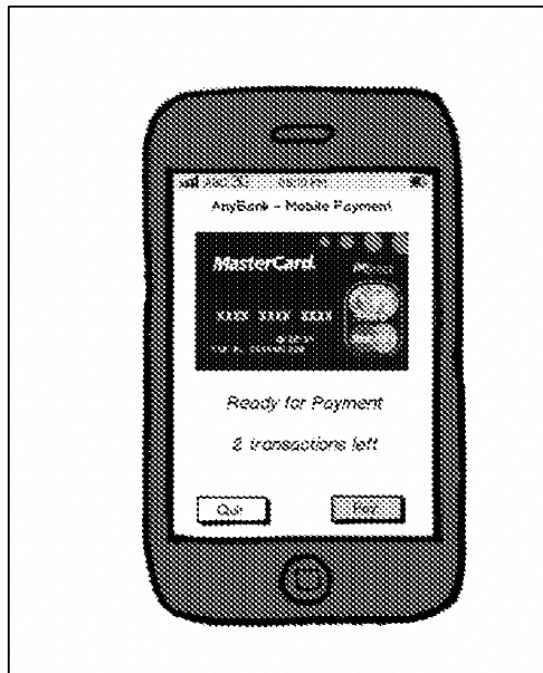
N. 15(h): wherein a card issuing authority is operable to validate generated limited-use payment information provided by the computing device in an authorized transaction completed by the computing device.

194. *See* Claim 15(f).

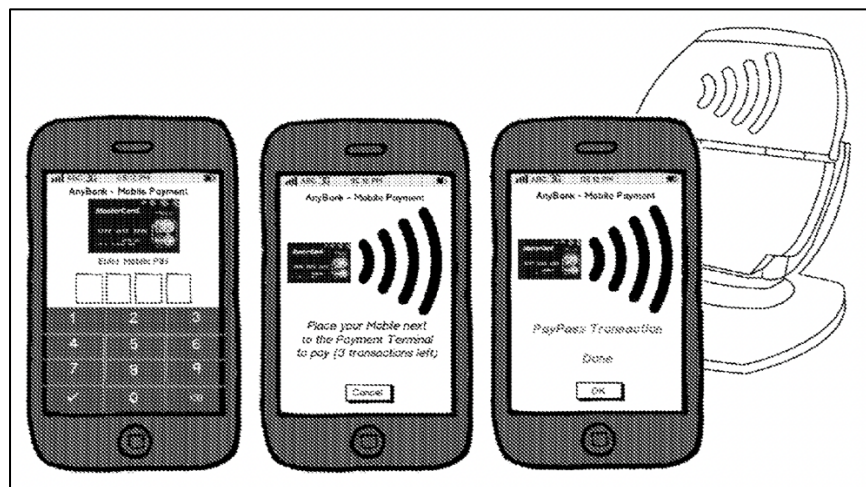
O. Claim 17(a): The system of claim 15, wherein the touch-screen display interface is operable to display a merchant facility transaction, and wherein the touch-screen display interface is operable to accept a user approval and denial of a payment transaction,

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

196. Collinge’s mobile device is operable to display a merchant facility transaction:



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



'098 Provisional (Ex. 1008), 99; '248 Provisional (Ex. 1006), Fig. 2B. A POSITA would have understood that Collinge teaches a merchant facility transaction. For example, Collinge states "mobile device 104 may be further configured to transmit a generated payment cryptogram and payment credentials to a point-of-sale

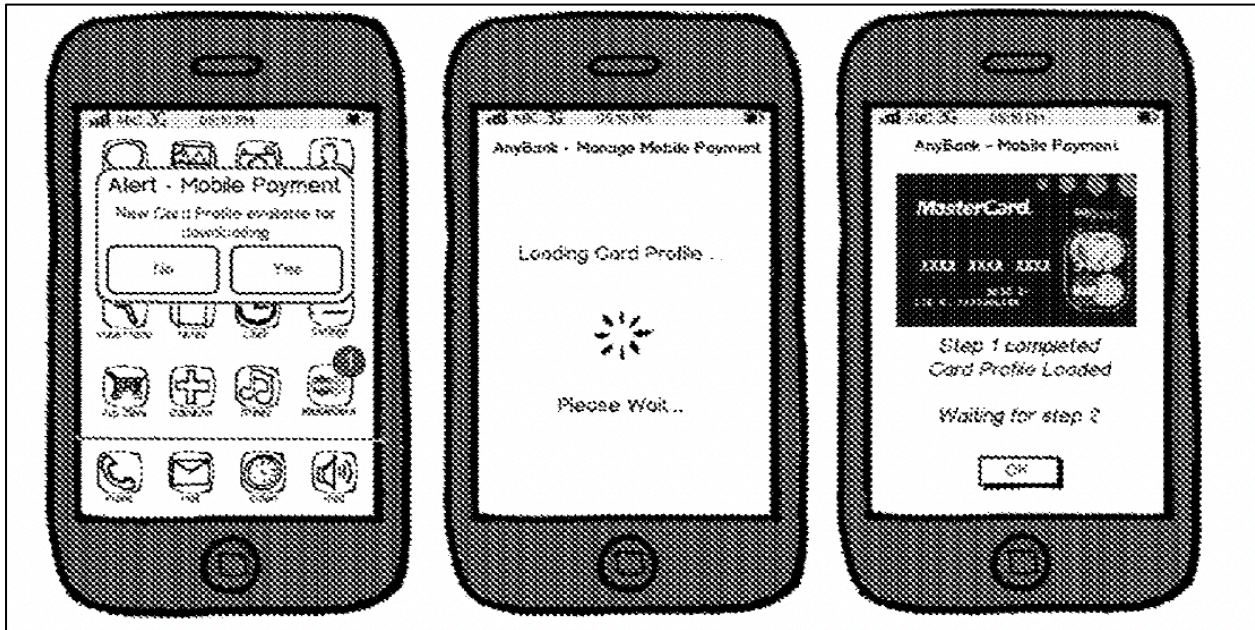
terminal 120 at a **merchant.**” *Collinge (Ex. 1004)*, [0044]. It was well known that a point-of-sale terminal at a merchant would be a merchant facility transaction.

P. 17(b): and wherein a card issuer authority is further operable to deny a card payment transaction from a user-denied merchant facility transaction, and to approve as authentic a card payment transaction from a user-approved facility transaction.

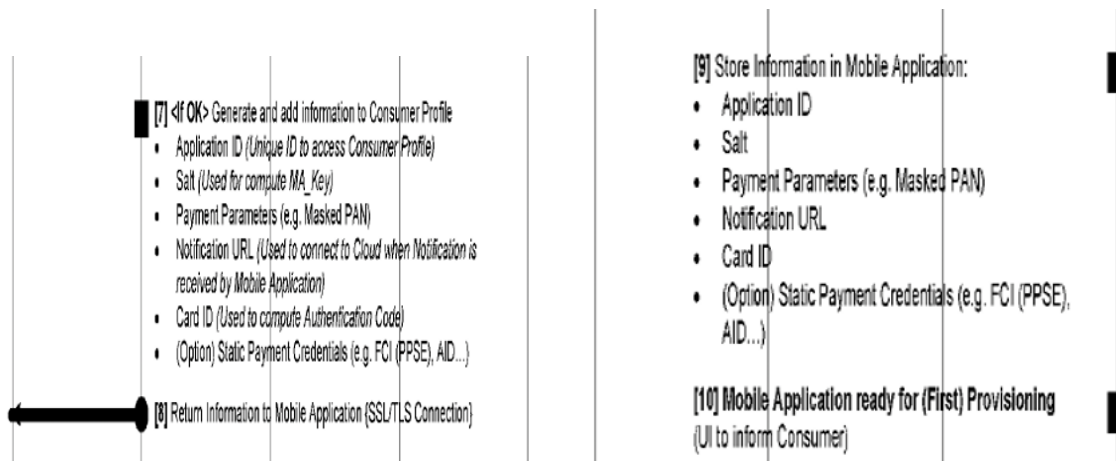
197. As discussed above an issuer is able to approve and deny card payment transactions. *See* Claim 15(f)-15(g); 1(j).

Q. Claim 18 (a): The system of claim 15, wherein a plurality of issuer-provided payment information is wirelessly downloaded into the personal computing device, and

198. *Collinge* teaches multiple card profiles (a plurality of issuer-provided payment information) are wirelessly downloaded into *Collinge*’s mobile (personal computing) device. For example, *Collinge* teaches “the card profile 116 is ready to be downloaded to the mobile payment application 106.” *Collinge (Ex. 1004)*, [0074]; ’098 *Provisional (Ex. 1008)*, Fig. 11 (excerpts). *Collinge*’s “communication interface” “allow[s] software and data to be transferred between the computer system 1900 and external devices.” *Collinge (Ex. 1004)*, [0154]. The “communications interfaces 1924 may include ...a network interface [.]” *Collinge (Ex. 1004)*, [0154]. This “[t]he network may be any network suitable for performing the functions as disclosed herein and may include...a wireless network...” *Collinge (Ex. 1004)*, [0150].



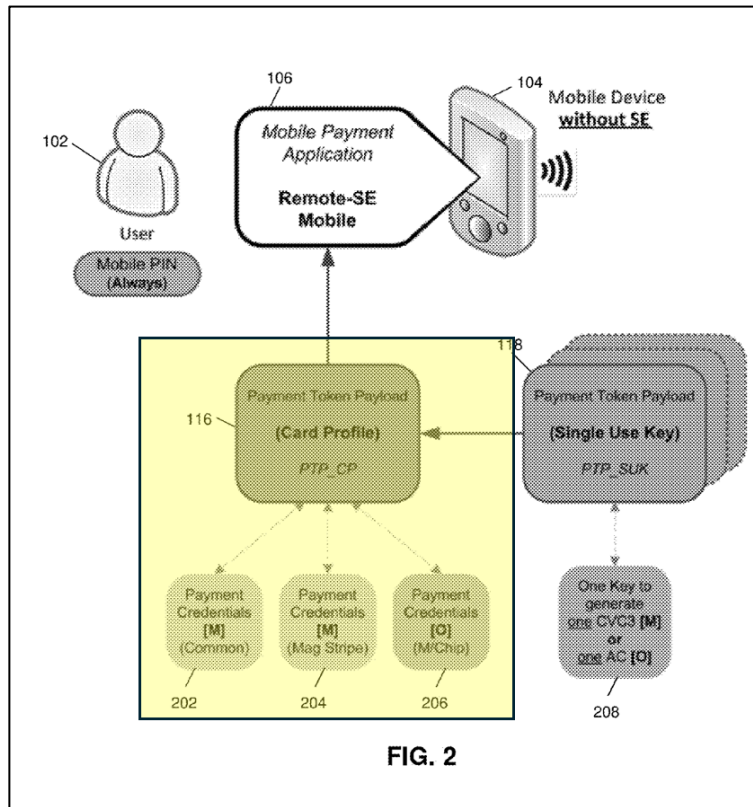
'098 Provisional (Ex. 1008), 97; '248 Provisional (Ex. 1006), Fig. 2B. Collinge teaches that “[t]he mobile payment application 106 may then...receive the card profile116 from the remote-SE system.” Collinge (Ex. 1004), [0074]; '098 Provisional (Ex. 1008), Fig. 11 (excerpts).



199. Each card profile in Collinge includes a plurality of issuer-provided payment information such as the “PAN, PSN + Track Data[.]” '098 Provisional (Ex.

1008), [0101]. *Collinge (Ex. 1004)*, [0127] “(the card profile 116 includes at least payment credentials corresponding to the associated payment account and a profile identifier.”).

200. *Collinge* teaches that a card profile includes multiple payment credentials. *Collinge (Ex. 1004)*, Fig. 2, [0051] (“The single use key 118 may also include an identifier used **to identify the card profile 116 to which it corresponds to.**”) (emphasis added), [0038] (“Payment Card—A card or data associated with a payment account that may be provided to a merchant in order to fund a financial transaction via the associated payment account. Payment cards may include credit cards, debit cards, charge cards, stored-value cards, prepaid cards, fleet cards, virtual payment numbers, virtual card numbers, controlled payment numbers, etc.”), [0048] (“The card profile 116 may include payment credentials provisioned to the mobile payment application 106 by the remote-SE system for use in conducting payment transactions. The 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.”).



Collinge (Ex. 1004), Fig. 2 (annotated).

201. Once the card profile is received Collinge “store[s] the received card profile116 in the local encrypted database 304.” Collinge (Ex. 1004), [0074];



'098 Provisional (Ex. 1008), Fig. 11 (excerpt).

R. 18 (b): wherein the user-interface is operable for a user selection, of at least one of issuer-provided payment methods via the touch-screen display interface, and

202. *See* Claim 15(b)(3).

S. 18 (c): wherein the payment card device is operable for a transaction with a user-selected payment method.

203. *See* Claim 15(d).

XI. OPINIONS REGARDING GROUND 2: CLAIMS 1, 5-8, 11, 20-27 ARE OBVIOUS OVER *COLLINGS, BONA, AND SMITH*.

A. Claim 1 (Pre): A payment system comprising:

204. *See* Claim 15(Pre).

B. 1(a): a payment card device free of any fixed payment numbers visible thereon and wherein said payment card device is operable for use in payment card reader equipment; and”

205. *See* Claim 15(a).

C. 1(b): a computing device comprising: a processor;

206. *See* Claim 15(b).

D. 1(b)(1): a memory;

207. *See* Claim 15(b)(5).

E. 1(b)(2): a wireless interface;

208. *See* Claim 15(b)(4).

F. 1(b)(3): a touch-screen user interface operable to provide a visual user-interface for user payment interactions; and

209. *See* Claim 15(b)(2).

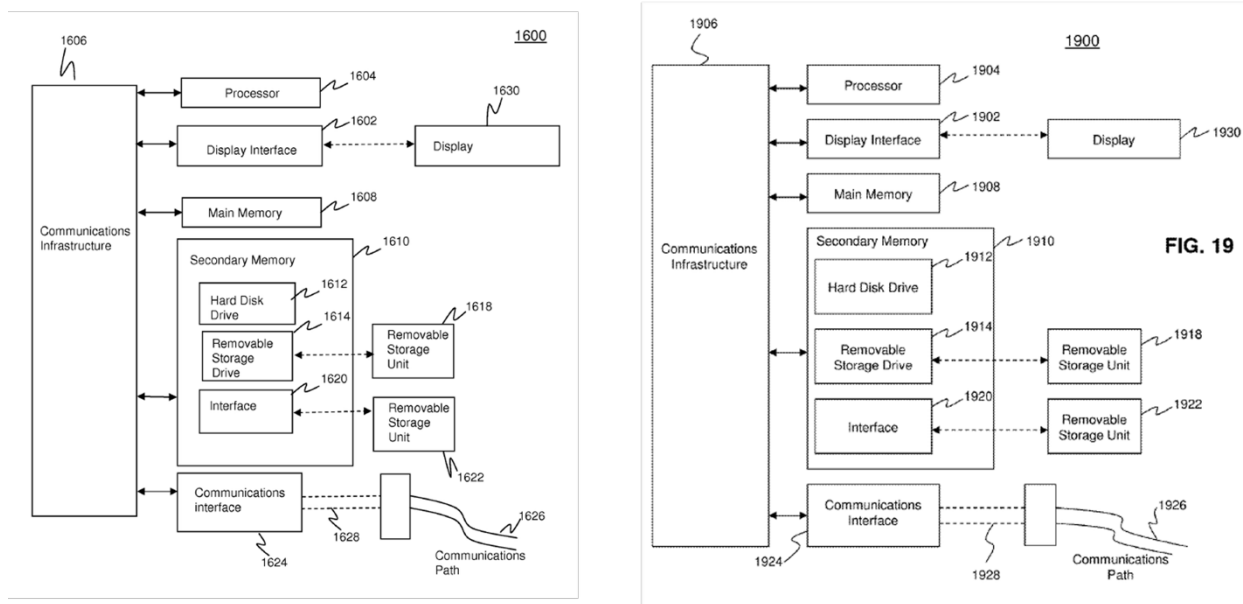
G. 1(c): a user-input device coupled to the processor, and

210. Collinge teaches that the user-input device (e.g., touch screen) of Collinge's mobile device 104 is coupled to the processor. Collinge specifically describes the touch screen of mobile device 104 as an input device. *Collinge (Ex. 1004)*, [0133] ("an input device (e.g., of the mobile device 104, such as a touch screen)"). A POSITA would have understood that Collinge's touch screen is a user input device because it "receives a **user's input** of a "mobile personal identification number (PIN)" during generation of a payment cryptogram. *Collinge (Ex. 1004)*, [0133].

211. A POSITA would have understood that Collinge's touch screen (i.e., user-input device) would have two parts –physical hardware components of a touch screen and software components (visual GUI component). For example, an article Mahapatra teaches that "[a] basic touch screen...is made up of 3 basic elements, a sensor, a controller and a software driver." *Mahapatra (Ex. 1041)*, 37.

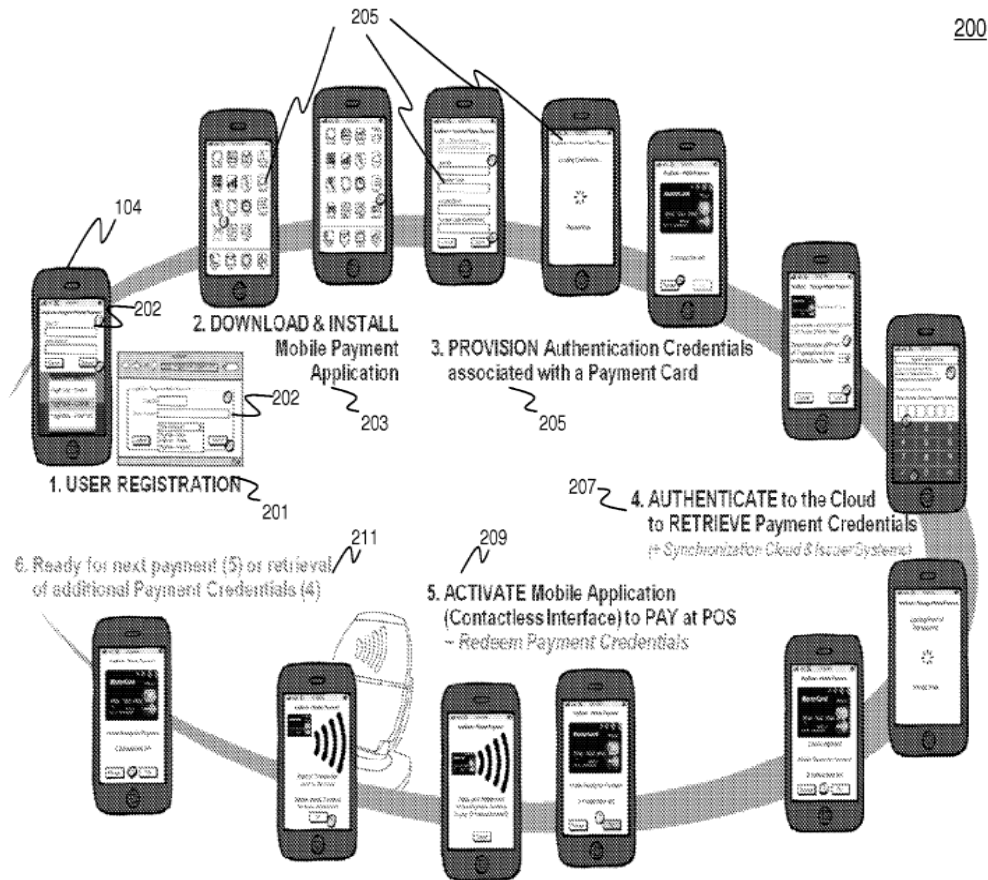
212. Collinge teaches that "at least one processor device" is used to implement the payment system taught by Collinge. *Collinge (Ex. 1004)*, [0147]. As shown in Fig. 19, a POSITA would have understood that Collinge teaches Collinge's touch screen (user-input device) is coupled to Collinge's processor. 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

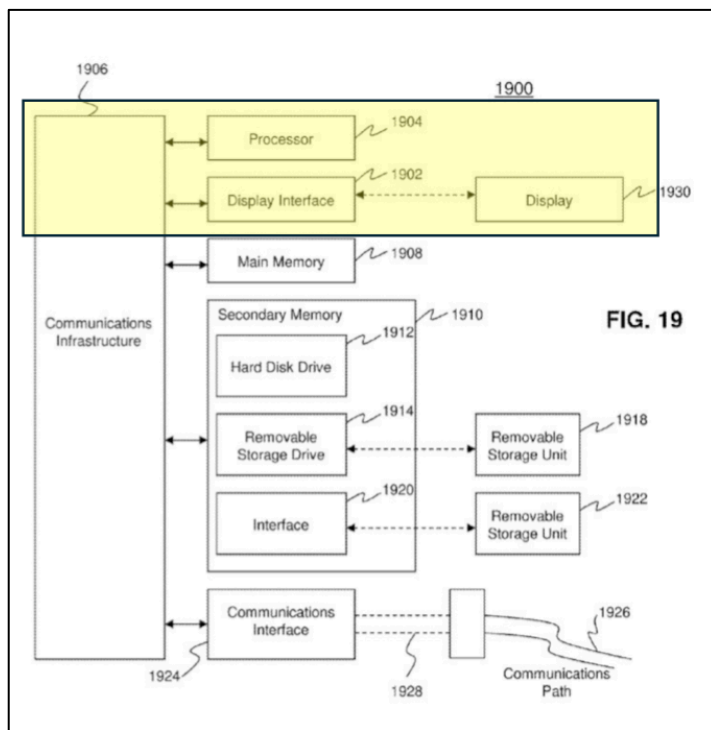
2B are expressly taught as being carried out by “mobile device 104[.]” ‘248
Provisional (Ex.1006) at [0048].



‘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 is that of mobile device 104. In other words, because processor 1604/1904

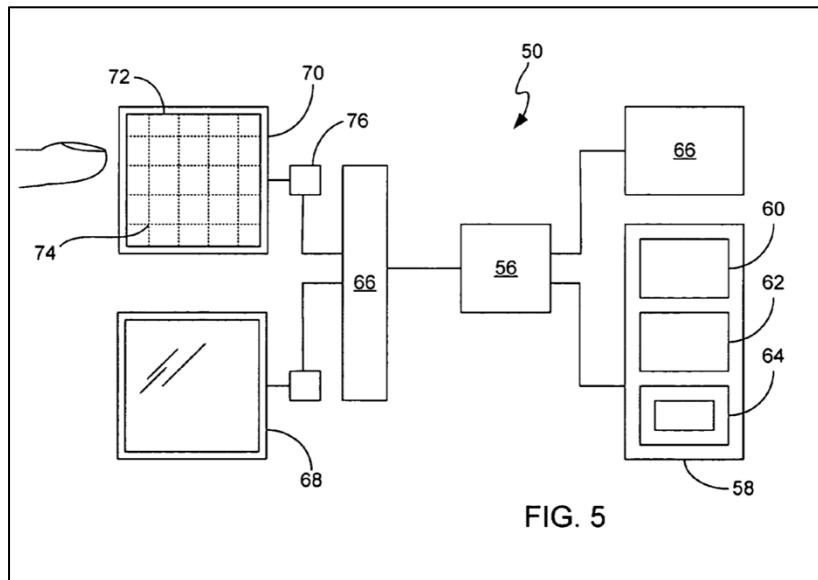
in the '248 Provisional (Ex.1006) implements computer programs on mobile device 104, a POSITA would understand that Figure 19 of Collinge represents mobile device 104 (the electronic device).

213. Collinge teaches that Collinge's payment system comprises a display interface that is "coupled" to the processor via the communication interface:

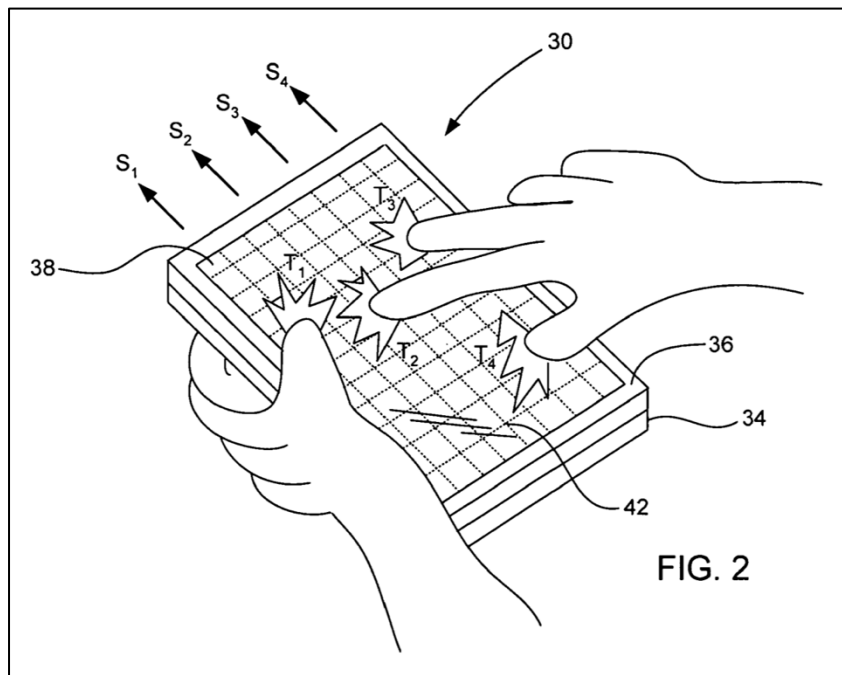


Collinge (Ex. 1004), Fig. 19 (annotated). A POSITA would have understood that Collinge's display interface is Collinge's touchscreen. It was well known that displays and processors are coupled in mobile devices. As one example, U.S. Patent Appl. No. 2006/0097991 to Hotelling et. al. ("Hotelling") teaches that

“[t]he computer system 50 also includes a touch screen 70 that is operatively coupled to the processor 56.” *Hotelling (Ex. 1042)*, [0052].

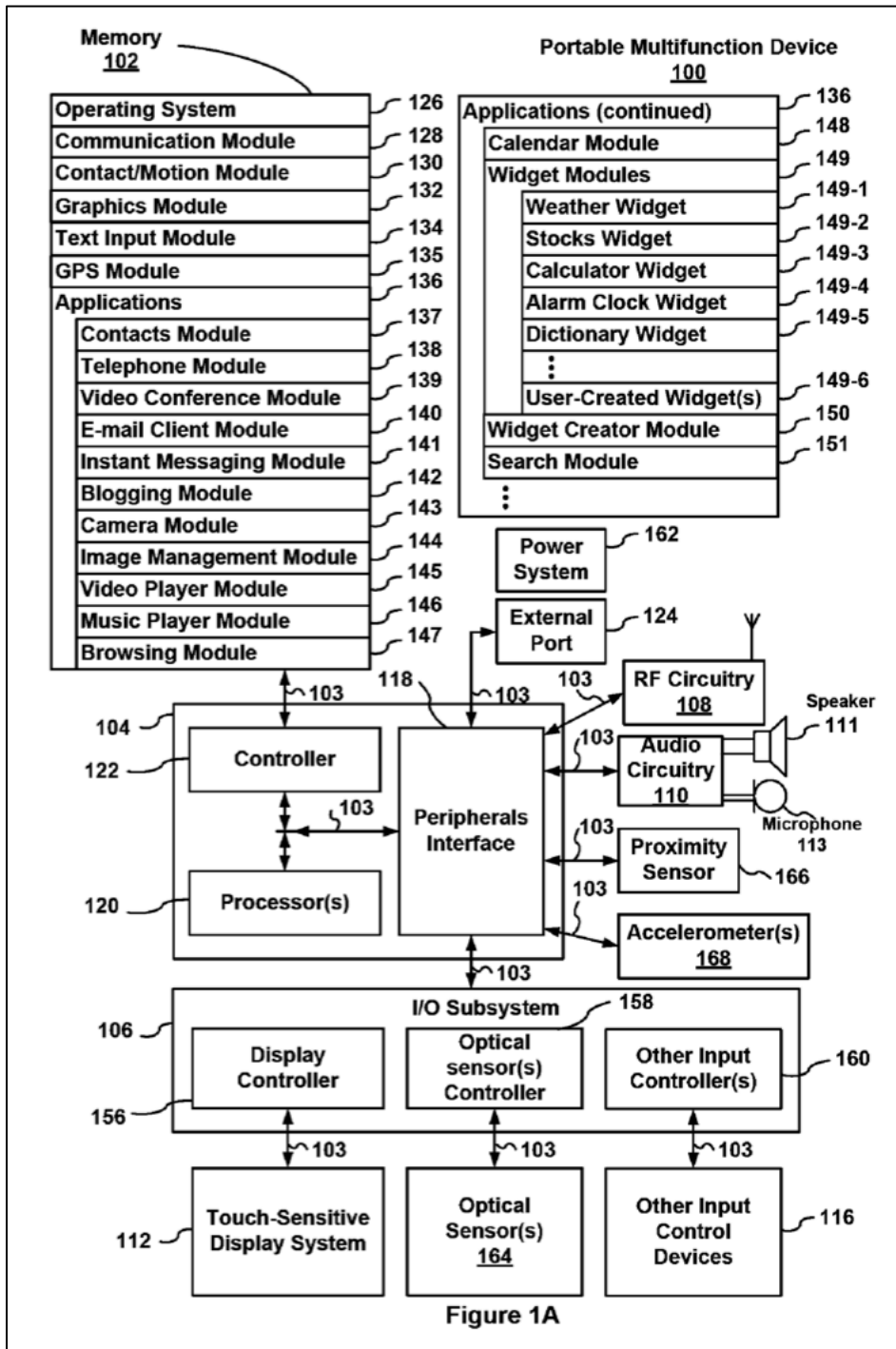


Hotelling (Ex. 1042), Fig. 5. Hotelling teaches that “[t]he touch screen also includes a sensing circuit that acquires data from the sensing device and that supplies the acquired data to the processor.” *Hotelling (Ex. 1042)*, [0013]. The sensing device detects “multiple touches or near touches[.]” *Hotelling (Ex. 1042)*, Abstract.



Hotelling (Ex. 1042), Fig. 2.

214. As another example, Jobs describes “peripherals interface 118 couples the input and output peripherals of the device to the CPU 120 and memory 102. The one or more processors 120 run or execute various software programs and/or sets of instructions stored in memory 102 to perform various functions for the device 100 and to process data.” *Jobs (Ex. 1043), [0098]*



Jobs (Ex. 1043), Fig. 1A.

215. A POSITA would have understood that Collinge teaches a touch screen coupled to a processor because Collinge teaches that its touch screen is operable to provide a visual user-interface (*see* claim 1(b)(3)) and accept and act on user input received at the touch screen. *Collinge (Ex. 1004)*, [0133] (“an input device (e.g., of the mobile device 104, such as a touch screen) may receive a mobile personal identification number (PIN) input by a user (e.g., the user 102) of the mobile device 104.”) A POSITA would have understood that for the touch screen in Collinge’s mobile device 104 to operate as described by Collinge, the touch screen must necessarily be coupled to a processor, similar to Hotelling. Therefore, a POSITA would have understood that for the touch screen in Collinge’s mobile device 104 to operate as described by Collinge, the touch screen must necessarily be coupled to a processor.

H. 1(d): wherein the processor is operable to store a transaction sequence count,

216. Collinge teaches an “application transaction counter (ATC)” (transaction sequence count) which is “a count of transactions used for fraud management and authentication.” *Collinge (Ex. 1004)*, [0050]. The ATC is provisioned from Collinge’s cloud system to Collinge’s mobile device and stored in storage 304, “an encrypted local database.” *Collinge (Ex. 1004)*, [0063] (shared mobile key is stored in storage 304), [0050] (single use key includes the ATC);

[0076] (“store the single use key 118 in the local encrypted database 304”), [0134] (“the single use key 118 includes at least an application transaction counter and a generating key.”).

217. A POSITA would have understood that the ATC is a transaction sequence count is a count of the number of transactions, as taught by Collinge. *Collinge (Ex. 1004)*, [0050]. Collinge teaches that the ATC is used when generating a cryptogram or dynamic card validation code to make a payment. *Collinge (Ex. 1004)*, [0050], [0063], [0076]. A POSITA would have been very familiar with this use of an ATC, as an ATC is a common security feature, which ensures that the cryptogram generated is not a duplicate of a cryptogram previously generated. For example, U.S. Patent Appl. No. 2013/0246269 to Roberts et al. (“Roberts”) teaches the following:

The application cryptogram returned in step 318 may be based, in part, on the application transaction counter (ATC), which is a counter in the chip card, two bytes long, which increments every transaction, and is a fundamental security mechanism employed with both contacted and contactless chips. It is one wherein the card and issuer **can ensure that cryptograms received from the card are not “old” cryptograms;** i.e., the ATC can be used to ensure that a cryptogram produced by the

card is not a previous cryptogram. Stated in another way, one of the things that would not be desirable is for a card to produce the same cryptogram that it produced for a previous transaction. By including the ATC in the cryptogram, it is ensured that the card will never produce a cryptogram that is the same as a previously-produced cryptogram.

Roberts (Ex. 1044), [0075]; *see also*, *Bona (Ex. 1009)*, [0102] (discussing role of an ATC in transaction authorization).

218. Therefore, a POSITA would have understood, and Collinge teaches that the ATC is stored in the storage 304 (encrypted local database) and is at least transitorily stored by Collinge's processor when the processor uses the ATC to generate a cryptogram or dynamic card validation code. *Collinge (Ex. 1004)*, [0050], [0135] (cryptogram is generated "by a processing device"). Collinge teaches that the ATC is included in a single use key 118 and that the "single use key 118 may be a payment token used one time to generate a payment cryptogram to be used in a payment transaction." *Collinge (Ex. 1004)*, [0050].

219. Collinge teaches that "[t]he 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 (Ex. 1004)*, [0041]. Collinge's mobile payment application

“106 may generate a payment cryptogram” such as a CVC3 value. *Collinge (Ex. 1004)*, [0070]; [0050].

220. Collinge teaches generating a CVC3 based on at least: “the supplied CVC3 value, the session key unpredictable number, the application transaction counter, and the reader unpredictable number.” *Collinge (Ex. 1004)*, [0145]; ‘248 *Provisional (Ex. 1006)*, Table 1.

FIG. 1000
The Mobile Payment Application use a specific process to generate the CVC3 using (KS_{UN}, Cloud_CVC3_{TRACK1/2}, ATC and UN_{READER})

A POSITA would have understood, and it was well known in the art, to use an application transaction counter when generating a dynamic security code. For example, Kranzley teaches that “[t]he dynamic code is, in some embodiments, generated based on the secret key and the value of a transaction counter. For example, each payment application may have a transaction counter that increments each time the payment application is used to conduct a transaction using a VPAN.” *Kranzley (Ex. 1013)*, [0042].

I. 1(d)(1): a device account number and

221. The combination of Collinge and Smith teaches a device account number. As discussed in greater detail below, a POSITA would have found it

obvious and would have been motivated to use Smith's "PPAN" (*device account number*) in place of the PAN in Collinge's static payment credentials.

222. In related art, Smith (also assigned to MasterCard) teaches a "mobile device" that "may...be used...with a near field communications enabled purchasing transaction." *Smith (Ex. 1010)*, Abstract.

223. Smith teaches that 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 (Ex. 1010)*, [0026].

224. 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 (Ex. 1010)*, [0040]. The PPAN is a different number from the actual PAN. As discussed in greater detail below, a POSITA would have recognized and Smith teaches that it is beneficial to use a PPAN in place of traditional payment account credentials so that if the mobile device and mobile wallet are compromised (i.e. lost or stolen), the PAN associated with the user's payment device (i.e. credit card) is not compromised. *Smith (Ex. 1010)*, [0026] ("an instantly-issued payment account that may be used by

the customer almost immediately after submitting a request for a new payment account.”)

225. Smith therefore teaches (1) a mobile device with a mobile wallet, (2) assigning a user’s PAN to a “PAAN” (device account number) to be used by the user in place of a PAN, and (3) allowing the user to present his/her mobile device with a PPAN at a point-of-transaction (POT) for payment. *Smith (Ex. 1010)*, [0024].

226. In the combination, Smith’s PPAN is used in place of Collinge’s PAN.

1. Collinge’s Teachings

227. 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 (Ex. 1004)*, [0043], [0143]; *see also ’098 Provisional (Ex. 1008)*, [0101] (“Payment Token Payload – Card Profile (PTP_CP_ contains **the Payment Credentials required to perform a [MasterCard] PayPass transaction**” including “data elements such as: **PAN**, PSN + Track Data.”) (emphasis added). As I explained above at VII, a PAN is the unique identifier number found on the front of a credit, debit, or prepaid card or the like. Collinge’s “card profile 116 may include payment credentials provisioned to the mobile payment application 106 by the remote-SE system for use in conducting payment transactions. The 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.”). *Collinge (Ex. 1004)*, [0048]. The common payment credentials “may include all data elements common to any type of payment transactions, such as both mag stripe and m/chip payment transactions. Such data elements may include payment account number, tracking data, and card layout description data. The mag stripe payment credentials 204 may include data elements specific to mag stripe transactions, such as the number of digits in an application transaction counter and a bitmap for an unpredictable number and the application transaction counter. The m/chip payment credentials 206 may include data elements specific to m/chip payment transactions, such as issuer action codes, risk management data, and offline data authentication object lists.” *Collinge (Ex. 1004)*, [0049]. Collinge’s card profile is stored in stored in Collinge’s mobile device storage 304. *Collinge (Ex. 1004)*, [0068] (“the remote-SE system 110 may then transmit the card profile including payment credentials for the account specified by the user 102 in step 502, which may then be stored by the mobile payment application 106 in the local encrypted database 304.”) Therefore, Collinge’s card profile which includes the PAN is stored in the storage 304 (encrypted local database) and at least transitorily stored by the processor when the PAN is received

by the mobile device from provisioning and when it is used by the mobile device to make a payment.

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

229. 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, Kranzley, another Mastercard reference, taught using a VPAN is used in place of a PAN as depicted below:

500 

VPAN <u>502</u>	PAN <u>504</u>	STATIC CARD VERIFICATION CODE <u>506</u>	COUNTER <u>508</u>	VPAN EXPIRY <u>510</u>
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 (Ex. 1013), Fig. 5.

230. Collinge also teaches that a virtual primary account number (VPAN) can be used as an alternative to the card PSN (PAN Sequence Number). '098 *Provisional* (Ex. 1008), 159 (“The use of a Virtual PAN can allow an Issuer to mitigate the risk of any misuse of a PAN value” and a “Virtual Pan can be used as a mechanism to provide segregation between the PAN (and PSN) value delivered to the Mobile Payment Application as part of a Card Profile[.]”) A PSN was known in the art to differentiate multiple cards linked to the same PAN. For example, U.S. Patent Appl. No. 2013/0151292 to Deloo et al. (“Deloo”) teaches that “[a] primary account hash sequence number (PSN) may be used to differentiate a primary card from an additional card on the same account.” *Deloo* (Ex. 1045), [0078]. As another example, Roberts, a Mastercard patent teaches that “a PAN Sequence Number...in combination with the PAN uniquely identifies the card.” *Roberts* (Ex. 1044), [0074].

2. *Smith's Teachings*

231. Smith teaches a “mobile device” that “may...be used...with a near field communications enabled purchasing transaction.” *Smith* (Ex. 1010), 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* (Ex. 1010), [0026].

232. This “temporary PAN is mapped to a **mobile PAN (e.g., such as a PayPass® PAN, or PPAN).**” *Smith (Ex. 1010)*, [0026] (emphasis added). The PPAN (device account number) is “assigned to the mobile device 104.” *Smith (Ex. 1010)*, [0016]. The PPAN is “stored in the mobile device 204.” *Smith (Ex. 1010)*, [0022].

233. Once an actual PAN is issued, the temporary PAN is swapped with the actual PAN. *Smith (Ex. 1010)*, [0026], [0040]. The PPAN (device account number) is then associated with a “related PAN[.]” *Smith (Ex. 1010)*, [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 (Ex. 1010)*, [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 (Ex. 1010), Fig. 6.

234. Smith’s “PPAN” (device account number) is “assigned to the mobile device 104.” *Smith (Ex. 1010), [0016]*. The PPAN is used in place of the actual PAN. *Smith (Ex. 1010), [0040]*. The PPAN is “stored in the mobile device 204.” *Smith (Ex. 1010), [0022]*. A POSITA would have understood that since Smith’s PPAN is specifically assigned to the mobile device it is device account number.

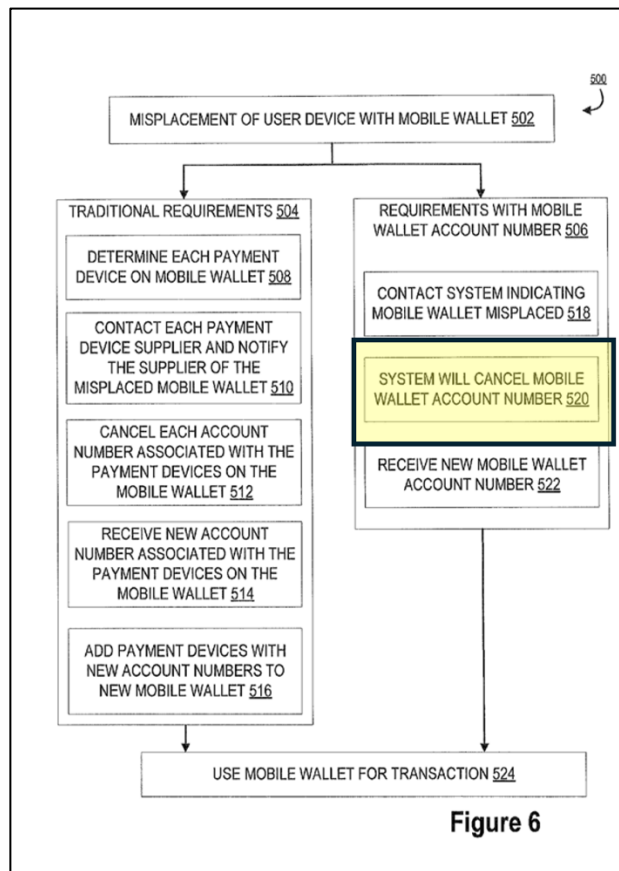
235. During a transaction “the point of sale device is provided with information including the PPAN stored in the mobile device 204” by using NFC. *Smith (Ex. 1010), [0024]*. Once the PPAN is sent the “payment network 218 identifies the PPAN and requests a look up of the related PAN from the

PAN mapping/account generation service 210.” *Smith (Ex. 1010)*, [0023]. Thus, supporting that the PPAN is different from the PAN.

236. The issuer can “implement dual account number structures” for “multiple NFC-enabled handsets may be managed for a single account.” *Smith (Ex. 1010)*, [0029]. It was well known that a dual account number has separate and distinct numbers for each device the overall account is used on. For example, U.S. Patent Appl. No. 2006/0186195 to Gray describes “[a]n additional benefit of having two separate but related numbers is that the consumer/cardholder may use the consumer account number to provide a third party the information to send the cardholder funds” via “a dual account number” *Gray (Ex. 1046)*, [0035]. Accordingly, a POSITA would have understood Smith’s PPAN is a distinct account number for a payment account on a particular “mobile device.”

237. Even if the same user wants to register a new device, a user will get a different PPAN for that device to use because the PPAN is assigned immediately upon registering the device. *Smith (Ex. 1010)*, [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.

238. Smith's PPAN is a static number; Smith teaches the expiration date associated with the account may be updated without updating the PPAN. *Smith (Ex. 1010)*, [0041] ("update an NFC-enabled payment account (e.g., to update an expiration month and/or year"). Therefore, a POSITA would have understood that Smith's PPAN is static for each PAN, in other words if a user registers multiple cards with underlying PANs, each PAN would have its own static PPAN. *See '286 Patent (Ex. 1001)*, claim 20. This was well known in the art. For example, Grigg teaches "[i]f the user misplaces "the user device 204, the user 202 may request cancellation of the mobile wallet account number." *Grigg (Ex. 1047)*, [0074], Fig. 6. A POSITA would have appreciated that such a modification would have improved card management, allowing the mobile wallet account number to be canceled if Collinge's mobile device is lost or compromised without affecting other devices using the same underlying PAN. Likewise, a POSITA would have been motivated to reject attempts to use an expired credit card number to prevent cardholders whose old cards are disposed of improperly of fraud.



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

3. Motivation To Combine

239. For many reasons, a POSITA would have found it obvious and been motivated to use Smith's mobile wallet account number in place of Collinge's PAN in Collinge's payment credential, akin to the Virtual PAN already taught by Collinge. '098 Provisional (Ex. 1008), 159-160.

240. A POSITA would have found it obvious and would have been motivated to use Smith's PPAN in place of the PAN in Collinge's static payment credentials because both Collinge and Smith expressly recognize that it is beneficial

to use an alternative to traditional financial institution account numbers when making a payment using a mobile device. Collinge teaches that an alternative payment number (which is calls a Virtual Primary Account Number or VPAN) is safer and can “mitigate the risk of any misuse of a PAN value”). *'098 Provisional (Ex. 1008)*, 159-160. Smith teaches a “PPAN” (device account number) that is used in place of the PAN/account number. *Smith (Ex. 1010)*, [0040]. Since Colline 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.

241. 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 (Ex. 1010)*, [0022]. Smith also teaches the issuer has to “requests a look up of the related PAN from the PAN mapping/account generation service 210.” *Smith (Ex. 1010)*, [0023]. Both supporting that the PAN does not need to be stored in Smith’s device.

242. It was well known in the art that a device without a secure element (SE), such as Collinge’s mobile device, could be vulnerable to malicious attacks and therefore, storing Smith’s PPAN instead of the PAN on Collinge’s mobile device would have increased security for the user’s account. *See Ghosh (Ex. 1048)*, 51

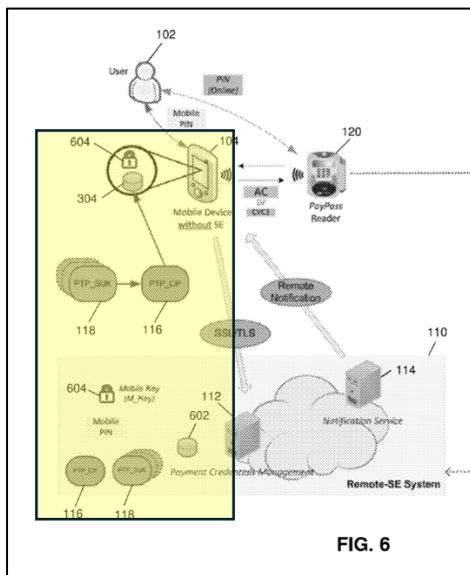
(“Without a secure infrastructure for computing on the device, achieving secure m-commerce may not be possible.”); *Collinge (Ex. 1004)*, [0003]-[0004]. (“In order to achieve this, mobile phones with secure element hardware (e.g., a Secure Element chip) are used to securely store payment account credentials, such as credit card credentials. However, not all mobile devices have secure elements. Furthermore, some issuers may not have access to a secure element on a mobile device, even if the mobile device has one available. As a result, a consumer who has a NFC-capable mobile device may not be able to use their device to conduct payment transactions if their mobile device lacks a secure element, and even in some cases where their mobile device has a secure element.”) For example, a POSITA would have understood that it is valuable to remove all traditional payment device account numbers from a user device so that if the device were stolen, the thief would have access only to PayPass PAN(s). *Bona (Ex. 1009)*, [0074]. A POSITA would have recognized that this is beneficial because if a user’s device is lost or stolen, only the PPAN(s) would have to be cancelled; automatic transactions using the traditional payment credentials (such as the credit card PAN) would not be impacted. *Bona (Ex. 1009)*, [0007], [0014], [0074], Fig. 6. For example, 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.

243. A POSITA would have had a reasonable expectation of success in implementing Smith’s PPAN in Collinge’s mobile payment application without undue experimentation because Collinge already teaches use of a Virtual PAN as an alternative to the card PAN and PSN (PAN Sequence Number) and a POSITA would have been familiar with using PAN-alternatives, particularly when making mobile PayPass payments. *See ’098 Provisional (Ex. 1008)*, 159-160 In the combination, Smith’s PPAN would perform the same function—provide an alternative account number that can be used for a payment transaction. *Smith (Ex. 1010)*, [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 (Ex. 1010)*, [0024].

244. In the proposed combination of Collinge and Smith, Collinge’s mobile device would receive the assigned PPAN(s) taught by Smith, in place of PAN information in Collinge’s payment credentials provisioned to the mobile payment application as part of Collinge’s card profile 116. *Collinge (Ex. 1004)*, [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.”); [0049] (“The common payment credentials “may include all data elements common to any type of payment transactions, such as both mag stripe and m/chip payment transactions. Such data elements may include payment account number, tracking data, and card layout description data.”)



Collinge (Ex. 1004), Fig. 6 (annotated excerpt). A POSITA would have appreciated that Smith already demonstrated feasibility of such a system. Collinge already receives the card profile (PTP_CP) through the remote-SE cloud system. *Collinge (Ex. 1004)*, 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 (Ex. 1013), Fig. 5.

245. 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 (Ex. 1004), [0068]; Smith (Ex. 1010), [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 (Ex. 1004), [0048]-[0049], [0063].*

246. It was well known in the art that storing sensitive information such as a PAN in fewer locations can lessen the risks of the sensitive information being compromised. For example, PCI SSC teaches that "[s]toring tokens instead of PANs

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

247. Likewise, a POSITA would have substituted Smith’s PPAN for Collinge’s PAN when making payment transactions, as taught by Smith. *Smith (Ex. 1010)*, [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 (Ex. 1010)*, [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.

248. 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 Bona’s payment card device in place of the PAN to better protect sensitive financial information.

J. 1(d)(2) secrets limited to the computing device, and

249. Collinge’s processor is operable to at least transitorily store a local storage encryption key, unique identifier, single use key, and key request (secrets limited to the computing device).

1. local storage encryption key

250. Collinge’s local storage encryption key is “generated by the mobile payment application” and used to “provide the storage 304 as an encrypted local database.” *Collinge (Ex. 1004)*, [0063]. A POSITA would have understood the local storage encryption key is private information (secrets) limited to Collinge’s

computing device because it is specifically used to encrypt the “local database” on Collinge’s computing device. *Id.* Collinge’s local storage encryption key is likewise limited to the computing device because it is generated by Collinge’s mobile device and not received by or shared with an external device.

251. Collinge teaches that Collinge’s *processor* is operable to store secrets limited to the computing device (i.e., local storage encryption key) because Collinge’s local storage encryption key is stored in memory (storage 304) and at least transitorily stored by the processor when the local storage encryption key is used by the mobile device to encrypt the storage 304 as an encrypted local database. *Collinge (Ex. 1004)*, [0063]. A POSITA would have understood that an encryption key must be at least transitorily stored by a processor in order to be used to encrypt or unencrypt data stored in memory. Therefore, Collinge’s local storage encryption key is limited in distribution since the local storage encryption key is generated on Collinge’s mobile device and stays on Collinge’s mobile device.

2. unique identifier

252. Collinge’s mobile payment application also generates “a **unique identifier** and additional values and keys, such as a local database storage key (e.g., mobile storage key).” *Collinge (Ex. 1004)*, [0093] (emphasis added). A POSITA would have understood Collinge’s unique identifier is private information (secrets)

limited to Collinge's computing device because it is generated by Collinge's mobile device and is unique and only identifies Collinge's mobile device. Therefore, Collinge's unique identifier is limited in applicability to other mobile devices and only identifies Collinge's mobile device.

253. Collinge teaches that “[t]he 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 (Ex. 1004)*, [0041] (emphasis added). Since Collinge's device generates the unique identifier, a POSITA would have understood that those values must be at least at least transitorily stored by the processor when generated by the mobile device because the processor is what generates the unique identifier.

4. *key request*

254. Collinge's mobile device also generates a “key request, wherein the key request includes at least a mobile identification number (PIN) and the profile identifier.” *Collinge (Ex. 1004)*, [0011]. A POSITA would have understood the key request is private information (secrets) limited to Collinge's computing device. Collinge's key request is likewise limited to the computing device because it is generated and for use only by Collinge's mobile device. Therefore, Collinge's key

request is limited in applicability to other mobile devices and only originates from Collinge's mobile device.

255. Since Collinge's device generates the key request, a POSITA would have understood that the key request must be at least at least transitorily stored by the processor when generated by the mobile device because the processor is what generates the key request.

5. *single use key*

256. Collinge is provisioned a **single use key** that “includes at least the profile identifier, an application transaction counter, and a generating key for use in generating a payment cryptogram” by Collinge's “mobile payment application” *Collinge (Ex. 1004)*, [0011], [0070]. Collinge's single use key and the components within the single use key, (*secrets*) are likewise limited to the computing device and for use only by Collinge's computing device when the single use key is used by Collinge's “mobile payment application” for generating a payment cryptogram. *Collinge (Ex. 1004)*, [0011], [0070].

257. Collinge teaches generating a CVC3 based on at least: “the supplied CVC3 value, the session key unpredictable number, the application transaction counter, and the reader unpredictable number.” *Collinge (Ex. 1004)*, [0145].

258. Collinge also stores “the single use key 118 in the local encrypted database 304.” *Collinge (Ex. 1004)*, [0076]. Collinge’s single use key is at least transitorily stored by the processor when the single use key is used by the mobile device to generate a payment cryptogram and when being provisioned to be stored in Collinge’s local encrypted database 304. *Collinge (Ex. 1004)*, [0011], [0070], [0145]; *’248 Provisional (Ex. 1006)*, Table 1. Therefore, Collinge’s single use key is limited in applicability to other mobile devices and only is for use in generating a payment cryptogram by Collinge’s mobile device.

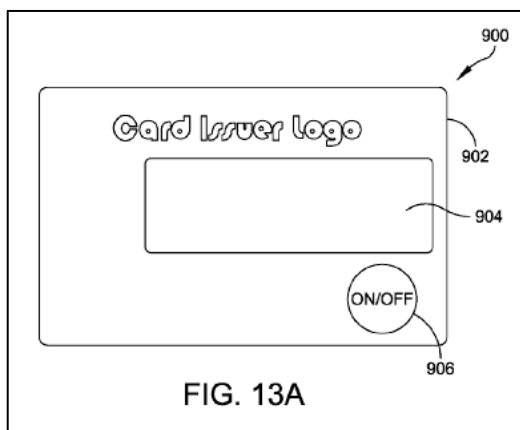
K. 1(e): wherein the computing device is operable to receive, store and transmit a card payment information not visible on the payment card device, and

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

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

1. Bona's Teachings

261. As I described above, when Bona's card is off, there is no information on the display of the payment card device, as shown in Figure 13A below. *Bona (Ex. 1009)*, [0110]. ("The smart card includes an on/off button 906 for powering the smart card on/off and a display 904 for displaying information to the user.")



Bona (Ex. 1009), Fig. 13(a). As I discussed above in detail, when Bona's companion card 900 is powered on, Bona teaches and a POSITA would have understood that payment information is not required to be shown on a payment card in order to perform a transaction via a magnetic stripe terminal at a POS reader. *Claim 1(a)*, *supra*.

2. Collinge's Teachings

262. Collinge's mobile device receives, stores, and transmits card payment information, including at least a PAN (modified to be a PPAN in combination per Smith, as discussed at claim 1(d)(1)) and an ATC.

263. Collinge's mobile device receives "keys, **payment credentials**, and an **application transaction counter**" that are "provisioned from the cloud system 302 to the mobile device 104 and stored in the storage 304." *Collinge (Ex. 1004)*, [0053] (emphasis added).

264. Collinge's mobile device stores "keys, **payment credentials**, and an **application transaction counter**" that are "...stored in the storage 304." *Collinge (Ex. 1004)*, [0053] (emphasis added).

265. Collinge's mobile device transmits "the generated cryptogram and **payment credentials** to a point-of-sale terminal 120." *Collinge (Ex. 1004)*, [0070] (emphasis added). Collinge also teaches that "the application transaction counter may be transmitted, via near field communication, to the point-of-sale terminal 120 for including in an authorization request in a financial transaction." *Collinge (Ex. 1004)*, [0145].

266. Collinge's **payment credentials** are "payment credentials corresponding to the associated payment account and a profile identifier[.]" *Collinge (Ex. 1004)*, Abstract. Specifically, Collinge teaches that the "Payment Token Payload – Card Profile (PTP_CP_ contains **the Payment Credentials required to perform a [MasterCard] PayPass transaction**" including "data elements such as: **PAN, PSN + Track Data.**" '098 *Provisional (Ex. 1008)*, [0101] (emphasis added).

267. Accordingly, a POSITA would have understood that Collinge teaches receiving, storing, and transmitting at least a PAN and ATC (card payment information), which is not visible on Bona's companion card 900 (*the payment card device*).

3. *Motivation to Combine*

268. *See* Claim 1(a).

L. 1(f): wherein the processor is operable to generate at least a portion of a limited-use card payment information for use by an authenticated card user, and

269. *See* Claim 15(c).

M. 1(g): wherein the computing device is operable to convey said limited-use card payment information via an interface of the computing device, and

270. *See* Claim 15(d).

N. 1(h): wherein a card issuer authority is operable to reject as invalid a transaction attempt outside of its limitations of use,

271. *See* Claim 15(g).

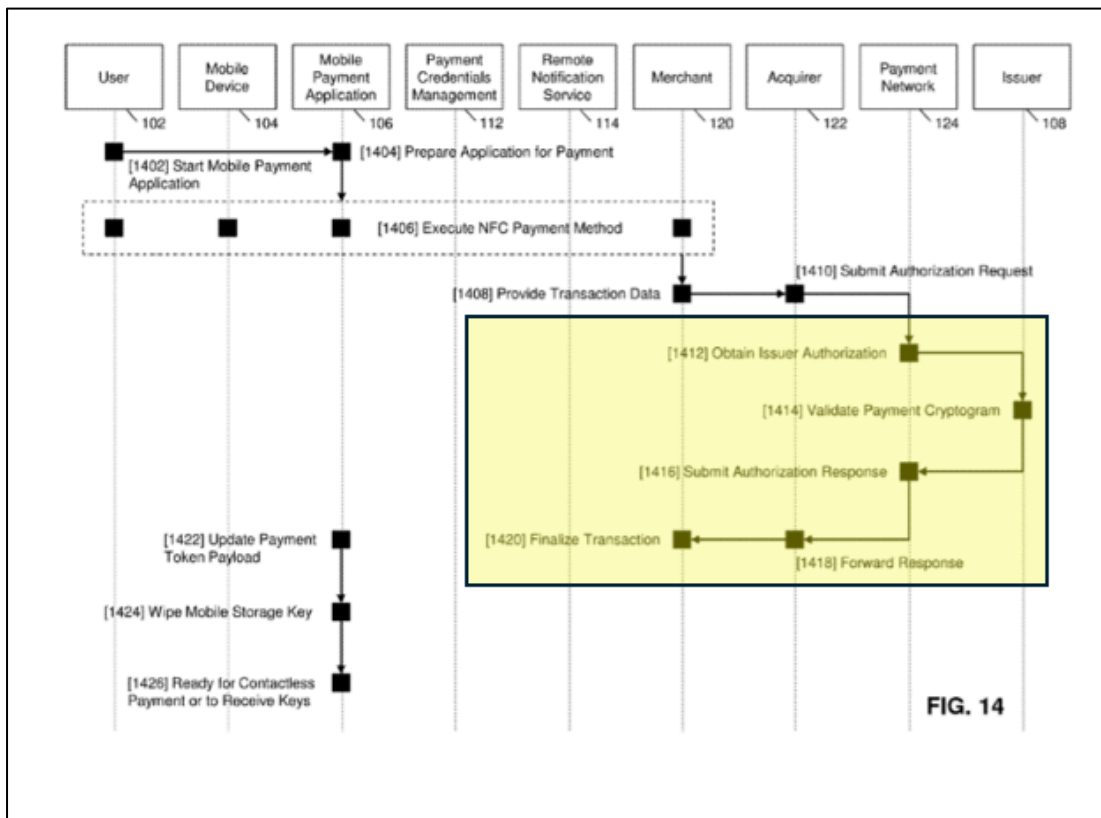
O. 1(i): wherein a card issuer authority is operable to validate a card payment information as authentic when received from at least one of: an authenticated users payment card; and an authenticated users computing device, and

272. *See* Claim 15(f).

P. 1(j): wherein the card issuer authority is operable to permit the authentic transactions to complete.

273. As discussed above, Collinge teaches that a transaction from a valid user within the limitations of use of the payment method (*authentic transactions*) will be approved by the issuer 108 (*card issuer authority*) and permit[ted]...to complete. *See* Claim 15(f).

274. Collinge further teaches that issuer 108 validates the payment cryptogram and if validation/authentication is successful may “approve the payment transaction” or if validation/authentication is unsuccessful, the card issuer may “deny the payment transaction.” *Collinge (Ex. 1004)*, [0077]. As taught by Collinge, once the issuer approves a transaction, the issuer will “notify the payment network124.” *Collinge (Ex. 1004)*, [0121]. Based on this notification, “the payment network 124 may submit an authorization response to the acquirer 122, which may then forward the response to the merchant 306 and/or point-of-sale terminal 120 at step 1418.” *Collinge (Ex. 1004)*, [0121]. After the merchant or point of sale terminal receives the authorization response, “the merchant may finalize the payment transaction, such as by providing the transacted goods or services to the user 102 or by providing a receipt to the user 102.” *Collinge (Ex. 1004)*, [0121].

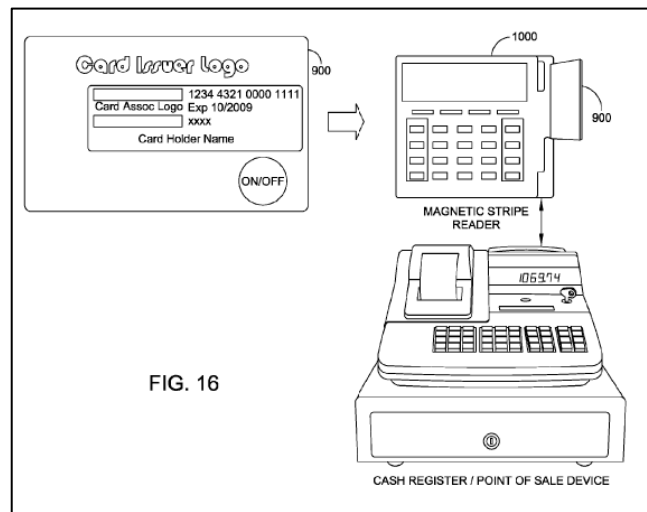


Collinge (Ex. 1004), Fig. 14 (annotated). A POSITA would have understood that the issuer approving a transaction based on validating the payment cryptogram, therefore permitting the transaction to complete.

Q. Claim 5: The system of claim 1, wherein the payment card device is absent a payment number information necessary for completing an online transaction, and wherein the information presented on an interface of said card device, are limited to an in-store merchant card reader facility use only.

275. Collinge, in view of Bona, renders obvious a payment card device (Bona's companion card 900) without any information on the display (absent a payment number information). See Claim 1(e); *Bona (Ex. 1009)*, [0109].

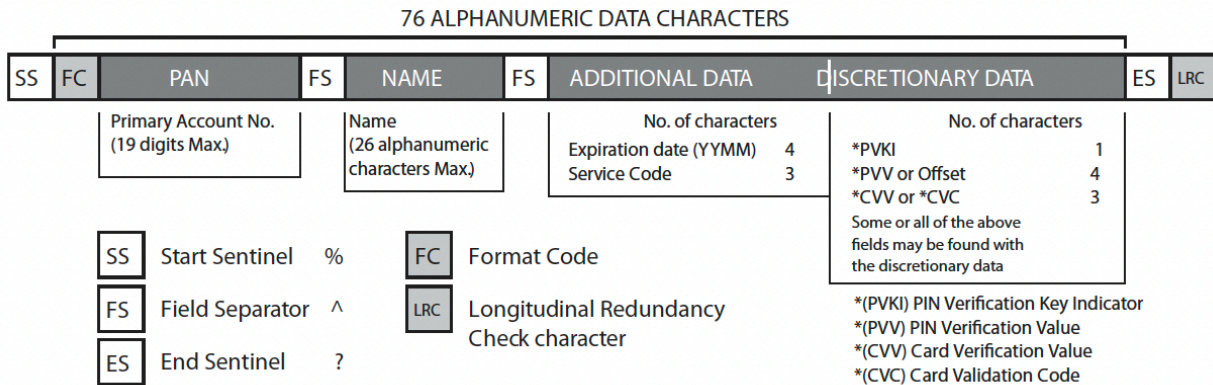
276. Collinge teaches the transaction with Bona's card is limited to an in-store merchant card reader facility only, for example by receiving a reader unpredictable number from a point-of-sale terminal that is used to generate a single use cryptogram. The transaction would not be able to be processed online in this instance. For example, Collinge's mobile device receives "a reader unpredictable number...via near field communication, from a point-of-sale terminal (e.g., the point-of-sale terminal 120)." *Collinge (Ex. 1004)*, [0145]. As discussed above, Collinge generates the CVC3 based in part on a reader unpredictable number. *See Claim 1(f)*. (Collinge teaches generating a CVC3 based on the following values: "the supplied CVC3 value, the session key unpredictable number, the application transaction counter, and the reader unpredictable number." *Collinge (Ex. 1004)*, [0145].) A POSITA would have understood Collinge's CVC3 is limited to an in-store transaction and therefore the information Bona's companion card 900 presents during a magnetic stripe transaction is limited to an in-store merchant card reader facility use only (e.g., magnetic card reader). For example, Bona's NFC-enabled companion card is operable for use in payment card reader equipment, such as "a traditional magnetic stripe reader" *Bona (Ex. 1009)*, [0125].



Bona (Ex. 1009), Fig. 16.

277. Bona teaches transmission of only “necessary data for display on the NFC enabled companion card 900 for use in the transaction” and a POSITA would understand that showing payment information on the face of Bona’s card is not necessary when conducting a magstripe transaction. *Bona (Ex. 1009)*, [0109]; *see also* claim 1(a). It was well known that during a magstripe transaction, the data necessary was located in the track data of for example, a card. For example, track 1 data includes the following:

Card Data Format - Track 1

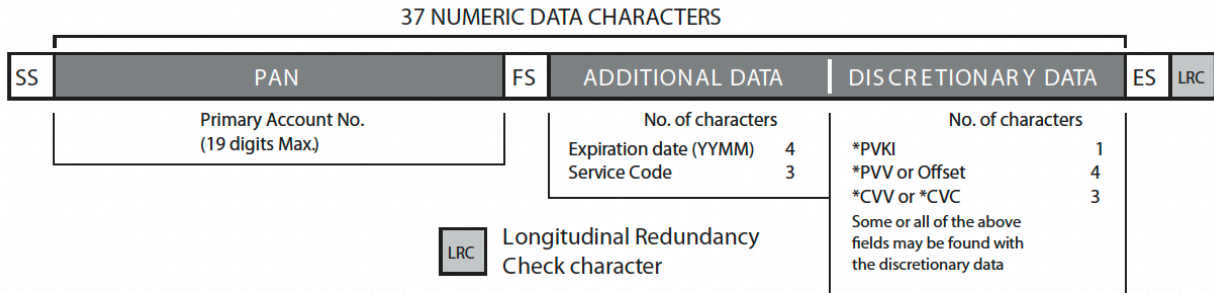


MagTek (Ex. 1022), 1. On a card's track:

“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. 1009), [0102]. Track 2 data includes the following data:

Card Data Format - Track 2

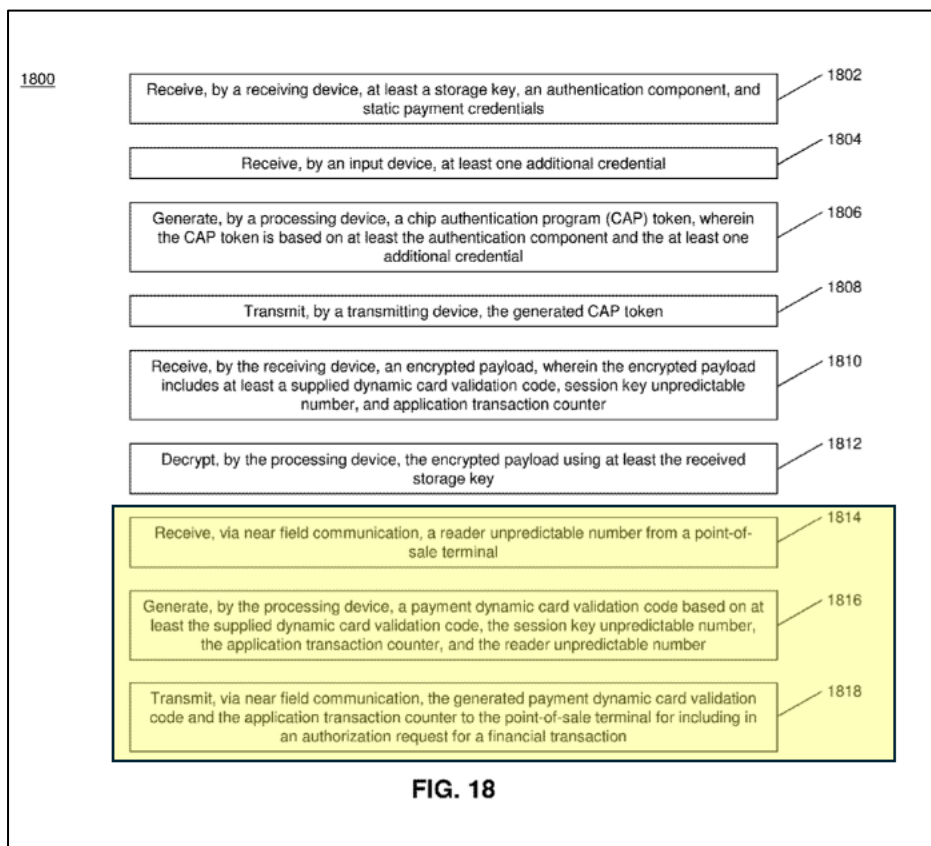


MagTek (Ex. 1022), 1.

R. Claim 8: The system of claim 1, wherein the computing device is further operable to transceive the limited-use card payment information via an NFC interface of the computing device in an in-store NFC reader facility transaction.

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

279. Collinge further teaches receiving a reader unpredictable number (UN_{READER}) from a “point-of-sale terminal” via “near field communication” which is then used to generate the payment cryptogram (e.g., CVC3 value). *Collinge (Ex. 1004), [0145].*

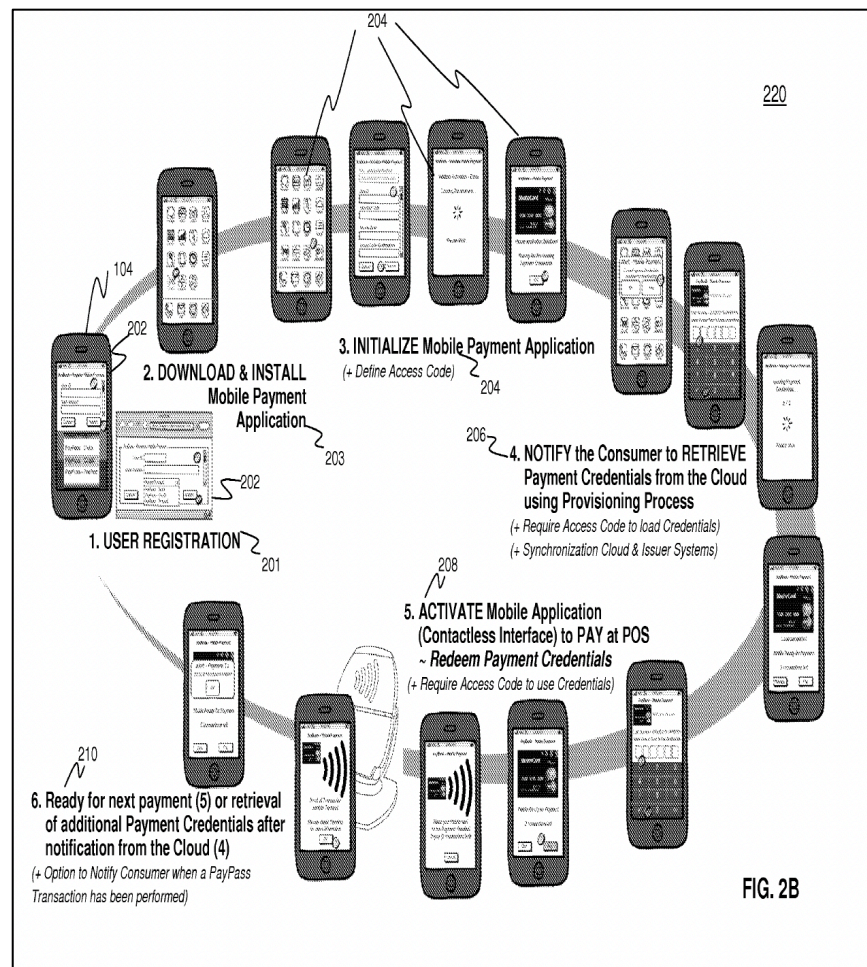


Collinge (Ex. 1004), Fig. 18 (annotated). Therefore, Collinge's mobile (computing) device is further operable to receive limited-use card payment information (since the UN_{READER} is used in generating a payment cryptogram – limited use card payment information) via an NFC interface of the computing device in an in-store NFC reader facility transaction.

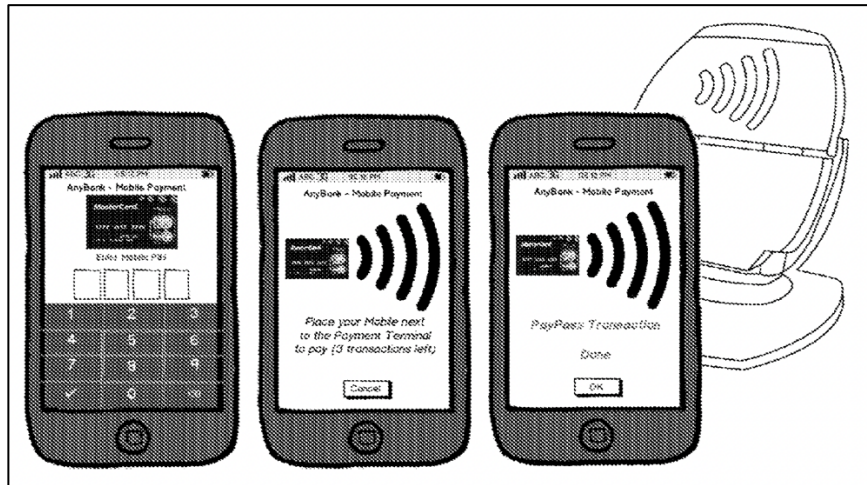
S. Claim 11(a): The system of claim 1, further comprising a touch-screen user interface control for a user approving and denying a transaction,

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

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



'248 Provisional (Ex. 1006), Fig. 2B(excerpt). Collinge's user interface instructs the user to provide a PIN and then "place your Mobile next to the Payment Terminal to pay":



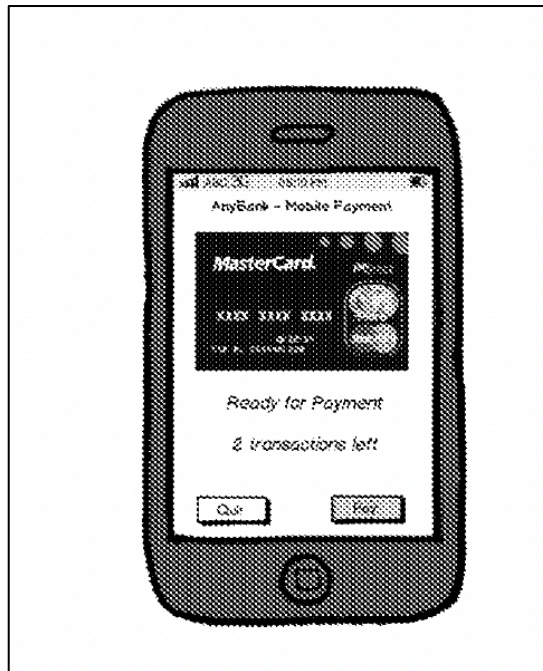
'098 Provisional (Ex. 1008), 99; '248 Provisional (Ex. 1006), Fig. 2B; see Claim [15(d)].

282. Collinge also teaches that the user may press the button cancel to deny the NFC transaction.



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

283. Collinge further teaches the user may “quit” or “pay” during a transaction.



'098 Provisional (Ex. 1008), 100; '248 Provisional (Ex. 1006), Fig. 2B. A POSITA would have further understood that by selecting “pay,” a user would approve the transaction and by selecting “quit” the user would deny the transaction.

T. 11(b): and wherein a card issuer authority is further operable to deny as authentic, a card payment transaction from a user-denied transaction, and to approve as authentic a card payment transaction from a user-approved transaction.

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

U. Claim 14: The system of claim 1, wherein a payment issuing authority is operable to decline transactions performed by the payment card device when a user fails at least one security challenge presented to a user by the computing device.

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

1. Bona's Teachings

286. Bona teaches that "the user is authenticated, such as using biometrics if the cell phone (or smart card) has biometric capabilities or a PIN or password authentication scheme." *Bona (Ex. 1009)*, [0120].

2. Collinge's Teachings

287. Per Collinge's teachings a payment issuing authority (issuer) can decline transactions when a user fails to accurately "provide a mobile PIN for

authentication” via “an input device (e.g., of the mobile device 104, such as a touch screen) [.]” *Collinge (Ex. 1004)*, [0051], [0076]-[0077], [0133].

3. *Motivation to Combine*

288. It would have been obvious and a POSITA would have been motivated to decline a transaction performed by Bona’s companion card where the user input an incorrect mobile PIN on Collinge’s mobile device. Collinge and Bona both expressly teach requiring user authentication with a PIN. For example, Bona teaches “the user is authenticated, such as using biometrics if the cell phone (or smart card) has biometric capabilities or a PIN or password authentication scheme.” *Bona (Ex. 1009)*, [0120]. Collinge teaches “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 (Ex. 1004)*, [0051]. Collinge teaches that this results in “additional security for the user 102, the issuer 108, and the merchant involved in the payment transaction.” *Collinge (Ex. 1004)*, [0051]; *see also* [0076]-[0077]. Collinge teaches that in the case of an incorrect PIN, the issuer may “not authorize” the transaction. *Id.* As discussed above, Collinge and Bona teach and it would have been well-known to a

POSITA that in a secure payment system, an unauthenticated user should not be permitted to make any payment via card or via the mobile device.

289. A POSITA would have had a reasonable expectation of success implementing Collinge's teaching of an issuer declining a payment transaction when an incorrect PIN is entered to payment transactions conducted using Bona's companion card because in either case the issuer receives payment information indicating that the PIN-based authentication challenge failed. Such an application of Collinge's teachings would have predictably improved the security of Bona's card and would have provided expected results. A POSITA would have recognized that applying these teachings to Bona's payment card would be a combination of prior art elements according to known methods would have predictably provided the user with greater control over use of Bona's companion card and a more secure payment system. A POSITA would have had a reasonable expectation of success in making such a combination, including because using a phone to control functions of a card device was well known to a POSITA.

V. Claim 20(Pre) A payment system comprising:

290. *See* Claim 1(Pre).

W. 20(a): a payment card device, free of any depictions of fixed payment numbers thereon, and operable for use in payment card reader equipment; and

291. *See* Claim 1(a).

X. 20(b): a computing device comprising:

292. *See* Claim 1(b).

Y. 20(b)(1): a processor;

293. *See* Claim 1(b).

Z. 20(b)(2): a memory;

294. *See* Claim 1(b)(1).

AA. 20(b)(3): a wireless interface;

295. *See* Claim 1(b)(2).

BB. 20(b)(4): a touch-screen user interface operable to provide a visual user-interface for user payment interactions; and

296. *See* Claim 1(b)(3).

CC. 20(b)(5): a user-input device coupled to the processor; and

297. *See* Claim 1(c).

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

298. As discussed above, these values are stored in Collinge's memory (storage 304). *See* Claims 1(d), 1(d)(1), and 1(d)(2).

EE. 20(d): wherein the computing device is operable to receive, store, display and transmit issuer-provided payment information, associated with, but not depicted on, the payment card device;

299. A POSITA would have understood that Collinge's payment credentials (modified by Smith to include a PPAN in place of the PAN) comprise issuer-

provided payment information (PAN). *See* Claim 1(e). Smith's PPAN is assigned by the financial institution application 258 and is issuer-provided payment information. *Bona (Ex. 1009)*, [0051].

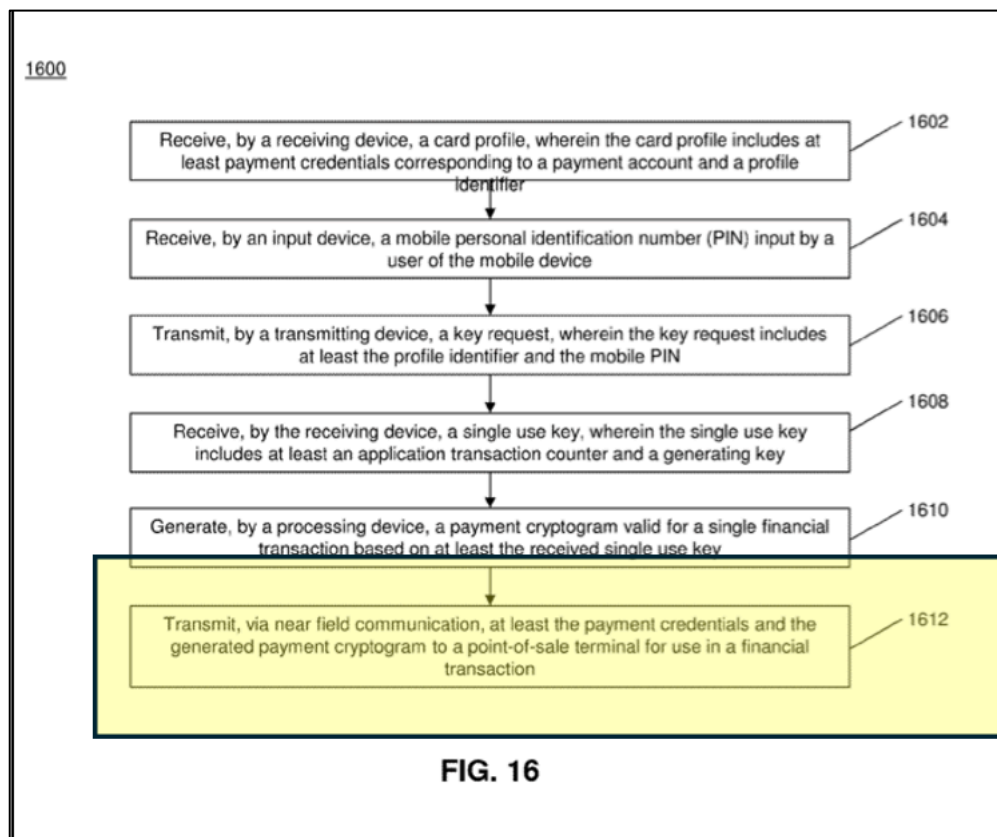
FF. 20(e): wherein the processor is operable to dynamically generate at least a portion of a limited-use payment information for use by an authenticated card user,

300. *See* Claim 1(f).

GG. 20(f): and to combine said at least a portion of the limited-use payment information with at least said static device account number to create combined payment information;

301. As discussed above, Collinge, in view of Smith, renders obvious creating combined payment information, including a CVC3 (*limited-use payment information*) and mobile wallet account number (*static device account number*) when sending complete payment information to a POS terminal via Collinge's NFC interface. *See* Claim 1(d)(1). Collinge also teaches generating payment cryptogram (*limited-use payment information*). *See* Claim 1(f).

302. 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 (Ex. 1004)*, [0070], [0077].



Collinge (Ex. 1004), Fig. 16 (annotated); *Collinge (Ex. 1004)*, [0048], Fig. 6, [0104] (card profile (PTP_CP)); *'098 Provisional (Ex. 1008)*. The card profile includes “at least payment credentials corresponding to the associated payment account and a profile identifier[.]” *Collinge (Ex. 1004)*, Abstract. Specifically, *Collinge* teaches that the “Payment Token Payload – Card Profile (PTP_CP_ contains the **Payment Credentials required to perform a [MasterCard] PayPass transaction**” including “data elements such as: **PAN**, PSN + Track Data.” *'098 Provisional (Ex. 1008)*, [0101] (emphasis added).

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

1. Motivation to Combine

304. As discussed above, Smith's PPAN would be used instead of a PAN in Collinge's payment system. *See* Claim 1(d)(1).

HH. 20(g): wherein the computing device is operable to convey said combined payment information via an interface of the computing device; and

305. *See* Claim 20(f).

II. 20(h): wherein the computing device is operable to receive information, from an issuer, in response to the conveyed combined payment information, indicating that a payment transaction is valid.

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

JJ. Claim 21: The system of claim 20 wherein the computing device is operable to wirelessly receive the static device account number.

307. *See* Claim 7.

KK. Claim 22: The system of claim 20, wherein the processor is operable to dynamically generate the at least a portion of a limited-use payment information based on a transaction sequence counter count, and further wherein the generated limited-use payment information is valid for a single use.

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

LL. Claim 23: The system of claim 22 wherein the processor is operable to dynamically generate the at least a portion of a limited-use payment information further based on payment processing authority secrets.

309. As discussed above, Collinge teaches that the payment cryptogram (limited-use payment information) is generated by the processor of Collinge's mobile phone based, in part, on an ATC, UN_{CLOUD} , and the KSUN (secrets). *See* Claim 1(f). Collinge further teaches that the ATC, UN_{CLOUD} , and the KSUN (secrets) are shared with an issuer (*payment processing authority*).

310. As discussed in Claim 1(i), the issuer uses the ATC, UN_{CLOUD} , and the KSUN to authenticate the payment cryptogram. *Collinge (Ex. 1004)*, [0077], [0145]. Therefore, these values are also issuer secrets as these values are specifically used by Collinge's mobile device to generate a payment cryptogram and the issuer (*payment processing authority secrets*) to validate Collinge's generated payment cryptogram.

MM. Claim 24: The system of claim 23 wherein the processor is operable to dynamically generate the at least a portion of a limited-use payment information further based on the static device account number.

311. *See* Claim 20(k).

NN. Claim 25: The system of claim 24 wherein the computing device is operable to wirelessly receive the static device account number.

312. *See* Claim 21.

OO. Claim 26: The system of claim 22 wherein the processor is operable to dynamically generate the at least a portion of a limited-use payment information further based on the static device account number.

313. *See* Claim 20(k).

PP. Claim 27: The system of claim 26 wherein the computing device is operable to wirelessly receive the static device account number.

314. *See* Claim 21.

XII. OPINIONS REGARDING GROUND 3: CLAIMS 2, 3, AND 14 ARE OBVIOUS OVER COLLINGE IN VIEW OF BONA, SMITH, AND PATTERSON

A. Claim 2: The system of claim 1, wherein the touch-screen user interface is operable to control an access for payment transactions by the card device, and is operable to enable as authentic payment transactions by the card device.

315. Collinge, in view of Bona as discussed in Claim 15(a), teach that the touch-screen user interface of Collinge's mobile device is used to (1) control the provisioning of payment credentials to Bona (control access for payment transactions) (*Bona (Ex. 1009)*, [0123]), and (2) authenticate payment transactions using, for example, a PIN or password. *Bona (Ex. 1009)*, [0120] ("the user is

authenticated, such as using biometrics if the cell phone (or smart card) has biometric capabilities or a PIN or password authentication scheme.”); *Collinge (Ex. 1004)*, [0093], [0123] (“the point-of-sale terminal 120 may be configured such that it may 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).”); *See also* Claim 15(c) and 15 (f).

316. Alternatively, *Collinge* and *Bona* in view of *Patterson* teach *Collinge*’s touch-screen user interface is operable to control access for payment transactions by *Bona*’s companion card (card device). *Collinge*’s touch-screen user interface is operable to enable as authentic (via a PIN) payment transactions by *Bona*’s companion card.

1. *Collinge*’s Teachings

317. *Collinge* teaches the registration process may be performed on a website. *Collinge (Ex. 1004)*, [0065]. (“The user 102 may register with the remote-SE system 110 using the mobile device 104 or another computing device, such as a desktop computer. Registration may be performed via a web browser, application program, or any other suitable method as will be apparent to persons having skill in the relevant art.”); [0089] (“At step 806, the user 102 may access the registration system of the remote-SE system 110. The user 102 may access the system via a web

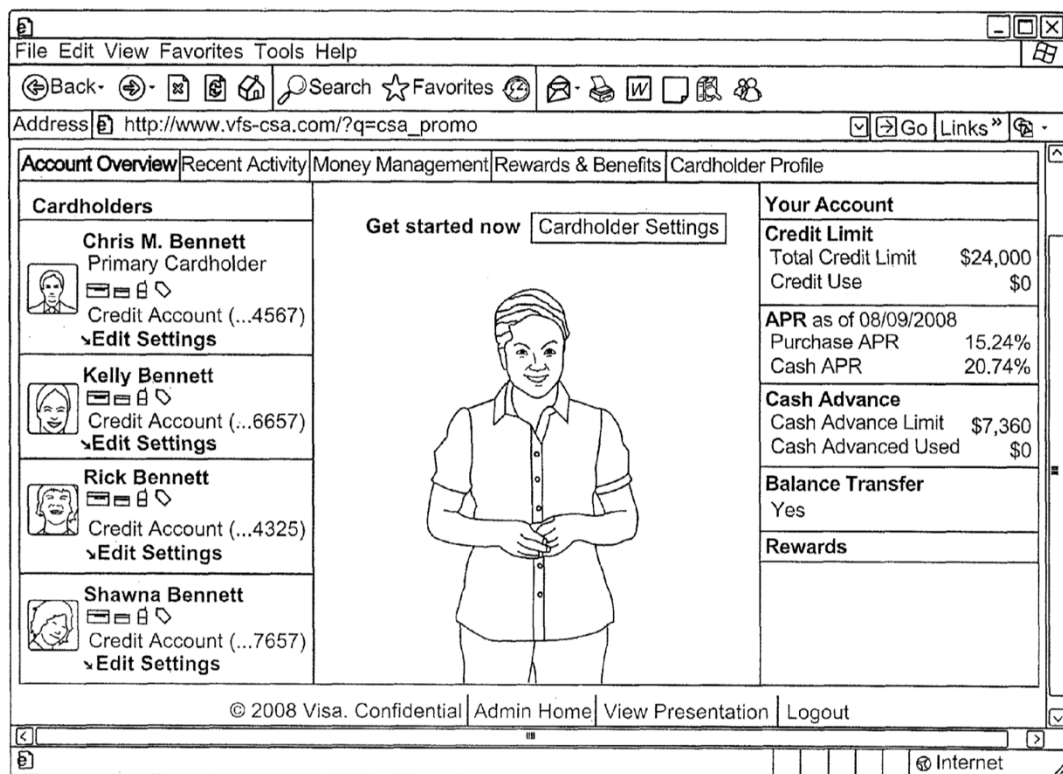
browser 804, which may be executed on a computing device. In one embodiment, the computing device may be the mobile device 104. The user 102 may navigate to a webpage hosted by or on behalf of the remote-SE system 110.”).

2. *Bona’s Teachings*

318. As discussed in Claim 15(a), Collinge’s mobile device allows Bona’s companion card to perform a transaction by provisioning Bona’s payment card payment credentials and a payment cryptogram. A motivation to combine was provided in Claim 15(a). As discussed in Claim 14, Collinge in view of Bona teaches that the payment issuing authority (issuer) can decline transactions performed by Bona’s companion card 900 (payment card device) when a user fails a security challenge presented to a user by Collinge’s mobile device (e.g., a request for a mobile PIN). Therefore, if the PIN is validated, then the transaction is therefore authentic. *See* Claims 1(f), 14, 15(c). Bona teaches that requiring a correct PIN to perform a transaction was well known. *Bona (Ex. 1009)*, [0007] (“Once the card has been verified as authentic, the customer enters a 4-digit PIN, which is checked against the PIN stored on the card; if the two match, the transaction completes.”), [0120] (“the user is authenticated, such as using biometrics if the cell phone (or smart card) has biometric capabilities or a PIN or password authentication scheme.”)

3. *Patterson’s Teachings*

319. Patterson teaches “a consumer 10 may be presented with a webpage via a client computer 16 to register for account level blocking, as shown in FIG. 7 and in step 405 of FIG. 4. This webpage or web application may be hosted at the payment processing network 40 or the issuer 50. A consumer may also register in other manners such as by phone, email, SMS, etc.” *Patterson (Ex. 1011)*, 6:12-16. The client computer may be a “a wireless phone[.]” *Patterson (Ex. 1011)*, 3:51-53.



Patterson (Ex. 1011), Fig. 7.

320. “As part of the registration, the consumer may be asked to provide identifying information to the registration web server, in order to authenticate to the server that the consumer is in fact who he claims to be. Once the consumer has been authenticated, he may then specify blocking criteria to be associated with one or more accounts. The use of such blocking criteria may allow the consumer 10 to place restrictions on his account that are more specific than restrictions that may be placed by the issuer 50 of the account.” *Patterson (Ex. 1011)*, 6:17-27.



FIG. 8

Patterson (Ex. 1011), Fig. 8. Patterson notes that:

Blocking criteria may include jurisdiction (e.g., countries or regions in which the transactions will not be allowed), merchant category code or merchant category group (e.g.,

type of business a merchant operates), merchant verification value (e.g., transactions that originate from a particular merchant, category of merchants, or list of merchants will not be allowed), payment channel (e.g., face-to-face, card not present, e-commerce), terminal ID (e.g., deny transactions that originate from specific terminals), transaction type (e.g., cash, POS purchase, quasi-cash, account funding transaction (AFT), original credit, payment), lost or stolen card (e.g., a “hotcard” list which will block all transactions from that card from being authorized), service code (e.g., a list of service codes from a card's magnetic stripe that should be blocked), recurring payment (e.g., stop all recurring transactions from specified merchants), single transaction limit, daily limit, or monthly limit.

Patterson (Ex. 1011), 6:28-46. A POSITA would have understood that a card designated as “lost or stolen” would be locked, as *Patterson* teaches that the issuer “will block all transactions from that card from being authorized.” *Patterson (Ex. 1011)*, 6:38-40. Likewise, terminal ID and transaction type restrictions control an access for payment transactions by the card device.

321. The transaction request will be “den[ied], using the server computer, the transaction clearing request if the transaction satisfies the stored blocking parameter.” *Patterson (Ex. 1011)*, Abstract. *Patterson* notes the “acquirer 30 and the issuer 50 may each have a server computer and a database associated with the server computer[.]” *Patterson (Ex. 1011)*, 4:35-38.

4. *Motivation to Combine*

322. It would have been obvious, and a POSITA would have been motivated to modify Collinge's payment system to allow a user to input blocking criteria for payment cards using Collinge's touchscreen (such as during Collinge's registration process), as taught by Patterson.

323. A POSITA would have been further motivated to have Collinge's issuer deny a transaction if "the transaction satisfies the stored blocking parameter" as proposed by Patterson. *Patterson (Ex. 1011)*, 4:35-38 ("acquirer 30 and the issuer 50 may each have a server computer and a database associated with the server computer[.]").

324. A POSITA would have understood that Collinge already teaches a similar process with a CAP token and control limits on purchase. *'095 Provisional (Ex. 1005)*, Claims 9-10 ("...an expiration date associated with a payment account; a merchant category corresponding to a point-of-sale (POS) terminal; a geographic location of a merchant; a spending limit for a payment account; a spending limit for a specified merchant category..."). Collinge teaches that these rules are in the form of "a chip authentication program (CAP) token" generated by Collinge's mobile device. *Collinge (Ex. 1004)*, [0054], [0084]; *'095 Provisional (Ex. 1005)*, 15 (The "CTVS [CAP token validation system] validates the CAP Token" and can be operated by...the Issuer."). Modifying Collinge to include Patterson's blocking

criteria would have been combining prior art elements according to known methods to yield the predictable results of increased security in Collinge's payment system and a POSITA would have had a reasonable expectation of success in making such a modification. A POSITA would have recognized that applying blocking criteria is useful to users who want to prevent overspending (by themselves or children as shown in figure 8 with multiple accounts), reduce fraud by preventing purchases on stores they do not frequent, or temporarily lock a card that may be stolen, or may be simply misplaced (rather than wholly cancel it).

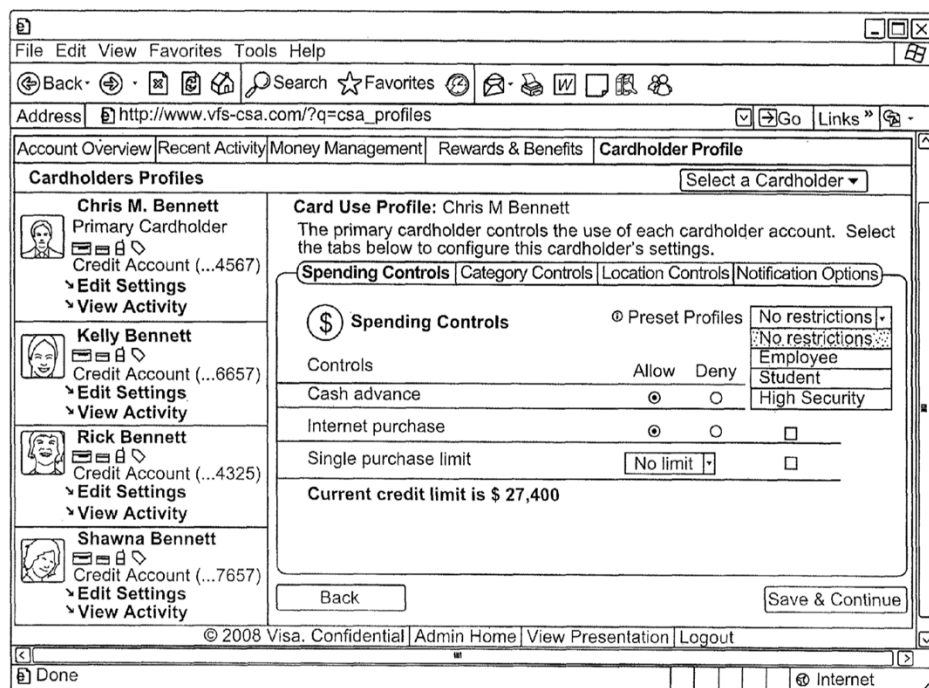


FIG. 8

Patterson (Ex. 1011), Fig. 8. Modifying Collinge to include Patterson's blocking criteria would have been combining prior art elements according to known methods

to yield the predictable results of increased security in Collinge's payment system and a POSITA would have had a reasonable expectation of success in making such a modification.

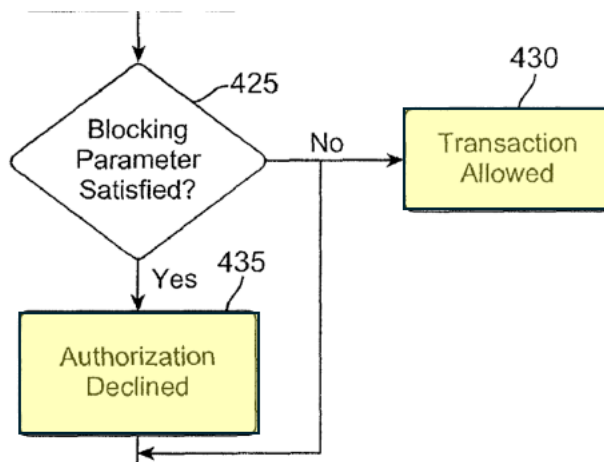
B. Claim 3: The system of claim 1, wherein the touch-screen user interface is operable to control an access of the card device for payment transactions at an NFC Card Reader facility, and is operable to enable and disable NFC payment transactions by the card device.

325. As discussed in Claim 2, one of the blocking criteria is "payment channel (e.g., face-to-face, card not present, e-commerce)" and "terminal ID (e.g., deny transactions that originate from specific terminals)" which would include transactions at an NFC Card Reader Facility, and therefore disable such transactions when the blocking criteria is present. *See* Claim 2; *Patterson (Ex. 1011)*, 6:28-46.

C. Claim 4: The system of claim 3, wherein the touch-screen user-interface is configurable for a locking and unlocking of payment transactions, and wherein a card issuer authority is further operable for denying a payment transaction from at least one of: a locked card device; and a locked card-users computing device, and wherein a card issuer authority is further operable to permit as authorized, a card payment transaction from an unlocked device.

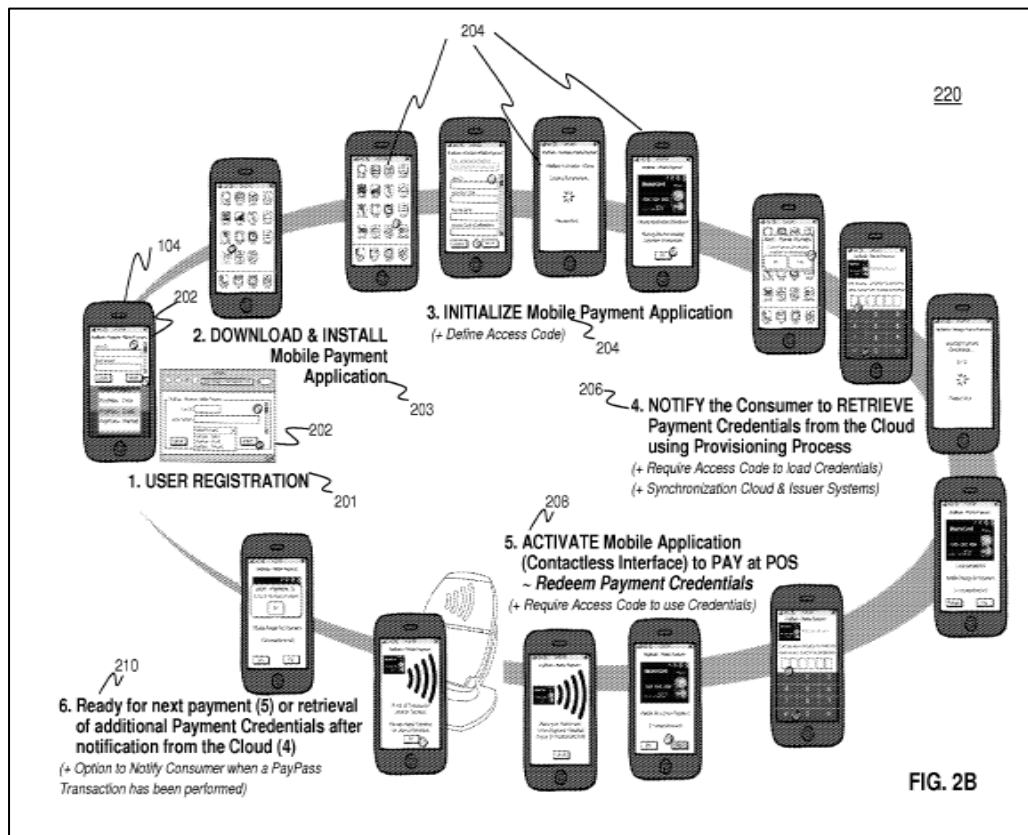
326. As discussed in Claim 2, Collinge-Bona as modified by Patterson teaches applying blocking criteria (locking and unlocking payment transactions). As also discussed in Claim 2, the card issuer authority will deny a payment transaction from a locked card device. *See* Claim 2. In the combined system, if the device is unlocked with no associated blocking criteria, a card issuer authority permits as

authorized, a card payment transaction as taught by Collinge and further supported by Patterson. *See* Claims 1(i)-1(j); *Patterson (Ex. 1011)*, Fig. 4.



Patterson (Ex. 1011), Fig. 4 (annotated excerpt).

327. Collinge teaches allowing a user to access (unlock) a mobile payment application by inputting a correct access code on Collinge's mobile device as shown below (require access code to load credentials).



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

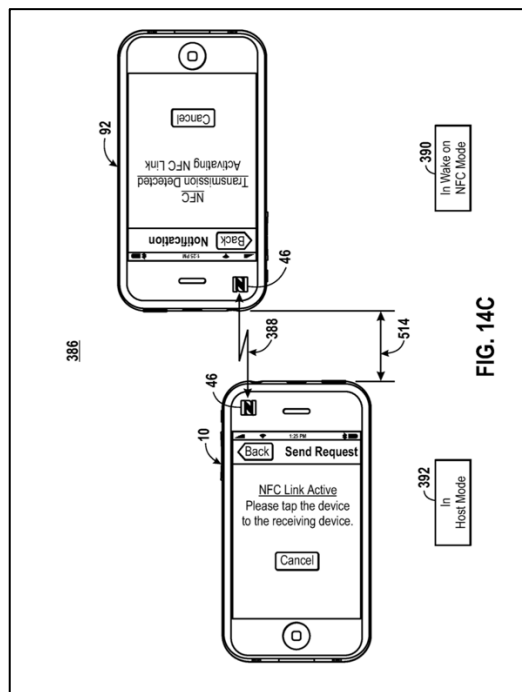
XIII. OPINIONS REGARDING GROUND 4: CLAIM 9 IS OBVIOUS OVER COLLINGE IN VIEW OF BONA, SMITH AND LIN

A. Claim 9: The system of claim 1, wherein the computing device is further operable to transceive the limited-use payment information wirelessly with another device via a wireless interface of the computing device, in a device-to-device transaction.

328. Collinge in view of Lin teaches transceiving limited-use payment information wirelessly from another device via a wireless interface of the computing device, in a device-to-device transaction.

1. Lin's Teachings

329. Lin depicts in Fig. 14C “the establishment of an NFC connection 388 between two devices, namely the payee device 10 and the payor device 92, by way of the tap operation 386 [.]” *Lin (Ex. 1012)*, 68:10-13.



Lin (Ex. 1012), Fig. 14C.

330. Lin teaches that once “active device 10 is placed within an acceptable distance 514 (e.g., 2-4 cm) from the payor device 92...the payor device 92 may transition from the passive to an active mode in which the NFC device 46 within the payor device 92 is powered on, thus enabling the payor device's 92 corresponding NFC interface 60 and providing the establishment of the NFC connection 388 between the payee device 10 and the payor device 92 through which the payment request may be transmitted.” *Lin (Ex. 1012)*, 68:13-25.

2. *Motivation to Combine*

331. It would have been obvious and a POSITA would have been motivated to modify Collinge's mobile phone to wirelessly receive and transmit limited-use payment information in a device-to-device transaction as taught by Lin. A POSITA would have recognized peer-to-peer payments options on mobile phones were becoming increasingly popular. For example, Bump Pay was released in 2012. *Tech (Ex. 1049)*, 1. Bump Pay only "works in-person." *Tech (Ex. 1049)*, 1. Bump Pay "lets you transfer money via PayPal to anyone in arm's reach." *Tech (Ex. 1049)*, 1. "To use the app, you just connect your PayPal account ahead of time, then type in the amount you want to pay, bump your iOS device against a friend's, and confirm the payment." *Tech (Ex. 1049)*, 1. A POSITA would have recognized that Collinge already teaches transmitting and receiving limited-use payment information from Collinge's mobile phone, and a POSITA would have recognized the value of the same payment information in a peer-to-peer transaction. *Collinge (Ex. 1004)*, [0044]; *Lin (Ex. 1012)*, Abstract, Fig. 14C. A POSITA would have appreciated that Lin's device-to-device payment was a known technique that could be used to improvise similar devices, like Collinge's mobile phone, in the same way, and therefore a POSITA would have had a reasonable expectation of success without undue experimentation in making such a combination.

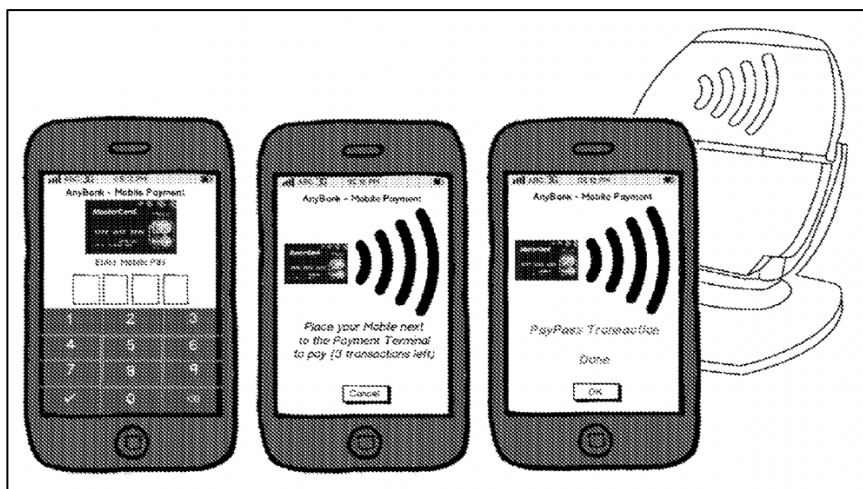
XIV. OPINIONS REGARDING GROUND 5: CLAIM 10 IS OBVIOUS OVER COLLINGE IN VIEW OF BONA, SMITH, AND KRANZLEY

A. Claim 10: The system of claim 1, wherein the computing device is further operable to transmit a payment information visually, in alphanumeric, graphical and iconography via the touch screen user interface.

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

1. Collinge

333. Collinge teaches a touch-screen user interface. *See* Claim 1(b)(3). Collinge further teaches graphically depicting a payment card as shown in the image below:



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

2. Kranzley

334. Kranzley teaches that “[t]he payment application of the mobile device 12 converts the data (including the PAN, expiry, and dynamic data) into a bar code image 13.” *Kranzley (Ex. 1013)*, [0028]. A POSITA would have understood that one example of Kranzley’s dynamic data would have included a CVC3, such as Collinge’s single use dynamic payment cryptogram. 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 (Ex. 1013)*, [0041]. The dynamic code is “generated based on the secret key and the value of a transaction counter” similar to Collinge. *Kranzley (Ex. 1013)*, [0042]. Collinge teaches generating a CVC3 based on at least: “the supplied CVC3 value, the session key unpredictable number, the application transaction counter, and the reader unpredictable number.” *Collinge (Ex. 1004)*, [0145].

335. Kranzley teaches “[o]ther bar code image formats may also be used (e.g., such as two-dimensional bar codes or other image formats that can hold at least 38 numeric digits of data and that are commonly used at merchant point of sale terminals).” *Kranzley (Ex. 1013)*, [0028]. The bar code image is “displayed on a display device 14 of the mobile device 12.” *Kranzley (Ex. 1013)*, [0033]-[0034]. “By allowing merchants to use their existing scanning equipment, embodiments

allow ready adoption of payments using mobile devices configured pursuant to the present invention.” *Kranzley (Ex. 1013)*, [0028].

336. Kranzley teaches displaying “the static VPAN...in plain text on a display device 14 of the mobile device 12 along with an expiry date and dynamic data)” *Kranzley (Ex. 1013)*, [0035], [0033]-[0036]. “The VPAN 502 may be, for example, an alphanumeric code (typically, in current systems, a sixteen digit numeric code)[.]” *Kranzley (Ex. 1013)*, [0065].

3. *Motivation to Combine*

337. A POSITA would have been motivated to modify Collinge’s mobile device to display payment information visually as an alphanumeric code, barcode and an image of a card via Collinge’s touch screen user interface such that the displayed information can be accepted at a merchant facility, as taught by Kranzley. A POSITA would have recognized that providing payment information visually as taught by Kranzley would provide the user and merchant with flexibility to accept payment in a variety of ways in the event that traditional card reader equipment is unavailable for nonfunctional. In fact Kranzley teaches “[b]y allowing merchants to use their existing scanning equipment, embodiments allow ready adoption of payments using mobile devices configured pursuant to the present invention.” *Kranzley (Ex. 1013)*, [0028].

338. A POSITA would have had a reasonable expectation of success in modifying Collinge based on Kranzley's teachings because these analogous references are both concerned with performing financial transactions with a mobile phone, both are assigned to Mastercard, and a POSITA would have been well-familiar with the operation of a GUI on a mobile device and how to modify that GUI to display various information, including payment information. *Kranzley* (Ex. 1013), Abstract; [0036]; *Collinge* (Ex. 1004), [0006].

XV. OPINIONS REGARDING GROUND 6: CLAIM 16 IS OBVIOUS OVER COLLINGE IN VIEW OF BONA AND KRANZLEY

A. Claim 16: The system of claim 15, wherein the touch-screen user interface is operable for displaying the limited-use payment information, and wherein a merchant is operable to accept the displayed payment card information in a transaction at a merchant facility.

339. Collinge in view of Kranzley teaches Collinge's mobile device (computing device) is further operable to display a payment information visually and wherein a merchant is operable to accept the displayed payment card information in a transaction at a merchant facility. *See* Claim 10.

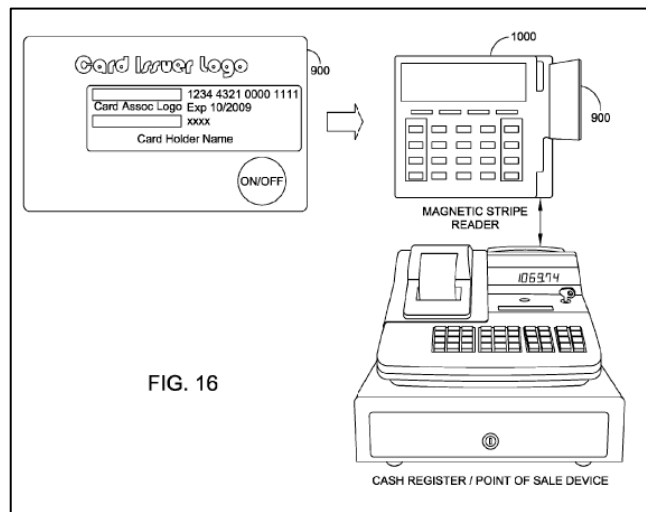
**XVI. OPINIONS REGARDING GROUND 7: CLAIM 19 IS OBVIOUS OVER
COLLIGE IN VIEW OF BONA AND ENG**

A. Claim 19(a): The card device of claim 15, wherein the payment card device comprises fixed payment information disposed thereon, and wherein the fixed payment information comprises only: a card-holder name; a payment issuing logo; a card payment network logo, and a card reader interface icon, and

340. Collige, in view of Bona and Eng, teaches Bona's companion card (payment card device) comprises fixed payment information comprises only a card-holder name, card issuer logo (payment issuing logo), card payment network logo, and a magnetic stripe and chip (card reader interface icon).

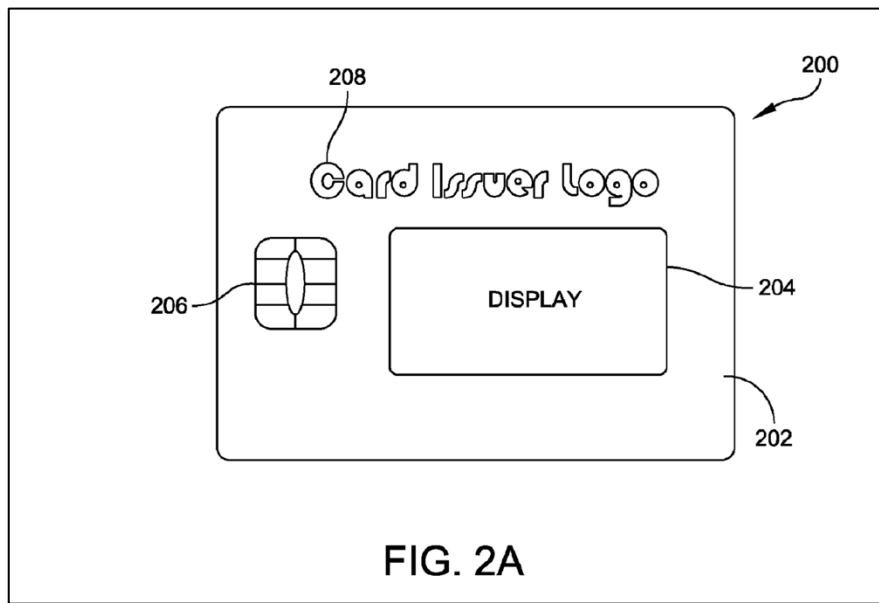
1. Bona's Teachings

341. Bona's NFC-enabled companion card 900 is a payment card device that is operable for use in payment card reader equipment. Bona's NFC-enabled companion card 900 "takes the shape of a standard plastic magnetic stripe card" and includes "display 204," an "internal power source 212" a "smart card controller 216" and a "magnetic stripe emulator 214." *Bona (Ex. 1009)*, [0045]-[0047], [0011]. Bona's companion card 900 is operable for use in payment card reader equipment, such as "a traditional magnetic stripe reader" *Bona (Ex. 1009)*, [0125].

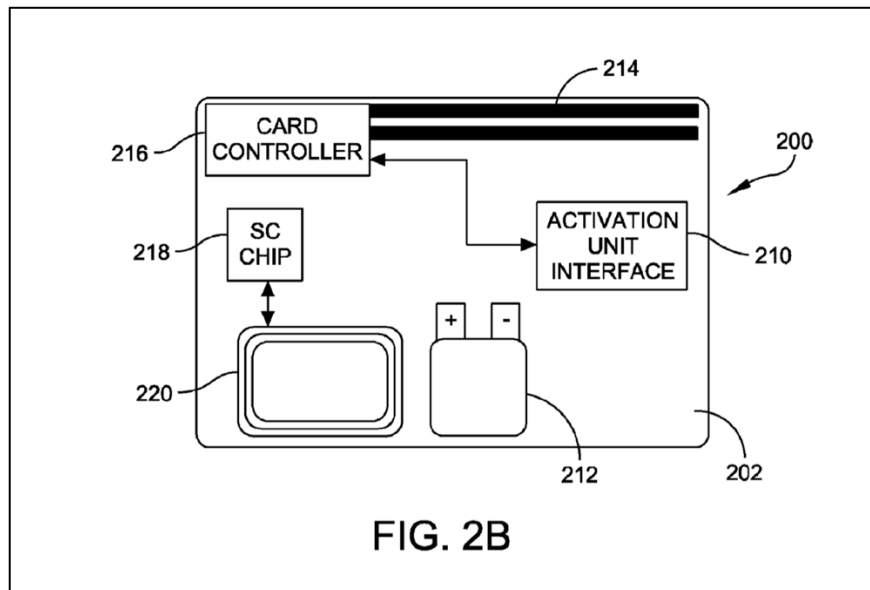


Bona (Ex. 1009), Fig. 16.

342. Bona's payment card device is free of any fixed payment numbers visible thereon. *Bona (Ex. 1009), Fig. 13(a), [0108]*. When Bona's card is off, there is no information on the display of the payment card device as shown below in Figure 13A. *Bona (Ex. 1009), [0110]*. ("The smart card includes an on/off button 906 for powering the smart card on/off and a display 904 for displaying information to the user."). Because Bona's card shows no visible payment numbers when the device is off, it is free of any fixed payment numbers. *See Claim 1(a)*. As depicted below Bona teaches card issuer logo (payment issuing logo) and magnetic stripe and chip (a card reader interface icon) on Bona's payment card. Bona teaches "[t]he card 200 may include the logo 208 of the card issuer or other source indicia." *Bona (Ex. 1009), [0045]*.



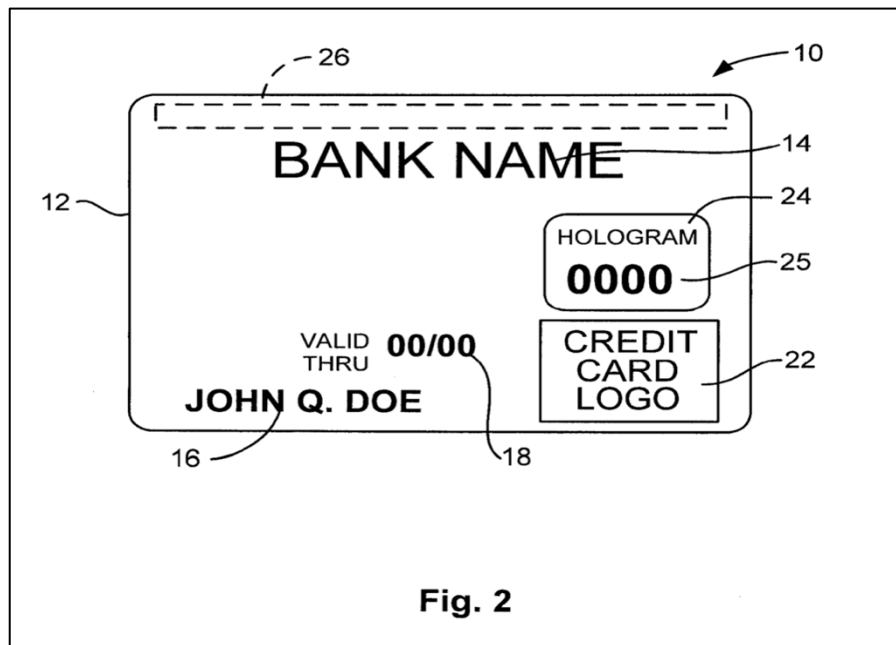
Bona (Ex. 1009), Fig. 2A.



Bona (Ex. 1009), Fig. 2B.

2. Eng's Teachings

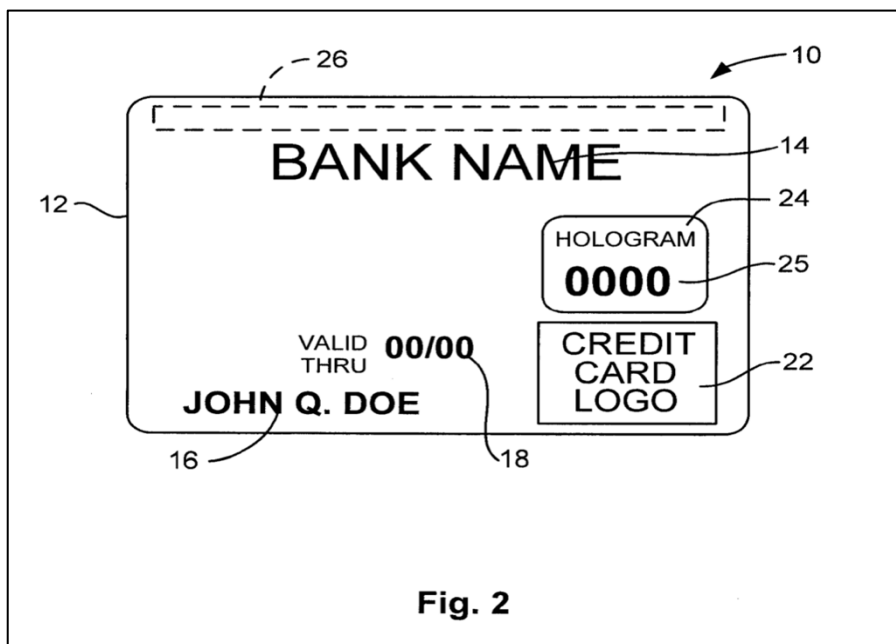
343. Eng teaches a card that has: (1) a card-holder name, (2) credit card logo (a card payment network logo), (3) Bank Name (payment issuing logo). *Eng (Ex. 1014), [0020]-[0021].*



Eng (Ex. 1014), Fig. 2.

3. Motivation to Combine

344. It would have been obvious and a POSITA would have been motivated to modify Bona's card to include a fixed cardholder name and credit card logo as taught by Eng. A POSITA would have understood that a user would have found it valuable to distinguish their cards visibly from each other (for example, with a credit card logo) and from similar cards that others in their household might have (with a cardholder name) as demonstrated by Eng.



Eng (Ex. 1014), Fig. 2. Each of these pieces of information was well-known to a POSITA and common on payment cards. A POSITA would have had a reasonable expectation of success in making this combination of known printed payment card elements without undue experimentation.

B. 19(b): wherein the payment card device is free of any account numbers, expiration dates, card security codes, or other fixed payment numbers, disposed thereon.

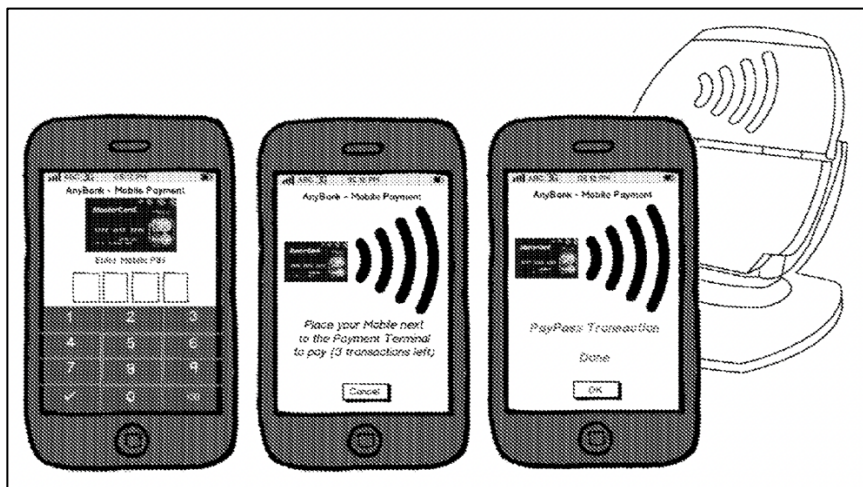
345. Bona's card is free of any fixed account numbers, expiration dates, card security codes, or other fixed payment numbers. *See* Claim 1(a), 19(a).

**XVII. OPINIONS REGARDING GROUND 8: CLAIM 12 IS OBVIOUS OVER
COLLIGE IN VIEW OF *BONA, SMITH, AND CHIN***

A. Claim 12(a): The system of claim 1, wherein the computing device is further operable to present at least one challenge, of a set of security challenges comprising: ...a user touch-screen entry...a user gesture of a device, a user passcode entry...and a biometric sensing of a recognized user, and

346. Collige’s mobile device presents at least one security challenge, such as a PIN (a user touch-screen entry), user gesture, user passcode entry, or biometric identifier. For example, Collige teaches that “[t]he mobile payment application 106 may transmit the activation code and any other additional user authentication information (e.g., a user identifier, a password, etc.) as a method of authentication.” *Collige (Ex. 1004)*, [0094]. Collige also teaches that the user “may provide a mobile PIN for authentication” via “an input device (e.g., of the mobile device 104, such as a touch screen) [.]” *Collige (Ex. 1004)*, [0051], [0133].

347. Collige teaches the user will “provide the Mobile PIN for all PayPass transactions...when using Remote-SE Mobile PayPass solution.” *’098 Provisional (Ex. 1008)*, 99.



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

B. 12(b): wherein the computing device is operable to reject and accept a user authorization to use the device based on the security challenge response, and

348. Collinge in view of Chin render obvious where Collinge's mobile device is operable to reject and accept a user authorization to use Collinge's device based on the input gesture (*security challenge response*).

1. Collinge's Teachings

349. As described in Claim 1(i), Collinge teaches the issuer will decline transactions performed by the computing device when a user inputs an incorrect PIN if the issuer cannot successfully validate a payment cryptogram. *See Collinge (Ex. 1004)*, [0076] ("In some instances, the single use key 118 may be incorrect (e.g., fake, not genuine, etc.) if the key request includes a mobile PIN for which authentication is unsuccessful."); '248 Provisional (Ex. 1006), 15-16; *Collinge (Ex.*

1004), [0077] (“If the validation is unsuccessful, the issuer may deny the payment transaction.”)

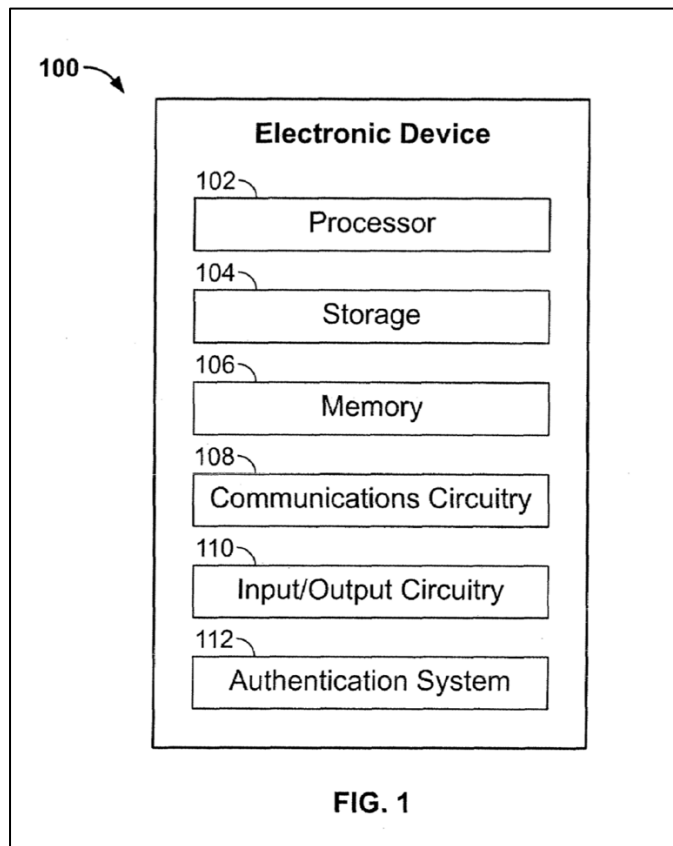
2. *Chin’s Teachings*

350. Chin teaches accepting a gesture on “the touch receptive input area (e.g., a touchscreen) of the target device [.]” *Chin (Ex. 1015)*, [0009]. The “target device is associated with a user-defined payment gesture (for e.g., a designated payment gesture defined by the user of the mobile device).” *Chin (Ex. 1015)*, [0008]. If the gesture input by the user “matches the user-defined payment gesture stored locally within the target device, the method may include permitting the wireless transmission (e.g., using NFC technology) of protected payment data resident on the target device to an initiator device (e.g., an NFC reader, a contactless smart card reader based on RFID technology, an NFC scanner, etc.).” *Chin (Ex. 1015)*, [0009].

351. However, “if the applied gesture on the touch receptive input area of the target device does not match the user-defined payment gesture stored locally within the target device, the method may include denying the wireless transmission of the protected payment data resident on the target device to the initiator device.” *Chin (Ex. 1015)*, [0009].

3. *Motivation to Combine*

352. A POSITA would have been motivated to modify Collinge to decline transactions based on a security challenge, such as a gesture as taught by Chin. Collinge already teaches a gesture to identify a user. *Collinge (Ex. 1004)*, [0139]. (“the additional credential may be at least one of: a gesture, a password, a passcode, and a biometric identifier.”). Collinge already teaches the issuer will decline transactions based on an incorrectly entered PIN by a user, but a POSITA would have been motivated to expand upon that teaching so Collinge’s device would deny transactions if the user were not able to authenticate themselves via a gesture as well. For example, U.S. Patent Publication No. 2009/0083850 to Fadell et al. (“*Fadell*”) teaches the mobile electronic device “authentication system 112 may be operative to receive secret or confidential entries identifying the user (e.g., gestures on the device, or touching a particular pattern of objects or colors on a display).” *Fadell (Ex. 1050)*, [0039].



Fadell (Ex. 1050), Fig. 1. *Fadell* teaches an example is the user “guessing the proper subset of shapes.” *Fadell (Ex. 1050)*, [0087]. “The electronic device may lock the device resources after a particular number of failed attempts to select the proper subset of shapes. Once locked, a user may need to couple the device with a host to re-enable the device (e.g., couple a mobile device to a fixed device) or use another authentication system (e.g., a biometric system) to re-enable the device.” *Fadell (Ex. 1050)*, [0087].

353. To decide if the gesture matches or not, processing would need to happen at the mobile device as taught by Chin and a POSITA would have

appreciated that Collinge already taught accepting a gesture. *See Collinge (Ex. 1004)*, [0139]. A POSITA would have appreciated that such a modification would have saved power, and a POSITA would have had a reasonable expectation of success in making such a modification since Collinge teaches being able to receive a gesture. A POSITA would have appreciated that such a modification was obvious to try. A POSITA would have appreciated that this biometric data would be collected and stored locally on Collinge's mobile device, increasing the security of a user's personal data, and reducing the locations of a user's personal data as demonstrated by Chin. *See Chin (Ex. 1015)*, [0009].

C. 12(c): wherein the computing device is operable to decline performing a payment transaction in the possession of an unauthorized user,

354. *See* Claim 12(b).

D. 12(d): and wherein the computing device is operable to perform a payment transaction while in the possession of a user correctly passing the at least one challenge.

355. *See* Claim 12(b).

E. Claim 13: The user computing device of claim 12, wherein a payment issuing authority is operable to decline transactions performed by the computing device when a user fails the at least one security challenge.

356. Collinge teaches that the issuer is operable to decline transactions performed by the computing device when a user inputs an incorrect PIN (fails at least one security challenge). *See* Claim 12; Claim 1(i),

XVIII. OPINIONS REGARDING GROUND 9: CLAIM 4 IS OBVIOUS OVER *COLLIGE* IN VIEW OF *BONA, SMITH, AND FISHER*

F. Claim 7: The system of claim 1, wherein the computing device is further operable to transceive the card payment information via the wireless interface for completing an online transaction.

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

1. Collinge's Teachings

358. Collinge teaches receiving the card profile from the remote-SE system and storing the card profile "by the mobile payment application 106 in the local encrypted database 304." *Collinge (Ex. 1004)*, [0068]. The communication network may be "wireless[.]" *Collinge (Ex. 1004)*, [0150].

359. As discussed in Claim 1(d)(1), a POSITA would have been motivated to send and receive Smith's PPAN to Collinge's mobile device with the card profile since account information was already included in Collinge's card profile. *Collinge*

(*Ex. 1004*), Abstract. (“wherein the card profile includes at least payment credentials corresponding to the associated payment account”).

2. *Fisher’s Teachings*

360. Fisher teaches a “mobile communication device” with a “mobile wallet application that executes PayPass[.]” *Fisher (Ex. 1016)*, [0024]. When “a consumer (or user) is shopping online and they are ready to pay for their products, the consumer opens his mobile wallet and selects one of the payment methods (e.g., credit card, debit card, prepaid card, etc.) from their mobile wallet.” *Fisher (Ex. 1016)*, [0018]. The user “waves their phone over the NFC reader present on the PC 404.” *Fisher (Ex. 1016)*, [0018]. The user’s “payment credentials are transferred from the phone to the merchant website (e.g., online store application 410)” *Fisher (Ex. 1016)*, [0018].

3. *Motivation to Combine*

361. For the reasons discussed in Claim 1(d)(1), a POSITA would have been motivated to use Smith’s PPAN in place of Collinge’s PAN in Collinge’s payment credentials, and to transceive Smith’s PPAN via NFC, a wireless interface when completing an online transaction.

362. It was well known that mobile wallets could be used in online transactions, and Fisher demonstrated the feasibility of using PayPass in an online system. Fisher teaches transceiving payment credentials to an “NFC reader” to

complete the online transaction, explaining that a “PayPass or other payment execution protocol” would be used. *Fisher (Ex. 1016)*, [0024]. A POSITA would have appreciated that performing an online transaction using Smith’s PPAN would have provided the user with flexibility to shop in more places while still protecting sensitive PAN information and a POSITA would have had a reasonable chance of success in making the combination as it combines known elements and would yield predictable results.

XIX. OPINONS ON GROUND 10: COLLINGE, BONA, SMITH, AND HAMMAD

G. Claim 6(a): A system of claim 1, wherein: the card issuer authority is operable to receive said transacted payment information, and wherein a card issuer authority is operable to compute a limited-use payment information from a transaction information, a merchant, a facility information, a sequence counter, a payment card account information, secrets and an information limited to said card device and to said computing device,

363. Collinge-Smith-Bona in view of Hammad renders obvious wherein the issuer is operable to receive said transacted payment information (Claim 1(h), 1(i); *Collinge (Ex. 1004)*, [0076]-[0077]) and computing a limited-use payment information (payment cryptogram) from a transaction information (transaction amount), a merchant (merchant ID), a facility information (terminal ID), a sequence counter (ATC), a payment card account information (track data), secrets (UN_{CLOUD} and KS_{UN}), and an information limited to said card device and to said

computing device (expiration date). As discussed above, Collinge in view of Smith teach a PPAN (alternative to the PAN). *See* Claim 1.

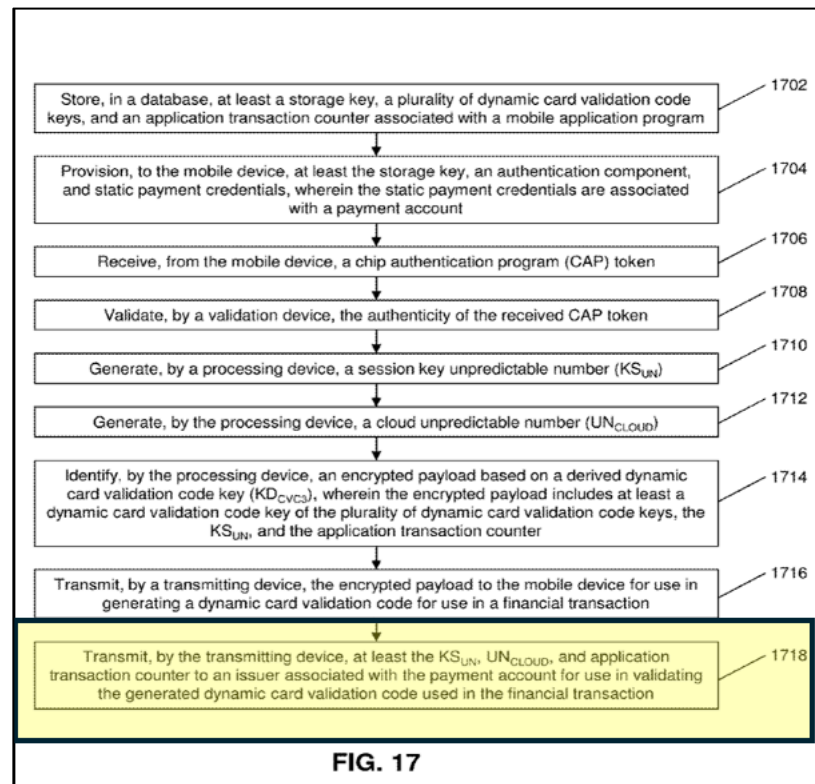
364. Hammad teaches dynamically generating a dCVV (cryptogram number) using an application on a mobile device for use in a mobile payment transaction. *Hammad (Ex. 1017)*, 2:65-3:11, 3:51-4:6. The DCV is generated from “at least two (e.g., at least three or four) dynamic data elements,” including an “application transaction counter (ATC),” “a cryptogram, digital signature, or hash value based on transaction data,” “a time of day, a current transaction amount, a terminal ID, a merchant ID, and a randomly generated number from a terminal, etc.,” or information “relat[ing] to a consumer’s portable consumer device.” *Id.*, 4:21-56, 4:62-7:5, Fig. 1. The dynamic data elements can also be used with “static data elements,” including “telephone number, a SIM card number, an account number, birthday, home address, expiration date, etc.” and “service code” to generate a dCVV. *Id.*, 4:52-60, 5:2-5. The dCVV is generated by cryptographically combining this information with multiple encryption keys, including a master derivation key, resulting in a 3-digit dCVV. *Id.*, 4:61-6:34, Figs. 1-3. The master derivation key is provided by the service provider. *Id.*, 5:38-57, Fig. 2.

365. The dCVV is embedded into the payment data, which is transmitted to the point of sale terminal and then to the service provider, e.g., “payment processing

organization or an issuer of the portable consumer device.” *Hammad (Ex. 1017)*, 2:18-20, 4:61-6:34, 6:40-42, 6:49-7:27, 7:29-32, 7:43-46, 7:55-62, Figs. 4-5. The service provider uses the dCVV to determine the authenticity of the payment. *Id.*, 7:29-8:50, Fig. 6.

2. Collinge’s Teachings

366. Collinge teaches that the issuer validates a payment cryptogram as authentic. *See* Claim 1(i). A POSITA would have been very familiar with methods of validating a payment cryptogram, as recognized by Collinge. *Collinge (Ex. 1004)*, [0077]. Typically, the issuer will recompute the payment cryptogram and compare the issuer-generated payment cryptogram to the cryptogram received from the merchant. In Collinge, the issuer 108 validates the generated payment cryptogram. *Collinge (Ex. 1004)*, [0141]. Specifically, as shown in Fig. 17, the issuer received “at least the KS_{UN} , UN_{CLOUD} , and application transaction counter” and the issuer 108 uses that information “in validating the generated CVC3 value used in the financial transaction.” *Collinge (Ex. 1004)*, [0141].



Collinge (Ex. 1004), Fig. 17 (annotated); *see also '248 Provisional (Ex. 1006)*, 54. The issuer may then “authenticate the dynamic card validation code[.]” *Collinge (Ex. 1004)*, [0056]. *Collinge’s* provisional details how the issuer validates the payment cryptogram. *Collinge* teaches generating a CVC3 based on at least: “the supplied CVC3 value, the session key unpredictable number, the application transaction counter, and the reader unpredictable number.” *Collinge (Ex. 1004)*, [0145]; *'248 Provisional (Ex. 1006)*, Table 1.

20150001

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

367. Specifically, based on the received information at the issuer above (KS_{UN} , UN_{CLOUD} , and ATC) the issuer will compute $Cloud_CVC3_{TRACK1/2}$. '095 Provisional (Ex. 1005), 24. The issuer also uses $IVCVC3_{TRACK1/2}$ which is a MAC calculated over track 1 and 2 data using KD_{CVC3} which is “kept in the Cloud/Issuer” '095 Provisional (Ex. 1005), 21. As discussed in Section VII, track data includes a payment account number along with other user account 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)

'095 Provisional (Ex. 1005), 24. After computing $Cloud_CVC3_{TRACK1/2}$, the issuer computes $CVC3_{TRACK1/2}$ which is directly used in generating the CVC3. '095 Provisional (Ex. 1005), 25.

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

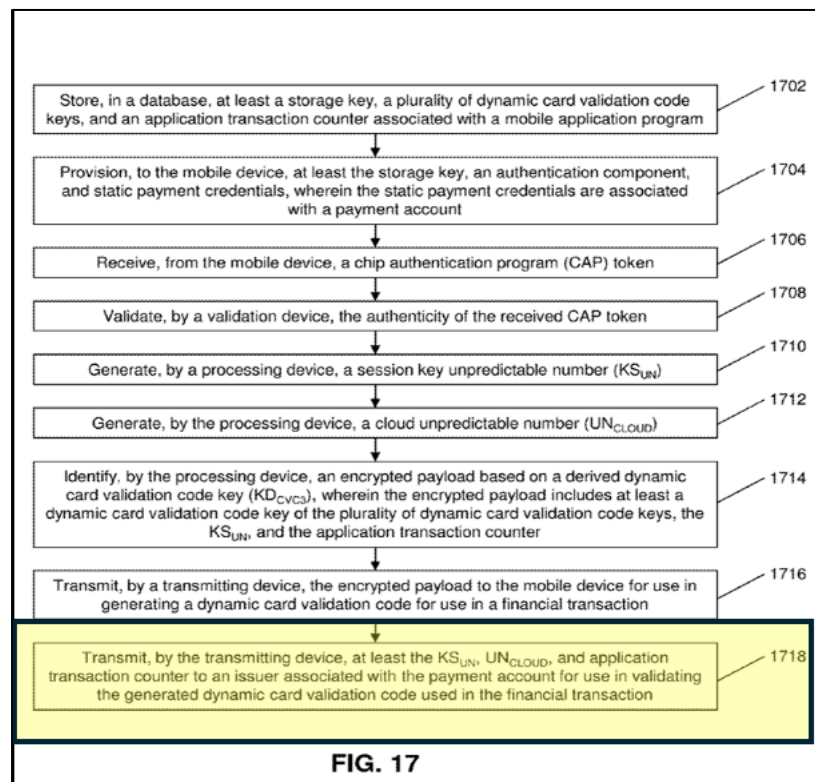
- ◊ $Cloud_CVC3_{TRACK1/2}$ (2 bytes)
- ◊ UN_{READER} (4 bytes)
- ◊ ATC (2 bytes)

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

'095 Provisional (Ex. 1005), 25. The issuer already has the rest of the values used when generating the CVC3 (KS_{UN} , UN_{CLOUD} , and ATC). '095 Provisional (Ex. 1005), 24-25. Based on the result of the authentication, the issuer will “approve or deny the payment transaction.” Collinge (Ex. 1004), [0056].

1. *Secrets*

368. When generating the cryptogram, the issuer will use the KS_{UN} , UN_{CLOUD} , and ATC. *Collinge (Ex. 1004)*, [0141]; Claim 1(i). Collinge also uses the KS_{UN} , UN_{CLOUD} , and ATC when generating a payment cryptogram. *Collinge (Ex. 1004)*, [0145] (“the supplied CVC3 value, the session key unpredictable number, the application transaction counter, and the reader unpredictable number.”) A POSITA would have understood that the KS_{UN} is private information (*secret*) that was shared (as shown in Fig. 17 below) between Collinge and the issuer specifically used by Collinge’s mobile device to generate a payment cryptogram and the issuer to validate Collinge’s generated payment cryptogram.



Collinge (Ex. 1004), Fig. 17 (annotated); see also '248 Provisional (Ex. 1006), 54. Additionally, Collinge teaches that the CVC3 payment cryptogram is generated using the single use key 118 that is “used one time to generate a payment cryptogram to be used in a payment transaction.” *Collinge* at [0050]. The single use key is shared with issuer 108. *Collinge* at [0128] (“...method 1500 may further include transmitting the generated single use key 118 to an issuer associated with the payment account). Single use key 118 is secret information because a user must input a valid PIN in order for a genuine single use key 118 to be generated, indicating that secret use key 118 is secret to anyone who does not have the valid PIN. (“...the single use key 118 may be genuine if the mobile PIN is successfully authenticated in step 1508, and fake if the mobile PIN is unsuccessfully authenticated.”) Therefore Collinge teaches the payment cryptogram CVC3 value (limited-use payment information) is generated based on the K_{SUN} and the generating key and values within the single use key 118 (secrets), and that the K_{SUN} and single use key 118 is secret information shared with issuer 108 (payment issuer secrets).

2. *Motivation to Combine*

369. A POSITA would have recognized that using additional data elements to generate Collinge’s cryptogram (e.g., transaction information (transaction amount), a merchant (merchant ID), a facility information (terminal ID), and an

information limited to said card device and to said computing device (expiration date)) would decrease the likelihood that, even if payment data were intercepted, that it could be used in a fraudulent manner since more data elements adds to the complexity of fraudulently fabricating a cryptogram. Therefore, a POSITA would have been motivated to include more data elements in Collinge generating a payment cryptogram, as taught by Hammad. A POSITA would have further recognized that modifications to Collinge-Bona would be minimal as it would simply require additional inputs to Collinge's payment cryptogram generation. As taught by Hammad, a POSITA would have been motivated to modify Collinge so that the issuer would therefore validate Collinge's payment cryptogram based on Hammad's data elements, as well as the data elements already taught by Collinge. *Hammad (Ex. 1017)*, 7:29-8:50, Fig. 6.

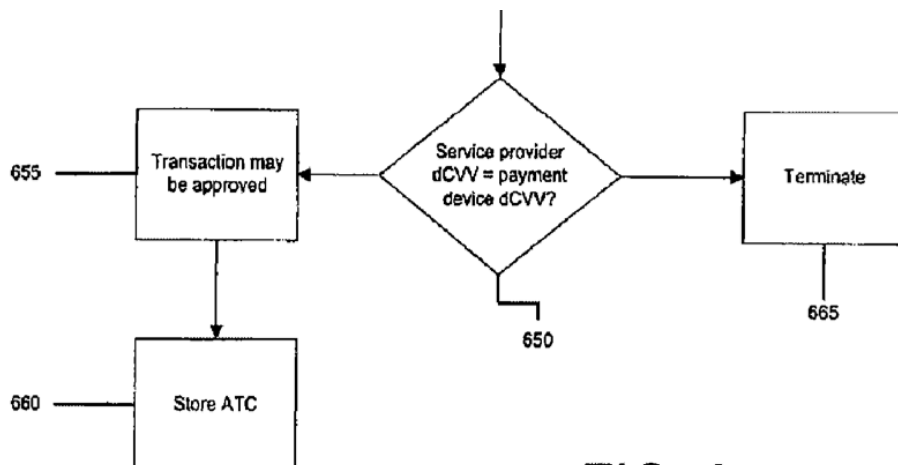


FIG. 6

Hammad (Ex. 1017), Fig. 6. (excerpt). Given Hammad's teachings regarding how to generate such a dynamic verification value, a POSITA would have had a reasonable expectation of success. This modification is applying known techniques (e.g., using various data elements to generate a card verification value to replace a static value) to improve similar devices (e.g., mobile devices used in payment transactions) in the same way would have yielded the predictable result of increasing security of the transaction.

H. 6(b): and wherein a card issuer authority is operable to compare said computed payment information to said device transacted information,

370. See Claim 1(i).

I. 6(c): and wherein a card issuer authority is operable to reject as invalid a device transaction used outside of a valid range of device limitations,

371. See Claim 1(h).

J. 6(d): and wherein a card issuer authority is operable to authenticate as valid, a device transaction use within valid range of device limitations.

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

XIX. CONCLUSION

373. 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: 8/18/2025

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 Quantify Smart-Grid Resilience", September 2017, In Proceedings of the 4th International Workshop on Cyber-Physical Systems at the Federated Conference on Computer Science and Information Systems, Prague, Czech Republic.
- 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 September 2016, at the Hague, 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 Intruding Detectors for Critical Applications*, in Proceedings of the 16th 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 Systems. USC-ISI Technical 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 Infrastructure 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

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.