UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner
v.

CARDWARE INC.,
Patent Owner

Inter Partes Review Case No. IPR2025-01147
U.S. Patent No. 10,628,820

PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT NO. 10,628,820

TABLE OF CONTENTS

I. INTRODUCTION

Apple Inc., ("Petitioner") respectfully requests *inter partes* review ("IPR") of claims 1-20 ("Challenged Claims") of U.S. Patent No. 10,628,820 ("'820 Patent").

II. THE '820 PATENT

A. Description of the '820 Patent

The '820 Patent describes an electronic payment card capable of "generating a limited-duration credit card number…which is limited in scope to a predetermined number of authorized transactions." *'820 Patent* (Ex. 1001) at 2:28-34, Fig. 7.

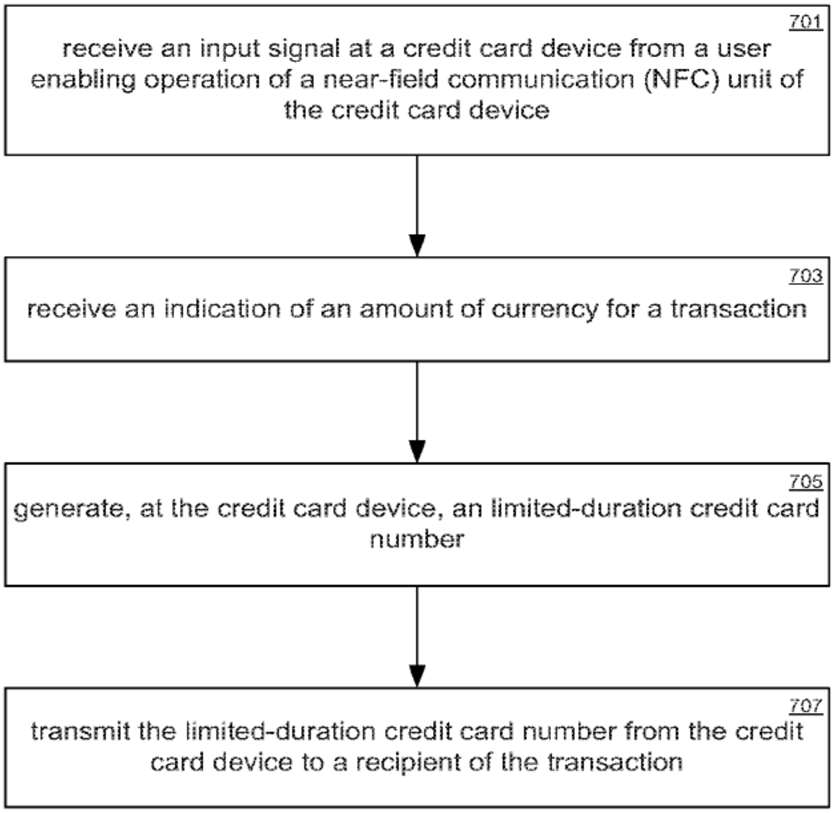

701
receive an input signal at a credit card device from a user enabling operation of a near-field communication (NFC) unit of the credit card device
703
receive an indication of an amount of currency for a transaction
705
generate, at the credit card device, an limited-duration credit card number
707
transmit the limited-duration credit card number from the credit card device to a recipient of the transaction

FIG. 7

'820 Patent, Fig. 7.

B. Field of Endeavor and Problem Solved by the Inventors

The ’820 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 devices and transaction processing thereof.” *’820 Patent* at 1:27-31, 1:66-2:3 (criticizing existing systems as “susceptible to theft and/or compromise”). A POSITA would have understood the field of endeavor of the ’820 Patent includes more secure payment cards, devices, and systems, and the ’820 Patent aims to solve the problem of providing payment solutions that limit opportunities for theft or compromise of payment credentials. *Dec.*, ¶¶32-36.

C. Priority and Prosecution History

The ’820 Patent claims priority to Provisional Application No. 61/794,891, filed March 15, 2013. Because the ’820 Patent claims the benefit of a filing date before March 16, 2013, Petitioner applies the pre-AIA versions of §§ 102, 103. For this proceeding, Petitioner applies March 15, 2013, as the priority date for the Challenged Claims.[1]

[1] Petitioner does not concede that any of the Challenged Claims are entitled to claim priority to March 15, 2013. Multiple claims of the ’820 Patent recite features not described in Cardware’s provisional application.

The ’820 Patent did not face any prior art rejections during prosecution. *’820 File History* (Ex. 1002).

D. Level of Skill of a POSITA

A POSITA at the time of the ’820 Patent would have had a bachelor’s degree in computer science, computer engineering, electrical engineering or the equivalent, and one or two years of experience working with payment processing and/or digital authentication systems, including familiarity with short-range wireless technology. *Dec.*, ¶28.[2] 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. *Id.*

III. REQUIREMENTS UNDER 37 C.F.R. § 42.104

A. Standing Under 37 C.F.R. § 42.104(a)

Petitioner certifies the ’820 Patent is eligible for IPR.

B. Identification of Challenge Under 37 C.F.R. § 42.104(b)

The Challenged Claims are unpatentable on the following grounds under 35 U.S.C. § 103:

Ground	Claim(s)	References
1	1, 8, 10	Walker (Ex. 1009) and Brown (Ex. 1010)
2	2	Walker, Brown, and Eng (Ex. 1014)
3	4-7, 9	Walker, Brown and Gauthier (Ex. 1011)
4	3	Walker, Brown, and Patel (Ex. 1012)

[2] All references to “*Dec.*” are to Ex.1003, Declaration of Dr. Neuman.

5	11, 13-15, and 17-20	Collinge (Ex. 1004), Kranzley (Ex.1013), and Brown
6	12, 16	Collinge, Kranzley, Brown, and Eng

The earliest claimed priority date of the ’820 Patent is March 15, 2013 (the “Critical Date”).[3] Each of the prior art references applied in this Petition qualifies as prior art to the ’820 Patent:

Reference	**Filed**	**Published**	**Prior Art Basis**
Walker	1/24/2006	6/8/2006	§102(b)
Brown	12/30/2006	9/6/2007	§102(b)
Gauthier	4/5/2006	3/8/2007	§102(b)
Eng	11/5/2012	3/21/2013	§102(e)
Patel	12/5/2011	6/7/2012	§102(a), (e)
Collinge	3/14/2013	10/3/2013	§102(e) [4]

[3] Unless specifically noted, the analysis presented in this petition remains the same regardless of whether March 15, 2013 or some later date is used as the Critical Date.

[4] Collinge is prior art of its filing date. Should Cardware attempt to establish an earlier date of reduction to practice, Apple will show that Collinge is entitled to a priority date of at least April 18, 2012, under 35 U.S.C. § 102(e) based on Collinge’s provisional applications. *In re Giacomini*, 612 F.3d 1380, 1383 (Fed. Cir. 2010); *Dec.*, ¶¶81-84. *See also Dynamic Drinkware, LLC v. Nat'l Graphics, Inc.,* 800 F.3d 1375, 1381 (Fed. Cir. 2015) (holding Petitioner did not have the burden of producing evidence relating to earlier effective filing date based on provisional application until Patent Owner argued for an earlier date of reduction to practice).

Kranzley	6/1/2009	5/20/2010	§102(b)

None of these references were cited or discussed during prosecution of the ’820 Patent.

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

In this proceeding, claims are interpreted under the same standard applied by Article III courts (i.e., the *Phillips* standard). 37 C.F.R. § 42.100(b); *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (*en banc*). For purposes of this proceeding, Petitioner applies the plain and ordinary meaning of all claim terms as understood by a POSITA.[5]

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

1. Claim limitations directed to printed matter are not entitled to patentable weight.

The Challenged Claims include several limitations that are directed to printed matter that has no structural or functional relationship to the claimed substrate on which the information is disposed or printed. The Federal Circuit has repeatedly found that such claim limitations are entitled to no patentable weight, and thus “will

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

not distinguish the invention from the prior art in terms of patentability." *In re Gulack*, 703 F.2d 1381, 1385 (Fed. Cir. 1983); *In re DiStefano*, 808 F.3d 845, 848-851 (Fed. Cir. 2015).

The following table identifies limitations from the Challenged Claims that are directed to printed matter and thus are entitled to no patentable weight.[6] As discussed below at §V, each limitation is nevertheless rendered obvious by the cited art.

Claim	Printed Matter
1	"having no fixed payment numbers disposed thereon"
2	"the fixed payment information includes only: a card-holder name; a payment issuing logo; and a card payment network logo" / "free of any account numbers, expiration dates, card security codes, or other fixed payment numbers, disposed thereon."
11	"comprising no fixed payment numbers visible thereon"
12	"bears no fixed payment numbers, and bears only: the cardholders name; a brand logo; and the card payment network logo"
15	"bears no fixed payment numbers on the card device"
16	"bears no fixed payment numbers, and bears only: the cardholders name; the brand logo; and the card payment network logo."

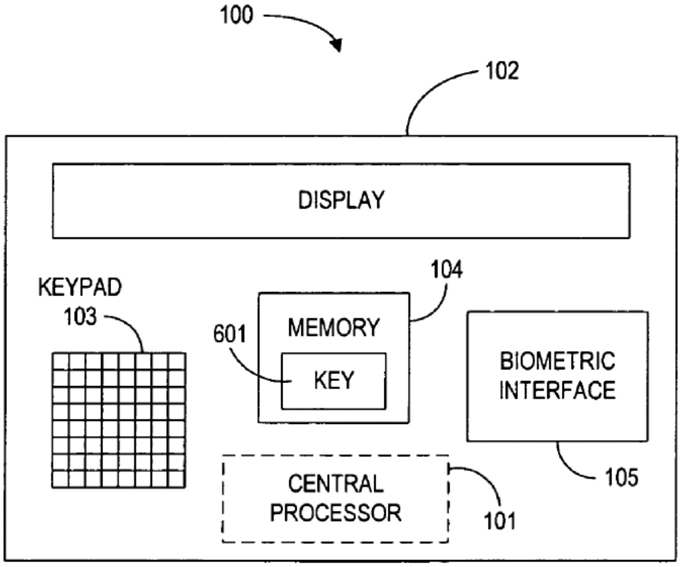
IV. SHOWING OF ANALOGOUS PRIOR ART

A. Walker

Walker teaches a device 100—"preferably a smart card" that "generate[s] a single-use credit card number" that can be used to purchase goods or services.

[6] The Board preliminarily agreed that these limitations are directed to printed subject matter and entitled to no patentable weight in IPR2023-00314, Paper 11 at 17-19.

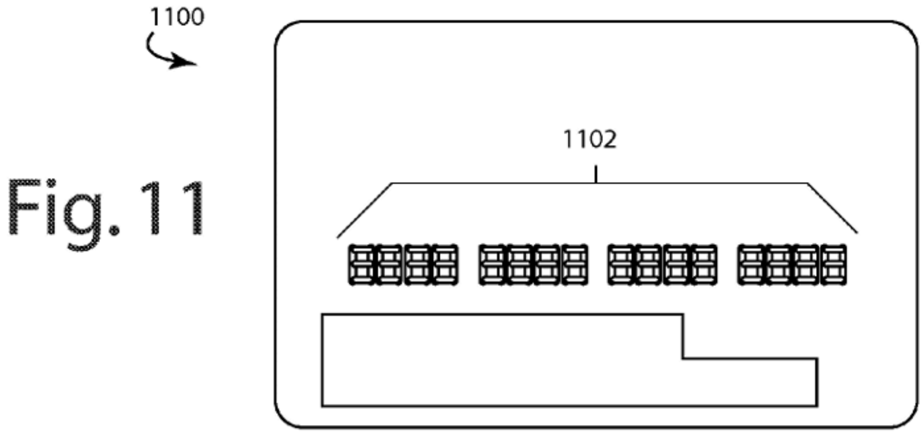
Walker, [0043], [0046]. Walker's single use credit card number "is generated by the device cryptoprocessor 205, using a private key 601" by cryptographically combining the initialization variable, account number and encrypted nonce value. *Walker,* [0050], [0060]-[0061]. When the single-use credit card number is used for payment, a card issuer "maps the single-use credit card number onto a conventional credit card account" to authorize the transaction. *Walker,* [0048].



Walker, Fig. 1.

B. Brown

Brown teaches a smart payment card that has a "full personal account number (PAN) [that] has been **implemented to be variable** on a visual display." *Brown,* [0200] (emphasis added).



Brown, Fig. 12.

C. Gauthier

Gauthier teaches a secured account number, different than the user's primary account number (PAN), that is **only** used for "wireless transactions" with a proximity reader, using "a contactless mode or an infrared mode, RF mode (i.e. Radio Frequency), and the like[.]" *Gauthier,* [0022], [0037], Fig. 1.

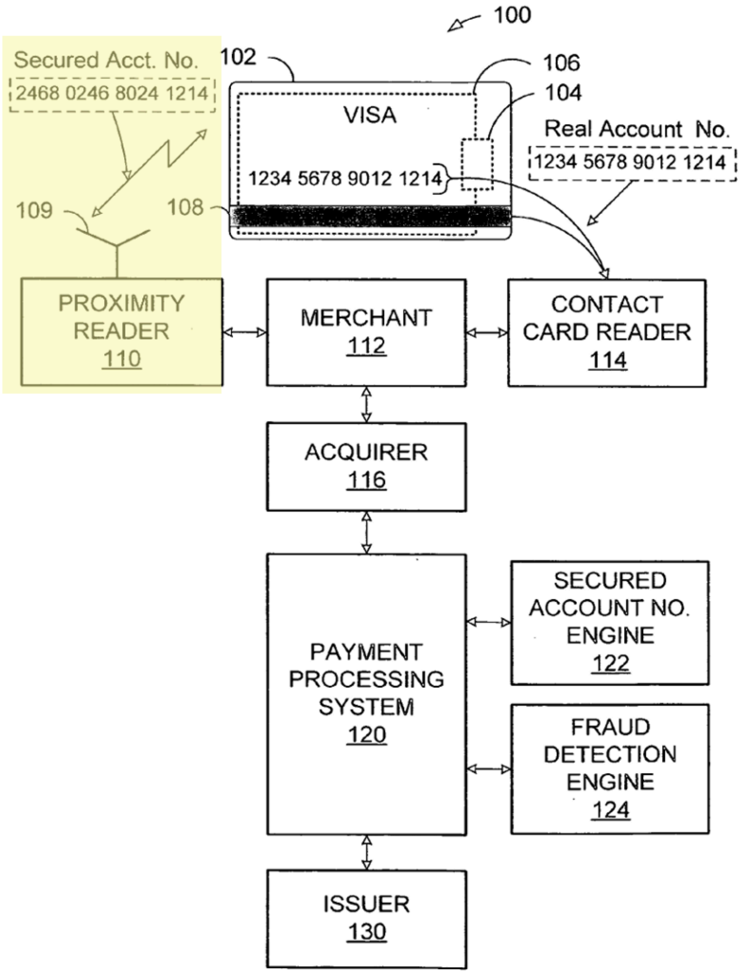


FIG. 1

Gauthier, Fig. 1 (annotated).

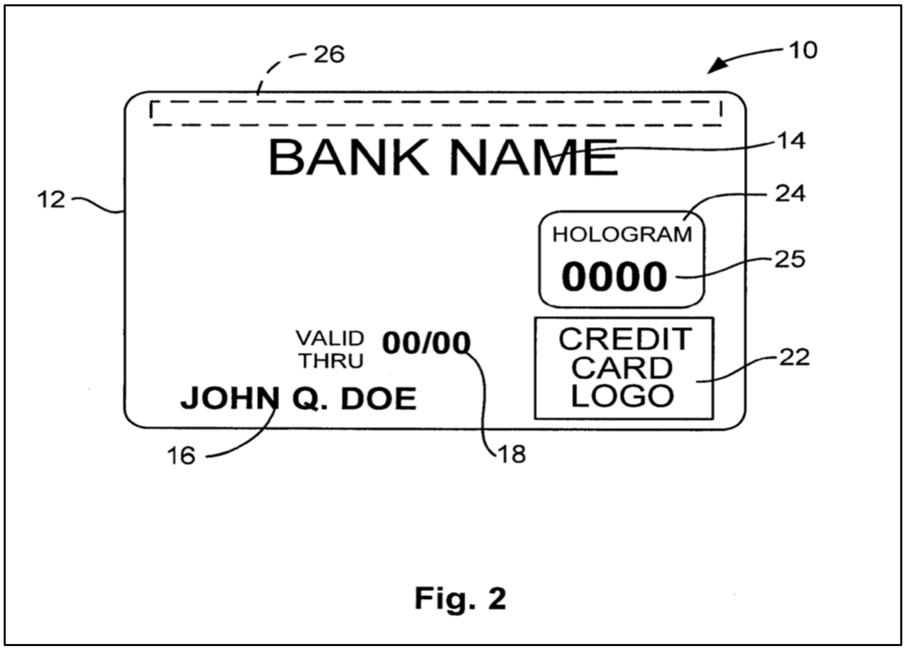
D. Patel

Patel teaches a "credit card, debit card, or other similar financial instrument" and "temporary assignment of a dynamic CVV" to the card "for increased card security." *Patel,* Abstract. "The dynamic CVV is read, changed, and rewritten to the card with each transaction." *Id.* Patel teaches that the dynamic CVV is used "[t]o pay for the goods or services" through "a magnetic card reader 130[.]" *Patel,* [0057].

The dynamic CVV is transmitted to the financial institution 150, which "authenticates the verification data, including the dynamic CVV 330, and transmits a verification code, including a new dynamic CVV 330 to the transaction device 130." *Patel*, [0059]. "The transaction device 130 reads the new dynamic CVV 330, and writes the new CVV 330[,]"received from the card issuer, "to the magnetic strip 220" of the payment card. *Patel*, [0060]. "The financial institution 150 may then update its database to expire the previous dynamic CVV 330, and enter the new dynamic CVV 330 as the valid dynamic CVV 330." *Patel*, [0062]. "Once the new CVV 330 has been provided, the old CVV 330 expires and is no longer valid." *Patel*, [0065].

E. Eng

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



Eng, Fig. 2.

F. Collinge

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

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

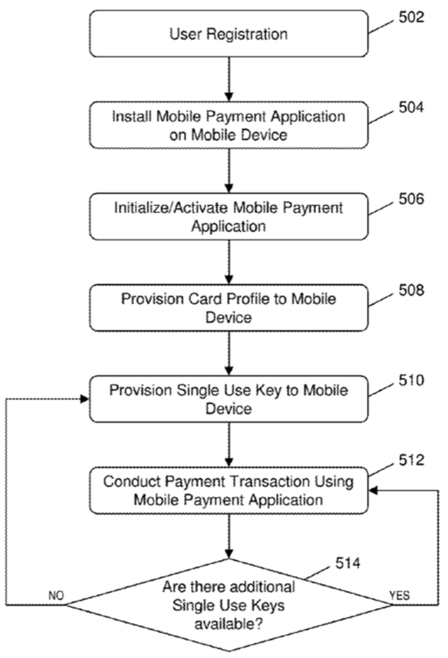

User Registration
502
Install Mobile Payment Application on Mobile Device
504
Initialize/Activate Mobile Payment Application
506
Provision Card Profile to Mobile Device
508
Provision Single Use Key to Mobile Device
510
Conduct Payment Transaction Using Mobile Payment Application
512
Are there additional Single Use Keys available?
514
NO
YES

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 cryptogram and payment credentials to a point-of-sale terminal[.]" *Collinge,* [0070], [0077].

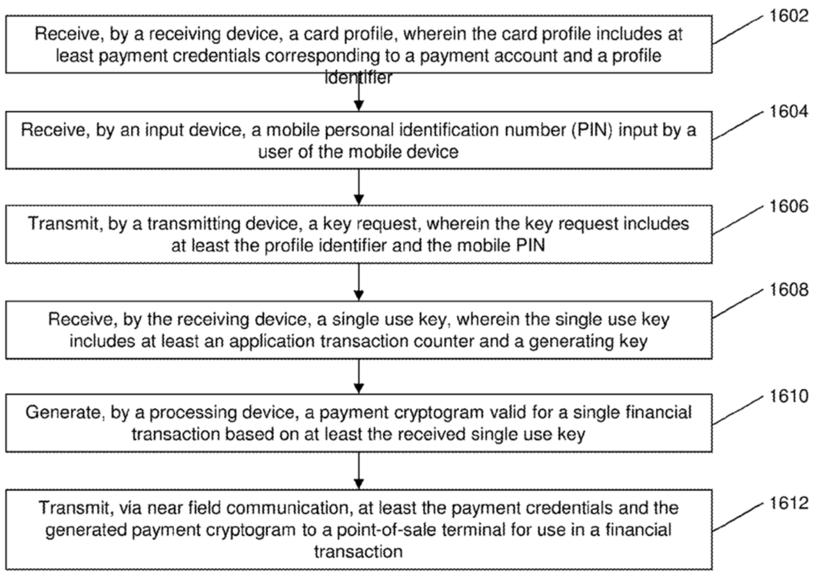

Receive, by a receiving device, a card profile, wherein the card profile includes at least payment credentials corresponding to a payment account and a profile identifier
1602
Receive, by an input device, a mobile personal identification number (PIN) input by a user of the mobile device
1604
Transmit, by a transmitting device, a key request, wherein the key request includes at least the profile identifier and the mobile PIN
1606
Receive, by the receiving device, a single use key, wherein the single use key includes at least an application transaction counter and a generating key
1608
Generate, by a processing device, a payment cryptogram valid for a single financial transaction based on at least the received single use key
1610
Transmit, via near field communication, at least the payment credentials and the generated payment cryptogram to a point-of-sale terminal for use in a financial transaction
1612

FIG. 16

Collinge, Fig. 16.

1. Collinge Incorporated all Provisionals for All Purposes

Collinge claims priority benefit of and expressly "incorporated by reference in their entirety" Provisional Nos. 61/619,095, 61/635,248, 61/735,383, and 61/762,098. *Collinge*, [0001]. Thus, Collinge's Provisionals form part of Collinge for all purposes as if explicitly contained therein. MPEP (8th Ed) §2163.07(b) ("information incorporated is as much a part of the application as filed as if the text was repeated in the application, and should be treated as part of the text of the application as filed."); *Ultradent Prods., Inc. v. Life-Like Cosmetics, Inc.*, 127 F.3d 1065, 1069 (Fed. Cir. 1997); *Apple Inc. v. Koss Corporation*, IPR2021-00255, Paper 54 (Final Written Decision) (P.T.A.B. May 31, 2022), at 25-30 (holding claims obvious over host reference, relying on material from two provisional applications incorporated in their entirety); *Unified Patents, LLC v. Rosen Technologies LLC*, No. IPR2022-01402, Paper 22 (Final Written Decision) (P.T.A.B. Feb. 28, 2024), at n.6 ("Because Geiwitz expressly incorporated by reference its entire provisional application [] the provisional's disclosures are part of 'Geiwitz' as asserted by Petitioner.").

2. Obvious to Combine Provisional Features

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 e.g., '098 Provisional*, Fig. 19 *with Collinge,* Fig. 6; *Collinge,* Fig. 19 *with* '095 Provisional Fig. 9 and '248 Provisional Fig. 16; *Dec.*, ¶¶81-87.

Even if Collinge's Provisionals were directed to different payment system embodiments, it would have been obvious, and a POSITA would have been motivated to apply the teachings in Collinge's Provisionals in Collinge's payment system. *Dec.*, ¶87. For example, Collinge's Provisionals detail what is shown on the GUI of Collinge's mobile device during user registration, user selection of a payment option, and an NFC transaction.*'248 Provisional*, Fig. 2A, 2B; *'098 Provisional*, 96-100; *Collinge*, [0133]. A POSITA would have found it obvious and would have been motivated to incorporate these disclosures into Collinge's payment system because implementing Collinge's payment system requires various display screens with user-selectable softbuttons and Collinge's Provisionals provide details regarding layout and softbutton functions that would assist a POSITA in implementing Collinge's teachings. *Dec.*, ¶87. Based on the interconnected disclosures, a POSITA would have found a teaching, suggestion, or motivation in Collinge itself that would have led them to apply the additional details in Collinge's Provisionals to Collinge's payment system with a reasonable expectation of success. *Id.*

G. Kranzley

Kranzley teaches using a virtual PAN (VPAN) in place of the PAN. The VPAN "may have its own virtual expiry date." *Kranzley*, [0036]. Kranzley teaches displaying "a VPAN, expiration date and dynamic account validation code on a display" of the mobile device to be used to complete an online transaction. *Kranzley*, [0040]-[0041].

H. Analogous Art

Each of the applied prior art references discloses conducting secure payment transactions and is in the same field of endeavor as the '820 Patent. *Compare '820 patent*, Abstract, 1:27-31, Fig. 1 *with Collinge,* Abstract, [0005], Fig. 1; *Walker,* [0021]-[0022]; *Brown,* [0004]; *Eng*, [0023]-[0024], Abstract, Fig. 2; *Kranzley,* Abstract, [0010], Fig. 1; *Eng,* Abstract, [0023]-[0024], Fig. 2; *Gauthier*, [0009]-[0010], [0019], Fig. 1; *Patel,* Abstract, [0003], [0007]; *Dec.* ¶¶32-34, 78-80, 90, 93, 96, 100, 103, 106.

Further, each of the applied prior art references is reasonably pertinent to problems addressed by the ’820 Patent such as increasing security of payment transactions. *Compare ‘820 Patent,* 1:27-31, 1:66-2:7, 9:55-62 and *Dec.*, ¶¶35-36 *with Collinge*, [0003]-[0005]; *Dec.*, ¶80; *Walker,* [0002]-[0021]; *Dec.*, ¶91; *Brown*, [0006]-[0021], [0024]-[0029]; *Dec.*, ¶94; *Kranzley*, [0003], [0065]; *Dec.*, ¶107; *Eng*, [0023], Abstract, Fig. 2; *Dec.*, ¶104; *Gauthier*, [0006]-[0007]; *Dec.*, ¶97; *Patel,* [0005]-[0006]; *Dec.*, ¶101. Therefore, each of the applied prior art references is analogous art to the ’820 Patent.

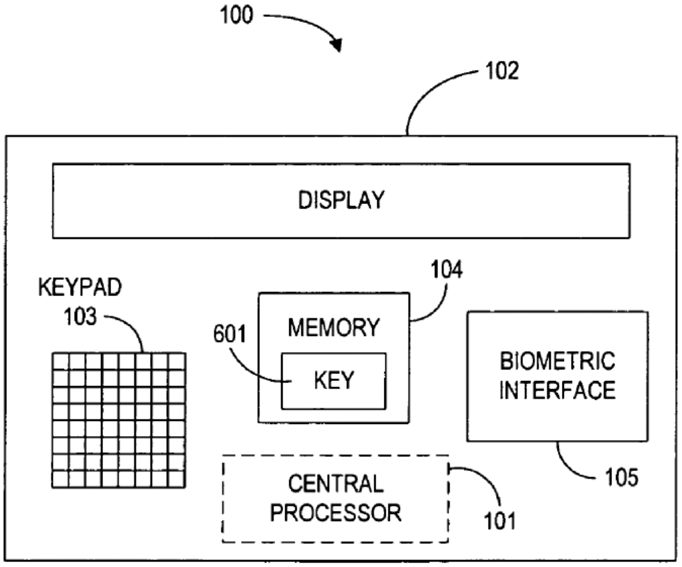
V. GROUND 1: CLAIMS 1, 8 AND 10 ARE OBVIOUS OVER *WALKER* IN VIEW OF *BROWN*

A. Claim 1

1. 1(Pre): “A payment device comprising:”

Walker teaches *a payment device*[7], device 100, which is preferably a “smart card[.]” *Walker,* [0043]. Walker’s device 100 “generate[s] a single-use credit card number” that can be used to purchase goods or services. *Walker,* [0043], [0046].

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



Walker, Fig. 1.

2. 1(a): "a thin shaped body having no fixed payment numbers disposed thereon"

As previously discussed, (Section III.C.1), the limitation that the payment device have "no fixed payment numbers disposed thereon" is directed to printed matter that has no functional or structural relationship to the claimed card device and is entitled to no patentable weight. *Dec.,* ¶¶110-113. Nevertheless, either (1) Walker alone or (2) the combination of Walker and Brown renders this limitation obvious.

(a) Walker

Walker's payment device 100 is a "hand-held **smart card** device" with a *thin shaped body*, as shown in Fig. 1. *Walker,* [0028] (emphasis added), [0043] ("device is preferably a smart card") Fig. 1. A POSITA would have been well-familiar with the term "smart card" by the Critical Date and would have understood that in the context of Walker's disclosures a "smart card" resembles a credit card in size and shape, but contains additional hardware such as an embedded processor. *Dec.,* ¶¶115-118; *'820 Patent*, 1:45-51 (smart cards are "credit cards [that] have a built in microprocessor with cryptographic capabilities").

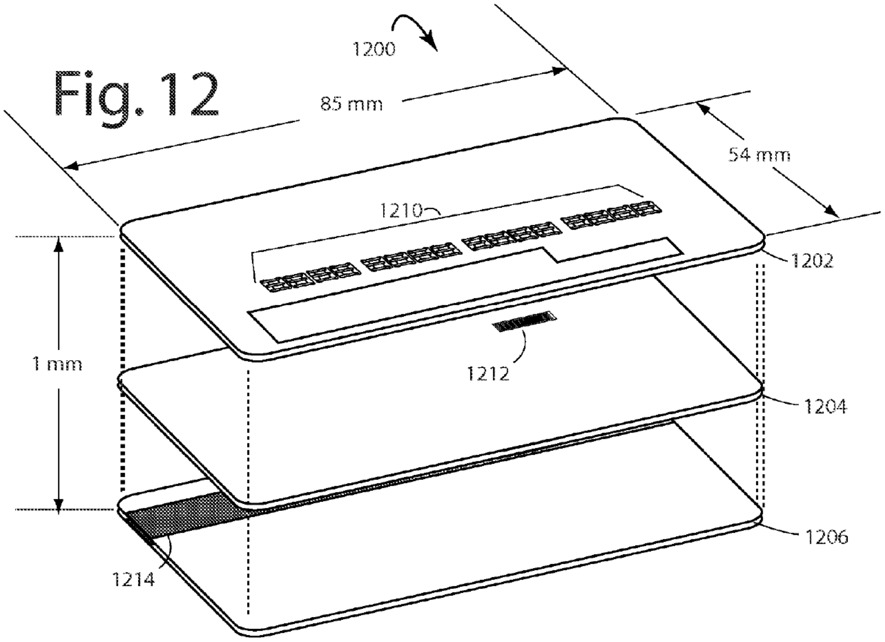
Walker's payment device 100 "generate[s] a single-use credit card number" that can be used to purchase goods or services. *Walker,* [0043], [0046].

Walker's "single-use credit card number" is "unique for the specific input variables set by the cardholder or by the device" and "may also be unique to the specific date and time to avoid so-called 'replay,' attacks for that card at that merchant with that exact purchase amount." *Walker*, [0047].

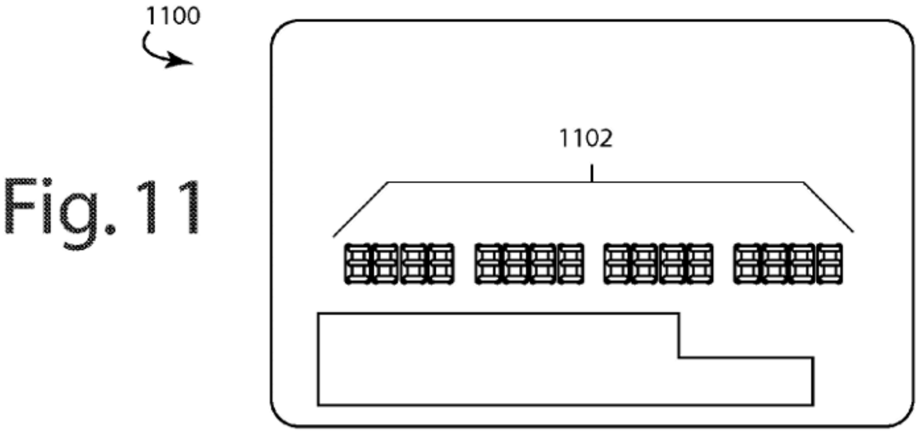
Therefore, *no fixed account numbers* are displayed on device 100 because (1) Walker does not display any payment numbers until the time-and-date-specific payment number is generated and (2) when Walker does display a payment number, it is single use.

(b) Brown

To the extent that Walker does not specify the thickness of Walker's smart card, Brown teaches a smart payment card that is "1mm" in thickness and therefore has a *thin shaped body*. *Brown,* [0091] (citing payment card thickness standards), [0200] (describing a "smart card" as "1mm" in thickness).



Brown, Fig. 12. Brown's payment card has a "full personal account number (PAN) [that] has been **implemented to be variable** on a visual display." *Brown,* [0200] (emphasis added).



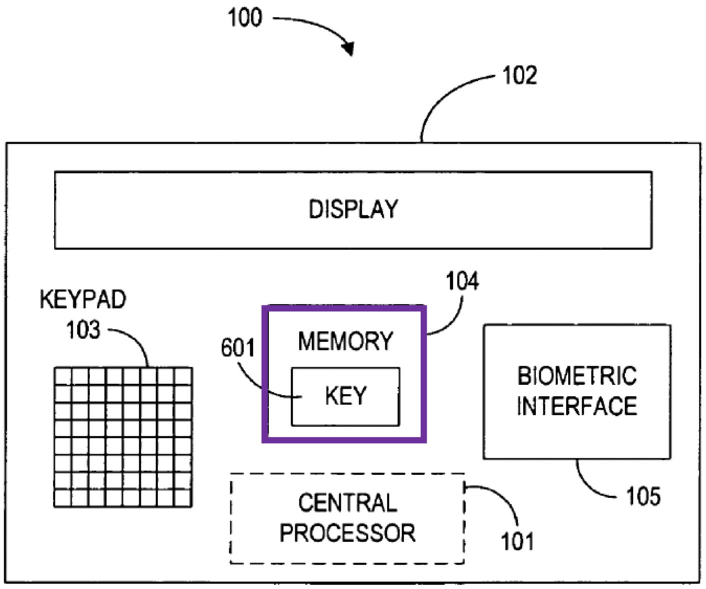
Brown, Fig. 12 (showing variable account number). Therefore, Brown also teaches that there are no fixed account numbers displayed on Brown's payment card at least because Brown teaches displaying a wholly variable payment account number.

(c) Motivation to Combine

A POSITA would have found it obvious and would have been motivated to implement Walker's payment device 100 with a ***thin-shaped body***. Smart cards had long been known in the art; the EMV specifications standardized smart card processing in 1994. *Dec.,* ¶122. Further, a POSITA would have found it obvious and would have been motivated to implement Walker's payment device to "resemble[] a typical payment or bank/ATM card" conforming to relevant form-favor standards "so as to allow rapid assimilation into the payment card system and its use by consumers" as explicitly taught by Brown. *Brown,* [0091]. A POSITA would have had a reasonable chance of success in making the modification because at the time it was already common for smart cards to be thin, resembling a typical payment card. *Dec.,* ¶122.

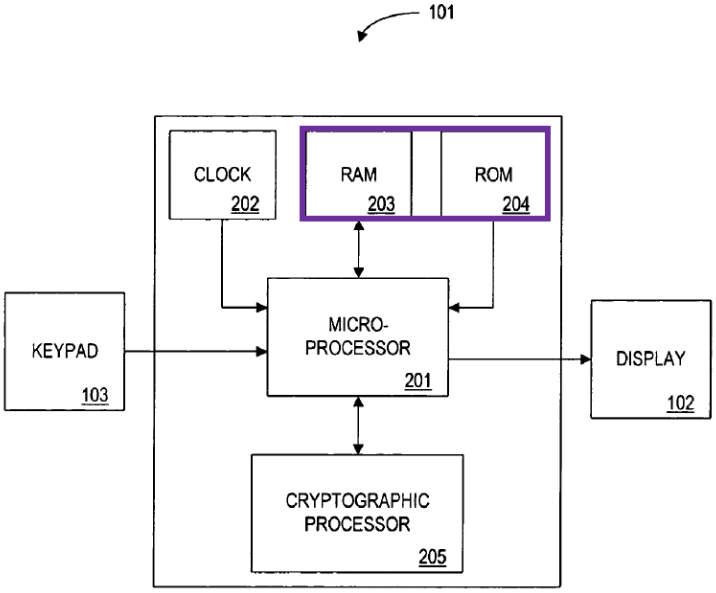
3. 1(b): "a memory;"

Walker's "device includes *a memory* device connected to the processing unit" which is "memory 104" Walker*,* [0024], [0043], [Abstract].



Walker, Fig. 1 (annotated).

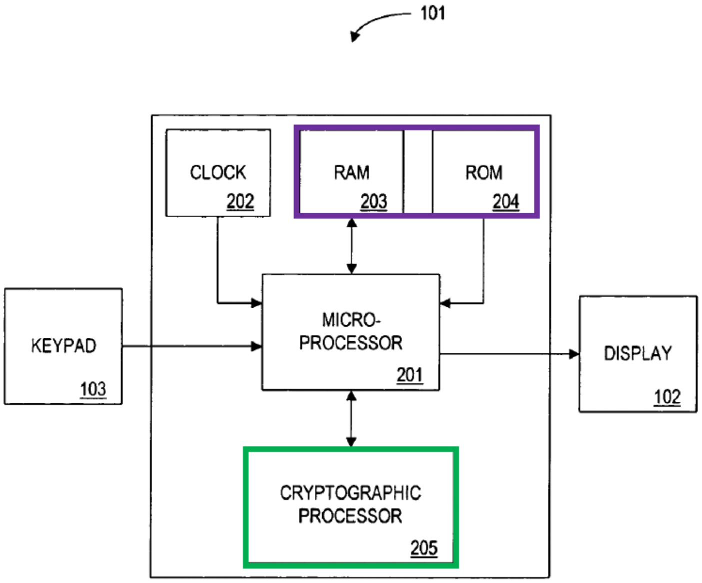
Further details of the central processor 101 of Walker's device 100 are shown in Fig. 2. Specifically, the central processor 101 includes a microprocessor of 201 "connected to a clock 202, **a random-access memory (RAM) 203, a read-only memory (ROM) 204**, and a cryptographic processor 205. *Walker,* [0044] (emphasis added).



Walker, Fig. 2 (annotated).

4. 1(c) "a cryptographic processor coupled to the memory; and"

Walker's device 100 includes a <u>*cryptographic processor*</u> 205. *Walker,* [0044], Fig. 2.



Walker, Fig. 2 (annotated).

Walker's "single-use credit card number is generated by the device **cryptoprocessor 205,** using a private key 601 stored in the device **memory 104 (preferably the ROM 204).**" *Walker,* [0050] (emphasis added). Accordingly, Walker's cryptographic processor 205 is coupled to and accesses the memory. *Walker,* [0044], [0050], Fig. 2.

5. 1(d) "a reader interface, including at least one interface selected from a set comprising: a magnetic-stripe, a smart card reader interface, a magstripe inductor interface, an RF interface, an NFC interface, and a wireless interface, and"

(a) Walker

Walker teaches that the cardholder "transmits a single-use credit card number 300 to the merchant" who then "transmits" the number to a credit card issuer. *Walker,* [0045], [0048]. Walker teaches that the cardholder may purchase goods "in person, via telephone or via the Internet[.]" *Walker,* [0046].

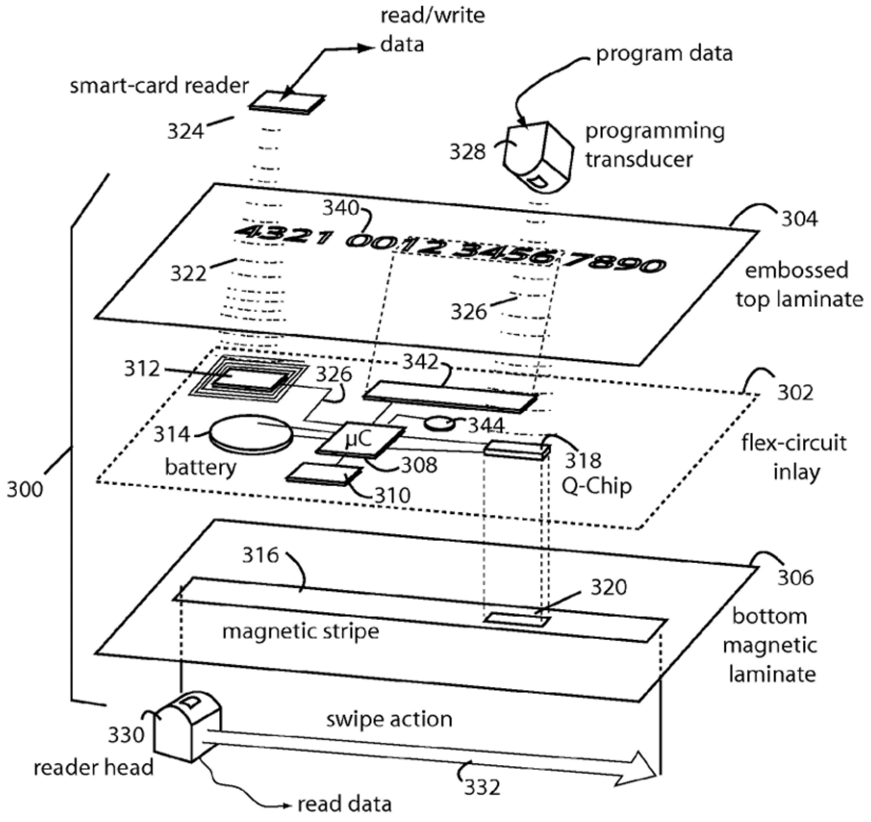
Walker does not provide specificity regarding how Walker's device transmits limited-use payment information to the merchant, noting that the single-use credit card number is "read, shown or otherwise transmitted to the merchant." *Walker,* [0063]. Walker notes that there is a risk of "incorrect keying" if the number is manually entered. *Walker,* [0048].

(b) Brown

In related art, Brown's smart card device includes a "dynamic magnetic stripe" (i.e., *<u>a magnetic-stripe</u>*) and an "internal dynamic account number generator

[] able to reprogram some of the magnetic bits encoded in the magnetic stripe to reflect the latest virtual account number." *Brown*, [0022], Abstract, [0041], [0066]-[0067], [0070].

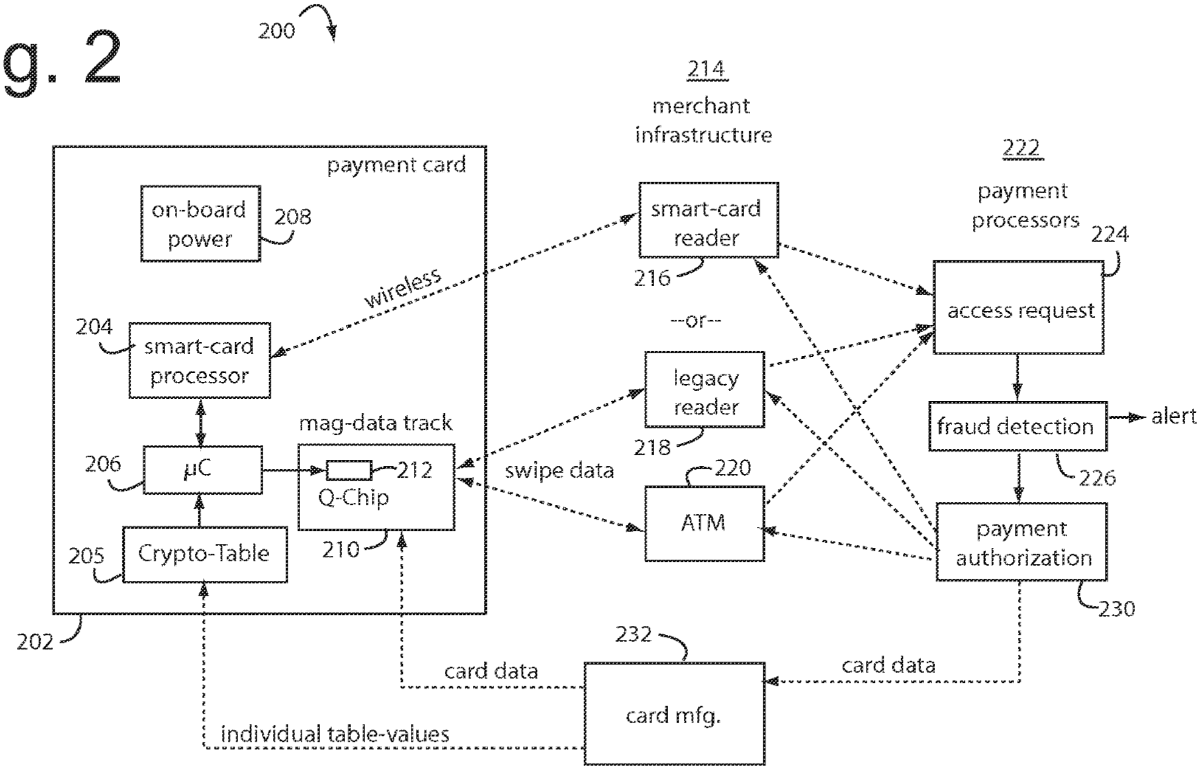
Brown's smart card device further includes a "contact/contactless programing inducer 312" and an "inductive or wireless coupling communication channel 326" that may be used "with *Near Field Communication* or similar *wireless communications*." *Brown,* [0094] (emphasis added). Brown explains that the "contact/contactless reader 324 (FIG. 3)" is "conventional" and "already typically deployed throughout the world[.]" *Brown,* [0112].



Brown, Fig. 3.

Brown teaches that it is advantageous for its smart card to work with both magnetic stripe readers and contact/contactless readers and demonstrates "how magnetic stripe and contact/contactless financial network infrastructures can be simultaneously supported." *Brown,* [0066]-[0069], [0112], Fig. 2.

Fig. 2



Brown, Fig. 2.

Thus, Brown teaches <u>*a reader interface*</u>. Brown's payment card further includes an "industry-standard contact/contactless smart-card processor" (smart-card processor 204) coupled to the reader interface. *Brown,* [0067], Fig. 2.

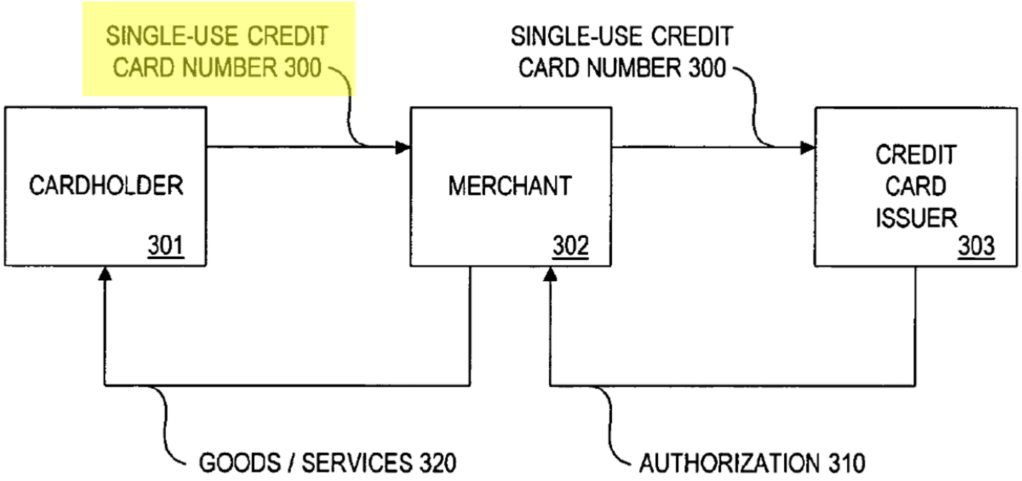
(c) Motivation to Combine

Based on the teachings of Brown, it would have been obvious, and a POSITA would have been motivated to configure Walker's device to include a reader interface comprising a dynamic magnetic stripe and/or NFC interface so that Walker's single-use credit card number can be transmitted to a merchant with conventional POS infrastructure. *Dec.,* ¶¶134-136. A POSITA would have been motivated to combine the prior art elements of Walker's smart card with Brown's dynamic magnetic stripe and NFC interfaces according to known methods to yield the predictable result of allowing Walker's smart card to communicate the single-use credit card number with a merchant POS terminal. *Id.* A POSITA would have recognized that without a reader interface, Walker's payment information would have to be manually input by the user or cashier even where a merchant POS terminal is available, increasing the time to complete the transaction, holding up the line for other customers, and increasing the chance of error should an incorrect payment number be input manually. *Walker,* [0048] (risk of "incorrect keying"); *Dec.,* ¶135. A POSITA further would have found it obvious and been motivated to couple a reader interface comprising a dynamic magnetic stripe and/or NFC interface to Walker's processor 201 to allow the reader interfaces to send and receive data, as taught by Brown. *Dec.,* ¶¶135-136.

Brown recognizes and a POSITA would have understood that magnetic stripe and NFC interfaces were already well-known and conventional (and, in fact, standardized) well-prior to the Critical Date. *Dec.,* ¶136. Given the ubiquity of magnetic stripe and NFC payment cards technology, there would have been a reasonable expectation of success configuring Walker's smart card device to include a dynamic magnetic stripe and NFC interface, per Brown. *Dec.,* ¶¶134-136.

6. 1(e): "wherein payment information for a transaction is operable to be conveyed via the reader interface and comprises limited-use payment information, and"

Walker teaches transmitting (*convey[ing]*) a single use credit card number to a merchant. *Walker*, [0045], Fig. 3A. Because Walker's single-use credit card number "is different for each transaction" and "is preferably a 16-digit number that can be recognized as a conventional credit card number[,]" it qualifies as *limited-use payment information*. *Walker,* [0050]-[0051], [0047]-[0048].



Walker, Fig. 3A.

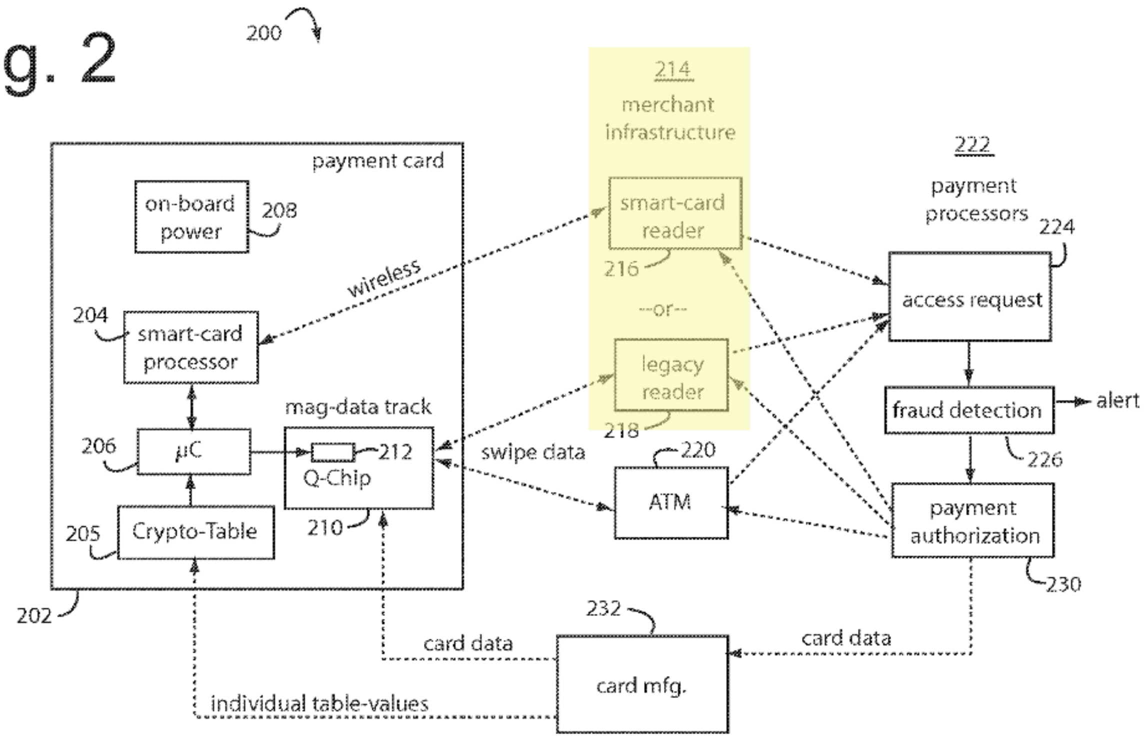
For the reasons discussed above, it would have been obvious to a POSITA to configure Walker's smart card device to transmit *payment information*, including the single-use credit card number to the merchant terminal via a dynamic magnetic stripe or NFC interface (i.e., *the reader interface*). *See* Claim 1(d).

7. *1(f): "wherein further the limited-use payment information is to be used in place of card issuer payment information for payment transactions by said device at payment card reader facilities."*

Walker's single-use credit card number (i.e., *the limited use payment information*) *is to be used in place of* a conventional credit card number (i.e., *card issuer payment information*). *Walker*, [0048], Fig. 3A; Walker teaches that "[a] cardholder 301, wishing to purchase goods or services from a merchant 302 … transmits a single-use credit card number 300 to the merchant" and "[t]he merchant 302 transmits the single-use credit card number 300 to a credit card issuer 303." *Walker,* [0045], Fig. 3A. "The credit card issuer 303 returns an authorization 310 to the merchant, based on which the merchant delivers the desired goods or services 320 to the cardholder." *Id.* Specifically, the card issuer "**maps the single-use credit card number onto a conventional credit card account** and determines whether the transaction is authorized (step 380); if so, the central system returns an authorization code for display on the merchant's authorization terminal" (i.e., *payment card reader facilities*). *Walker,* [0048] (emphasis added). Thus, Walker's single-use credit card number is used *for payment transactions* at the merchant's authorization terminal (i.e., *payment card reader facilities*).

To the extent that Walker does not specifically teach that the merchant's payment terminal includes a *payment card reader,* Brown teaches that the merchant infrastructure at the time included magnetic stripe readers 218 and contact/contactless smart-card readers 216, and it would have been obvious to convey Walker's limited-use payment information through these payment card readers for the reasons discussed above at Claim 1(d). *Brown,* [0066]-[0069], [0112], Fig. 2.

Fig. 2



Brown, Fig. 2.

B. Claim 8

1. 8(a): The device of claim 1, wherein the reader interface is operable to wirelessly receive cardholder transaction information and to identify a valid user through at least one user-validation action, selected from a set of [sic]comprising:… a device user interface receiving a user entered a valid PIN or Key-Code; […] a device biometric recognition of a valid user…

(a) Walker

Walker's payment device 100 "may be activated through the input of a unique cardholder identifier such as a personal identification number (*PIN*)" or "a suitable ***biometric*** record such as the cardholder's fingerprint." *Walker,* [0043] (emphasis added), [0046] (before a "transaction-specific, single-use credit card number" is generated, the cardholder "first inputs ***his PIN*** or ***biometric*** data to access the device (step 351).") (emphasis added).

Walker's "single-use credit card number is generated by the device cryptoprocessor 205 using a private key 601 stored in the device memory" as well as a nonce value, initialization variable, and account number. *Walker,* [0050], [0056], [0060]-[0063]. Walker does not teach how the values required for generating the single-use credit card number come to be stored in the device memory nor discuss specific messages exchanged with a point of sale merchant during a transaction.

(b) Brown

Brown teaches that during "initial card personalization" a "stream of [personalization] data" is sent "over an inductive or wireless interface 326" to appropriate memory locations in the card. *Brown,* [0094]-[0095]. For example, a "table of cryptographic values associated with the PAN [Payment Account Number]" may be stored and then used in financial transactions. *Brown,* Abstract, [0048]-[0049], [0134]. Brown further teaches "maintaining this channel for use with

Near Field Communication or similar wireless communications." *Id.*, [0094], [0110] (describing "data receptor[s]" on the card, such as a "Near field Communication (NFC) device[,]" that provide the card with "initial programming and personalization data" that is stored in the card's non-volatile memory). Therefore Brown teaches that a payment account number (*cardholder transaction information* that will be used to complete a transaction) is received via the card's NFC interface (*the reader interface*).

Brown's payment card 202 includes "data formats" dictated by industry standards including ISO and EMV standards. *Brown,* [0070] (all components "must fit within these constraints."). A POSITA would have understood that at the time, the relevant standards included EMV Version 4.3, which identifies transaction-related data sent to the card during the payment process, including *cardholder transaction information*. Ex.1034; *Dec.,* ¶144.

(c) Motivation to Combine

In the combination, the NFC interface (reader interface) wirelessly receives *cardholder transaction information* first when account information is wirelessly provisioned to the card and second, during a transaction from the POS (point-of-sale) reader in accordance with EMV standards.

As discussed above at Claim 1(d), it would have been obvious to include an NFC reader interface on Walker's card as taught by Brown. A POSITA would have been further motivated to use that interface to transfer <u>*cardholder transaction information*</u> including Walker's account number and nonce values to the memory of Walker's payment card. A POSITA would have recognized the benefit of using an existing card communications channel to load payment information to memory, rather than adding further hardware. *Dec.,* ¶146. A POSITA would have had a reasonable expectation of success in transferring transaction information to the memory of Walker's payment card using NFC because NFC technology was well-known and standardized by the Critical Date, and a POSITA would have been familiar with how to implement NFC to transfer data to a card memory, as taught by Brown. *Id.*

In addition, a POSITA would have been motivated to use the NFC interface to receive <u>*cardholder transaction information*</u> from the POS terminal during the transaction based on the teachings of Brown and a POSITA's understanding the EMV standards. *Dec.,* ¶147. A POSITA would have understood that when transaction-specific data (e.g. merchant data) is available to the payment card and available when generating a cryptogram it can increase security. *Id.* A POSITA would have understood that the standards discussed POS terminals sending such information to a payment card. *Ex.1034* (*EMV4.3)*, 54-56. A POSITA would have been motivated to make a payment card that is compliant with industry standards—including EMV standards—so that the payment card will already be compatible with existing POS terminals and with payment processing systems, as specifically taught by Brown. *Brown,* [0070]. Because the relevant feature—receiving cardholder transaction information wirelessly—from a POS terminal was standardized, a POSITA also would have had a reasonable expectation of success in making the proposed combination. *Dec.,* ¶146.

2. 8(b): wherein a display of the device is operable to display transaction information through a user interface, and wherein transaction information includes at least one of a set comprising: a transaction time; a transaction amount; transaction merchant information; a transaction location; a transaction facility; card information; a partial card number; graphical card images; and

Walker's device includes a "display 102 for prompting the user or displaying information." *Walker*, [0044], Figs. 1-2. The device also "quer[ies] the cardholder on display 102 whether it should generate a single-use credit card number" and further asks the user to enter "the amount of the purchase" (*a transaction amount*) and "a merchant code" (*transaction merchant information*) through a keypad 103 to be shown on display 102 (*user interface*). *Walker,* [0046], [0043], Fig. 3B.

3. Claim 8(c): wherein upon validating the user, the user-interface is operable to receive a valid user input, of at least one user action selected from a set comprising: a payment approval

authorization; a payment denial; and an adjustment of a transaction payment.

Walker teaches that "[i]f access is granted" after the cardholder inputs his PIN or biometric data, the device "quer[ies] the cardholder on display 102 whether it should generate a single-use credit card number" and "[t]he cardholder responds by requesting generation of a credit card number (for example, by keying 'YES')[,]" which is a *payment approval authorization*. *Walker,* [0046].

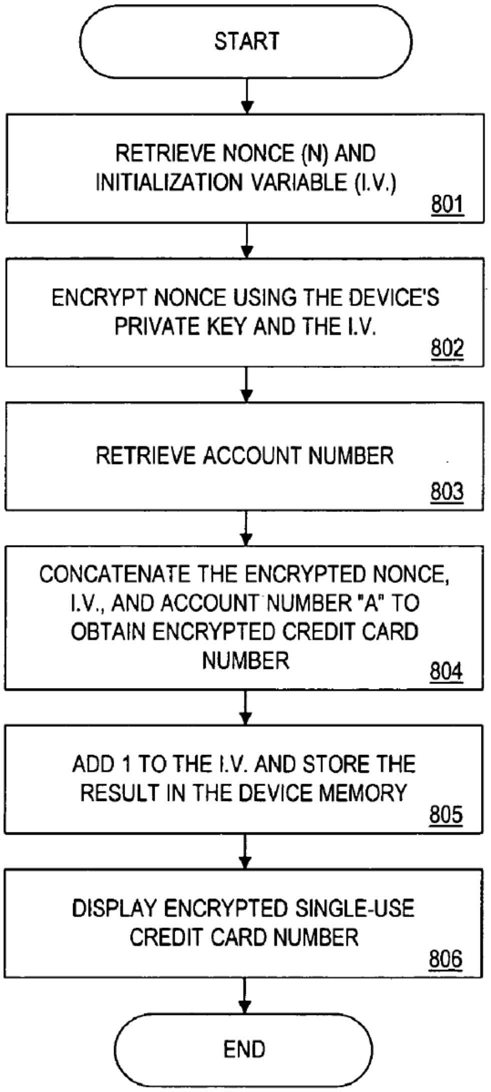
C. Claim 10

1. 10(a): The device of claim 1, wherein the processor cryptographically dynamically generates a one-time limited-use number based on combination of a card device transaction sequence count, and

Walker teaches that the cryptographic processor dynamically generates the single-use credit card number (i.e., *a one-time limited-use number*) based in part on an "initialization variable" that "is set at 0 (zero) when the card is newly issued, and is incremented each time a single-use credit card number is generated." *Walker*, [0056], [0050], [0079] ("Each time the credit card is used the IV increments by 1."). Because the initialization variable is initially set at zero and then incremented each time a single-use credit card number is generated, it qualifies as *a card device transaction sequence count*.

Walker shows the steps for "generating an encrypted single-use credit card number" in Fig. 8. *Walker,* [0060]. First in step 801 "the device central processor 101 retrieves the nonce 602 **and the initialization variable 704** from the device memory 104." Then "[i]n step 802, the nonce is **encrypted using** the user's private key K and **the IV**" as represented by the equation "C=E$_k$(N, IV)." *Walker,* [0060].

Ultimately, "the encrypted nonce C, the initialization variable IV, and account number A are concatenated to form an encrypted, single-use credit card number CCN: CCN=C_IV_A, where _ denotes concatenation." *Walker,* [0061]. The IV is then incremented and the result is stored. *Walker,* [0062].


START
RETRIEVE NONCE (N) AND INITIALIZATION VARIABLE (I.V.)
801
ENCRYPT NONCE USING THE DEVICE'S PRIVATE KEY AND THE I.V.
802
RETRIEVE ACCOUNT NUMBER
803
CONCATENATE THE ENCRYPTED NONCE, I.V., AND ACCOUNT NUMBER "A" TO OBTAIN ENCRYPTED CREDIT CARD NUMBER
804
ADD 1 TO THE I.V. AND STORE THE RESULT IN THE DEVICE MEMORY
805
DISPLAY ENCRYPTED SINGLE-USE CREDIT CARD NUMBER
806
END

Walker, Fig. 8.

2. 10(b): at least one of a set of information including:

…
a user card account number;
a device account number;
device secret keys;
card issuer keys;
…
an account information;
…

Walker's single use credit card number "is generated by the device cryptoprocessor 205, using a private key 601" (*device secret keys* or *card issuer keys*) by cryptographically combining the initialization variable with the account number (i.e., *a user card account number)* and the encrypted nonce value (*account information*), which is itself a cryptographic combination of the user's private key, the nonce (device secret key) and the IV. *Walker,* [0060]-[0061].

3. 10(c): wherein the processor increments the card device transaction sequence count on each transaction.

Walker teaches that *the processor increments* the initialization variable (i.e., *the card device transaction sequence count*) each time a single-use credit card is generated for a transaction (i.e., *on each transaction*). *Walker*, [0056], [0062] ("The initialization variable is incremented and the result is stored in the device memory 104 (step 805): IV=IV+1"), [0079].

VI. GROUND 2: CLAIMS 4-7 AND 9 ARE OBVIOUS OVER WALKER, BROWN, AND GAUTHIER

A. Claim 4 [8]

1. Walker

Walker's "limited-use payment information" comprises Walker's account number, which is limited-use payment information provided by the issuer. *See* Claim 9(b).

2. Gauthier

Gauthier teaches a secured account number, different than the user's primary account number (PAN), that is **only** used for "wireless transactions" with a proximity reader, using "a contactless mode, or an infrared mode, RF mode (i.e. Radio Frequency), and the like[.]" *Gauthier,* [0022], [0037], Fig. 1. Gauthier teaches that if a user "enters the secured account number onto a Web form to conduct a transaction, the transaction is not authorized by the issuer[.]" *Gauthier,* [0023]. Gauthier teaches that the secured account number might be entered into a web form by a thief that "surreptitiously intercepts the secured account number during a contactless purchase transaction" and that because it "is configured to resemble a real account number, it will deceive the unauthorized user into believing that it is an operable account number" that can be used for web transactions. *Id.* Since the limited

[8] *See* Claim Listing Appendix.

use account number is not usable for online transactions, it will "prevent the transaction that the thief tries to conduct from being authorized." *Id.* Therefore Gauthier teaches that use of the secured account number in an online (card-not-present) transaction is rejected by the card processing authority as not valid. *Id.*

In contrast, "[i]f the secured account number is valid and if the transaction is identified as a wireless transaction" the secured account number is converted to the user's real account number and transmitted for payment authorization. *Gauthier,* [0043], [0054]-[0059], Figs. 3-4. Therefore, Gauthier teaches that use of the secured account number in a card-present transaction with a proximity reader with a valid transaction identifier is approved as valid by the card processing authority. *Gauthier,* [0057] ("the transaction is authorized…the transaction is cleared and settled"), [0058]-[0059].

Gauthier teaches a "smart card." *Gauthier,* [0019], [0034]. The "secured account number may be stored in a database…preferably accessible to at least one of the payment processing system 120 and/or the issuer 130, since the issuer 130 authorizes or does not authorize the user's transaction." *Gauthier,* [0039]. A POSITA would have understood that the card issuer and the card processing authority may be the same entity (as in the case of American Express or Discover) and therefore Gauthier teaches or renders obvious the *card processing authority* rejecting the transaction as invalid. *Dec.,* ¶159; *Gauthier*, [0029], [0035].

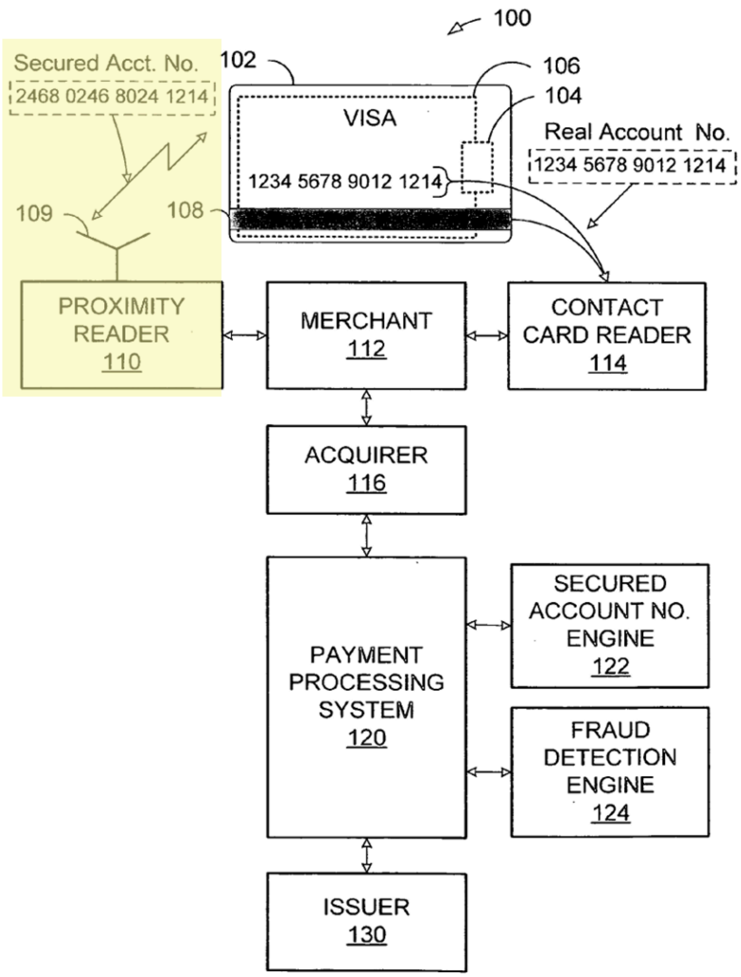


FIG. 1

Gauthier, Fig. 1 (annotated).

Gauthier further teaches "a POS [point-of-sale] transaction type identifier" that indicates "that the transaction was a wireless type of proximity transaction[.]" *Gauthier*, [0042]. If a secured account number is received by the payment processing system 120 but there is no identifier "indicating a proximity transaction" then the "fraud detection engine 124" associated with the payment processing system 120

(<u>card processing</u> *authority*) may "deny the transaction." *Gauthier,* [0047], [0058]-[0059].

Gauthier teaches or renders obvious that the secured account number is <u>*provided by the issuer.*</u> Specifically, Gauthier teaches that the secured account number may be generated "when generating real account numbers" and "preloaded" on the consumer's device. *Gauthier,* [0040]-[0041]. A POSITA would have understood, or found it obvious, that credit card account numbers are generated and assigned by card issuing authorities. *Dec.,* ¶161. Further, it would have been desirable for the real account number to be generated by a card issuing authority because, ultimately, the secured account number must be stored in a lookup table accessible to the issuer along with the real account number. *Id.; Gauthier,* [0039].

Gauthier teaches that the secured account number changes when "the user's real account number expires" and it is therefore <u>*limited use payment information*</u>. *Gauthier,* [0020].

3. Motivation to Combine

It would have been obvious and a POSITA would have been motivated to use an issuer-supplied secured account number in place of Wal65ker's account number when making NFC payments, as taught by Gauthier. *Dec.,* ¶¶163-165. In the Walker-Brown combination, the payment information transmitted via NFC to a merchant for payment includes an account number—an unchanging identifier for the cardholder. *Walker,* [0048]-[0049], [0051]; *see* Claim 1(d). Walker's account number may resemble a traditional 16-digit card number and, if intercepted, a thief may attempt to use that number for an online payment transaction. *Walker,* Fig. 6.

Gauthier teaches and a POSITA would have recognized that proximity-type wireless financial transactions may be intercepted, "a major concern[.]" *Gauthier*, [0005]-[0006]. Further, a consumer may not immediately know when their information has been intercepted, making enforcement efforts against bad actors challenging. *Gauthier,* [0006]. Gauthier teaches that if the secured account number is intercepted, and the thief attempts to use it for an online transaction, not only will the transaction be denied, but further "a fraud protocol" is initiated and the authorities may be alerted. *Gauthier,* [0047], [0058]. A POSITA would have understood and would have been motivated to implement a system that prevents unauthorized transactions and allows fraudulent transaction attempts to be immediately reported, recognizing the greater security of such a system. *Dec.,* ¶164.

A POSITA would have had a reasonable expectation of success in implementing an NFC-specific account number into Walker's payment card as it would merely change one issuer-provided (generally 16-digit) account number for another issuer-provided account number. *Dec.,* ¶165. In the combination, the secured account number would continue to have an expiration date, as taught by both Walker (*Walker,* [0083]) and Gauthier (*Gauthier,* [0020]). Notably, Gauthier cites an earlier patent in the Walker patent family (U.S. Patent No. 6,163,771), further confirming the relatedness of the references' teachings.

B. Claim 5

1. Claim 5(a):

(a) Walker

Walker's smart card device asks the cardholder "whether it should generate a single-use credit card number" and the cardholder responds "YES" and enters "the amount of the purchase in step 356 or a merchant code number provided by the merchant" (*transaction information* and *merchant information*). *Walker,* [0046].

Walker teaches that the single-use credit card number is then sent to the credit card issuer for authorization (as part of a *request for payment*). *Walker,* [0045], Fig. 3A, [0048], Fig. 3B. The credit card issuer stores information associated with a transaction, including the transaction amount and merchant identification number, in a database. *Walker*, [0055], Fig. 7.

Walker does not specify how the transaction and merchant information is used in the payment authorization process or what information is sent to the issuer during the authorization process other than the single-use credit card number. Walker does teach that issuers may chose not to "approve purchases that exceed available credit" indicating that the issuer is also sent the transaction amount (*transaction information*) at this time. *Walker,* [0069]; *Dec.,* ¶168.

(b) Gauthier

Gauthier teaches that an "authorization request message" (*request for payment*) can include "an account holder's payment account number" (*payment information*), "sale amount" (*transaction information*), "merchant transaction stamp" (*merchant information*), "POS transaction number [and] POS transaction type" (*payment card reader information*). *Gauthier,* [0030]; *'820 Patent* at 19:30-34 (identifying "amounts" as "credit card transaction information"). Gauthier teaches that the "authorization request message for a transaction is created after a customer purchases a good or service at a POS terminal" and is "sent from the POS terminal located at a merchant to the merchant's acquirer, to a payment processing system, and then to an issuer." *Gauthier,* [0027], [0042]-[0043].

(c) Motivation to Combine

It would have been obvious and a POSITA would have been motivated to include a purchase amount and merchant information in Walker's request for payment sent to the card issuer for authorization, as taught by Gauthier. *Dec.,* ¶170. Walker already teaches that a request for authorization is sent to the issuer which may deny authorization if the purchase "exceed[s] available credit[,]" which requires the issuer to know the transaction amount. *Walker,* [0069]; Therefore, a POSITA would have understood and been motivated to include the purchase amount in the request for payment sent to the issuer. *Dec.,* ¶170. Likewise, a POSITA would have understood that including a merchant information in the payment authorization would provide the issuer with a record of where fraud has occurred, in the case that Walker's card was stolen and used improperly, and to also provide a history of a user's transactions. *Id.* Indeed, a POSITA would have understood that the issuer database including the merchant identifier and transaction amount for each transaction would first need to receive this information before storing it in the database. *Id.*; *Walker*, [0055], Fig. 7. A POSITA would have had a reasonable chance of success in making the proposed combination because merchant information and transaction information was already commonly received by and processed by issuers by the Critical Date. *Dec.,* ¶170.

2. Claim 5(b):

(a) Gauthier

See Claim 4. Gauthier further teaches that a secured account number is transmitted to a proximity reader device 110 (*payment card reader*) and further that "a POS [point-of-sale] transaction type identifier (indicative that the transaction was a wireless type of proximity transaction) [*valid payment card reader information*] is received by the merchant 112 and is transmitted to the acquirer 116" and further to the "payment processing system 120[.]" *Gauthier*, [0042]; *see also* [0058]-[0059], Fig. 4.

Gauthier further teaches that someone may attempt to use the secured account number online (in a *card-not-present* transaction). *Gauthier,* [0023]. In that case, the "authorization request message…does not have the transaction type identifier (e.g., POS 91), or other indicator, indicating a proximity transaction." *Gauthier,* [0047], [0058], Fig. 4. Thus, Gauthier teaches there would be no *valid payment card reader information* if the secured account number is entered on a Web form as there is no payment card reader involved in the transaction. *Id.*

(b) Motivation to Combine

It would have been obvious and a POSITA would have been motivated to include payment card reader information in Walker-Brown's request for payment sent to the card issuer for authorization, as taught by Gauthier. *Dec.*, ¶173. A POSITA would have recognized that it was conventional in the credit card industry to include transaction type identifiers in transactions as Gauthier, a VISA-owned patent application, explains. *Gauthier,* [0043] (identifying "a conventional number used in the credit card industry" as "POS entry code 91" and further recognizing "international standards organization (ISO) indicator[s]"). Further, a POSITA would have recognized that different payment methods have different risk profiles, and that it may be easier to surreptitiously obtain payment credentials via contactless payment methods versus through a mag-stripe reader. *Gauthier,* [0006]; *Dec.*, ¶173. A POSITA would further have understood the benefits of including a merchant identifier, as discussed above at Claim 5(a). A POSITA would have had a reasonable chance of success in making the proposed combination because the use of merchant identifiers was known to a POSITA and the subject of standards. *Dec.*, ¶173.

3. Claim 5(c):

See Claim 4.

4. Claim 5(d):

See Claim 4.

5. Claim 5(e):

See Claim 5(d).

C. Claim 6

See Claims 4, 5(b)-(c).

D. Claim 7

1. Claim 7(Pre):

See Claims 4, 5(b)-(c).

2. Claim 7(a):

Walker's account number expires when Walker's payment card expires. *Walker,* [0083]-[0084]. Gauthier likewise teaches that the secured account number changes when "the user's real account number expires[.]" *Gauthier,* [0020]. A POSITA would have understood or found obvious that an expiration date is a *finite amount of time* for which the payment information is valid for use, after which attempts to use the payment information will be declined. *Dec.*, ¶179. A POSITA therefore would have found it obvious and would have been motivated to implement a secured account number (per Gauthier) that expires on Walker's payment card for the reasons discussed in Claim 4. *Id.*

3. Claim 7(b):

See Claim 5(a). Walker teaches that the account number assigned to Walker's device cannot be used for payment alone but rather must be used to generate a single-use credit card number. *Walker,* [0050] ("knowledge of the account number does not allow an attacker to generate a valid single-use credit card number"), [0072]. Walker further teaches that the single-use credit card number can only be generated with user approval for the transaction. *Walker,* [0046] (cardholder responds "YES" and enters "the amount of the purchase in step 356 or a merchant code number provided by the merchant"). Therefore, Walker teaches that the issuer limits use of the account number for *transactions with the user approving* where the account number is invalid when used on its own, i.e. *when the card user is denying an approval* and therefore a single-use credit card number is not generated. *Walker,* [0046], [0050];

It would have been obvious and a POSITA would have been motivated to implement Gauthier's secured account number on Walker's payment device in place of Walker's account number such that the secured account number cannot be used for payment alone, but rather as part of a single-use credit card number generated when the user approves the transaction—as taught by Walker—for the reasons discussed in Claim 4. *Dec.*, ¶181.

4. Claim 7(c):

Walker's account number is assigned to Walker's payment device for use by the payment device and cannot also be assigned to another device unless Walker's card expires. *Walker,* [0083]-[0084]. Even after Walker's card expires, any new card provided with the same account number must be assigned a "different nonce and private key" so that "any credit card numbers generated with the old credit card will not match any new credit card numbers[.]" *Walker,* [0084]-[0085].

Gauthier's secured account number likewise is assigned to a particular payment device (*__Gauthier,__* [0019], [0021], [0040]) and likewise must be converted to the user's real account number (is used *__in place of card issuer information__*). *Gauthier,* [0055].

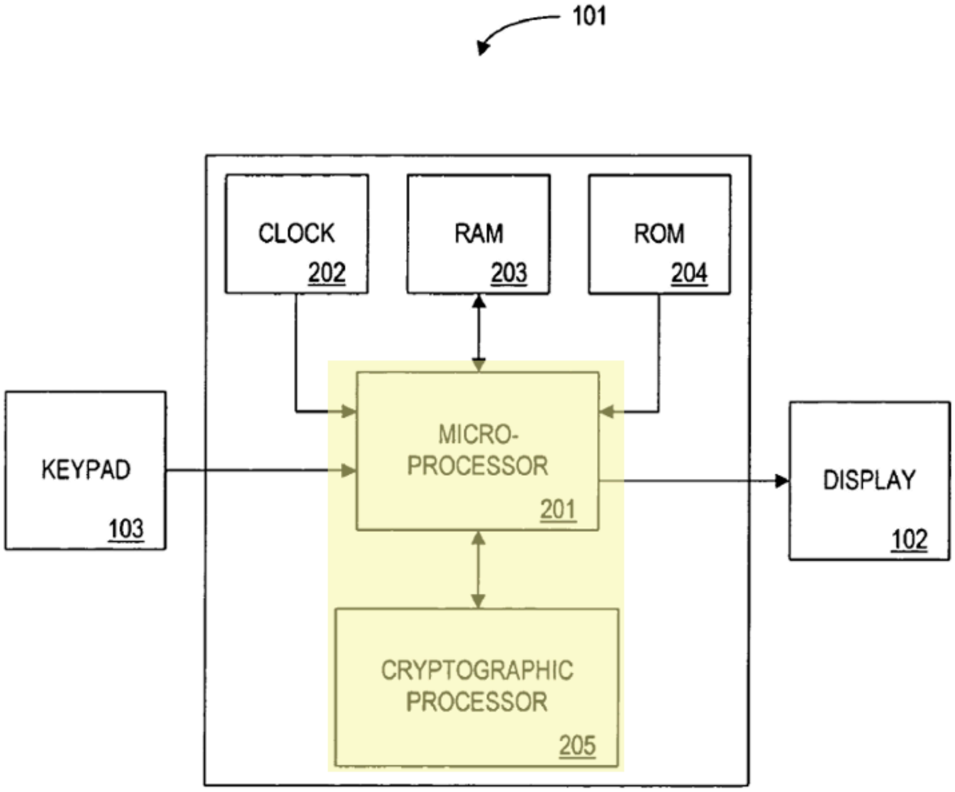
Therefore, it would have been obvious and a POSITA would have been motivated to implement Gauthier's secured account number on Walker's payment device to (1) be limited to use by Walker's payment device and (2) be used in place of card issuer information for the reasons discussed in Claim 4. *Dec.*, ¶184.

E. Claim 9

1. Claim 9(a):

Walker teaches a single-use credit card number that is *__dynamically-generated__* by the cryptoprocessor of Walker's payment card. *Walker,* [0050], [0056].

As discussed above at Claim 1(d), in the Walker-Brown combination, Walker's payment card includes a reader interface comprising a dynamic magnetic stripe and/or NFC interface coupled to Walker's micro-processor. In the combination, the reader interface *is accessible* to Walker's cryptographic processor through Walker's microprocessor to generate the single-use credit card number (*one-time limited-use payment information*).



Walker, Fig. 2.

2. *Claim 9(b):*

Walker's one-time use credit card number is a concatenation of "the encrypted nonce C, the initialization variable IV, and account number A… CCN:

CCN=C_IV_A[.]" *Walker,* [0061]. In combination with Gauthier (*see* Claim 4) it would have been obvious and a POSITA would have been motivated to use an issuer-supplied secured account number in place of Walker's account number. Therefore, Walker's credit card number includes a ***static limited-use portion*** (secured account number) and an encrypted nonce generated from the private key and incremented IV (***dynamically-generated limited-use portion***). *Walker*, [0060].

Walker's account number is ***limited-use*** because it expires. *Walker,* [0059], [0084] ("After a cardholder's card expires, his account number can be reused."). Further, the number of times the account number can be used is limited by the size of the initialization variable (IV) allowed, with a limit of 512 uses with a 9-bit initialization variable. *Walker,* [0058]-[0059]. In the combination, the secured account number would likewise expire, as taught by both Walker and Gauthier. *Gauthier,* [0020] ("The term 'static' means that the secured account number does not have to change between transactions, but may change when…the user's real account number expires.").

The encrypted nonce is ***limited-use*** because it can only be used for the transaction with the associated IV. *Walker*, [0065]-[0067].

3. Claim 9(c):

In the combination, Gauthier's secured account number is used by Walker in place of the assigned conventional credit card account number. *See* Claim 4;

Gauthier, [0020], [0043], [0054]-[0059], Figs. 3-4 (describing conversion of secured account number to a user's real account number in payment processing); *Dec.,* ¶190.

VII. GROUND 3: CLAIM 2 IS OBVIOUS OVER WALKER, BROWN, AND ENG

A. Claim 2

To the extent this limitation is entitled to patentable weight (*see* Section III.C.1), it is taught by Walker and Brown in view of Eng. *Dec*., ¶¶191-19494.

Walker teaches a card with a card body *free of any account numbers, expiration dates, card security codes, or other fixed payment numbers, disposed thereon*. *See* Claim 1(a).

In related art, Eng teaches a card that has: (1) *a card-holder name,* (2) credit card logo (*card payment network logo*), and a (3) Bank Name (*payment issuing logo)*. *Eng*, [0020]-[0021], [0042]. *Dec*., ¶196.

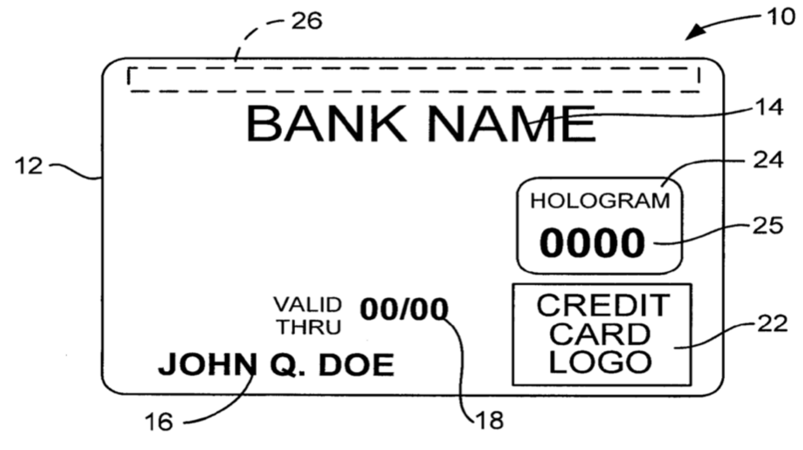


Fig. 2

Eng, Fig. 2.

To the extent embodiments of Eng's card also includes an expiration date and a portion of a PAN, a POSITA would have no reason to include those pieces of information on Walker's smart card device, since the payment credentials used by Walker's smart card constantly change and are one-time use. *See* Claim 1(e); *Walker,* [0043], [0046]; *Dec.*, ¶197.

1. Motivation to Combine

It would have been obvious and a POSITA would have been motivated to modify Walker's smart card to include a fixed card-holder name, payment issuing logo, and card payment network logo as taught by Eng. A POSITA would have understood that a user would have found it valuable to distinguish their cards from each other (for example, with a payment issuing logo and card payment network logo) and from similar cards that others in their household might have (with a cardholder name). *Dec.*, ¶198. Each of these pieces of information was well-known to a POSITA and common on payment cards. *Id.* A POSITA would have had a reasonable expectation of success in making this combination of known elements without undue experimentation. *Id.*

VIII. GROUND 4: CLAIM 3 IS OBVIOUS OVER WALKER, BROWN AND PATEL

A. Claim 3

1. Claim 3(a):

(a) Walker-Brown

As discussed above at Claim 1(d), in the Walker-Brown combination, Walker's payment card is provided with a dynamic magnetic stripe, as taught by Brown. In the combination, Walker's magnetic stripe would be reprogramed "to reflect the latest" one-time use payment information per Brown. *Brown,* [0022]. The magnetic stripe would further include the information required by standards to be present in mag-stripe track data to ensure that Walker's payment card is usable in conventional POS infrastructure, including a CVC value. *Brown,* [0023], [0045], Fig. 2, [0069] (218, "legacy reader"); *Dec*., ¶199.

(b) Patel

Patel teaches assigning a payment card a "dynamic CVV" that "is read, changed, and rewritten to the card with each transaction." *Patel,* Abstract. Patel's dynamic CVV is coded to the magnetic stripe "[t]o pay for the goods or services" through "a magnetic card reader 130[.]" *Patel*, [0057]. The dynamic CVV is transmitted to the financial institution 150 (card issuer) which "authenticates the verification data, including the dynamic CVV 330, and transmits a verification code, including a new dynamic CVV 330 to the transaction device 130." *Patel*, [0059].

"The transaction device 130 reads the new dynamic CVV 330, and writes the new CVV 330," which was received from the card issuer, "to the magnetic strip 220" of the payment card. *Patel*, [0060].

Patel teaches that "a static CVV may also be provided for manual entry" to "facilitate online transactions." *Patel,* Abstract, [0007]. [0072] ("[A] static CVV 230 is printed on the card and it is retained as perpetually valid only for purchases where card data are input manually."). Therefore, Patel teaches that the dynamic CVV code is *limited-use payment information* that is *conveyed via the magnetic-stripe*. It is further *unique to the payment device and to the magnetic stripe*, as Patel teaches that the dynamic CVV is assigned by the financial institution to a specific payment card.

(c) Motivation to Combine

A POSITA would have been motivated and would have found it obvious to implement Patel's dynamic CVV techniques in the Walker-Brown payment device for use in mag-stripe payments. A POSITA would have understood that in magstripe payment transactions, track data is transferred to the merchant, including a verification code. *Dec*., ¶202, *Brown,* [0109] (citing ISO/IEC Standards 7810, 7811-1-6, and 7813). Typically, the discretionary data segment includes the card verification code. *Dec*., ¶202 (discussing ISO7813). Replacing the static CVV in the magnetic stripe data with a dynamic alternative would have increased the security of the payment system as another barrier for an unauthorized user to use the payment credentials, which a POSITA would have been motivated to implement. *Dec.*, ¶¶202-03.

A POSITA would have found it obvious to modify the Walker-Brown combination based on Patel's teachings because a dynamic CVV value was a known solution and it would have improved Walker's similar system in the same way, allowing the POSITA to obtain the predictable result described in Patel. *Id.* A POSITA would have had a reasonable chance of success in implementing a dynamic CVC into the Walker-Brown payment device because the Walker-Brown payment device already includes a programmable magstripe and because Brown already contemplates a dynamic CVV value being programmed to the magstripe. *Id.; Brown,* [0043].

2. Claim 3(b):

Patel's dynamic CVV and the complete limited-use payment information provided to the merchant through the magnetic stripe are *<u>both limited to the payment device</u>* and would be conveyed *<u>to the magnetic-stripe payment card reader</u>* in the combination. *See* Claims 1(d), 3(a).

3. Claim 3(c):

Patel's dynamic CVV and the complete limited-use payment information are both one-time use information. *See* Claims 1(e), 3(a); *see also Walker,* [0050] ("different for each transaction"); *Patel,* [0007] ("dynamic CVV is rewritten to the card with each transaction").

4. Claim 3(d):

Patel teaches that the dynamic CVV is coded to the magnetic stripe, and further that "a static CVV may also be provided for manual entry" to "facilitate online purchases[.]" *Patel,* Abstract, [0007]. Therefore, Patel teaches that the dynamic CVV coded to the magnetic stripe is only used in card present transactions and would not be valid for online transactions. In the combination, the complete limited-use payment information encoded on Walker's payment card is only used for magnetic stripe payments with a magnetic stripe payment card reader. *Dec.*, ¶206.

IX. GROUND 5: CLAIMS 11, 13-15, AND 17-20 ARE OBVIOUS OVER COLLINGE, KRANZLEY AND BROWN

A. Claim 11

1. 11(pre): An online payment system, the system comprising:

(a) Collinge

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

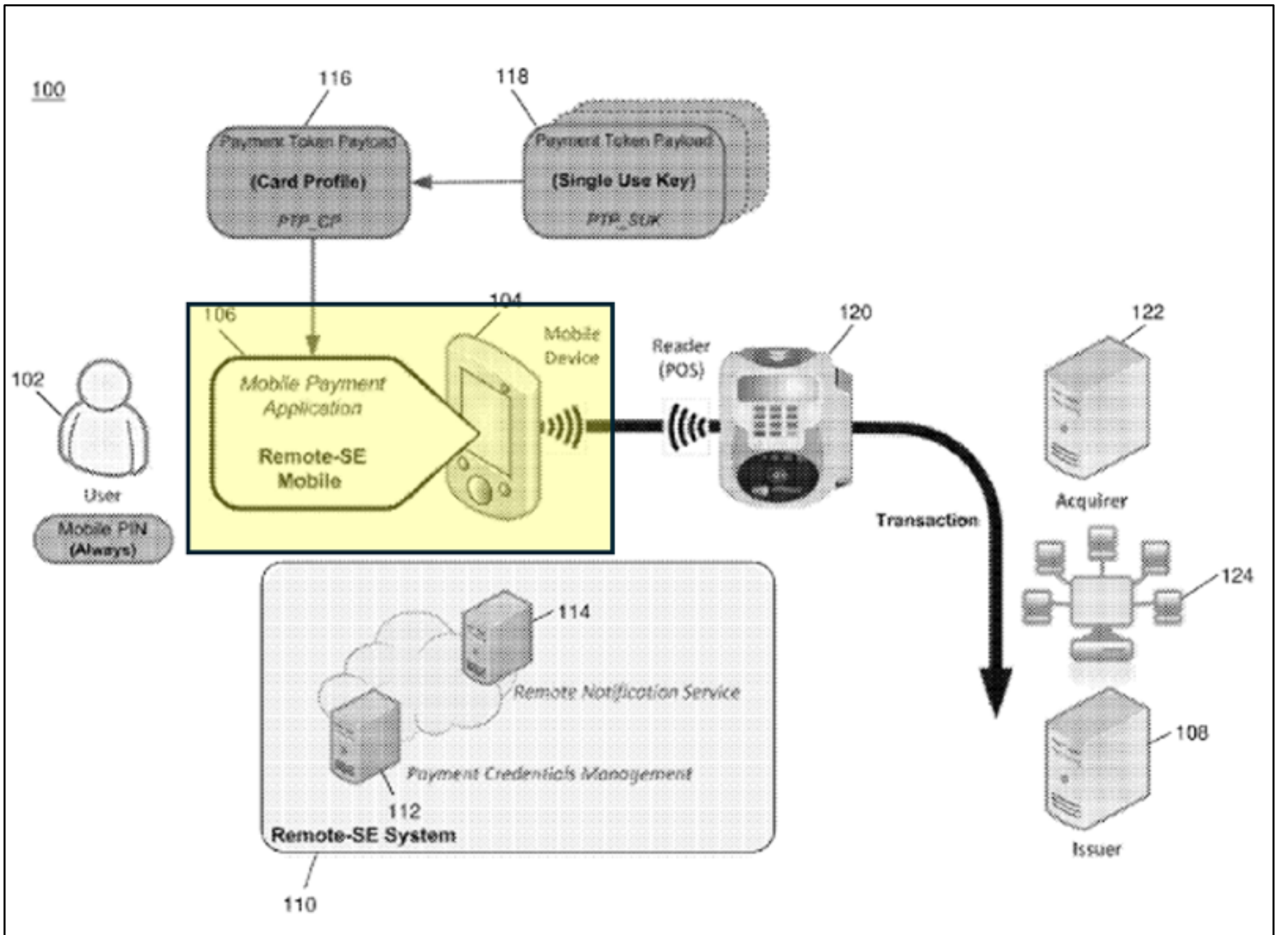
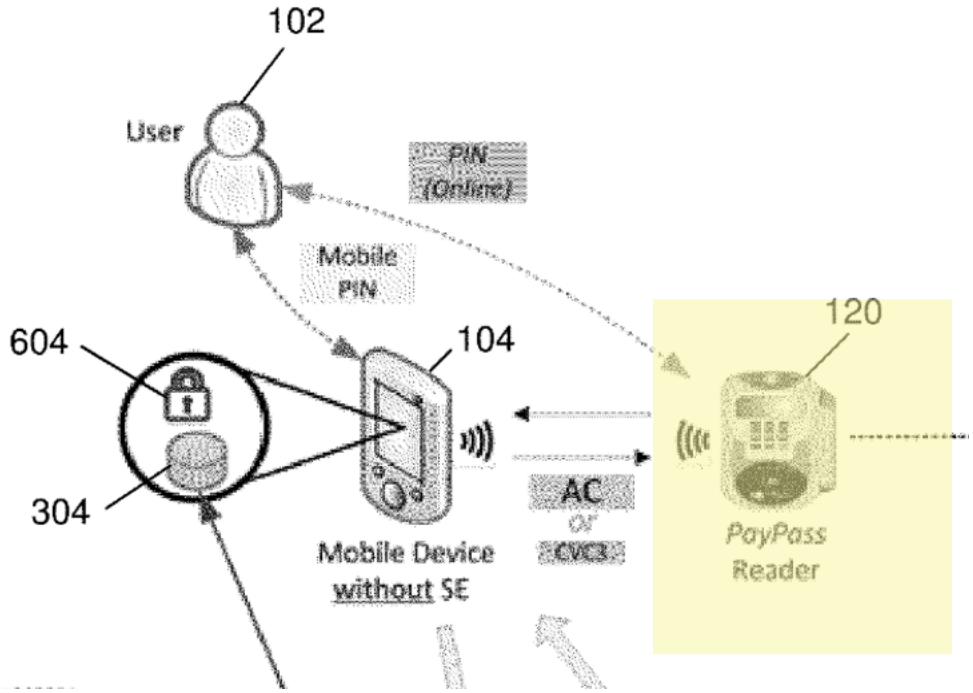


FIG. 1

Collinge, Fig. 1 (annotated).

One motivation for Collinge's invention was to allow a user to "conduct PayPass® transactions at PayPass®-enabled merchants with a mobile device[.]" *'095 Provisional,* [0003].



Collinge, Fig. 6 (excerpted, annotated).

Collinge teaches that a virtual primary account number (VPAN) can be used as an alternative to the card PAN. *'098 Provisional*, 159-160. Collinge teaches that using a VPAN is safer and can "mitigate the risk of any misuse of a PAN value" but provides limited implementation details. *'098 Provisional*, 159-160.

However, Collinge does not specifically teach how Collinge's payment credentials would be used to make purchases from a website.

(b) Kranzley

In related art, Kranzley teaches a mobile device 102 which includes a mobile payment application that may be used at "a physical storefront or **electronic commerce merchant**." *Kranzley,* [0038] (emphasis added). Kranzley teaches that the payment application may be "configured to operate in accordance with the PayPass standard[.]" *Kranzley,* [0020].

Kranzley teaches a "static virtual payment account number (or 'VPAN')" is used as an "alternative" to the issued PAN. *Kranzley,* [0036]. "An authorized user of the payment application may access the VPAN and use it to make a purchase transaction…along with its expiry date, and a dynamic code (generated by the payment application) to the merchant[.]" *Kranzley,* [0036]. Then, "[t]he payment provider uses the VPAN to look-up an actual PAN associated with a payment account of the customer[.] *Kranzley,* [0037]. The VPAN "may have its own virtual expiry date." *Kranzley*, [0036]. Use of the VPAN "ensure[s] that merchants are not made aware of the actual payment card information, as they are only exposed to the VPAN information." *Kranzley,* [0049].

Kranzley teaches "in electronic commerce environments, the customer may cause the payment application in the mobile device to display a VPAN, expiration date and dynamic account validation code" on the mobile device's display so that "[t]he customer may read the information from the display device and then key in that data into a Web page on a computer to complete the ecommerce transaction." *Kranzley,* [0040].

(c) Motivation to Combine

It would have been obvious and a POSITA would have been motivated to modify Collinge's mobile device to display payment credentials to complete an online payment transaction, as taught by Kranzley. *Dec.*, ¶¶214-223. It was well known that mobile wallets could be used in online transactions, and Kranzley demonstrated the feasibility of using PayPass in an online system. *Kranzley,* [0036]; *Dec.*, ¶215. A POSITA would have appreciated that performing an online transaction using Collinge's payment credentials and mobile payment application would have beneficially provided the user with flexibility to shop in more places with Collinge's secure payment credentials. *Id.* A POSITA would have had a reasonable chance of success in making the combination, including because (1) both Kranzley and Collinge teach compliance with PayPass standards when generating payment information and (2) the primary modification is simply displaying payment information that Collinge's mobile device already has on Collinge's touchscreen display (that Collinge's mobile device already has), which would have been well-within the skill level of a POSITA. *Dec.*, ¶216. Therefore, use of Collinge's payment credentials for online payment would have combined known elements to predictable result in display of payment credentials for use in online payment systems. *Id.*

A POSITA would have further been motivated to assign a VPAN to payment cards registered with Collinge's payment system, as taught by both Collinge and Kranzley, and to use the VPAN in place of a PAN for increased security. *'098*

Provisional, 159-160; *Kranzley,* [0049]; *Dec*., ¶¶217-223. A POSITA would have appreciated the risk that a user may inadvertently find themselves on a fraudulent webpage online that asks for payment credentials. *Id.* If the user's PAN is entered and stolen, the user will require a new payment card with a new account number, and they will have to re-setup any existing automatic payments, but not-so with a VPAN. *Dec.,* ¶218. In the combination, Collinge's mobile device would receive the VPAN, in place of PAN information in Collinge's payment credentials provisioned to the Collinge's mobile payment application as part of card profile 116. *Collinge,* [0048]. Collinge would simply use the VPAN instead of a PAN when generating payment credentials; nothing else about how Collinge generates payment information would change. The simple substitution of Collinge's PAN with a VPAN is a substitution of one known element for another and a POSITA would have understood that the substitution would have predictably increased the security of Collinge's payment system and protected the user's sensitive PAN information. *Dec*., ¶¶219-223.

2. *11(a): a thin payment device comprising no fixed payment numbers visible thereon; and*

As previously discussed, (Section III.C.1), the limitation "free of any fixed payment numbers visible thereon" is directed to printed matter and entitled to no patentable weight. *Dec.,* ¶224. Nevertheless, it is obvious based on Brown's teachings.

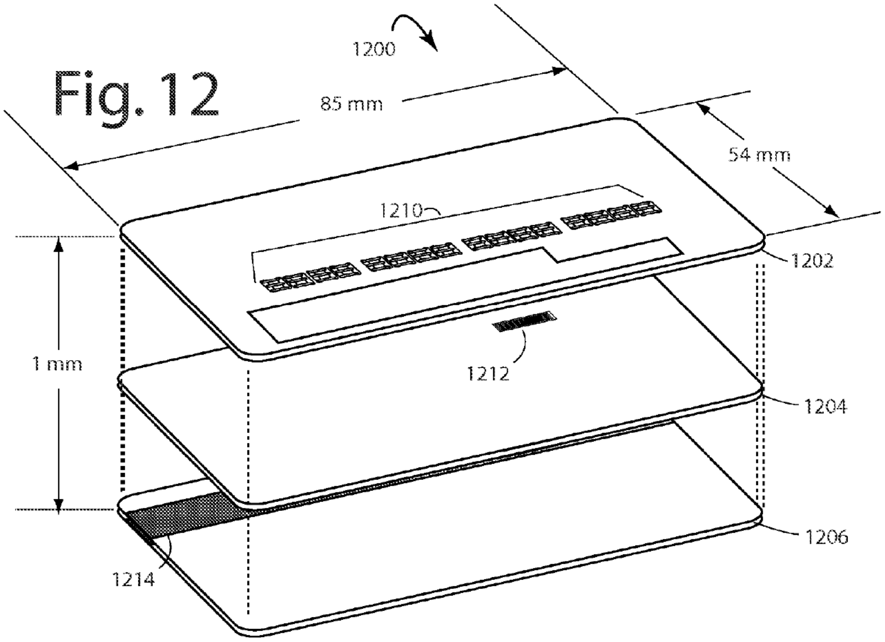
(a) Collinge

Collinge teaches that a "[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*, [0038]. Collinge further teaches that the authentication credentials provisioned to Collinge's mobile device are "associated with a payment card[.]" *'095 Provisional,* [0051], Fig. 2.

(b) Brown

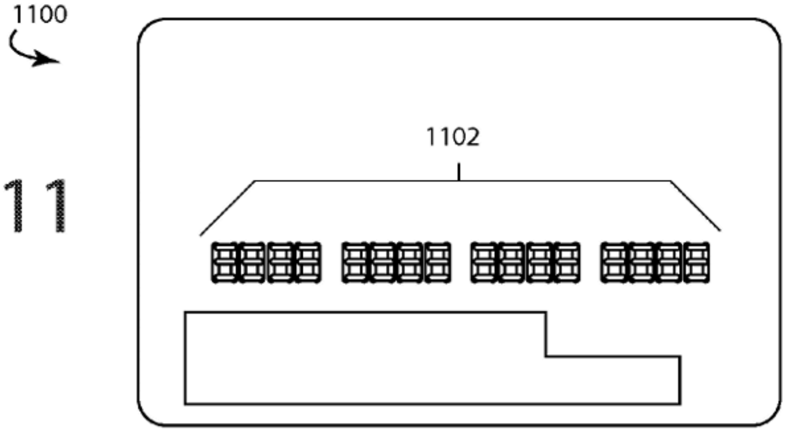
Brown teaches a smart payment card (*payment card device*) that is a thin card-shaped device. *Brown,* [0091] (citing payment card thickness standards), [0200] (describing a "smart card" as "1mm" in thickness).

Fig. 12



Brown, Fig. 12. Brown's payment card has a "full personal account number (PAN) [that] has been **implemented to be variable** on a visual display." *Brown,* [0200] (emphasis added).

Fig. 11



Brown, Fig. 1 (showing variable account number). Therefore, Brown teaches that there are *no fixed account numbers* visible on Brown's payment card at least because Brown teaches displaying a wholly variable payment account number.

Brown's smart card includes a "dynamic magnetic stripe[.]" *Brown,* [0022], Abstract, [0041], [0066]-[0067], [0070].

(c) Motivation to Combine

A POSITA would have found it obvious and would have been motivated to use Brown's payment card device free of any fixed payment numbers visible thereon with Collinge's NFC-enabled computing device (i.e., cell phone) and payment system. *Dec*., ¶¶227-234. 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 predominant point of sale reader technology deployed worldwide. *Dec.*, ¶228. It was well-known that many point-of-sale terminals only accepted a physical magstripe payment method, and existing contactless transaction enabled cell phones could not be used for magnetic stripe transactions. *Dec.*, ¶¶229-230.

A POSITA would have desired 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. *Dec.*, ¶231.

A POSITA would have had a reasonable expectation of success in combining Brown's smart card with Collinge's payment system as a combination of known elements that would yield predictable results. *Dec.*, ¶232. In the combined system, the functionality of Collinge and Brown would not change, but the user would have predictably had access to a greater variety of payment methods. *Id.*

A POSITA considering what payment cards would be compatible with Collinge's payment system would also have been motivated to look to Brown's payment card because both were designed with reference to the same well-known technical industry standards. *Dec.*, ¶233; *Brown,* [0110], [0173]; '095 *Provisional*, [0063]-[0064].

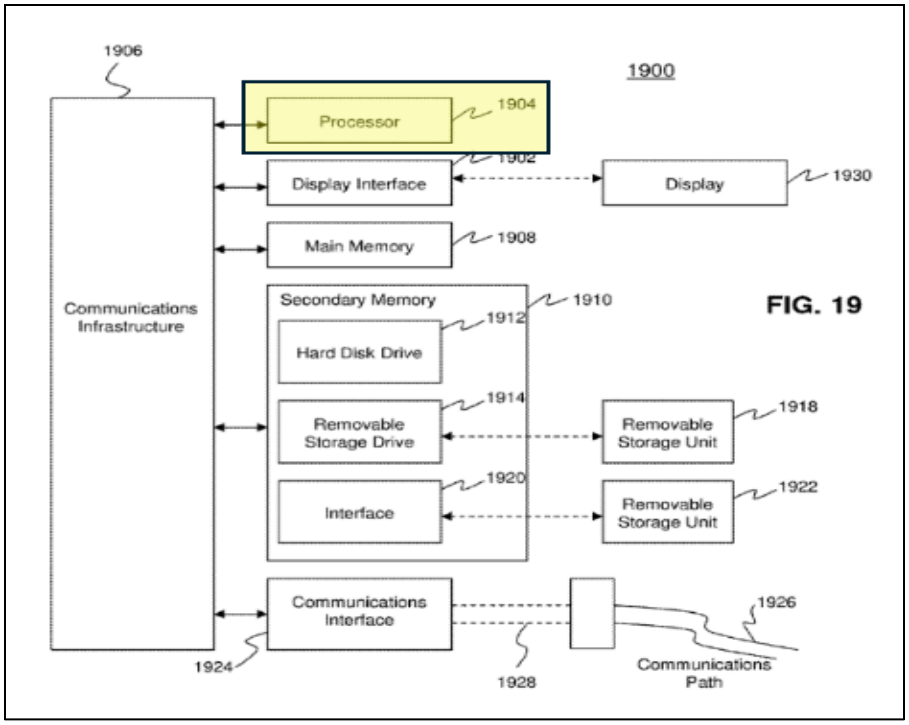
In the combination, Brown’s payment card would be assigned a VPAN, just like any other payment card registered in Collinge’s payment system. *See* Claim 11(pre).

3. 11(b): a personal computing device, wherein the personal computing device comprises:

Collinge’s mobile device 104 is a *personal computing device*. It is described as belonging to a user, having a “mobile personal identification number (PIN)” to identify the user, and as having authentication processes to confirm that the device is being used by an authenticated user. *Collinge,* [0040], [0051], [0128]; *’248 Provisional*, Fig. 2B.

4. 11(c): a processor;

Collinge’s mobile device includes “an application program stored in data storage of the mobile device” that is “executed by *a processor* included in the mobile device[.]” *Collinge*, [0041] (emphasis added), [0147] (“at least one processor device… may be used to implement the above described embodiments”).

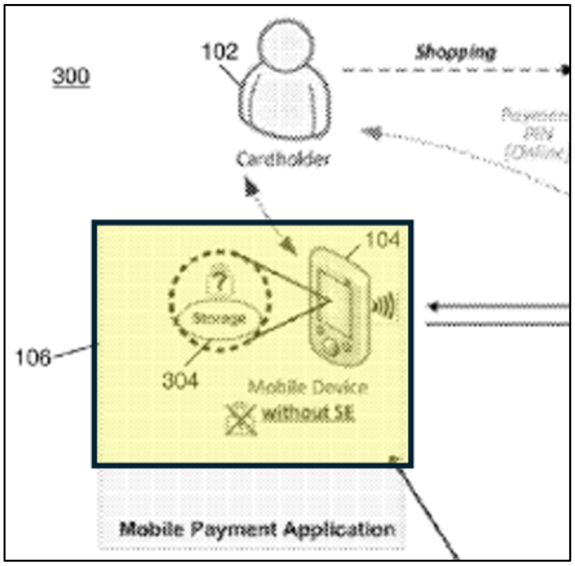


Collinge (Ex. 1004), Fig. 19 (annotated). Collinge teaches and a POSITA would have found it obvious that Collinge's mobile device 104 would be implemented as the computer system 1900. *Dec.,* ¶249.

5. 11(d): a memory;

Collinge's mobile device includes <u>*a memory*</u> for storing a payment card information accessible to the processor. Collinge teaches "an application program stored in **data storage** of the mobile device 104 and executed by a processor included in the mobile device 104." *Collinge*, [0041], [0147] ("at least one processor device and <u>*a memory*</u>") (emphasis added). Collinge's memory includes storage 304, which may include a "local encrypted database." *Collinge*, [0067], [0147]. Storage

304 stores “received payment credentials[.]” *Collinge*, [0063], [0048]-[0049] (describing payment credentials contents).

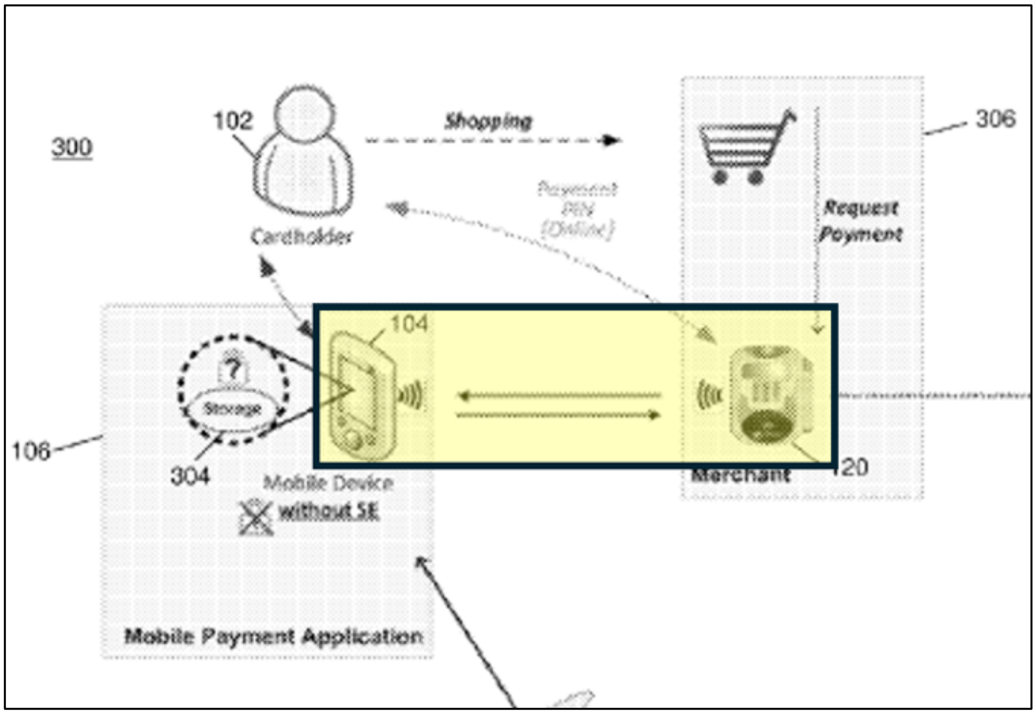


Collinge, Fig. 3 (annotated excerpt).

6. 11(e): a wireless interface;

Collinge teaches a <u>*wireless interface*</u> (NFC interface). Collinge’s mobile device can “receive and store payment credentials and conduct payment transactions via near field communication[.] *Collinge,* [0041]. Per Collinge, a POSITA would have been familiar with methods for performing contactless payments via NFC. *Collinge,* [0041], [0044], [0070], [0086], [0120]. NFC had long been standardized by the time of the ’820 Patent, and a POSITA would have recognized that Collinge teaches that mobile device 104 has an NFC interface, and that an NFC interface is necessarily required to conduct NFC payment transactions as taught by Collinge. *Collinge,* [0041]; *Dec.*, ¶¶237-241.

A POSITA would have understood that Collinge's NFC interface is a wireless interface because it is a short-range wireless technology that allows communication wirelessly over short distances. *Dec.*, ¶241.



Collinge, Fig. 3 (annotated excerpt).

The processor of Collinge's mobile device is connected to a network, such as "a wireless network (e.g., WiFi), a mobile communication network, a satellite network, [or] the Internet[.]" *Collinge,* [0150]. A POSITA would have understood that these are further teachings of a wireless interface of Collinge's mobile device. *Dec.*, ¶241.

7. *11(f): a display operable to provide a visual user-interface operable for performing online transactions; and*

(a) Collinge

Collinge's mobile device includes a touch-screen _*display*_ which is a _*visual user-interface*_. *Collinge*, [0133] ("a touch screen" of "the mobile device 104"). Collinge teaches that "a touch screen" of "the mobile device 104" provides a visual user-interface for user payment interactions. *Collinge*, [0133].

Collinge's '248 Provisional application, incorporated by reference (*see* Section IV.F.1) provides further details of how the touch screen display of Collinge's mobile device provides a visual user-interface when Collinge's payment credentials are used to perform a transaction via Collinge's NFC interface.

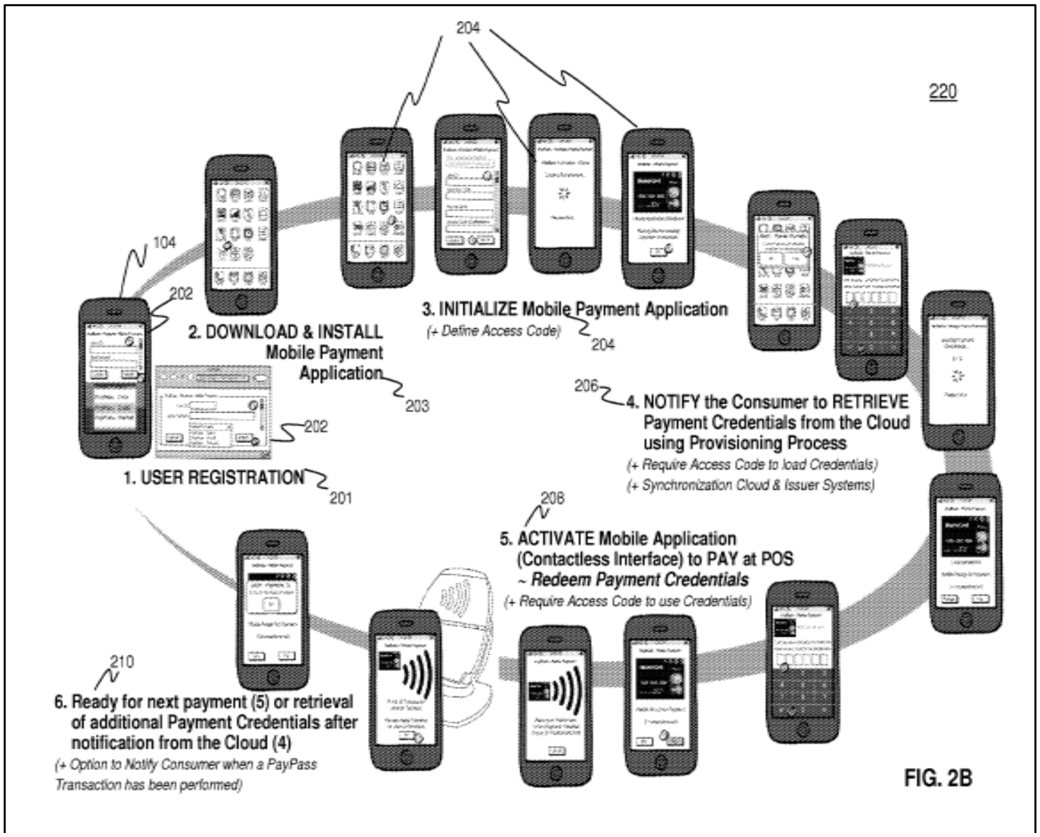

204
220
104
202
2. DOWNLOAD & INSTALL Mobile Payment Application
203
3. INITIALIZE Mobile Payment Application
(+ Define Access Code)
204
206
4. NOTIFY the Consumer to RETRIEVE Payment Credentials from the Cloud using Provisioning Process
(+ Require Access Code to load Credentials)
(+ Synchronization Cloud & Issuer Systems)
202
1. USER REGISTRATION
201
208
5. ACTIVATE Mobile Application (Contactless Interface) to PAY at POS
~ Redeem Payment Credentials
(+ Require Access Code to use Credentials)
210
6. Ready for next payment (5) or retrieval of additional Payment Credentials after notification from the Cloud (4)
(+ Option to Notify Consumer when a PayPass Transaction has been performed)

FIG. 2B

'248 Provisional, Fig. 2B.

(b) Kranzley

Kranzley's payment application displays payment information required for an online transaction, and the customer "may read the information from the display device and then key in that data into a Web page on a computer[.] *Kranzley,* [0040]. Kranzley's display of online-usable payment information is a *visual user-interface operable for performing online transactions*. Further, a POSITA would have understood that a mobile device is a computer, therefore a POSITA would have understood (and it would have been obvious that) Kranzley teaches entering payment data into a Web page on the display of Kranzley's mobile device, which is likewise a *visual user-interface operable for performing online transactions*. *Dec*., ¶245.

(c) Motivation to Combine

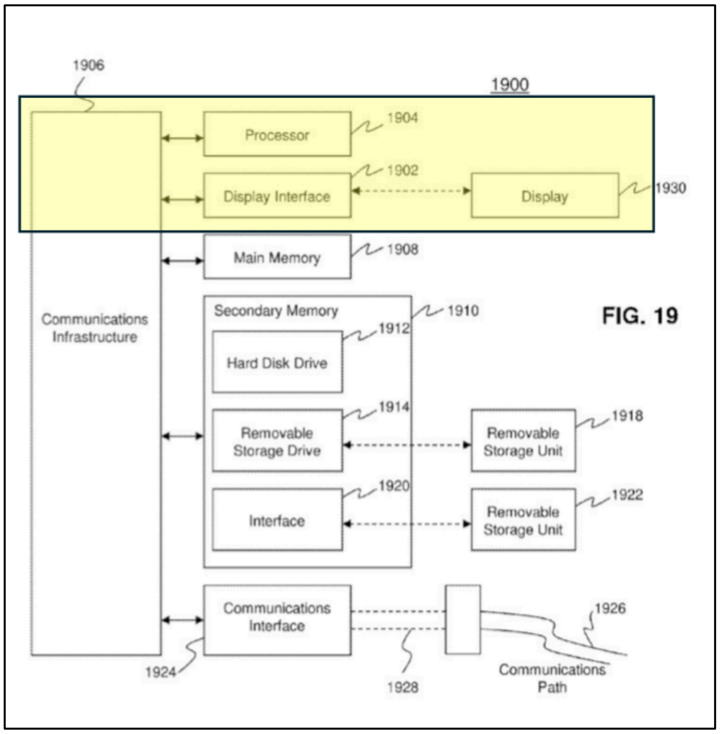
As discussed above at 11(pre), in combination with Kranzley, Collinge's display would be *operable for performing online transactions*. *Dec*., ¶246. In the combination, the touch-screen display of Collinge's mobile device would continue to be used by the user to select the payment method for the POS transaction and enter an authentication PIN. *Collinge*, [0038] ("[p]ayment cards may include credit cards, debit cards…"); *'098 Provisional,* 96 (showing selection of Debit, Credit, or Prepaid) on Collinge's touch screen display; *'248 Provisional*, Fig. 2A-2B (same); *Collinge*, [0133] (touch screen receives a mobile PIN).

Further, it would have been obvious and a POSITA would have been motivated to display payment credentials on Collinge's screen so that a user can input those credentials into a Web page on the display of Collinge's mobile device and complete an online transaction. *Dec*., ¶246; Claim 11(pre).

8. 11(g): a user-interface coupled to the processor, and

Collinge's touch-screen display (*user-interface*) is *coupled to* Collinge's *processor*. Collinge teaches that "at least one processor device" is used to implement the payment system taught by Collinge. *Collinge,* [0147]. The touch screen of Collinge's mobile device 104 is *coupled to the processor* so that user input can be received and acted upon by mobile device 104. For example, the touch screen "receives a user's input of a "mobile personal identification number (PIN)" during generation of a payment cryptogram. *Collinge*, [0133]. Collinge teaches and a POSITA would have understood that for the touch screen in Collinge's mobile device 104 to display information and receive and act on user input as taught by Collinge, the touch screen must be coupled to a processor. *Collinge,* [0147] (describing generation of a cryptogram by the processing device), *Dec*, ¶¶247-252.

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



Collinge, Fig. 19 (annotated). *Collinge*, [0150] (the communications infrastructure may be a "bus, message queue, network, multi-core message-passing scheme, etc."). Collinge teaches and a POSITA would have found it obvious that Collinge's mobile device 104 would be implemented as the computer system 1900. *Dec*., ¶249.

9. *11(h): wherein the wireless interface is operable to wirelessly obtain card device payment account information, and*

Collinge and Kranzley both teach that card device payment account information is *wirelessly obtained*.

Collinge teaches "the payment token payload [is] provisioned to the mobile device 104[.]" *Collinge,* [0047]. The payload includes a "card profile 116 and the single use key 118" and the card profile 116 further includes "payment credentials provisioned to the mobile payment application 106 by the remote-SE system for use in conducting payment transactions." *Collinge,* [0048], [0150] (Collinge's mobile device is connected to a network, such as "a wireless network (e.g., WiFi), a mobile communication network, a satellite network, [or] the Internet[.]"). Collinge teaches and a POSITA would have found it obvious that when Collinge receives payment credentials from the remote-SE system, they are received *wirelessly*, however, Collinge does not specify which wireless method is used.

Kranzley (like Collinge) teaches that to use the payment application on Kranzley's mobile device "a cardholder must first register a payment card" and "install (or activate) a payment application on a mobile device." *Kranzley,* [0050]. During registration, "the payment provider 110 creates a VPAN" and "delivers the VPAN to the cardholder's mobile device…**using over the air ('OTA') techniques."** *Kranzley,* [0054]. A POSITA would have understood that OTA techniques are wireless, and include receiving information over Wi-Fi or a cellular network. *Dec.*, ¶¶254-255.

It would have been obvious and a POSITA would have been motivated to send card device payment account information (including a VPAN and CVC associated with Brown's card), to Collinge's mobile device wirelessly over WiFi or a cellular network as taught by Collinge and Kranzley. *Dec.*, ¶256. A POSITA would have recognized that for Collinge's mobile device to function as a ***mobile*** device, it required a wireless communication interface, and it was well-known that mobile devices at the time could connect to WiFi and cellular networks wirelessly. *Id.* Therefore, a POSITA would have had a reasonable chance of success in using the known methods of WiFi or a cellular network to provision payment credentials to Collinge's mobile device as taught by Kranzley. *Id.*

10. 11(i): wherein the processor is operable to generate limited-use payment information based on the card device payment account information, and

Collinge teaches a processor operable to dynamically generate limited-use payment information (a payment cryptogram).

In the Collinge-Brown combination, Collinge's mobile payment application is provisioned with payment credentials (including a VPAN and CVC3) associated with Brown's card (*see* Claim 11(pre)) and Collinge generates limited-use payment information based on Brown's payment account information.

(a) Brown

Brown teaches "use of a card-holder's real personal account number (PAN) such that an issuing bank can authorize all transactions without support from a third party." *Brown,* [0040]. Brown further teaches that the PAN will be assigned an "expiration date[.]" *Id.* Brown teaches that "account numbers" and "expiration dates" are assigned before the user receives their card. *Brown,* [0048], [0052]-[0053]. While embodiments of Brown discuss a variable payment account number displayed on Brown's card, as discussed above at claim 11(pre), Brown teaches and a POSITA would understand that those virtual account numbers must be correlated to the user's assigned real personal account number for payment to be processed. *Brown,* [0040]; *Dec.*, ¶256. A CVC is also assigned to each payment account. *Brown,* [0177].

(b) Collinge

Collinge's mobile payment application is "stored in data storage of the mobile device 104 and **executed by a processor** included in the mobile device 104." *Collinge*, [0041].

The processor executing the mobile payment application of Collinge's mobile device generates a **payment cryptogram** which "may be, for example, an application cryptogram or a dynamic card validation code (CVC3)." *Collinge,* [0077]. Collinge teaches the payment cryptogram is single-use, "valid for a single financial transaction." *Collinge*, [Abstract], [0128], Fig. 16. The payment cryptogram is generated "using the generating key included in the single use key" that was previously provisioned to the mobile device. *Collinge*, [0077], [0043]. Collinge teaches generating a CVC3 based on: "the supplied CVC3 value, the session key unpredictable number, the application transaction counter, and the reader unpredictable number." *Collinge*, [0145].

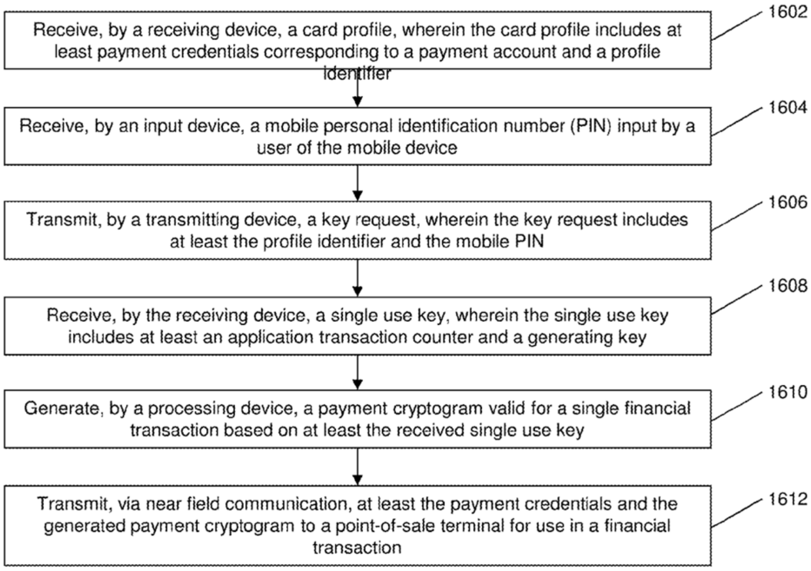

Receive, by a receiving device, a card profile, wherein the card profile includes at least payment credentials corresponding to a payment account and a profile identifier
1602
Receive, by an input device, a mobile personal identification number (PIN) input by a user of the mobile device
1604
Transmit, by a transmitting device, a key request, wherein the key request includes at least the profile identifier and the mobile PIN
1606
Receive, by the receiving device, a single use key, wherein the single use key includes at least an application transaction counter and a generating key
1608
Generate, by a processing device, a payment cryptogram valid for a single financial transaction based on at least the received single use key
1610
Transmit, via near field communication, at least the payment credentials and the generated payment cryptogram to a point-of-sale terminal for use in a financial transaction
1612

FIG. 16

Collinge, Fig. 16.

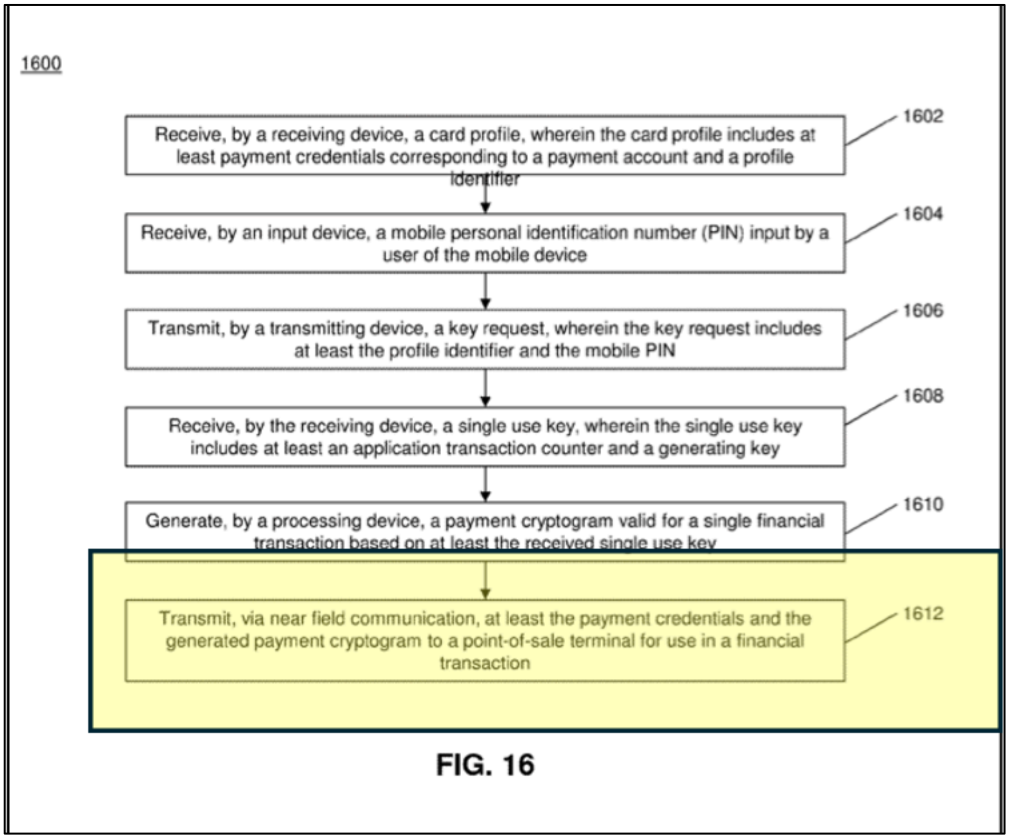
(c) Motivation to Combine

See claim 11(pre), (a).

11. 11(j): wherein the personal computing device is operable to generate complete payment information, including the limited-use payment information, and to convey said complete payment information via at least one interface of a set comprising: said display; and the wireless interface, and

Collinge teaches generating *complete payment information* and Collinge in light of Kranzley further teaches conveying the complete payment information via Collinge's *display*.

Collinge teaches generating *limited-use payment information* (a payment cryptogram/CVC). *See* Claim 11(i). Collinge further teaches sending the dynamically generated payment cryptogram combined with payment credentials (which includes a Payment Account Number (PAN) or VPAN) to a point-of-sale terminal in a payment transaction via NFC (a <u>*wireless interface*</u>). *Collinge*, [0048]-[0049], [0070], [0077], [0135], Fig. 16. The payment cryptogram and payment credentials are <u>*complete payment information*</u> because they include the information required to process payment.



Receive, by a receiving device, a card profile, wherein the card profile includes at least payment credentials corresponding to a payment account and a profile identifier

Receive, by an input device, a mobile personal identification number (PIN) input by a user of the mobile device

Transmit, by a transmitting device, a key request, wherein the key request includes at least the profile identifier and the mobile PIN

Receive, by the receiving device, a single use key, wherein the single use key includes at least an application transaction counter and a generating key

Generate, by a processing device, a payment cryptogram valid for a single financial transaction based on at least the received single use key

Transmit, via near field communication, at least the payment credentials and the generated payment cryptogram to a point-of-sale terminal for use in a financial transaction

FIG. 16

Collinge, Fig. 16. (annotated); *Collinge,* [0048], Fig. 6, [0104] (card profile (PTP_CP)); *'098 Provisional*, [0101] ("Payment Token Payload – Card Profile (PTP_CP_ contains the Payment Credentials required to perform a [MasterCard] *PayPass* transaction" including "data elements such as: **PAN,** PSN + Track Data.").

As discussed at Claim 11(pre), it would have been obvious and a POSITA would have been motivated to convey complete payment information on Collinge's display, including (in the combination) a VPAN and a dynamic CVC (payment cryptogram).

12. 11(k): wherein the limited-use payment information is configured to be used in place of a card issuer payment information.

Collinge teaches that the payment cryptogram (<u>*limited-use*</u> payment information) is a "dynamic card validation code (CVC3)" that is used in place of a static card CVC, which, in the combination, is the CVC assigned to Brown's payment card by the card issuer. *Collinge,* [0050], [0077]. *See* Claim 11(a).

B. Claim 13

1. Claim 13(a):

Collinge teaches generating a <u>*limited-use card security code number*</u> (payment cryptogram) used in place of a card-issuer provided static CVC. *See* Claim 11k.

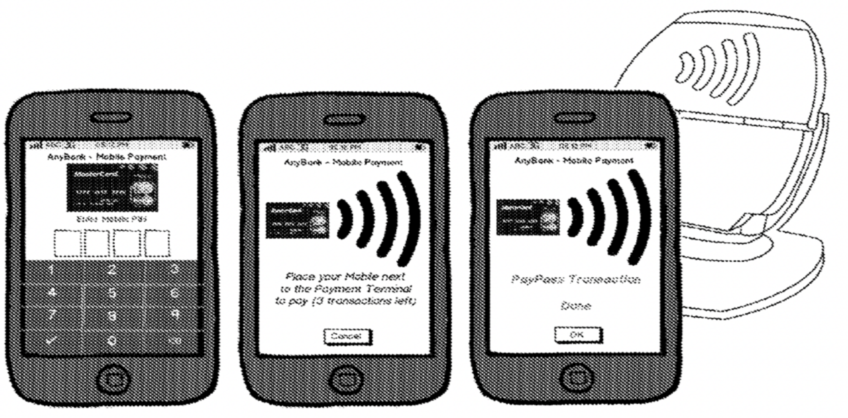
In related art, Kranzley teaches a "**dynamic code** is a three or four digit code that may be used **in place of a 'CVV', 'CVC'** or other code (a code generally used in payment card systems and used to verify that a cardholder was in possession of a payment card during a transaction)." *Kranzley*, [0041] (emphasis added). Kranzley teaches this "dynamic code **is displayed on the display device**." *Kranzley*, [0011], [0040] (teaching displaying the code for use in online transactions).

It would have been obvious and a POSITA would have been motivated to modify Collinge's mobile payment application to display Collinge's payment cryptogram on Collinge's display as taught by Kranzley for the reasons discussed at Claim 11(pre). A POSITA would have recognized a user's desire for flexibility to make payments online, and that many online transactions required a CVC-type value to be provided, as taught by Kranzley. *Kranzley,* [0011], [0040]. *Dec.,* ¶266.

2. Claim 13(b):

Collinge teaches that the touch screen of mobile device 104 receives a user's input of a "mobile personal identification number (PIN)" (*input request*) to kick-off the process of a payment cryptogram and to validate the user. *Collinge*, [0128], [0133]. The payment cryptogram is "based on…the mobile PIN" and is therefore generated responsive to input of an accurate mobile PIN by the user. *Collinge*, [0135]; *'248 Provisional*, Fig. 2B ("Request Access Code to use credentials").

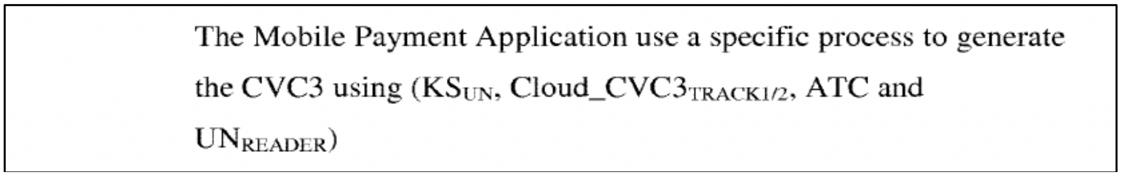
Collinge teaches that user "must always provide the Mobile PIN for all PayPass transactions[.]" *'098 Provisional*, 99.



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

3. Claim 13(c):

Collinge’s mobile device generates a payment cryptogram (CVC3) using the single use key [*computing device key/computing device secret*]. *Collinge*, [0050]. More specifically, Collinge’s CVC3 is generated based on at least “the supplied CVC3 value [a payment card security code/*payment device secret*], the session key unpredictable number [*computing device secret/payment device issuer secret*], the application transaction counter [*a payment device sequence counter*], and the reader unpredictable number.” *Collinge*, [0145]; *Dec.,* ¶269.



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

’248 Provisional, Table 1. Collinge teaches that the payment cryptogram is generated by cryptographically combining information. *Id., Collinge,* [0145]; *Dec.,* ¶269.

C. Claim 14

1. Claim 14(a):

See Claim 11(pre); *Kranzley,* [0040] (“display a VPAN [*limited-use card account number*], *expiration date* and dynamic account validation code”).

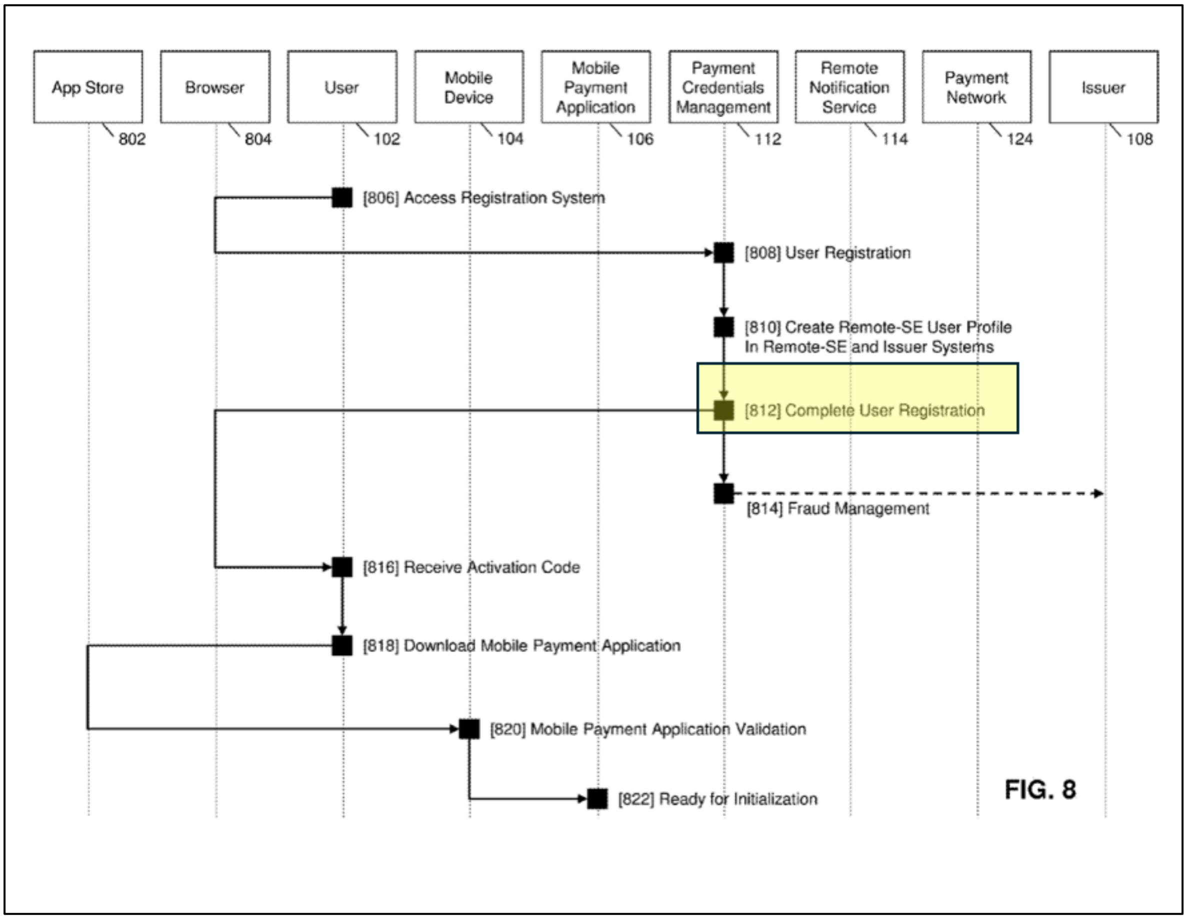
2. Claim 14(b):

See Claim 13(b).

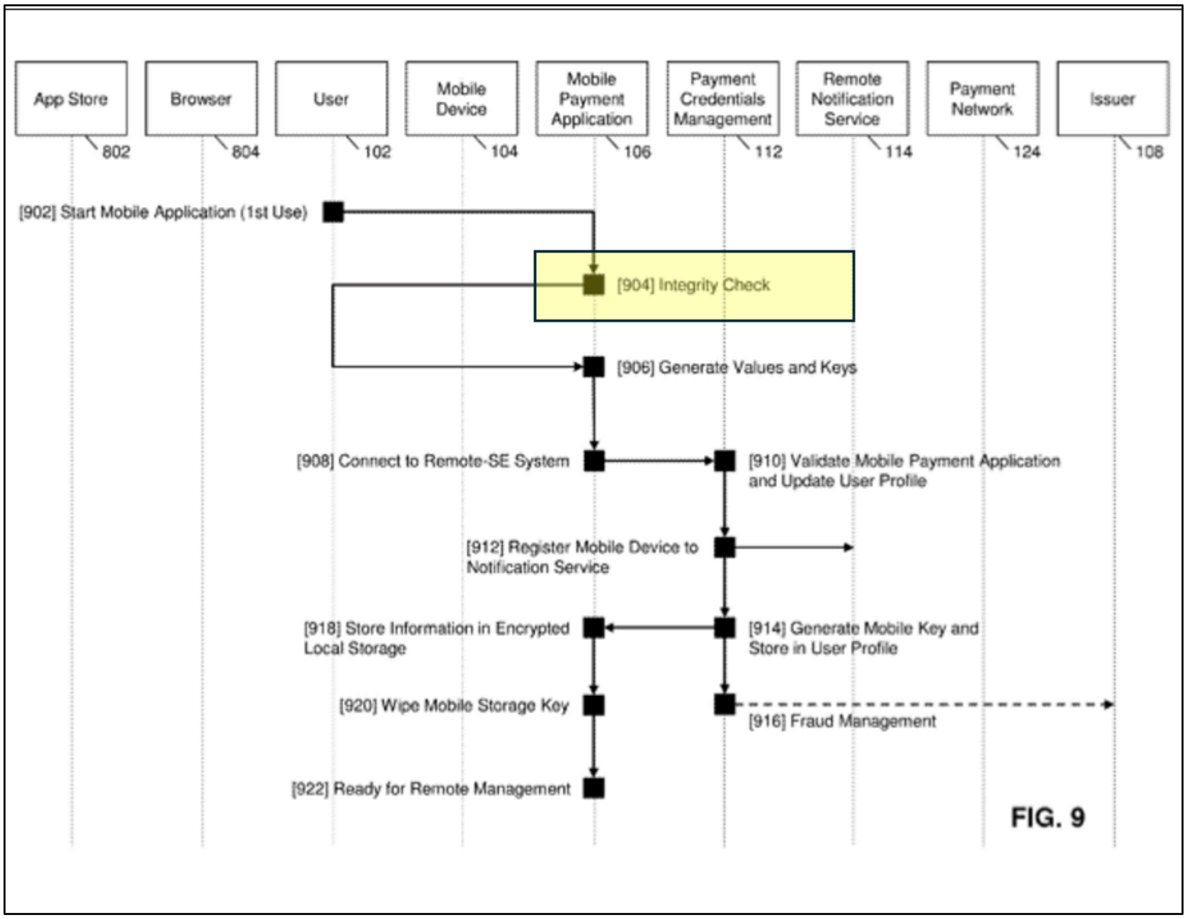
3. Claim 14(c):

See Claim 13(b).

Collinge teaches that in the registration process, the user "receive[s] an activation code and…**a unique identifier used to identify the user 102**." *Collinge*, [0065] (emphasis added). When the mobile payment application is loaded, during an integrity check, "the mobile payment application 106 may **authenticate the user 102 and request the activation code** provided to the user 102 during the registration process (e.g., at step 812 in FIG. 8)." *Collinge*, [0093] (emphasis added).


App Store
802
Browser
804
User
102
Mobile Device
104
Mobile Payment Application
106
Payment Credentials Management
112
Remote Notification Service
114
Payment Network
124
Issuer
108
[806] Access Registration System
[808] User Registration
[810] Create Remote-SE User Profile In Remote-SE and Issuer Systems
[812] Complete User Registration
[814] Fraud Management
[816] Receive Activation Code
[818] Download Mobile Payment Application
[820] Mobile Payment Application Validation
[822] Ready for Initialization
FIG. 8

Collinge, Fig. 8. (annotated).


App Store
802
Browser
804
User
102
Mobile Device
104
Mobile Payment Application
106
Payment Credentials Management
112
Remote Notification Service
114
Payment Network
124
Issuer
108
[902] Start Mobile Application (1st Use)
[904] Integrity Check
[906] Generate Values and Keys
[908] Connect to Remote-SE System
[910] Validate Mobile Payment Application and Update User Profile
[912] Register Mobile Device to Notification Service
[918] Store Information in Encrypted Local Storage
[914] Generate Mobile Key and Store in User Profile
[920] Wipe Mobile Storage Key
[916] Fraud Management
[922] Ready for Remote Management
FIG. 9

Collinge, Fig. 9 (annotated); [0130] (receipt of code is through touch screen input device).

Figure 2B (below) which Collinge incorporates by reference further describes a code used to identify a user. For example, in Step 4 the user must provide their access code in order to load payment credentials, and in Step 5 the user must provide an access code in order to use payment credentials—each time authenticating the user via input on the touchscreen user-interface. *Dec.*, ¶275.

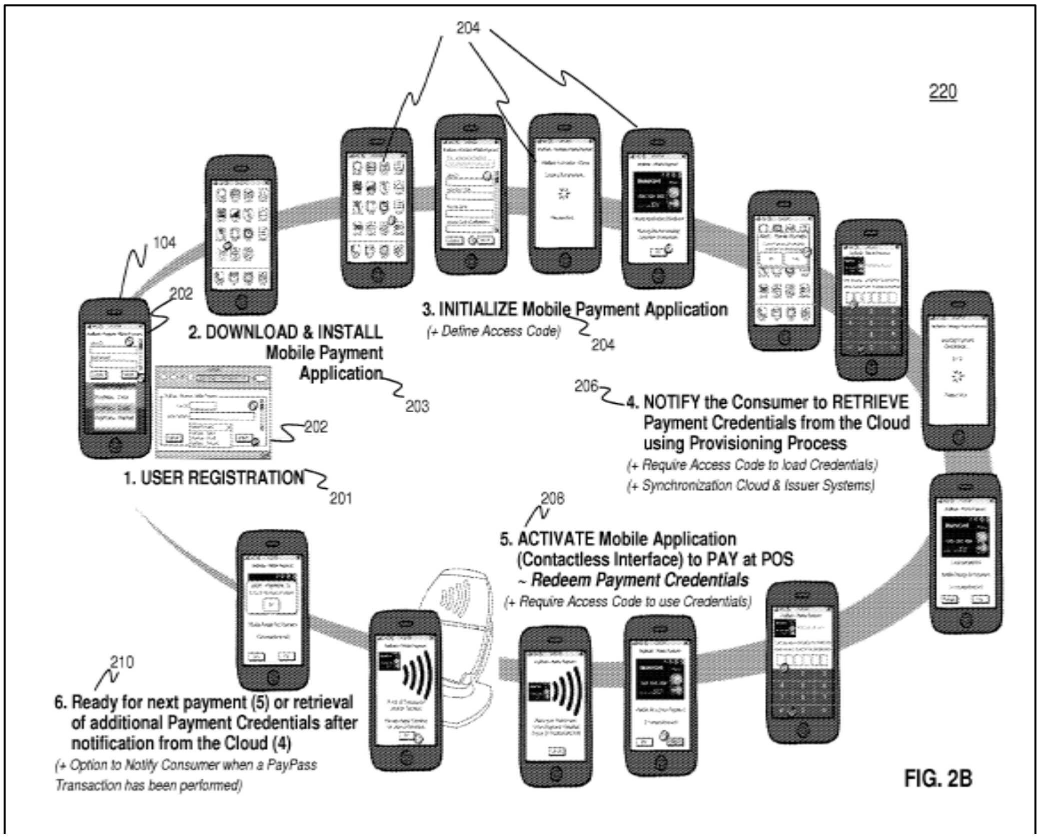

204
220
104
202
2. DOWNLOAD & INSTALL Mobile Payment Application
203
3. INITIALIZE Mobile Payment Application
(+ Define Access Code)
204
202
206
4. NOTIFY the Consumer to RETRIEVE Payment Credentials from the Cloud using Provisioning Process
(+ Require Access Code to load Credentials)
(+ Synchronization Cloud & Issuer Systems)
1. USER REGISTRATION
201
208
5. ACTIVATE Mobile Application (Contactless Interface) to PAY at POS
~ Redeem Payment Credentials
(+ Require Access Code to use Credentials)
210
6. Ready for next payment (5) or retrieval of additional Payment Credentials after notification from the Cloud (4)
(+ Option to Notify Consumer when a PayPass Transaction has been performed)

FIG. 2B

’248 Provisional, Fig. 2B.

4. *Claim 14(d):*

See Claim 14(a).

D. Claim 15

1. *15(pre): An online payment system comprising:*

See Claim 11(pre).

2. *15(a): a thin card-shaped payment card device that bears no fixed payment numbers on the card device; and*

See Claim 11(a).

3. *15(b): a computing device operable for completing an online payment transaction and comprising:*

See Claim 11(pre), (b).

4. *15(c): a display;*

See Claim 11(f).

5. *15(d): a user-interface;*

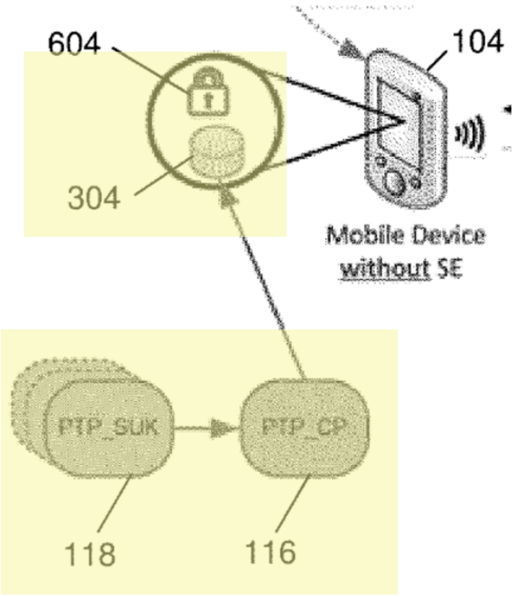
See Claim 11(g).

6. *15(e): a processor; and*

See Claim 11(c).

7. *15(f): a memory for storing a payment card information accessible to the processor,*

See Claim 11(d). Collinge teaches storing *payment card information* in storage 304 (*a memory*). Specifically, Collinge teaches storing a card profile 116 (which "include[s] payment credentials") and a single use key 118 (including "generating key" to "generate a dynamic card validation code CVC3 or an application cryptogram (AC)") in storage 304. *Collinge,* [0048]-[0049], Fig. 6.



Collinge, Fig. 6 (excerpted, annotated).

Collinge's card profile 116 and single use key 118 are accessible to and used by Collinge's processor to generate and send complete payment information to an NFC terminal. *Collinge,* [0048]-[0050], [0118]-[0120], Fig. 14.

8. 15(g): wherein card issuer provided payment card information is wirelessly downloaded into the computing device, and

See Claim 11(h).

9. 15(h): wherein at least one of the set comprising: the computing device; and the card-shaped payment device, is configured to dynamically generate a limited-use payment information, upon the authorization of a valid computing device user, and

See Claims 11(i), 14(c) (identifying a valid user).

10. 15(i): wherein the payment information provided by the computing device is used in online transactions in place of a card issuers payment card information.

See Claim 11(k).

E. Claim 17

See Claim 14(a).

F. Claim 18

1. Claim 18(a):

As discussed in Claim 11(i), the limited-use payment information generated by Collinge's mobile device includes a payment cryptogram (dynamic CVC3, a <u>*limited-use card security code*</u>). *Collinge*, [0077]. Claim 11(i) further explains that Collinge generates complete limited use payment information which includes the payment cryptogram and payment credentials. Collinge's payment credentials include a payment account number (VPAN in the combination) and an expiration date. *Collinge*, [0049], [0124] ("expiration date in the payment credentials included in the card profile 116,"); Dec., ¶286 (magstripe credentials referenced include an expiration date). The VPAN is a *static limited-use card account number*. *Kranzley,* [0039] (describing a "static VPAN" with "an expiration date").

2. Claim 18(b):

In the combination, Collinge's limited-use payment information is conveyed to the user by the screen of Collinge's mobile device so that it can be used to complete an online transaction. *See* Claim 11(f). Further, Collinge's mobile device conveys the payment information when it is submitted to a webpage shown on Collinge's mobile device for payment. *Id.*

G. Claim 19

1. Claim 19(a):

See Claim 13(c). Collinge teaches generating a payment cryptogram such as a CVC3 based on at least Collinge's processor cryptographically combining: "the supplied CVC3 value [*payment card security code*], the session key unpredictable number [(KS_{UN}), *device secret/issuer secret*], the application transaction counter [*device sequence counter*], and the reader unpredictable number." *Collinge*, [0145]. Dec., ¶288.

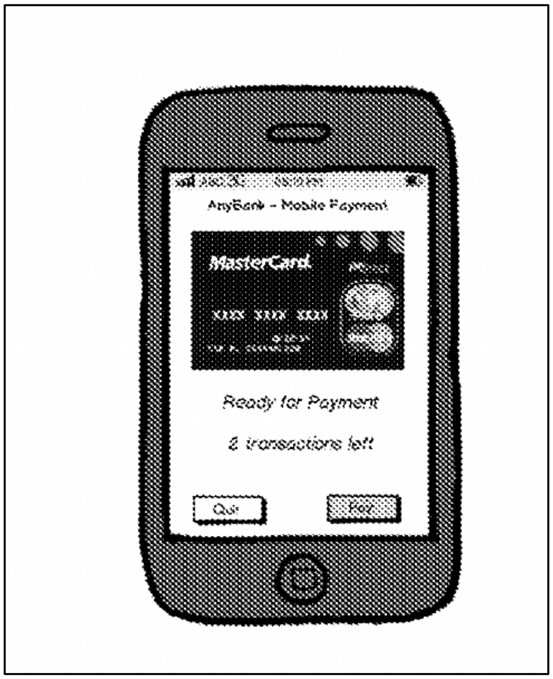
2. Claim 19(b):

See Claim 13(a).

H. Claim 20

1. Claim 20(a):

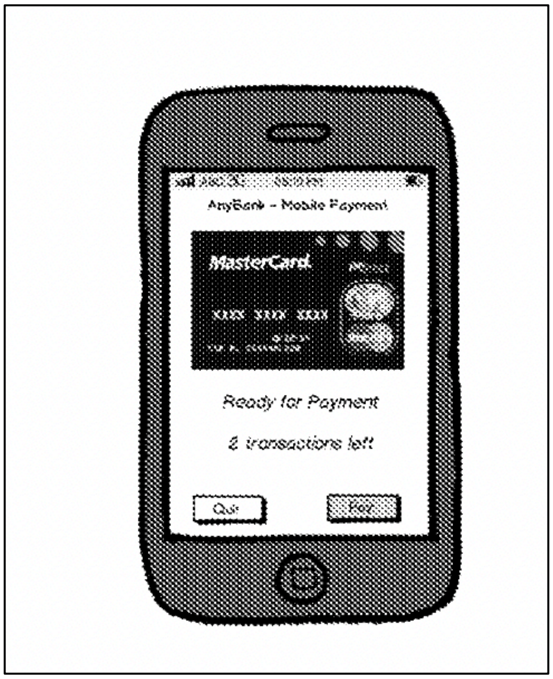
Collinge's device *touchscreen user interface* is operable to accept *a user approval* (selecting a pay option).



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

2. Claim 20(b):

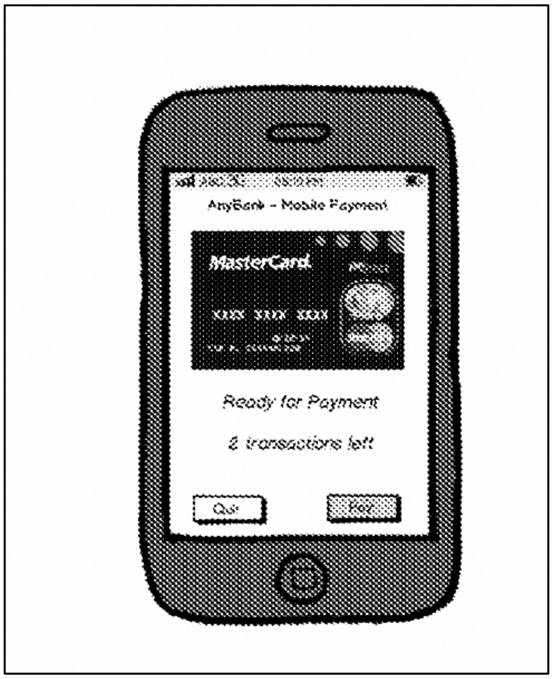
Collinge teaches how to display a *payment card image,* including a MasterCard logo, on Collinge's mobile device.



’098 Provisional, 100; *’248 Provisional*, Fig. 2B. Collinge teaches that the payment card is displayed when the user is choosing the payment method to be used in the transaction, prior to the user selecting “pay” to complete the transaction. *Id.*

3. Claim 20(c):

Collinge’s device touchscreen *user-interface* is operable to accept *a user approving* (selecting a “pay” option) or *denying* (selecting a “quit” option).



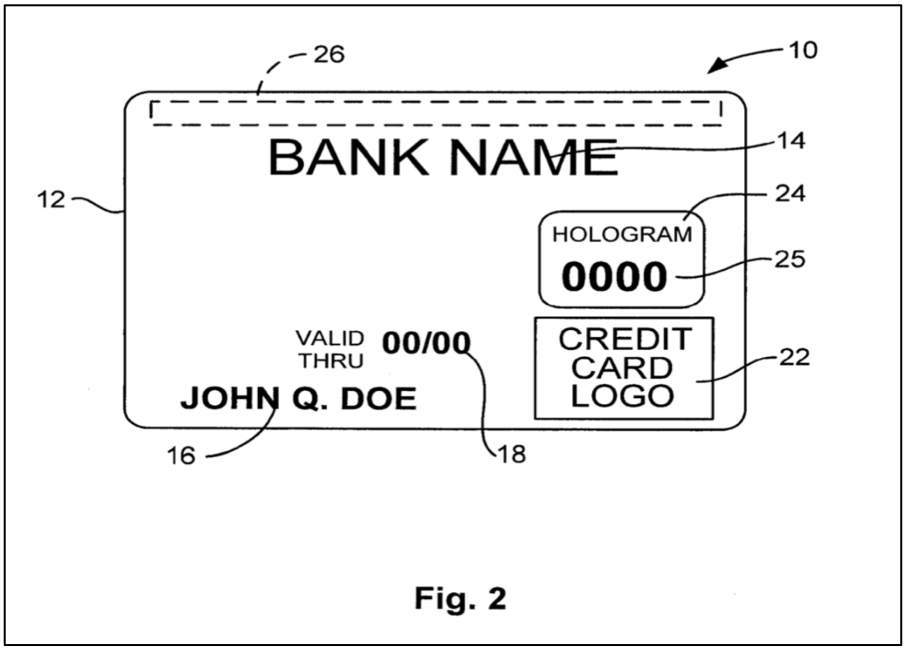
’098 Provisional, 100; ’248 Provisional, Fig. 2B.

X. GROUND 6: CLAIMS 12 AND 16 ARE OBVIOUS OVER COLLINGE, KRANZLEY, BROWN, AND ENG

A. Claim 12

To the extent this limitation is entitled to patentable weight (*see* Section III.C.1), it is taught in view of Eng. Brown teaches a thin card with no fixed payment numbers. *See* Claim 11(a).

In related art, Eng teaches a card that has: (1) *a card-holder name,* (2) credit card logo (*card payment network logo*), and a (3) Bank Name (*brand logo)*. *Eng*, [0020]-[0021], [0042]. *Dec*., ¶295 (discussing Bank Name logos).



Eng, Fig. 2.

To the extent embodiments of Eng's card also includes an expiration date and a portion of a PAN, a POSITA would have no reason to include those pieces of information on Brown's smart card device, since the payment credentials used by Walker's smart card constantly change. *See* Claim 1(a); *Brown,* [200], Fig. 12.

(a) Motivation to Combine

It would have been obvious and a POSITA would have been motivated to modify Brown's smart card to include a fixed card-holder name, payment issuing logo, and card payment network logo as taught by Eng for the same reasons discussed above at Claim 2; *Dec.*, ¶297.

B. Claim 16

See Claim 12.

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

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

XII. CONCLUSION

For the forgoing reasons, Petitioner respectfully requests *inter partes* review of the Challenged Claims.

Respectfully submitted,

ERISE IP, P.A.

BY: /s/ Adam P. Seitz
Adam P. Seitz, Reg. No. 52,206
adam.seitz@eriseip.com
7015 College Boulevard, Suite 700
Overland Park, Kansas 66211
(913) 777-5600 Telephone
(913) 777-5601 Facsimile

COUNSEL FOR PETITIONER

XIII. MANDATORY NOTICES UNDER 37 C.F.R. § 42.8

A. Real Party-in-Interest Under 37 C.F.R. § 42.8(b)(1)

Petitioner is the real party-in-interest.

B. Related Matters Under 37 C.F.R. § 42.8(b)(2)

The ’820 Patent is the subject of a civil action in *CardWare Inc. v. Apple Inc.*, 1:25-cv-00446 (W.D. Tex.).

The ’820 patent was previously the subject of an IPR Petition in *Samsung Electronics Co., Ltd., v. CardWare Inc.*, IPR2023-00314 which is no longer pending.

Other patents in the same patent family as the ’820 Patent are the subject of IPR Petitions in *Apple Inc., v. CardWare Inc.,* IPR2025-01150; *Apple Inc., v. CardWare Inc.,* IPR2025-01149; *Apple Inc., v. CardWare Inc.,* IPR2025-01146; *Apple Inc., v. CardWare Inc.,* IPR2025-01145; *Apple Inc., v. CardWare Inc.,* IPR2025-01152; *Apple Inc., v. CardWare Inc.,* IPR2025-01151; *Apple Inc., v. CardWare Inc.,* IPR2025-01148.

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

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

Lead Counsel	Back-Up Counsel
Adam Seitz (Reg. No. 52,206) Adam.seitz@eriseip.com PTAB@eriseip.com Postal and Hand-Delivery Address: ERISE IP, P.A. 7015 College Blvd., Suite 700 Overland Park, Kansas 66211 Telephone: (913) 777-5600 Fax: (913) 777-5601	Mark Lang (Reg. No. 55,356) Mark.Lang@eriseip.com Lydia Raw (Reg. No. 76,436) Lydia.raw@eriseip.com PTAB@eriseip.com Postal and Hand-Delivery Address: ERISE IP, P.A. 7015 College Blvd., Suite 700 Overland Park, Kansas 66211 Telephone: (913) 777-5600 Fax: (913) 777-5601

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

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

CLAIM LISTING APPENDIX
U.S. Patent No. 10,626,820 for Claims 1-20

Claim Designation	Claim Language
Claim 1(Pre)	A payment system comprising:
Claim 1(a)	a thin shaped body having no fixed payment numbers disposed thereon;
Claim 1(b)	a memory;
Claim 1(c)	a cryptographic processor coupled to the memory; and
Claim 1(d)	a reader interface, including at least one interface selected from a set comprising: a magnetic-stripe, a smart card reader interface, a magstripe inductor interface, an RF interface, an NFC interface, and a wireless interface, and
Claim 1(e)	wherein payment information for a transaction is operable to be conveyed via the reader interface and comprises limited-use payment information, and
Claim 1(f)	wherein further the limited-use payment information is to be used in place of card issuer payment information for payment transactions by said device at payment card reader facilities.
Claim 2	The device of claim 1, wherein the body comprises fixed payment information disposed thereon and wherein the fixed payment information includes only: a card-holder name; a payment issuing logo; and a card payment network logo, and wherein further, the body is free of any account numbers, expiration dates, card security codes, or other fixed payment numbers, disposed thereon.
Claim 3(a)	The device of claim 1, wherein the limited-use payment information is conveyed via the magnetic stripe and is unique to the payment device and to the magnetic stripe, and
Claim 3(b)	wherein the limited-use payment information is limited to use by the payment device and is operable for conveying payment information to a magnetic-stripe payment card reader, and
Claim 3(c)	wherein said limited-use payment information has a limited period of valid use, and
Claim 3(d)	wherein said limited-use payment information is not valid when used other than through a magnetic stripe payment card reader.
Claim 4	The device of claim 1, wherein said limited-use payment information is provided by a card issuing authority for use by the

Claim Designation	Claim Language
	payment device and wherein the card processing authority rejects as invalid, any use of said limited-use payment information obtained via any means other than: a payment card reader reading said limited-use payment information from the reader interface.
Claim 5(a)	The device of claim 1, wherein a request for payment includes at least one of a set comprising: payment information, transaction information, merchant information, and payment card reader information, and
Claim 5(b)	wherein a card-present transaction is one including the limited-use payment information, and valid payment card reader information, and wherein a card-not-present transaction is one including at least a portion of said limited-use card payment information, and not including valid payment card reader information; and,
Claim 5(c)	wherein a processing authority is operable to approve as valid, a card-present payment transaction; and,
Claim 5(d)	wherein said card processing authority is operable to reject, as not valid, a use of the limited-use card payment information in a card-not-present payment transaction; and
Claim 5(e)	wherein a card issuing authority receiving said request for payment is operable to decline a transaction not involving a valid card-present use of a limited-use card payment information portion used in place of card issuer supplied payment information.
Claim 6	The device of claim 1, wherein a card processing authority is operable to reject as invalid, a use of the limited-use payment information provided via the reader interface, in online payment transactions.
Claim 7(Pre)	The device of claim 1, wherein a card issuer providing the limited-use payment information, for use by the payment device, limits valid approval of said limited-use payment information to performing a card-present payment transaction by the card device, and wherein said card issuer declines as invalid a use of said limited-use payment information in transactions other than wherein the payment device is present, and

Claim Designation	Claim Language
Claim 7(a)	wherein a card issuer limits said card payment information to use for a finite amount of time, and declines as invalid use when said amount of time has expired, and
Claim 7(b)	wherein a card issuer limits use to payment for transactions with the user approving, and declines as invalid use when the card user is denying an approval, and
Claim 7(c)	wherein a card issuer limits to use in place of card issuer information for payments by the payment device.
Claim 8(a)	The device of claim 1, wherein the reader interface is operable to wirelessly receive cardholder transaction information and to identify a valid user through at least one user-validation action, selected from a set of [sic]comprising:… a device user interface receiving a user entered a valid PIN or Key-Code; a device user interface receiving a user entered a valid password; a device user interface reading a user swipe or gesture; a user tapping a predetermined sequence on the device; a user motioning the device in accordance with a sequence; a skin-contact sensing identifying a valid user; a device sensor array reading a touch of an identified user; a device biometric recognition of a valid user; and
Claim 8(b)	wherein a display of the device is operable to display transaction information through a user interface, and wherein transaction information includes at least one of a set comprising: a transaction time; a transaction amount; transaction merchant information; a transaction location; a transaction facility; card information; a partial card number; graphical card images; and
Claim 8(c)	wherein upon validating the user, the user-interface is operable to receive a valid user input, of at least one user action selected from a set comprising: a payment approval authorization; a payment denial; and an adjustment of a transaction payment.
Claim 9(a)	The device of claim 1, wherein a dynamically-generated one-time limited-use payment information portion is generated by said processor when coupled to a reader interface accessible to said processor, and
Claim 9(b)	wherein the payment information conveyed to a payment card reader, at the time of transaction, includes at least one of a portion

Claim Designation	Claim Language
	of: a static limited-use portion; and a dynamically-generated limited-use portion, and
Claim 9(c)	wherein said static limited-use payment information is provided by a card issuing authority for use in place of a card issuer payment information.
Claim 10(a)	The device of claim 1, wherein the processor cryptographically dynamically generates a one-time limited-use number based on combination of a card device transaction sequence count, and
Claim 10(b)	at least one of a set of information including: a user information; a user card account number; a device account number; device secret keys; card issuer keys; a time; a merchant; a location; an online address; a payment information; a card reader information; an account information;
Claim 10(c)	wherein the processor increments the card device transaction sequence count on each transaction.
Claim 11(Pre)	An online payment system, the system comprising:
Claim 11(a)	a thin payment device comprising no fixed payment numbers visible thereon; and
Claim 11(b)	a personal computing device, wherein the personal computing device comprises:
Claim 11(c)	a processor;
Claim 11(d)	a memory;
Claim 11(e)	a wireless interface;
Claim 11(f)	a display operable to provide a visual user-interface operable for performing online transactions; and
Claim 11(g)	a user-interface coupled to the processor, and
Claim 11(h)	wherein the wireless interface is operable to wirelessly obtain card device payment account information, and
Claim 11(i)	wherein the processor is operable to generate limited-use payment information based on the card device payment account information, and
Claim 11(j)	wherein the personal computing device is operable to generate complete payment information, including the limited-use payment information, and to convey said complete payment information via at least one interface of a set comprising: said display; and the wireless interface, and

Claim Designation	Claim Language
Claim 11(k)	wherein the limited-use payment information is configured to be used in place of a card issuer payment information.
Claim 12	The system of claim 11, wherein the thin payment device bears no fixed payment numbers, and bears only: the cardholders name; a brand logo; and the card payment network logo.
Claim 13(a)	The system of claim 11 wherein the personal computing device is configured for presenting on the display a limited-use card security code number for use in payments in place of card issuer payment information, and
Claim 13(b)	wherein the personal computing device is further configured to generate said limited-use card security code responsive to an input request from a valid user, via said user-interface, and
Claim 13(c)	wherein said limited-use number is generated on the personal computing device from at least one information from a set comprising: a payment device user information; a payment device account number; a payment device sequence counter; a payment device identifier; payment device secrets; a payment device key; computing device secrets; computing device keys; payment device issuer secrets; payment device issuer keys; a time; an expiration date; an amount; a merchant locality; an online location; a transaction information; and a cryptographic combination of at least two of the above.
Claim 14(a)	The system as described in claim 11 wherein the personal computing device is configured for presenting on the display, a limited-use card account number, and a limited-duration expiration date, for use in payments in place of a card issuer payment information, and
Claim 14(b)	wherein said personal computing device is further configured to generate said limited-use card payment information responsive to an input request from a valid user, and
Claim 14(c)	wherein the personal computing device is configured to identify a valid device-user through at least one user-validation input available to the personal computing device, of a set comprising: a touch ID sensor operable to identify the touch a valid user; a user entering of a valid passcode on a touch sensor-array; a user entering of a valid passcode on a key-pad; a user entering of a valid PIN or Key-Code on the user-interface a user entering of a

Claim Designation	Claim Language
	valid password on the user-interface; a valid user swiping or gesturing on a touch sensor-array; a valid sequence of a user tapping of the device detectable by device accelerometer; a valid user sequence of user motioning of the device detectable by device motion sensor unit; a skin-contact sensing identifying a valid user on a device contact sensor; a touching of an identified user's skin on a device touch sensor array; a device biometric recognition of a valid user via a device biometric sensing; and a biometric sensing of the device remaining continuously in the proximity possession of a valid user via device skin-proximity sensor;
Claim 14(d)	and, wherein the personal computing device conveys the limited-use payment information through the user interface.
Claim 15(Pre)	An online payment system comprising:
Claim 15(a)	a thin card-shaped payment card device that bears no fixed payment numbers on the card device; and
Claim 15(b)	a computing device operable for completing an online payment transaction and comprising:
Claim 15(c)	a display;
Claim 15(d)	a user-interface;
Claim 15(e)	a processor; and
Claim 15(f)	a memory for storing a payment card information accessible to the processor,
Claim 15(g)	wherein card issuer provided payment card information is wirelessly downloaded into the computing device, and
Claim 15(h)	wherein at least one of the set comprising: the computing device; and the card-shaped payment device, is configured to dynamically generate a limited-use payment information, upon the authorization of a valid computing device user, and
Claim 15(i)	wherein the payment information provided by the computing device is used in online transactions in place of a card issuers payment card information.
Claim 16	The system of claim 15 wherein the card device bears no fixed payment numbers, and bears only: the cardholders name; the brand logo; and the card payment network logo.

Claim Designation	Claim Language
Claim 17	The system of claim 15 wherein the dynamically generated limited-use payment information is displayable on a display of the computing device.
Claim 18(a)	The system of claim 15 wherein the limited-use payment information includes a static limited-use card account number, a limited-duration card expiration date, and a limited-use card security code and,
Claim 18(b)	wherein the dynamically generated limited-use payment information is conveyed by the computing device to complete an online transaction.
Claim 19(a)	The system of claim 15 wherein the computing device is operable to generate a limited-use card security code number, for use in place of a card issuers card security code by generating said limited-use number via cryptographically combining information from at least one of a set comprising: a user information; an internet address; an email address; a device transaction sequence counter; a device account number; device identifiers; device secrets; device keys; issuer secrets; issuer keys; a payment card account number; a payment card security code; a time; an expiration date; an amount; a merchant locality; a transaction information; and a cryptographic combination of at least two of the above set,
Claim 19(b)	and wherein the computing device is operable to display the generated limited-use card security code on the display.
Claim 20(a)	The system of claim 15 wherein the computing device is further operable to obtain a user payment approval through at least one user-interface element of the computing device, from a set comprising: a display interface, a touch-screen interface, a touch ID button, input buttons, a touch key-pad, a key-pad, a key-board, an optical sensor array, a motion detection unit, an accelerometer, the swiping of a recognized user skin over a device sensor array, a biometric sensor, a wireless interface, an NFC interface, an RF interface, a device biometric sensing the device is continuously remaining in contact with a valid user; and,
Claim 20(b)	wherein the computing device is operable to display at least one of a set comprising: the transaction information, the merchant information, the time, the location of the transaction, the payment

Claim Designation	Claim Language
	bank logo, the card issuer icon, the payment card image, and the amount, on a display of the computing device, and,
Claim 20(c)	a user input providing for at least one user action from a set comprising: an approving of a transaction, a denying of a transaction, and an adjusting of a transaction, via the user-interface.

APPENDIX OF EXHIBITS

Exhibit 1001	U.S. Patent No. 10,628,820 (“*’820 Patent*”)
Exhibit 1002	File History of the ’820 Patent (“*’820 File History*”)
Exhibit 1003	Declaration of Dr. Clifford Neuman
Exhibit 1004	U.S. Patent Publication No. 2013/0262317 to Collinge et al. (“*Collinge*”)
Exhibit 1005	U.S. Provisional Patent Application No 61/619,095 to Collinge et al. (“*’095 Provisional*”)
Exhibit 1006	U.S. Provisional Patent Application No 61/635,248 to Collinge et al. (“*’248 Provisional*”)
Exhibit 1007	U.S. Provisional Patent Application No 61/735,383 to Collinge et al. (“*’383 Provisional*”)
Exhibit 1008	U.S. Provisional Patent Application No 61/762,098 to Collinge et al. (“*’098 Provisional*”)
Exhibit 1009	U.S. Patent Publication No. 2006/0122931 to Walker et al. (“*Walker*”)
Exhibit 1010	U.S. Patent Publication No. 2007/0208671 to Brown et al. (“*Brown*”)
Exhibit 1011	U.S. Patent Publication No. 2007/0055630 to Gauthier et al (“*Gauthier*”)
Exhibit 1012	U.S Patent Publication No. 2012/0143754 to Patel (“*Patel”*)
Exhibit 1013	U.S. Patent Publication No. 2010/0125509 to Kranzley et al. (“*Kranzley*”)
Exhibit 1014	U.S. Patent Publication No. 2013/0068366 to Eng (“*Eng*”)
Exhibit 1015	U.S. Patent No. 8,103,588 B2 to Patterson (*“Patterson”)*
Exhibit 1016	“Computer,” Merriam-Webster Dictionary (1997)
Exhibit 1017	*This Month in History: The First Credit Card,* Banker & Tradesman (Sept 25, 2022), https://bankerandtradesman.com/this-month-in-history-the-first-credit-card/ (“*Banker & Tradesman*”)
Exhibit 1018	*Bank Card catalog: Bank Card: Debit Card: Bank of America,* Colnect https://colnect.com/en/bank_cards/bank_card/25144-Bank_of_America-Bank_of_America-United_States_of_America (“*Colnect*”)
Exhibit 1019	U.S. Patent Publication No. 2011/0140841 to Bona (“*Bona*”)
Exhibit 1020	IBM, *The Magnetic Stripe*, IBM, https://www.ibm.com/history/magnetic-stripe. (“*IBM*”)

Exhibit 1021	Vedat Coskun, Near Field Communication: Theory to Practice (John Wiley & Sons, 1st ed. 2012) ("*Coskun*")
Exhibit 1022	MagTek, Magnetic Stripe Card Standards, (MagTek Inc. eds., 2011) ("*MagTek*")
Exhibit 1023	EMVCo, LLC, EMV Integrated Circuit Card Specifications for Payment Systems: Book 2 – Security and Key Management (EMVCo, LLC eds., Version 4.3 2011) ("*EMV*")
Exhibit 1024	Klaus Finkenzeller, RFID Handbook (John Wiley & Sons, 3rd ed. 2010) ("*Finkenzeller*")
Exhibit 1025	MasterCard, *MasterCard PayPass ™ in Action*, MASTERCARD (Jun. 11, 5:35 PM), https://www.mastercard.com/us/company/en/ourbusiness/paypass_in_action.html#:~:text=MasterCard%20PayPass%E2%84%A2%20in%20Action&text=Developed%20to%20replace%20the%20need,the%20way%20they%20view%20cash. ("*PayPass*")
Exhibit 1026	Smart Card Alliance, EMV and NFC: Complementary Technologies that Deliver Secure Payments and Value-Added Functionality (Smart Card Alliance, Inc. eds., 2012) ("*Smart*")
Exhibit 1027	U.S. Patent Publication No. 2012/0011058 to Pitroda et al. ("*Pitroda*")
Exhibit 1028	MasterCard, *MasterCard Approved Mobile Devices*, MASTERCARD (Aug. 3, 2012), http://www.mastercard-mobilepartner.com/docs/MasterCard_Approved_Mobile_Devices.pdf, [https://web.archive.org/web/20120906234255/http:// www.mastercard-mobilepartner.com:80/docs/MasterCard_ Approved_ Mobile_Devices.pdf] ("*MasterCard Mobile Partner*")
Exhibit 1029	U.S. Patent Publication No. 2013/0054474 to Yeager ("*Yeager*")
Exhibit 1030	EMVCo, LLC, *EMV Chip At-a-Glance: Enabling Seamless and Secure Contact and Contactless Payments Around the World*, EMVCO (2002), https://www.emvco.com/wp-content/uploads/2022/09/EMV%C2%AE-Chip-At-A-Glance-EMVCo-eBook.pdf ("*EMVCo*")
Exhibit 1031	Scoping SIG & Tokenization Taskforce PCI Security Standards Council, PCI Data Security Standard (PCI DSS) – Information Supplement: PCI DSS Tokenization Guidelines (pci Security Standards Council eds., Version 2.0 2011) ("*PCI SSC*")
Exhibit 1032	Alessandro Vizzarri et al., Security in Mobile Payments (2013) ("*Vizzarri*")

Exhibit 1033	U.S. Patent Publication No. 2008/00110983 to Ashfield ("*Ashfield*")
Exhibit 1034	EMVCo, LLC, EMV Integrated Circuit Card Specifications for Payment Systems: Book 3 – Application Specification (EMVCo, LLC eds., Version 4.3 2011) ("*EMV4.3 Book 3*")
Exhibit 1035	Tore Fjellheim, *Over-the-air Deployment of Applications in Multi-Platform Environments*, IEEE, Proceedings of the 2006 Australian Software Engineering Conference (ASWEC'06) (2006)
Exhibit 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) ("*Study Summary*")
Exhibit 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) ("*Study*")
Exhibit 1038	ConsumerWorld, *Two Months After the Deadline, Most Major Retailers Still Can't Read Chipped Credit Cards,* CONSUMERWORLD (Dec. 7, 2015), https://www.consumerworld.org/pages/creditcardreaders.htm ("*ConsumerWorld Survey*")
Exhibit 1039	Ann Cavoukian, *Mobile Near Field Communications (NFC)"Tap 'n Go" Keep it Secure & Private*, IPC (2011), https://www.ipc.on.ca/sites/default/files/legacy/Resources/mobile-nfc.pdf ("*Cavoukian*")
Exhibit 1040	Annika Paus, Near Field Communication in Cell Phones (2017) ("*Paus*")
Exhibit 1041	Ashis K. Mahapatra, *Touch Screen Systems*, ORISSA REVIEW (2005), https://magazines.odisha.gov.in/orissareview/jun2005/engpdf/touch_screen_system.pdf ("*Mahapatra*")
Exhibit 1042	U.S. Patent Publication No. 2006/0097991 to Hotelling et al. ("*Hotelling*")
Exhibit 1043	U.S. Patent Publication No. 2008/0122796 to Jobs et al. ("*Jobs*")
Exhibit 1044	U.S. Patent No. 7,793,851 to Mullen ("*Mullen*")
Exhibit 1045	WIPO International Publication No. WO 2010/039337 to Lin et al. ("*Lin*")
Exhibit 1046	Mike Rosulek, *The Joy of Cryptography OE*, Oregon State University, Chapter 12:Hash Functions (1ST ED. 2017), https://open.oregonstate.education/cryptographyOEfirst/chapter/chapter-12-hash-functions/ ("*Rosulek*")

Exhibit 1047	U.S. Patent Publication No. 2014/0006276 to Grigg et al. (“*Grigg*”)
Exhibit 1048	Anup K. Ghosh & Tara M. Swaminatha, *Software Security and Privacy Risks in Mobile E-Commerce*, 44 CACM 51 (2001) (“*Ghosh*”)
Exhibit 1049	CardWare’s Preliminary Infringement Contentions

CERTIFICATION OF WORD COUNT

The undersigned certifies pursuant to 37 C.F.R. §42.24 that the foregoing Petition for *Inter Partes* Review, excluding any table of contents, mandatory notices under 37 C.F.R. §42.8, certificates of service or word count, or appendix of exhibits, contains 13,862 words according to the word-processing program used to prepare this document (Microsoft Word).

Dated: June 27, 2025

Respectfully submitted,

ERISE IP, P.A.

BY: /s/ Adam P. Seitz
Adam P. Seitz, Reg. No. 52,206
adam.seitz@eriseip.com
7015 College Boulevard, Suite 700
Overland Park, Kansas 66211
(913) 777-5600 Telephone
(913) 777-5601 Facsimile

COUNSEL FOR PETITIONER

CERTIFICATE OF SERVICE ON PATENT OWNER UNDER 37 C.F.R. § 42.105(a)

Pursuant to 37 C.F.R. §§ 42.6(e) and 42.105(b), the undersigned certifies that on June 27, 2025, a complete and entire copy of this Petition for *Inter Partes* Review and Exhibits were provided via Federal Express to the Patent Owner by serving the correspondence address of record for the '820 patent:

David Wyatt
c/o Murabito, Hao & Barnes
1500 E Hamilton Ave, Suite 118
Campbell, CA 95008

A courtesy copy of the Petition for *Inter Partes* Review was emailed to counsel of record in the parallel litigation:

Caroline M. Walters (cwalters@reichmanjorgensen.com)
Navid Cyrus Bayar (nbayar@reichmanjorgensen.com)
Timothy A. Trost (ttrost@reichmanjorgensen.com)
Khue V. Hoang (khoang@reichmanjorgensen.com)
Matthew G. Berkowitz (mberkowitz@reichmanjorgensen.com)
Patrick R. Colsher (pcolsher@reichmanjorgensen.com)
Yue (Joy) Wang (ywang@reichmanjorgensen.com)
Eric H. Findlay (efindlay@findlaycraft.com)

Respectfully submitted,

ERISE IP, P.A.

BY: /s/ Adam P. Seitz
Adam P. Seitz, Reg. No. 52,206
adam.seitz@eriseip.com
7015 College Boulevard, Suite 700
Overland Park, Kansas 66211
(913) 777-5600 Telephone
(913) 777-5601 Facsimile

COUNSEL FOR PETITIONER