US 20080210754A1

(19) United States

(12) Patent Application Publication

Lovett

(10) Pub. No.: US 2008/0210754 A1

(43) Pub. Date: Sep. 4, 2008

(54) ACCOUNT PAYMENT USING BARCODE INFORMATION EXCHANGE

(76) Inventor: **Robert Lovett**, Finger, TN (US)

Correspondence Address:
JAMES RICHARDS
58 BONING RD
FAYETTEVILLE, TN 37334 (US)

(21) Appl. No.: 12/077,872

(22) Filed: Mar. 22, 2008

Related U.S. Application Data

(63) Continuation-in-part of application No. 11/484,081, filed on Jul. 11, 2006, now Pat. No. 7,347,361, which is a continuation-in-part of application No. 11/445,553, filed on Jun. 2, 2006.

(60) Provisional application No. 60/689,576, filed on Jun. 13, 2005.

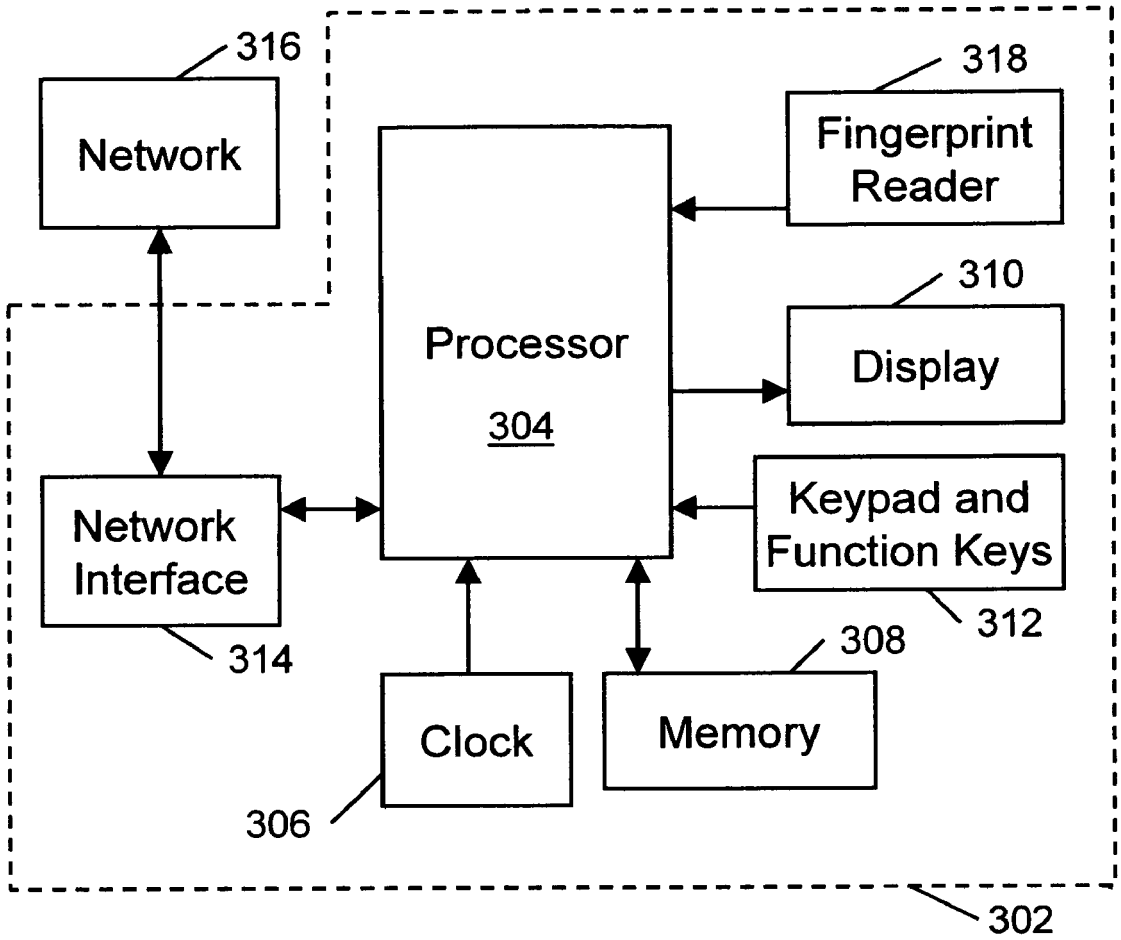
Publication Classification

(51) Int. Cl.
G06K 5/00 (2006.01)

(52) U.S. Cl. 235/380

(57) **ABSTRACT**

A system for effecting transactions, typically retail transactions, by using account information stored on a computing device, such as a cell phone, wherein the computing device is placed on an optical reader at the merchant's establishment. The computing device generates a pattern, such as a bar code, on a visual display, which can be read by the merchant's optical reader. The display encodes account number and other information for the transaction. The merchant's optical reader also includes a display, which can be read by the computing device by using the cell phone camera. The merchant's display includes transaction amount and other information allowing updating of account information in the computing device. The computing device may include security codes and/or a fingerprint reader to allow access to the account information. The use of the fingerprint reader can provide positive identification of the individual, which may be used for restricted items such as age restricted items such as beer, cigarettes, and senior discounts.



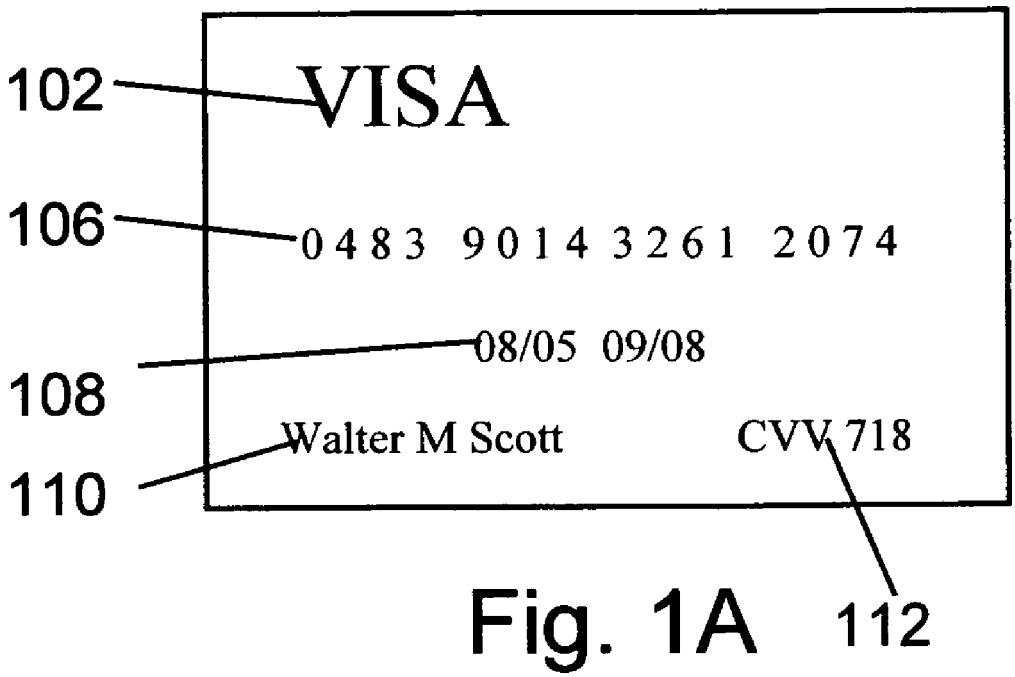

102
VISA
106
0483 9014 3261 2074
108
08/05 09/08
110
Walter M Scott
CVV 718
112

Fig. 1A

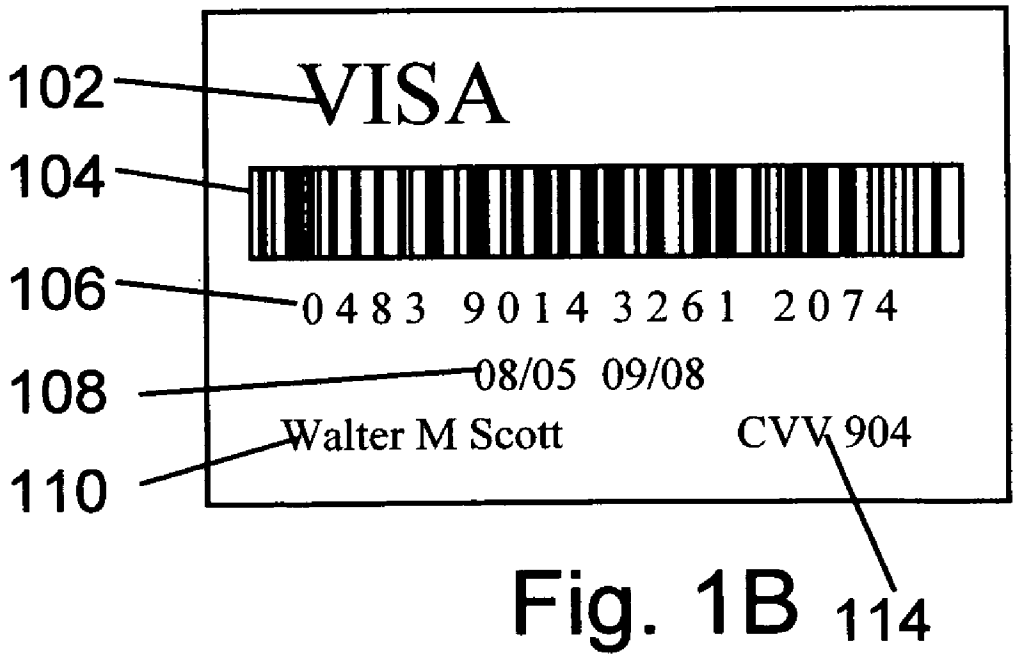

102
VISA
104
106
0483 9014 3261 2074
108
08/05 09/08
110
Walter M Scott
CVV 904
114

Fig. 1B

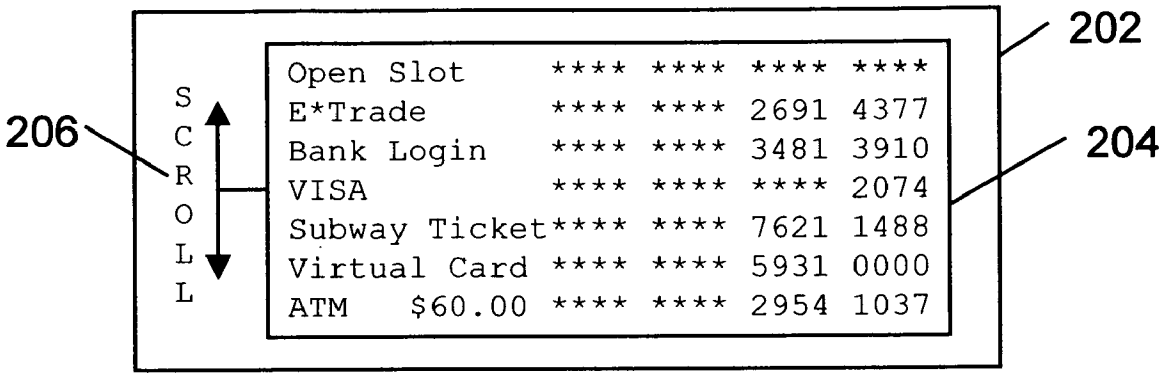

202
204
206
SCROLL
Open Slot **** **** **** ****
E*Trade **** **** 2691 4377
Bank Login **** **** 3481 3910
VISA **** **** **** 2074
Subway Ticket **** **** 7621 1488
Virtual Card **** **** 5931 0000
ATM $60.00 **** **** 2954 1037

Fig. 2

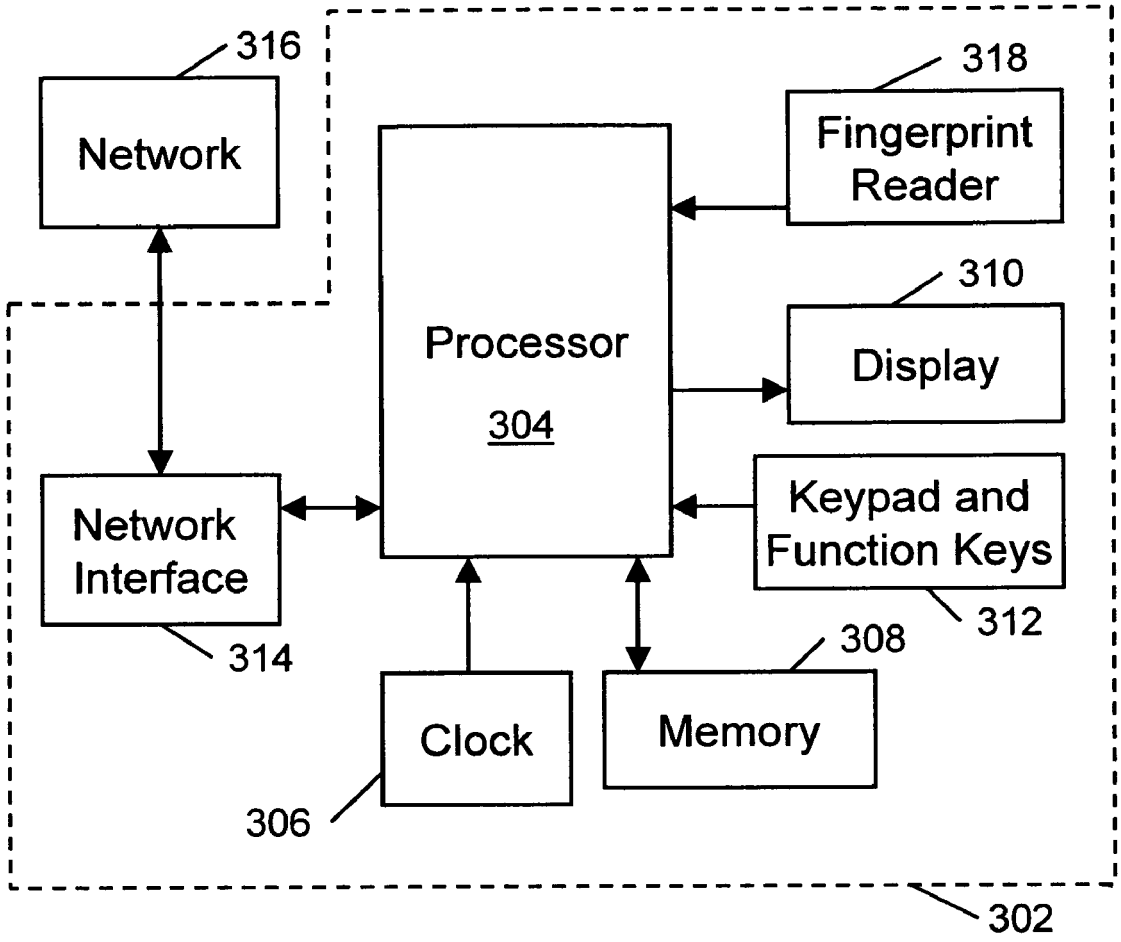

316
Network
318
Fingerprint Reader
Processor
304
310
Display
Network Interface
Keypad and Function Keys
314
312
308
Clock
Memory
306
302

Fig. 3

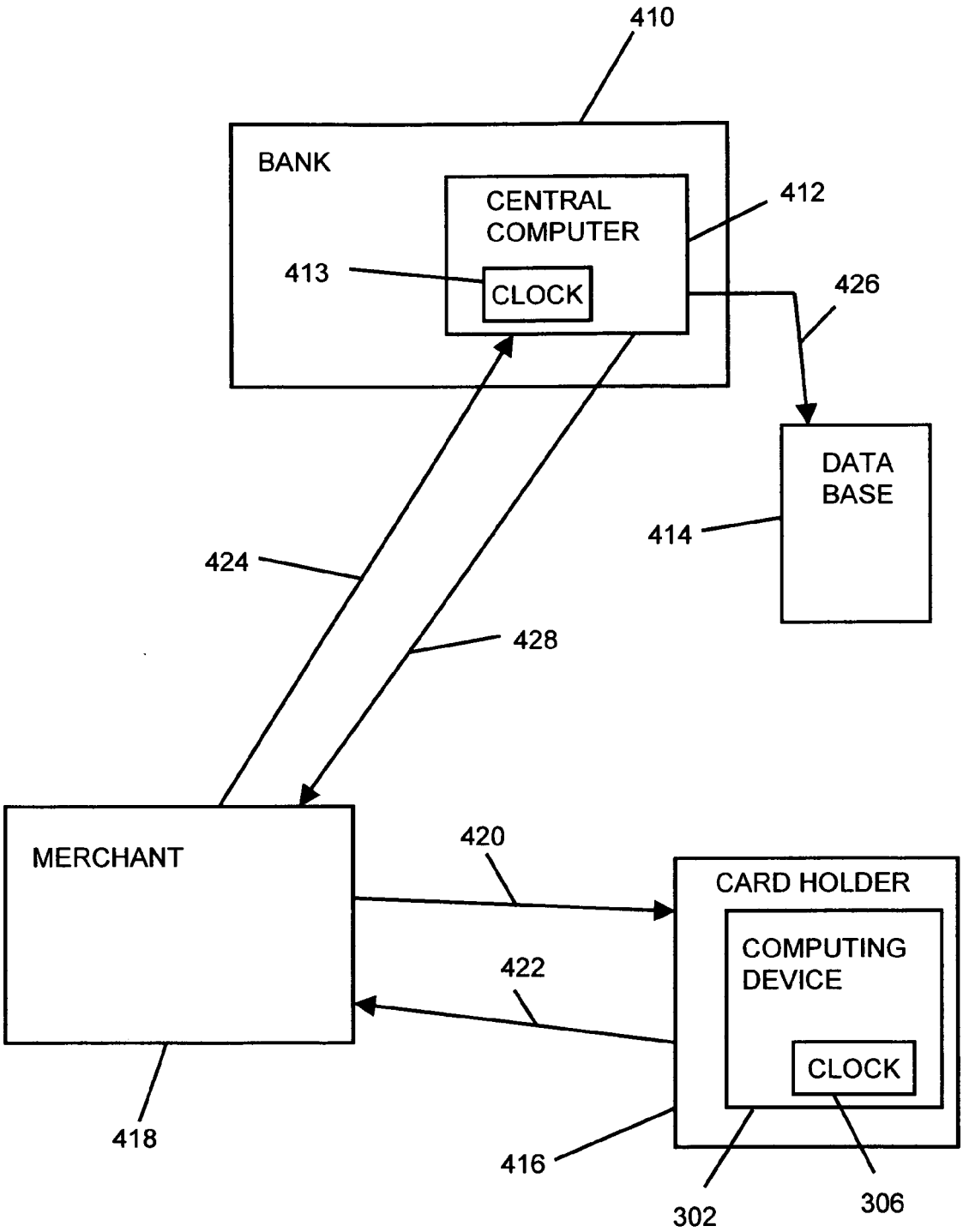

410
BANK
CENTRAL COMPUTER
412
413
CLOCK
426
DATA BASE
414
424
428
MERCHANT
420
CARD HOLDER
COMPUTING DEVICE
422
CLOCK
418
416
302
306

Fig. 4

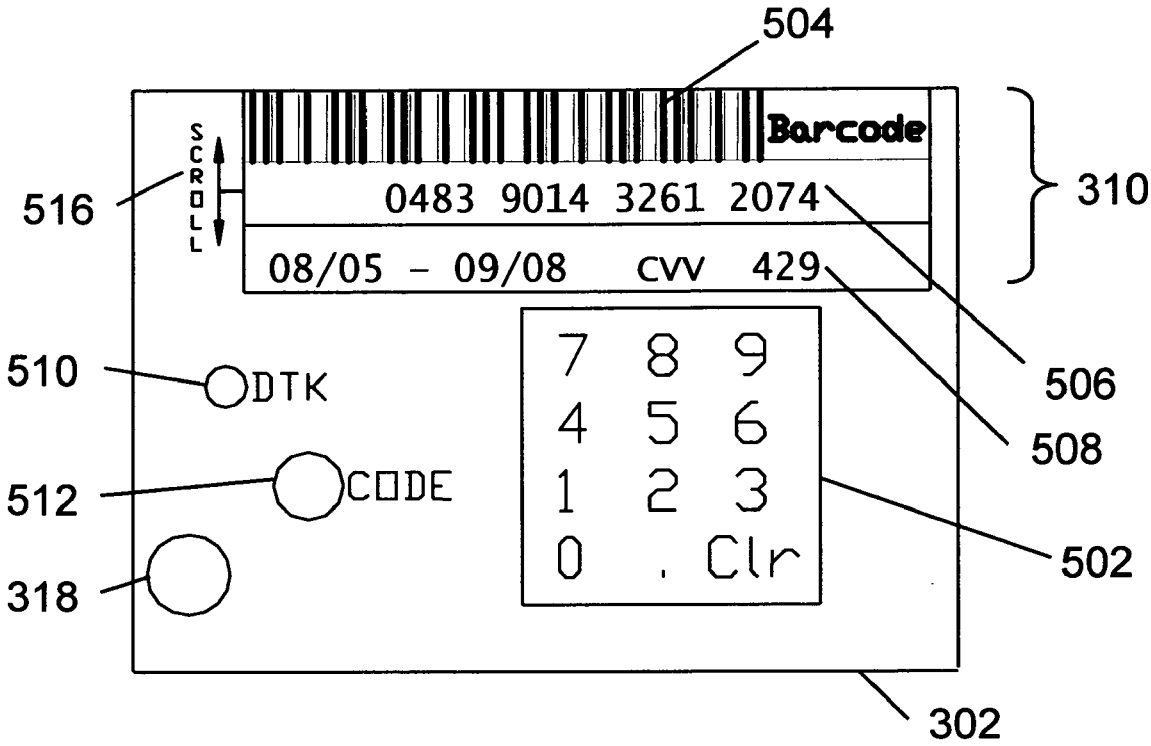

504
Barcode
SCROLL
516
0483 9014 3261 2074
08/05 - 09/08 CVV 429
310
506
508
510
DTK
512
CODE
318
7 8 9
4 5 6
1 2 3
0 . Clr
502
302

Fig. 5

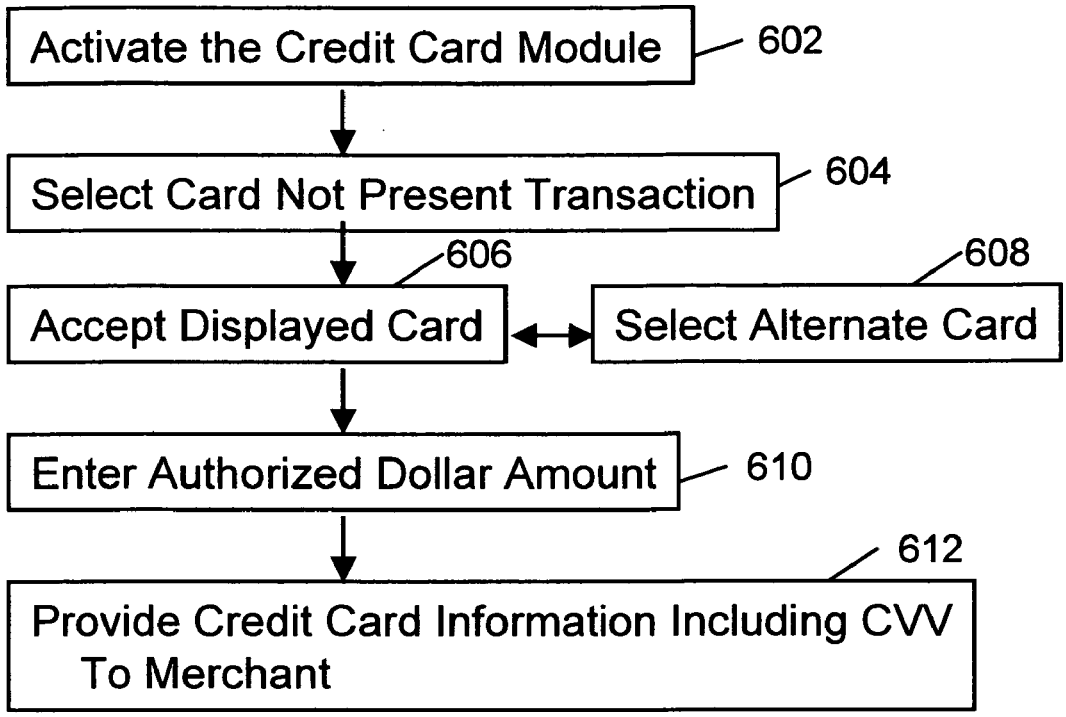

Activate the Credit Card Module
602
Select Card Not Present Transaction
604
606
608
Accept Displayed Card
Select Alternate Card
Enter Authorized Dollar Amount
610
612
Provide Credit Card Information Including CVV To Merchant

Fig. 6

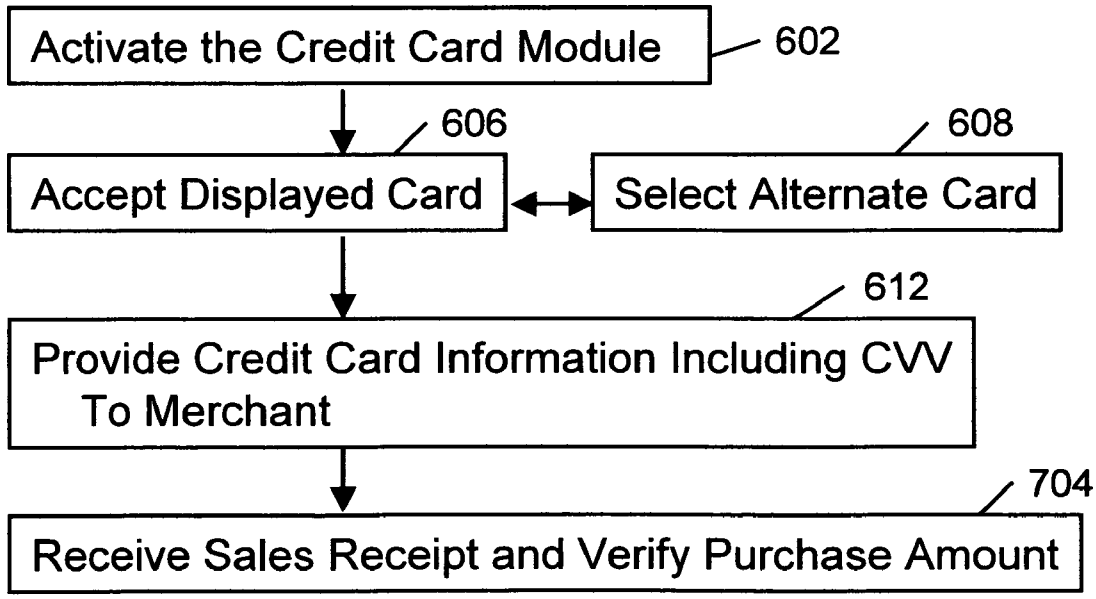

Activate the Credit Card Module
602
606
608
Accept Displayed Card
Select Alternate Card
612
Provide Credit Card Information Including CVV To Merchant
704
Receive Sales Receipt and Verify Purchase Amount

Fig. 7

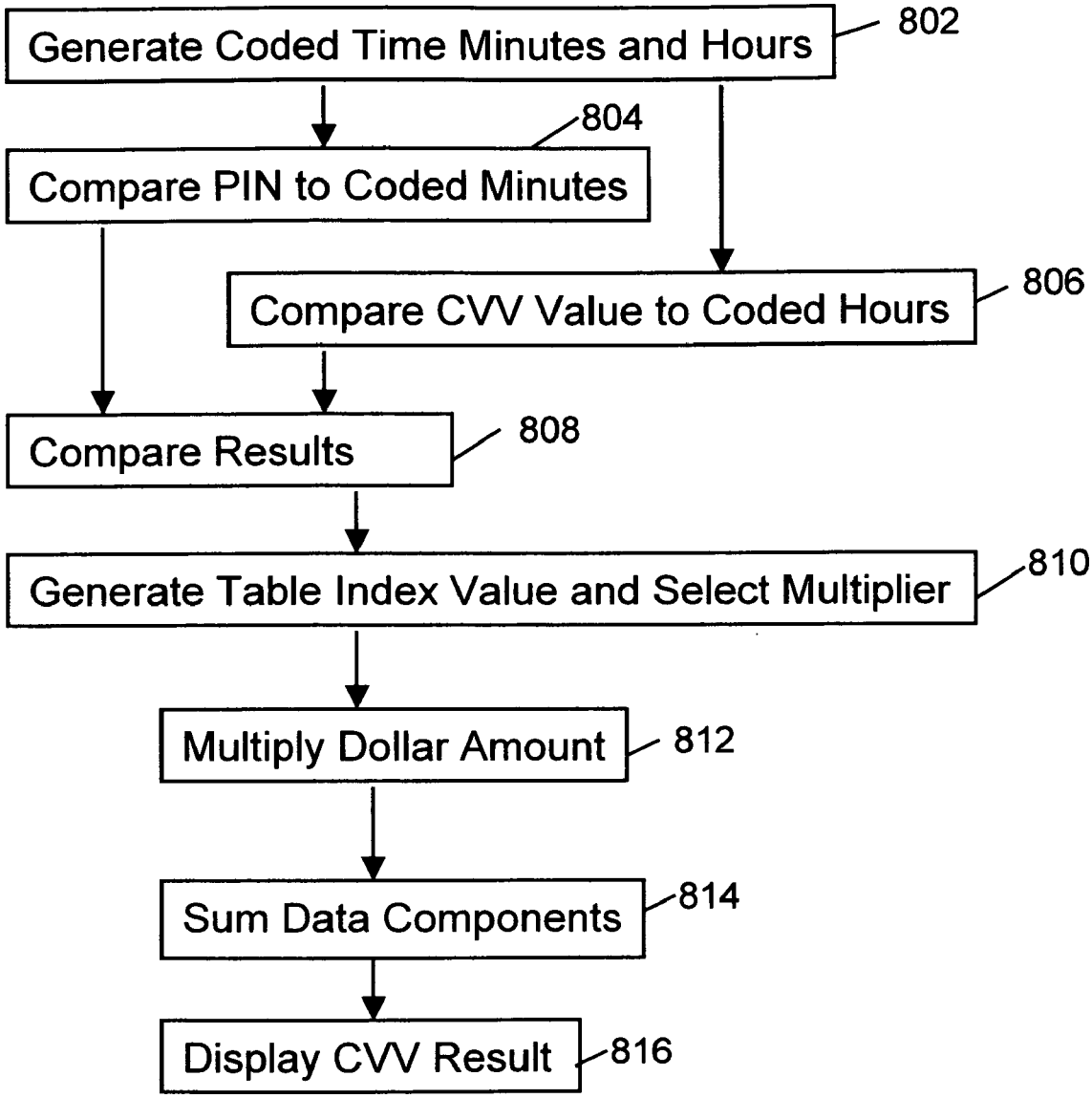

Generate Coded Time Minutes and Hours
802
Compare PIN to Coded Minutes
804
Compare CVV Value to Coded Hours
806
Compare Results
808
Generate Table Index Value and Select Multiplier
810
Multiply Dollar Amount
812
Sum Data Components
814
Display CVV Result
816

Fig. 8

Fig. 9A

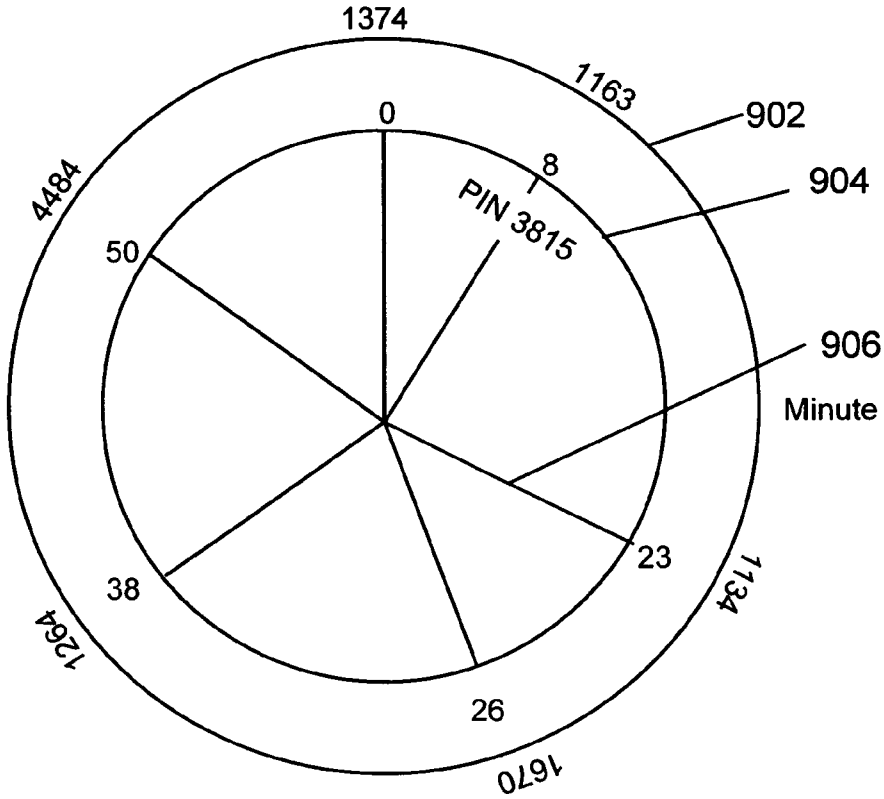
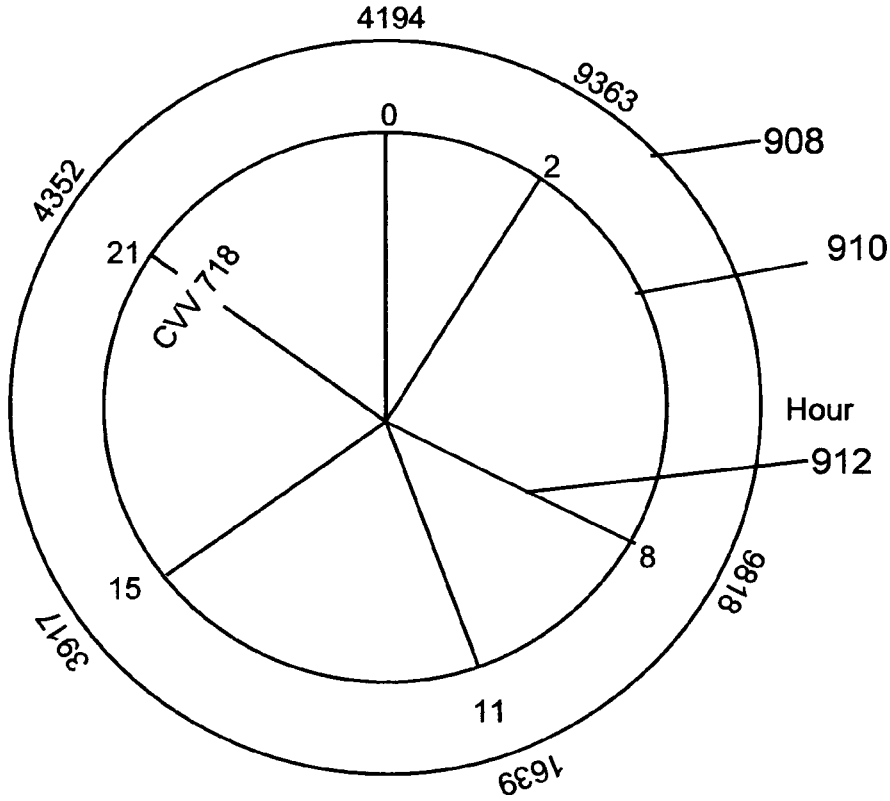

1374
1163
902
904
906
Minute
1134
1670
1264
4484
0
8
23
26
38
50
PIN 3815

Fig. 9B


4194
9363
908
910
Hour
912
9818
1639
3917
4352
0
2
8
11
15
21
CVV 718

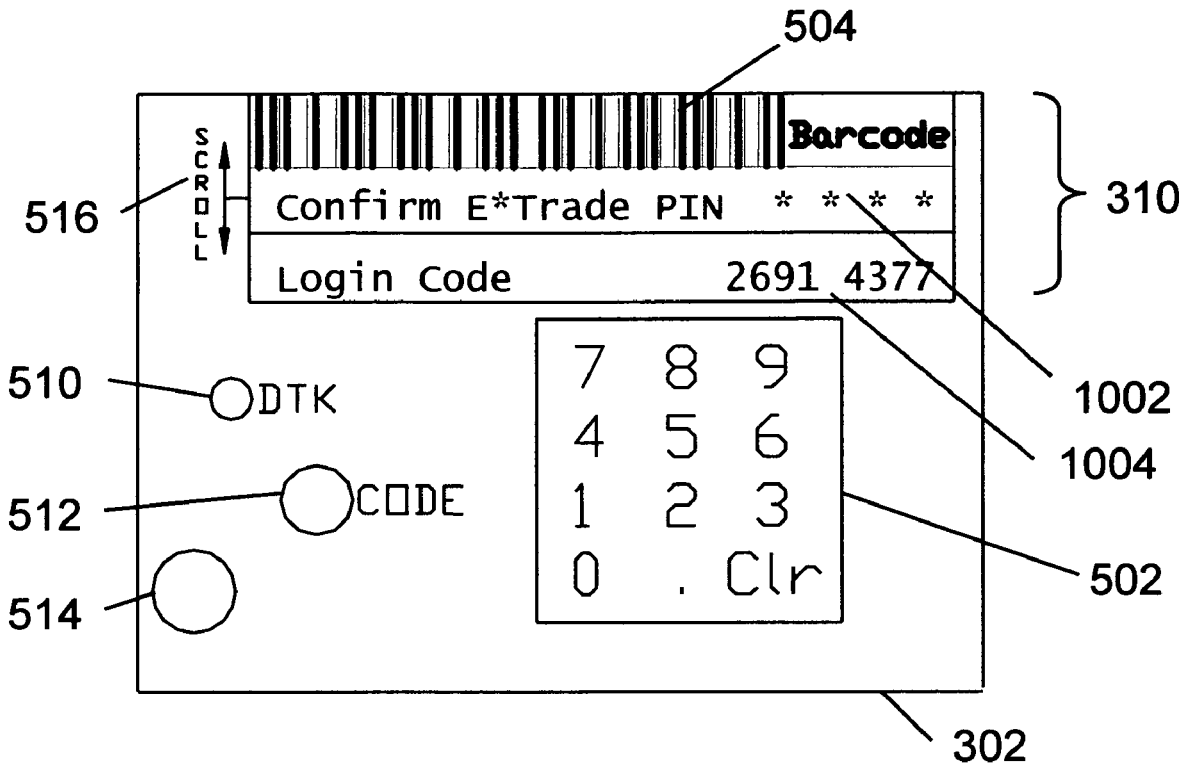

504
Barcode
SCROLL
516
Confirm E*Trade PIN * * * *
Login Code 2691 4377
310
510
DTK
512
CODE
514
7 8 9
4 5 6
1 2 3
0 . Clr
1002
1004
502
302

Fig. 10

Fig. 11A

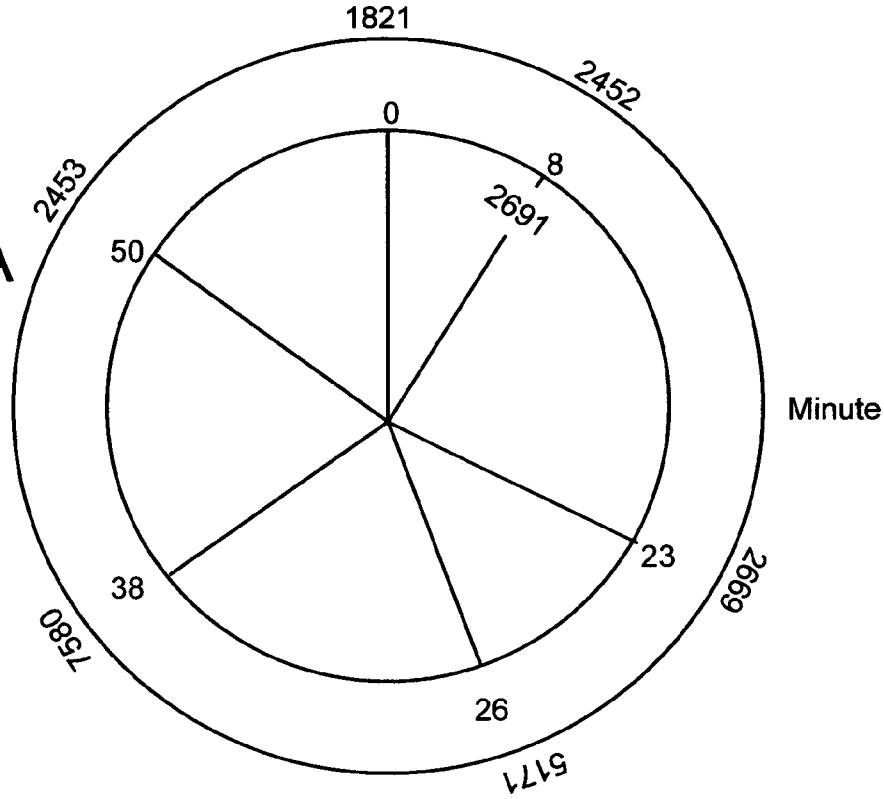
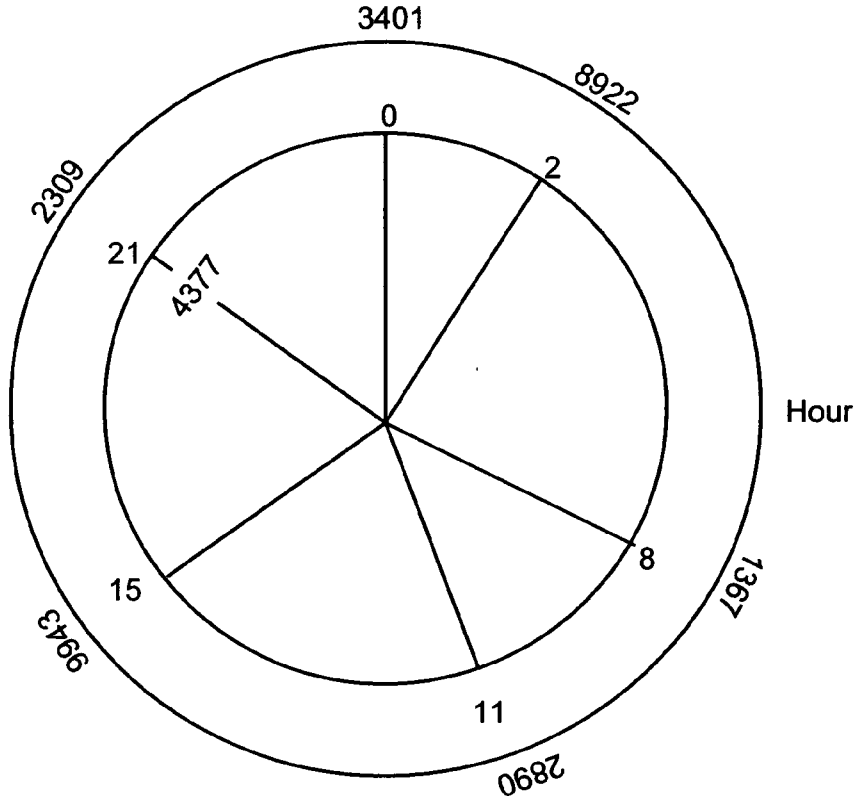


Fig. 11B



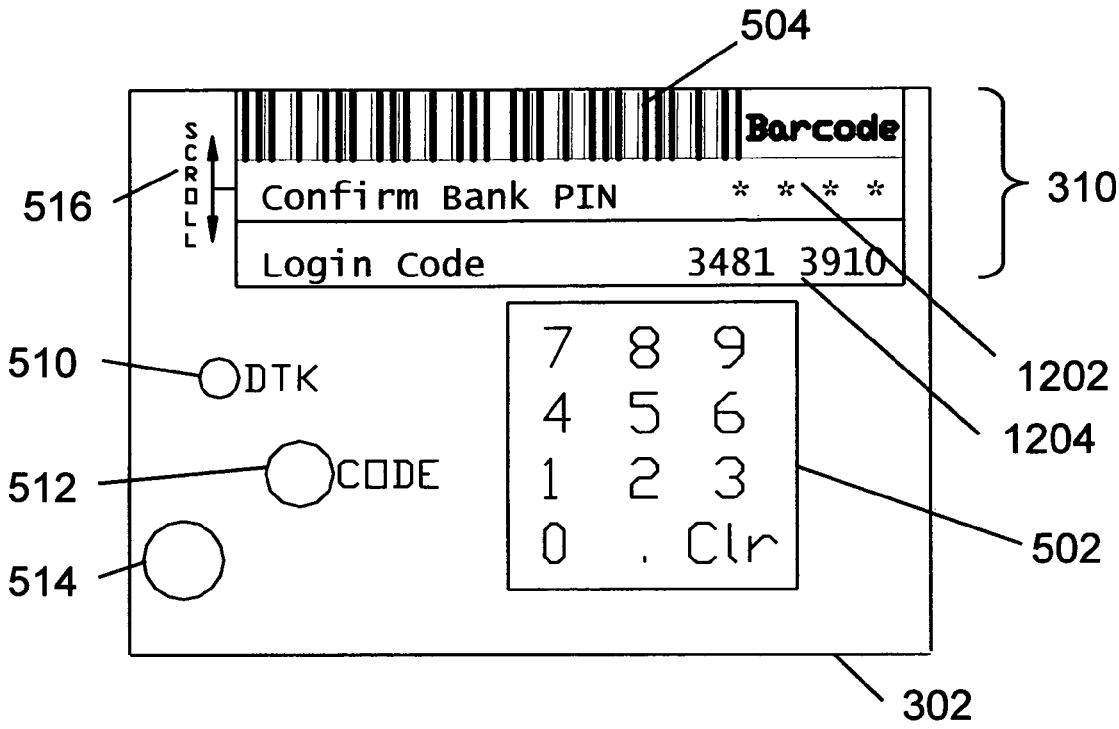

504
Barcode
SCROLL
516
Confirm Bank PIN * * * *
Login Code 3481 3910
310
510
DTK
7 8 9
4 5 6
1 2 3
0 . Clr
1202
1204
512
CODE
502
514
302

Fig. 12

Fig. 13A

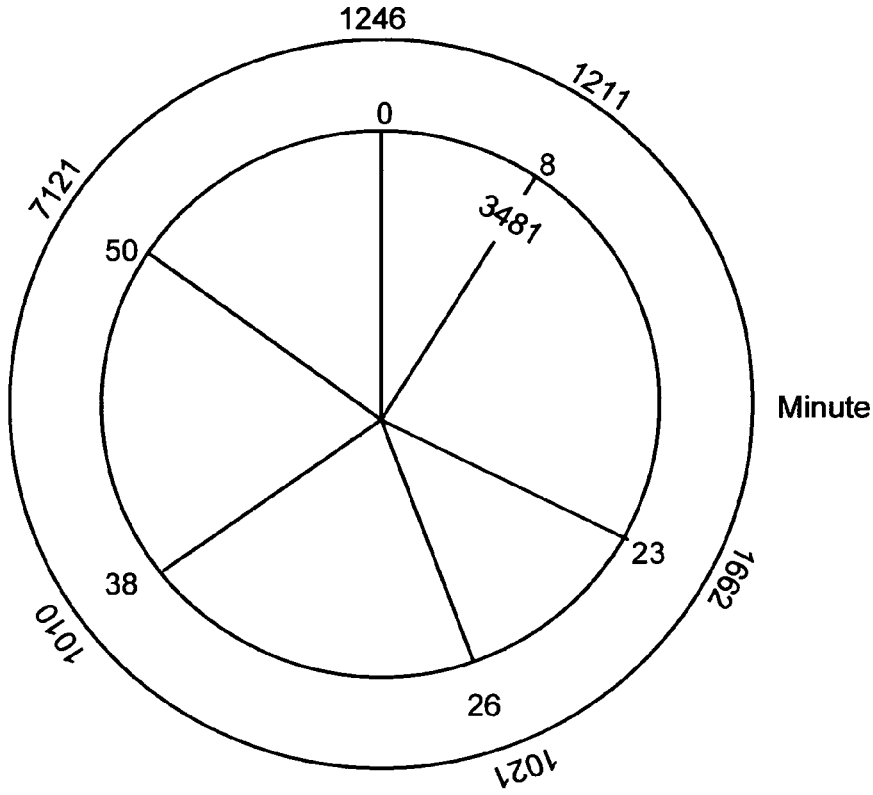
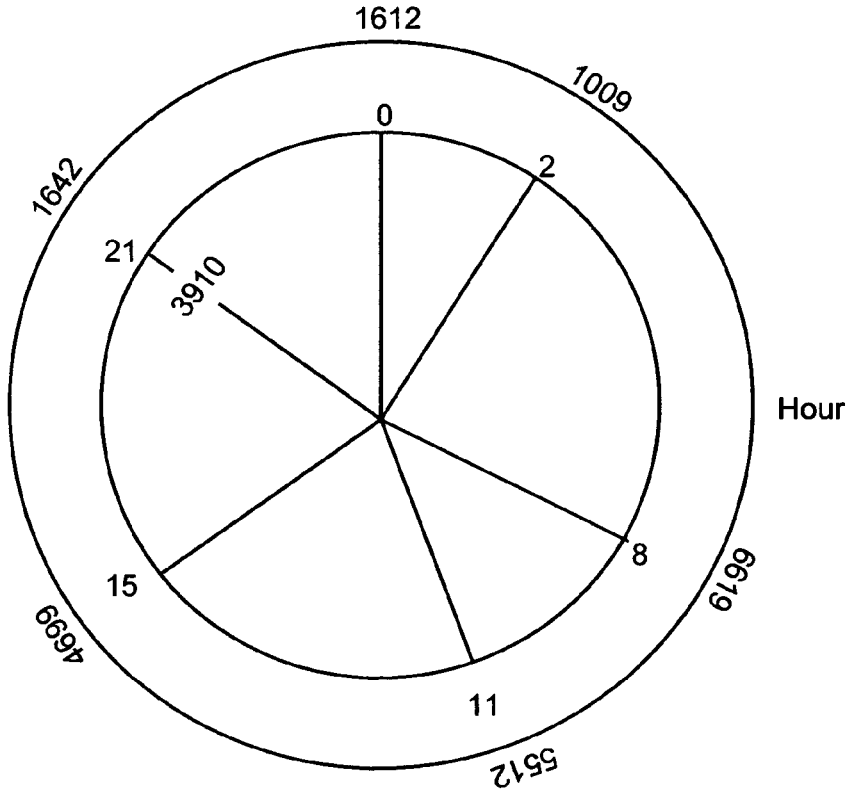


Fig. 13B



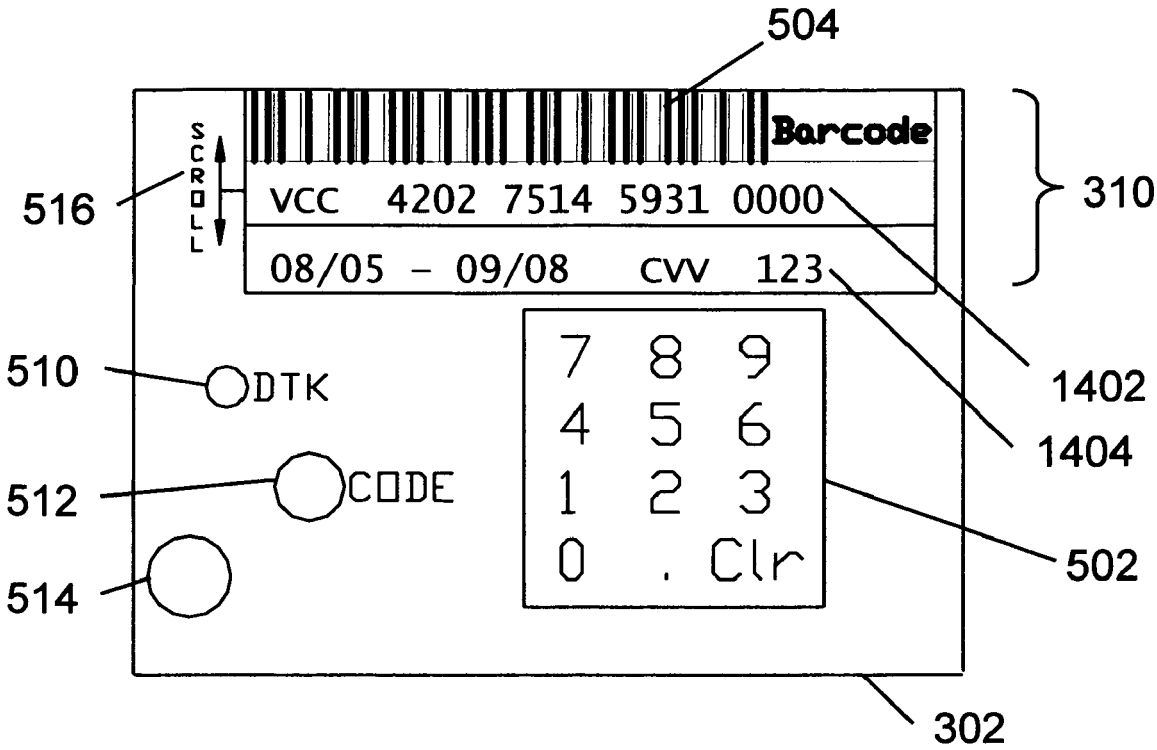

504
Barcode
SCROLL
516
VCC 4202 7514 5931 0000
08/05 - 09/08 CVV 123
310
1402
1404
510
DTK
512
CODE
514
7 8 9
4 5 6
1 2 3
0 . Clr
502
302

Fig. 14

Fig. 15A

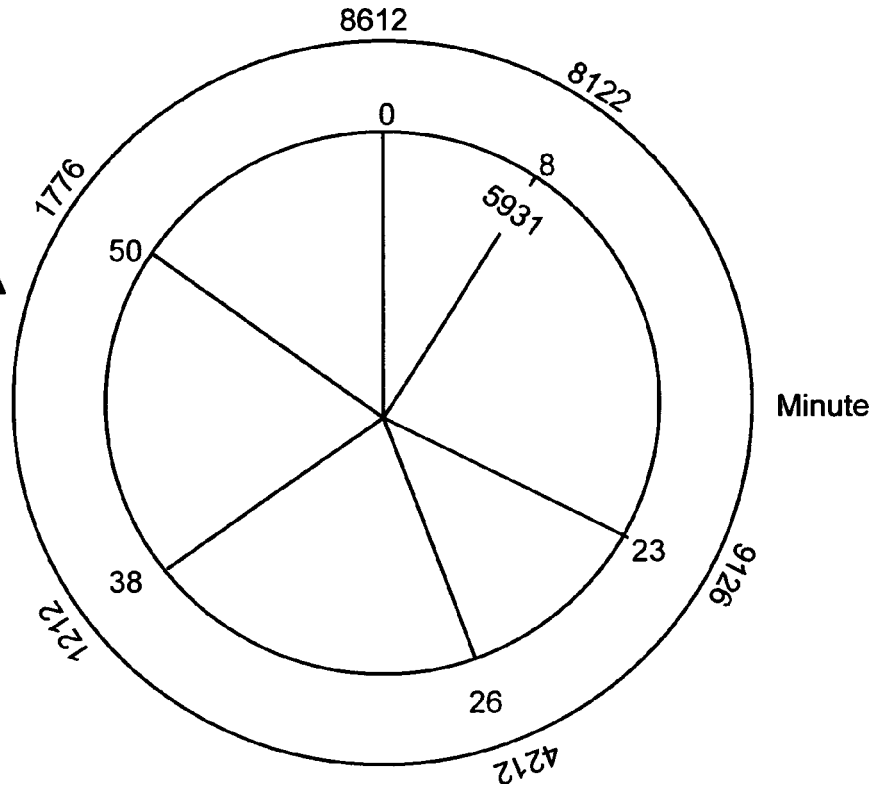
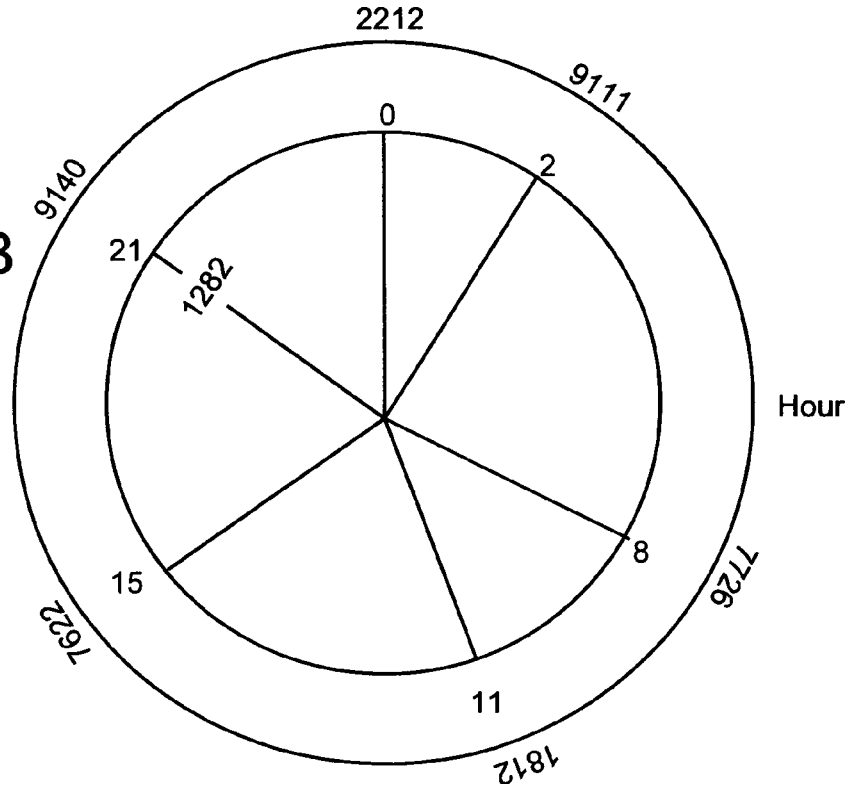


Fig. 15B



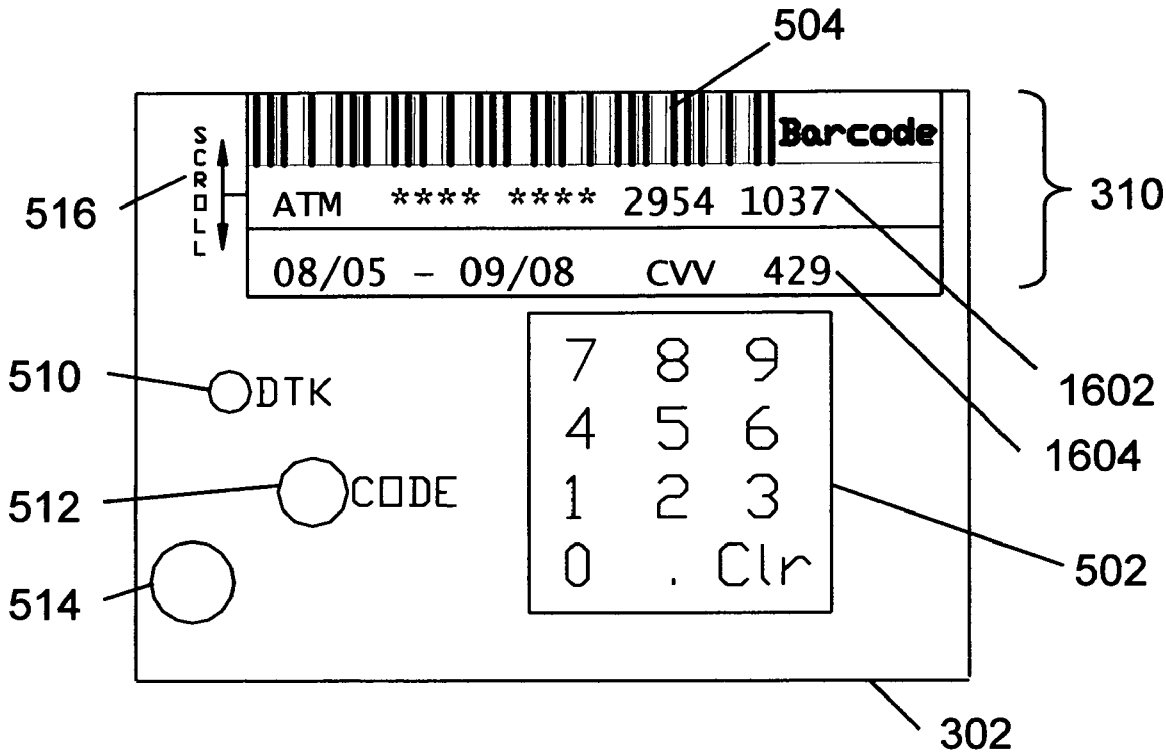

504
Barcode
SCROLL
516
ATM **** **** 2954 1037
08/05 - 09/08 CVV 429
310
1602
1604
510
DTK
512
CODE
514
7 8 9
4 5 6
1 2 3
0 . Clr
502
302

Fig. 16

Fig. 17A

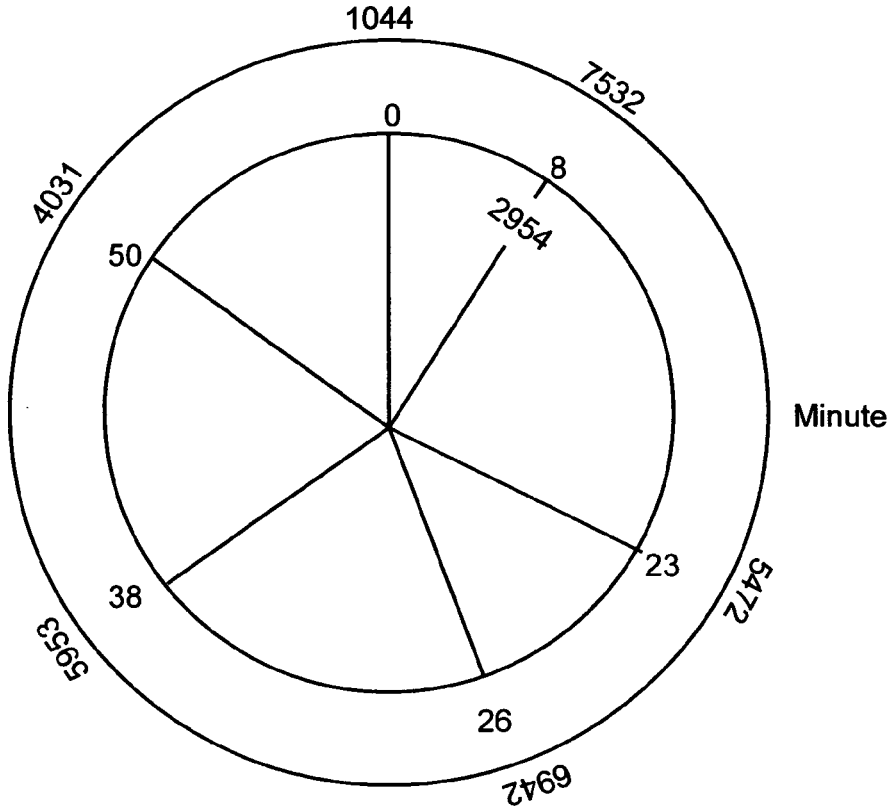
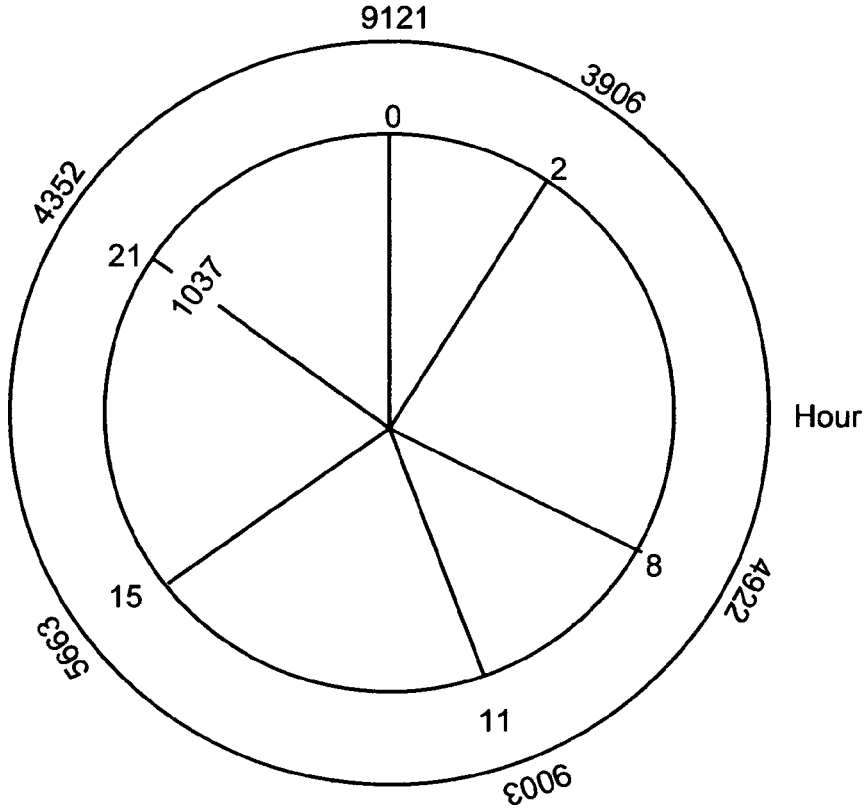


Fig. 17B



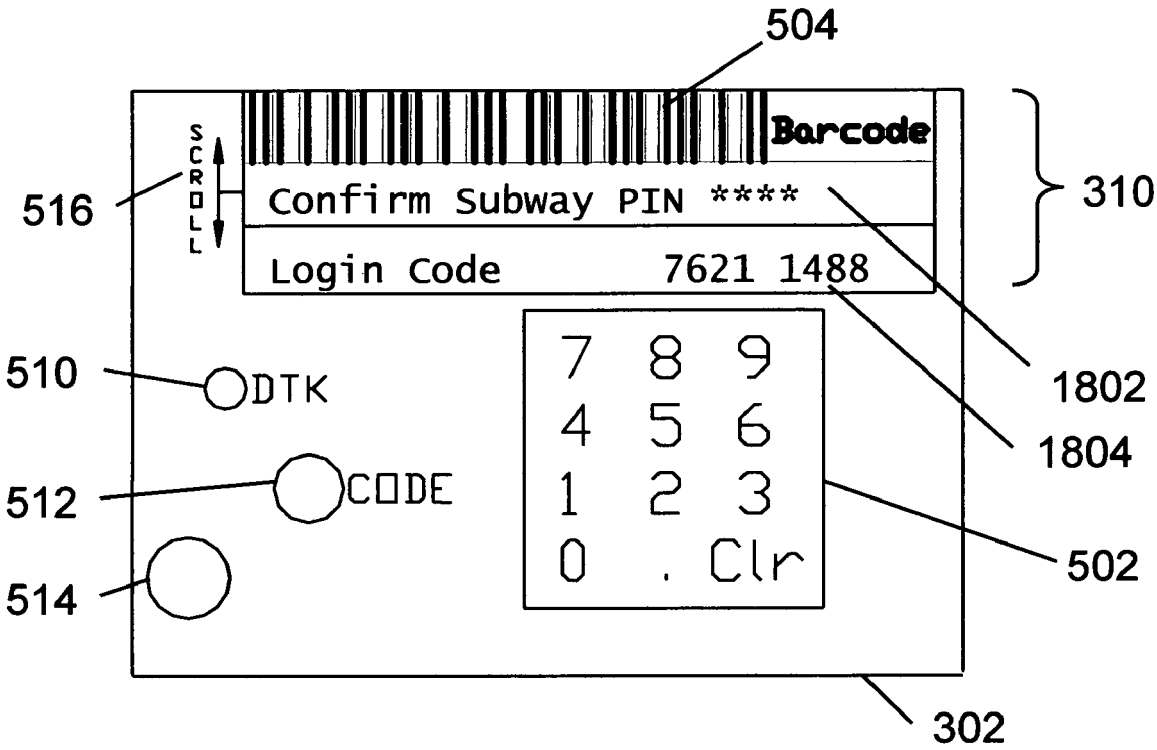

504
Barcode
SCROLL
516
Confirm Subway PIN ****
Login Code 7621 1488
310
510
DTK
7 8 9
4 5 6
1 2 3
0 . Clr
1802
1804
512
CODE
502
514
302

Fig. 18

Fig. 19A

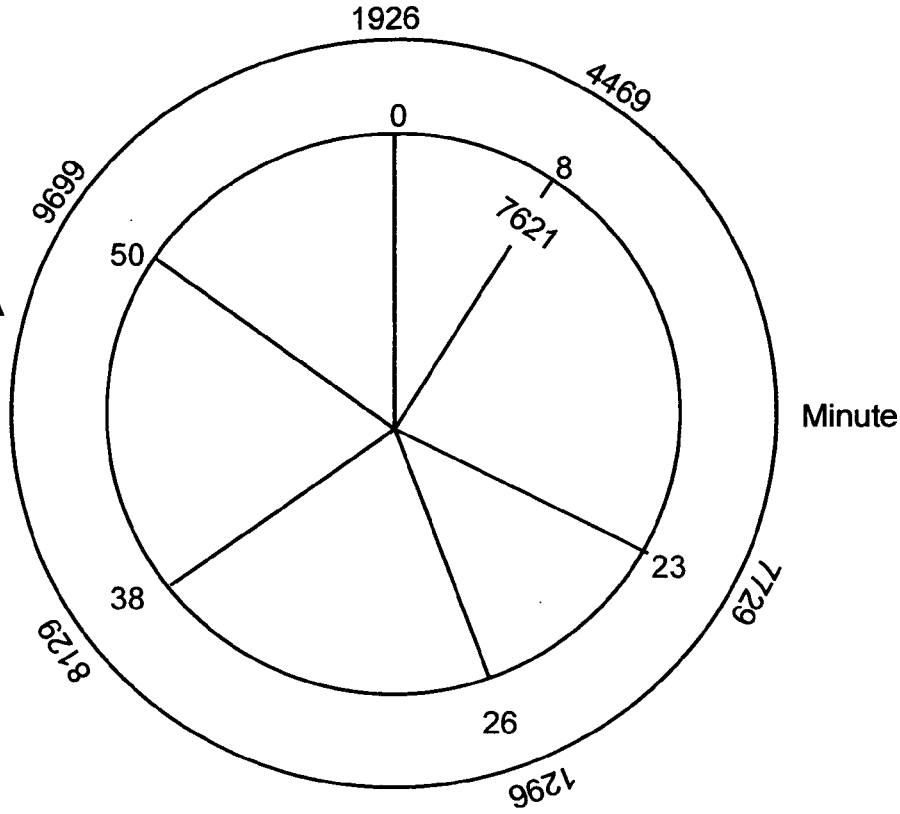
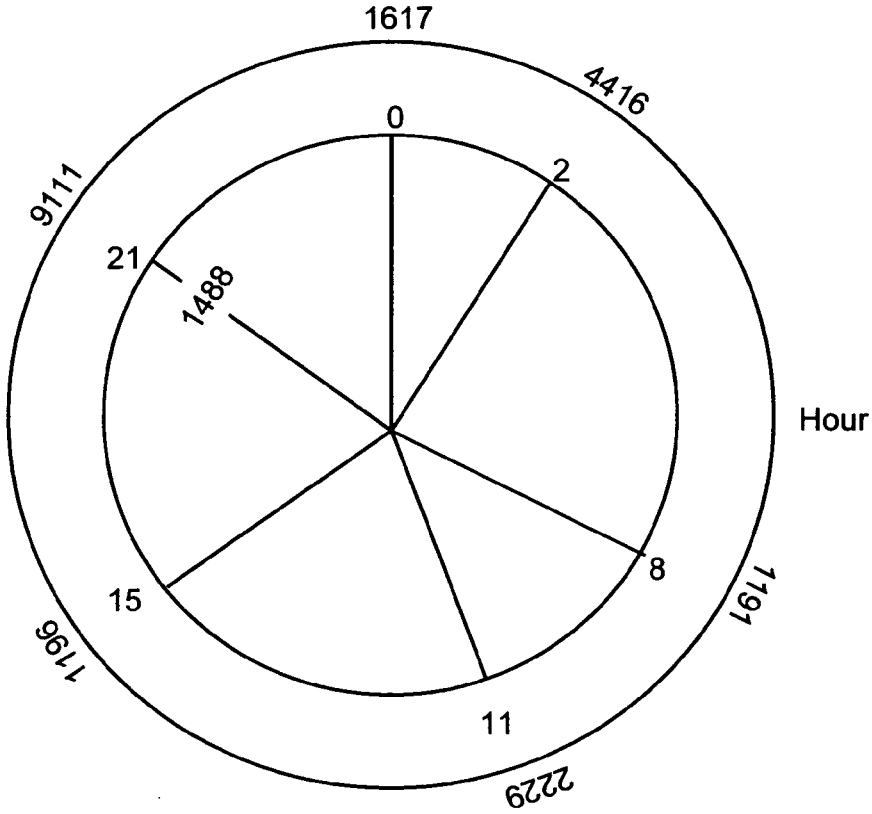


Fig. 19B



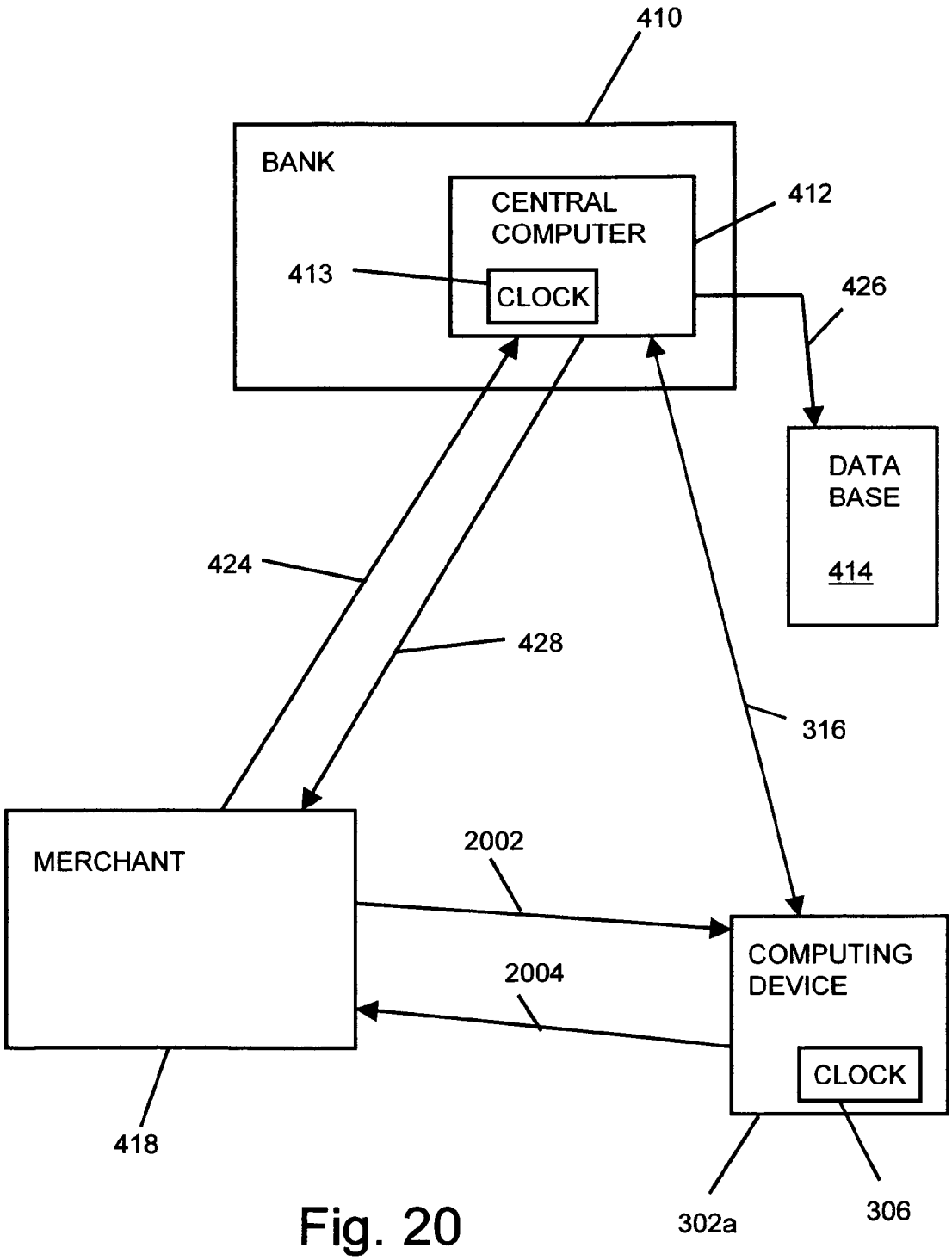

410
BANK
CENTRAL COMPUTER
412
413
CLOCK
426
DATA BASE
414
424
428
316
MERCHANT
2002
COMPUTING DEVICE
2004
CLOCK
418
302a
306

Fig. 20

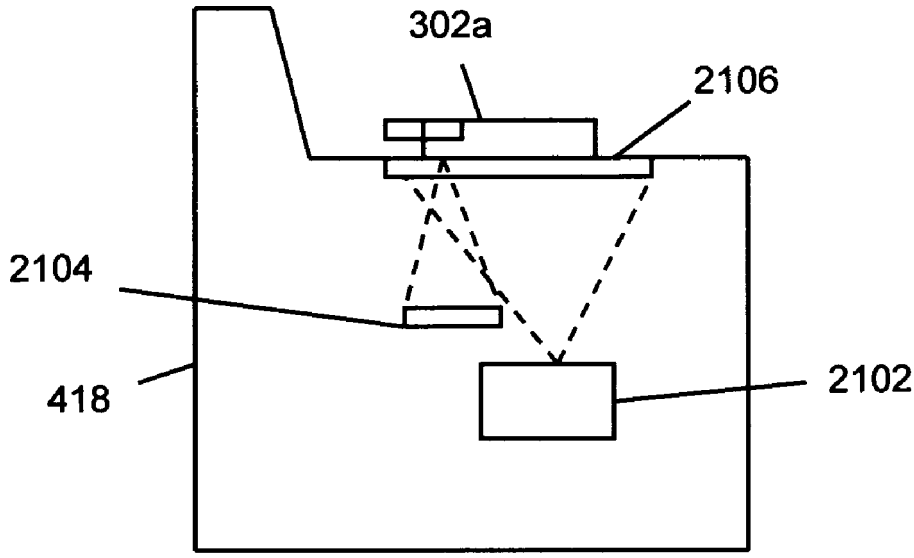


Fig. 21A

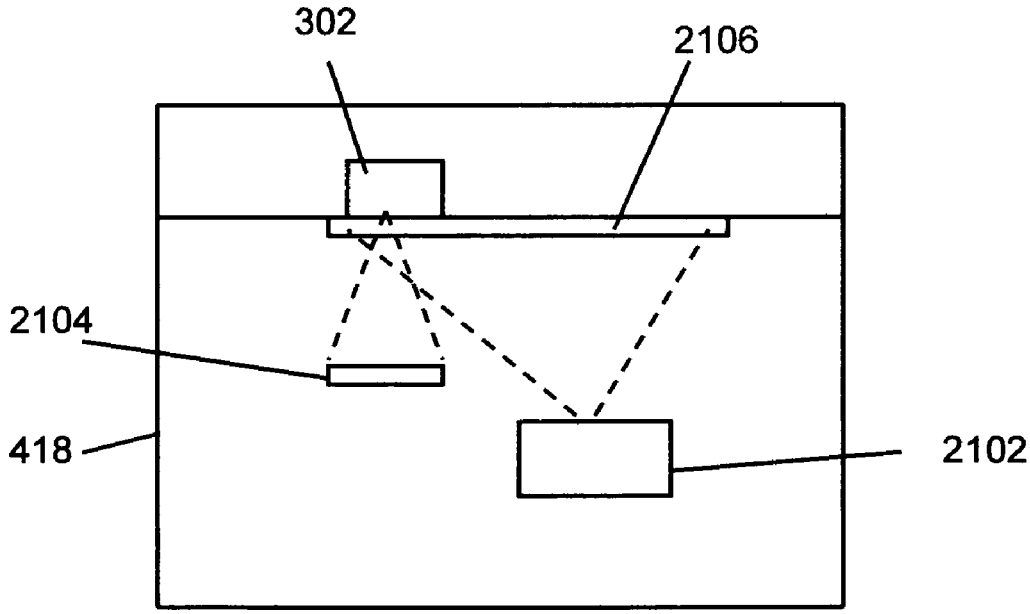


Fig. 21B

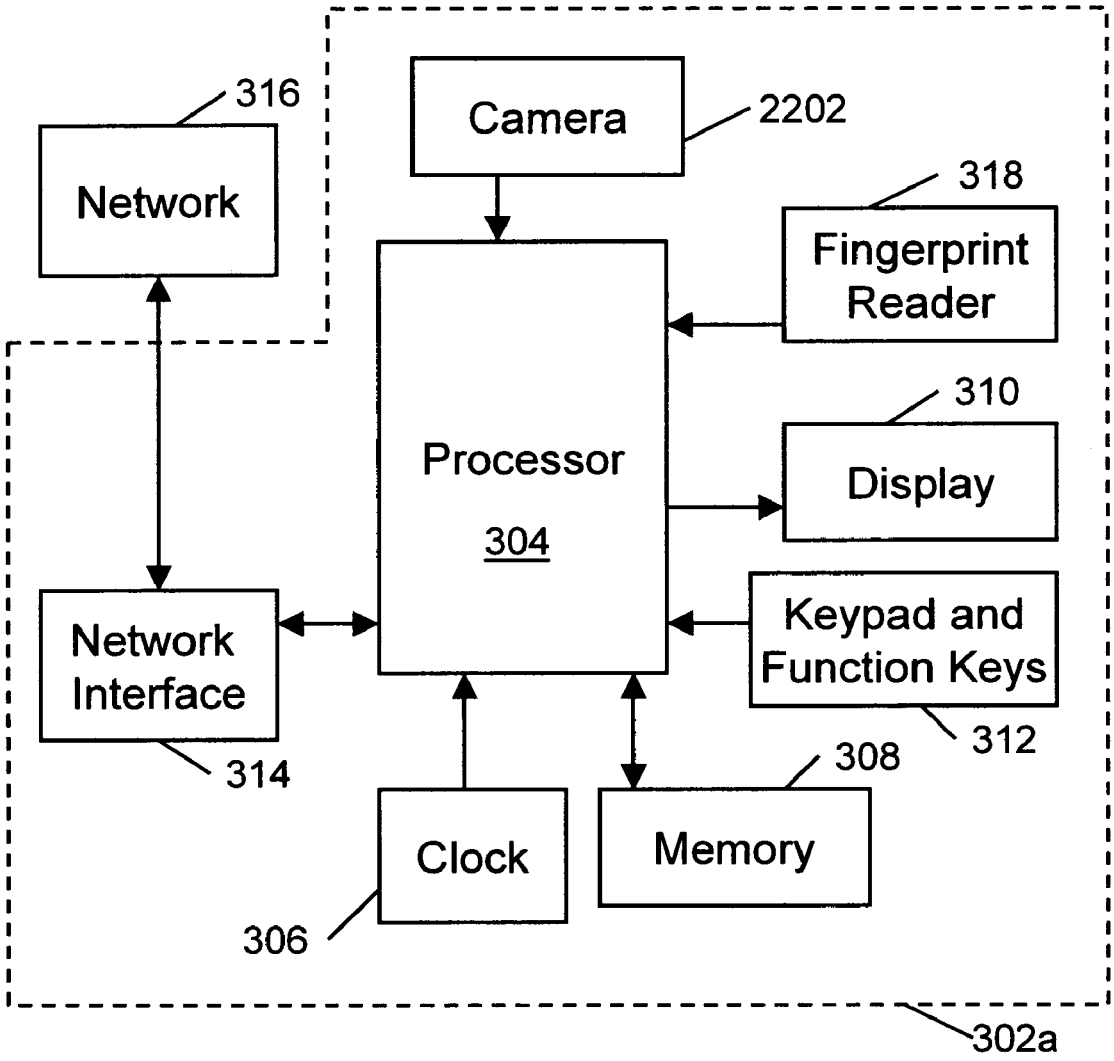

316
Network
Camera
2202
318
Fingerprint Reader
Processor
304
310
Display
Network Interface
Keypad and Function Keys
312
314
308
Clock
Memory
306
302a

Fig. 22

ACCOUNT PAYMENT USING BARCODE INFORMATION EXCHANGE

RELATED APPLICATIONS

[0001] This application is a continuation in part of U.S. patent application Ser. No. 11/484,081 titled System, Method And Program Product For Account Transaction Validation, filed Jul. 7, 2006 by Robert Lovett, which is a continuation in part of U.S. patent application Ser. No. 11/445,553, Titled "System, Method and Program Product For Credit Card Transaction Validation," filed Jun. 2, 2006 by Robert Lovett, which claims the benefit under 35 USC 119(e) of U.S. Provisional Application 60/689,576, filed Jun. 13, 2005 by Robert Lovett, all of which are incorporated herein by reference in their entirety.

FIELD OF THE INVENTION

[0002] This invention relates to account transactions, and more particularly to wireless account transactions.

BACKGROUND OF THE INVENTION

[0003] There have been many attempts to prevent the illegal use of credit cards in shopping malls, by telephone, Internet and especially Automated Teller Machines (ATM).

[0004] These efforts include Personal Identification Numbers (PIN) the use of mother's maiden names as a secret identification, and requiring credit card holders to use additional ID cards such as a driver license. All attempts to use static information have drawbacks since they are easily learned and passed on to other users. Once the static identification number is learned, it may be used to make fraudulent credit card purchases until the fraud is detected and the credit card account is closed.

[0005] Today, each purchase using a credit card, where the credit card is not present such as for internet or telephone transactions, must be accompanied by an additional security number, designated the CVV (card verification and validation) number. The CVV number may be alternatively called CVV2 or CID (card identification) or CCV (credit card verification or validation) by various credit card companies. The CVV number is typically on the back of the credit card, as with Master Card or Visa, but may be on the front of the card, as with American Express. The CVV number typically uses three digits, but may use four as with American Express. Merchants are not allowed to store CVV numbers in their database with the credit card number as a security measure. Because CVV numbers are not in the merchant's database, CVV numbers will not be disseminated if a merchant's database is compromised, assuming the merchant follows the rules and does not record the CVV number. Since the CVV number is not in the database, each transaction must be accompanied by a new request for the CVV number from the cardholder.

[0006] However, since the CVV numbers are disclosed to the merchants, their employees, and anyone in the communications chain, they may easily be recorded and passed on.

[0007] Thus, there is a need for a system and method for securing credit card transactions that does not generate information that may be easily determined, circumvented or passed on to others and used to generate fraudulent transactions.

SUMMARY OF THE INVENTION

[0008] Briefly, the present invention relates to a system for effecting transactions, typically retail transactions, by using account information stored on a computing device, such as a cell phone, wherein the computing device is placed on an optical reader at the merchant's establishment. The computing device generates a pattern, such as a bar code, on a visual display, which can be read by the merchant's optical reader. The display encodes account number and other information for the transaction. The merchant's optical reader also includes a display, which can be read by the computing device by using the cell phone camera. The merchant's display includes transaction amount and other information allowing updating of account information in the computing device. The computing device may include security codes and/or a fingerprint reader to allow access to the account information. The use of the fingerprint reader can provide positive identification of the individual, which may be used for restricted items such as age restricted items such as beer, cigarettes, and senior discounts.

[0009] System and computer program products corresponding to the above-summarized methods are also described and claimed herein.

[0010] Additional features and advantages are realized through the techniques of the present invention. Other embodiments and aspects of the invention are described in detail herein and are considered a part of the claimed invention. For a better understanding of the invention with advantages and features, refer to the description and to the drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] The subject matter which is regarded as the invention is particularly pointed out and distinctly claimed in the claims at the conclusion of the specification. The foregoing and other objects, features, and advantages of the invention are apparent from the following detailed description taken in conjunction with the accompanying drawings in which:

[0012] FIG. **1**A illustrates an exemplary display for a credit card on a computing device.

[0013] FIG. **1**B illustrates an exemplary display for credit card information including a bar code and an encrypted CVV code in accordance with the present invention.

[0014] FIG. **2** illustrates an exemplary display showing the selection of transaction types and hosts available.

[0015] FIG. **3** is an exemplary system block diagram for a networked computing device in accordance with the present invention.

[0016] FIG. **4** is a schematic diagram of a system using the present invention.

[0017] FIG. **5** illustrates the face of an exemplary computing device in accordance with the present invention.

[0018] FIG. **6** illustrates a process for using the computing device of FIG. **5** to execute a credit card transaction.

[0019] FIG. **7** illustrates a process for using the computing device of FIG. **5** to execute an over the counter credit card transaction.

[0020] FIG. **8** shows an exemplary method for calculating an encrypted time dependent CVV code.

[0021] FIG. **9**A and FIG. **9**B illustrate an exemplary coded clock in accordance with the present invention.

[0022] FIG. **10** illustrates the computing device of FIG. **5** with an E*Trade transaction selected.

[0023] FIGS. **11**A and **11**B illustrate the code minute and code hour tables for the E*trade transaction of FIG. **10**.

[0024] FIG. **12** illustrates the computing device of FIG. **5** with a Bank transaction selected.

[0025] FIGS. **13**A and **13**B illustrate the code minute and code hour tables for the bank transaction of FIG. **12**.

[0026] FIG. **14** illustrates the computing device of FIG. **5** with a Virtual Credit Card (VCC) transaction selected.

[0027] FIGS. **15**A and **15**B illustrate the code minute and code hour tables for the VCC transaction of FIG. **14**.

[0028] FIG. **16** illustrates the computing device of FIG. **5** with an ATM (Automatic Teller Machine) transaction selected.

[0029] FIGS. **17**A and **17**B illustrate the code minute and code hour tables for the ATM transaction of FIG. **16**.

[0030] FIG. **18** illustrates the computing device of FIG. **5** with a subway fare transaction selected.

[0031] FIGS. **19**A and **19**B illustrate the code minute and code hour tables for the subway fare transaction of FIG. **18**.

[0032] FIG. **20** illustrates an exemplary system having a direct optical interface between the merchant equipment and the customer's computing device.

[0033] FIG. **21**A and FIG. **21**B illustrate two views of an exemplary barcode scanner including a barcode generator in accordance with the present invention.

[0034] FIG. **22** illustrates an exemplary cell phone in accordance with the present invention.

[0035] The detailed description explains the preferred embodiments of the invention, together with advantages and features, by way of example with reference to the drawings.

DETAILED DESCRIPTION OF THE INVENTION

[0036] Briefly, the present invention relates to a system for effecting transactions, typically retail transactions, by using account information stored on a computing device, such as a cell phone, wherein the computing device is placed on an optical reader at the merchant's establishment. The computing device generates a pattern on a visual display, such as a bar code display, which can be read by the merchant's optical reader. The display encodes account number and other information for the transaction. The merchant's optical reader also includes a display, which can be read by the cell phone by using the cell phone camera. The merchant's display includes transaction amount and other information allowing updating of account information in the computing device. The computing device may include security codes or a fingerprint reader to allow access to the account information. The use of the fingerprint reader can provide positive identification of the individual, which may be used for sales of restricted items such as age restricted items like beer and cigarettes.

[0037] The present invention is for a cell phone networked device or other networked device for generating credit card protection codes and assisting in efficient transaction processing.

[0038] The present invention overcomes the vulnerability of the static CVV number by providing an encrypted CVV code which is newly computed for each new card transaction. A code calculation is never reused for a different transaction. Thus, the merchant, or anyone else observing the transaction would be unable to duplicate the transaction or generate another transaction with the information provided. Any attempt to re-use the CVV code would generate a security alert which could be provided at the time of the fraudulent transaction. As a further benefit of the present invention, a cardholder may use a PIN to enable the device to generate the CVV code, protecting the device from loss or theft. As a further benefit, the transaction amount may be used in addition to time to generate the CVV code, thus validating the amount entered by the merchant, thus preventing an unauthorized amount from being sent to the card processing center. Since the invention utilizes the CVV number structure that is already in place, little change is required in the field equipment now in place. Store equipment to read and process credit cards and communicate with the card processing center is unchanged. Each cardholder may utilize new software installed on a cell phone or other device, and the card processing centers may add software to perform the additional processing. Regular credit cards may be processed as before with no change to the equipment.

[0039] The present invention envisions the use of a multi-function cell phone which may include web and music downloading features, may allow storing of notes, exchange of pictures, and may include the storage of credit card information, eliminating the plastic. In accordance with the present invention, such multi-function cell phone device, however, may include more capability than simply storing credit card information. The cell phone device may compute encrypted validation codes (CVV codes) to improve credit card security. Further, the cell phone device may display a barcode having the complete credit card information including the computed encrypted validation code. The barcode may be read by a merchant's terminal device, eliminating transcription errors. Further features of the cell phone device may include the entry of a PIN to activate the credit card information, providing security in the case of a stolen cell phone. The stolen cell phone credit card information may be quickly disabled by calling the cell phone and providing a disabling code. In one embodiment, the cell phone device may include a fingerprint reader to provide alternate user validation and eliminate the need to enter the PIN, simplifying and speeding sales transactions.

[0040] The present invention generates an encrypted time dependent validation code (CVV code) to validate each transaction. The CVV code may be preferably three or four characters long and may be transmitted in place of the CVV validation number presently in use and thus may utilize much of the same card processing equipment and infrastructure presently in place. In accordance with one embodiment of the invention, the credit card may be a virtual credit card (VCC), which may exist entirely within a computer or network and have no physical plastic embodiment. The virtual credit card exists as a software program on a computer and can be referenced by using the computer display. In a conventional credit card, the information is static, whether embossed, printed or written into the magnetic stripe. The virtual credit card program can include dynamic and computed information. In particular, the virtual credit card can compute an encrypted validation code with significant security advantages. The virtual credit card may also use improved identification features to insure the authorized owner of the card is present. In particular, the VCC may require entry of a PIN to reference the card. In advanced cards, a fingerprint reader may be installed to obviate the need for entry of the PIN and speed the transaction process. In one embodiment, a traditional credit

card may have a virtual credit card capability and may be usable with the static CVV number and/or the encrypted CVV code as the user may select.

[0041] In a further embodiment, the VCC may be networked and the network connection may be used in part of the validation process. The network may be a cell phone network, telephone network, or computer network like, for example, the Internet.

[0042] FIG. **1**A illustrates an exemplary display for a credit card on a computing device. Referring to FIG. **1**A, the display is presented on the screen of the computing device, which may be a cell phone or other device, preferably a personal and portable, hand held computing device. Information is displayed in a rectangular format simulating a plastic credit card so that the different types of information are easily identified by one familiar with plastic credit cards. Information includes a type of card **102**, a card number **106**, expiration date **108**, name of a cardholder **110**, and a static CVV number **112**. The static CVV number may be more typically located on the back of a plastic card, but is shown on the screen within the rectangle for convenience. The static CVV number shown in FIG. **1**A is the static CVV number that would be displayed on the back of an associated the plastic card embodiment and may be displayed in one embodiment of a display for the credit card stored in the computing device.

[0043] FIG. **1**B illustrates an exemplary display for credit card information including a bar code and an encrypted CVV code in accordance with the present invention. The display of FIG. **1**B may be shown on the screen of the computing device in accordance with the present invention. The display of FIG. **1**B includes the information of FIG. **1**A and further includes a bar code **104**. The bar code **104** information may include the card number **106**, expiration date **108** and encrypted CVV code **114**. The encrypted CVV code **114** shown in FIG. **1**B may be a time dependent encrypted CVV code **114**. The use of the bar code **104** permits rapid automatic transcription of all pertinent credit card data, eliminating errors and improving speed and convenience. The encrypted CVV code **114** improves the security of a transaction validation process.

[0044] FIG. **2** illustrates an exemplary display showing the selection of transaction types and hosts that may be available. Referring to FIG. **2**, the display **202** may be shown as part of the screen on a cell phone or other device and may be shown separately or in conjunction with the display of FIG. **1**B. The display **202** of FIG. **2** shows a menu **204** of transaction types and allows scrolling **206** through the menu to select the desired transaction type. The illustrated transaction types **204** include E-Trade® account, Bank account, VISA® credit card, subway ticket, Virtual Credit Card, or ATM account. Certain other accounts and types of transactions may be included as well. Each account is set up with its own PIN number and static CVV number **112** or equivalent. Further, each account may include its own set of coding variables for encryption of time and other information, and/or may include its own specific encryption method.

[0045] FIG. **3** is an exemplary system block diagram for a networked computing device in accordance with the present invention. The network **316** is preferably a cell phone network and the networked computing device **302** is preferably a cell phone. The networked computing device **302** typically includes one or more processors **304** coupled to memory **308**. Typically the memory **308** may include several types of different densities and speeds and may be volatile and nonvolatile. The processor **304** is coupled to a clock **306** providing the time of day and date. The processor **304** typically displays information on a display **310** such as an LCD display and typically has a keypad **312** for entry of numbers and selection of modes. The processor **304** is connected to the network **316** through a network interface **314** for connection to a bank or other processing center (not shown). The network interface **314** may be a cell phone or cell phone module for connection to a cell phone network or wireless LAN (local area network) device for connection to a digital network. The network **316** may be used for downloading card information and/or coding information, and for making or validating transactions. The network **316** may also provide voice communications for the cell phone **302** and/or may provide the date and time of the device clock **306**. In a preferred alternative embodiment, the computing device may include a fingerprint reader **318**. The fingerprint reader may be used in place of the PIN for cardholder identification.

[0046] FIG. **4** is a schematic diagram of a system using the present invention. The system includes a financial institution shown in FIG. **4** and referred to hereafter as bank **410**. The bank **410** includes a central computer **412** connected to a database **414** in which credit card accounts are maintained. The central computer **412** further includes a bank clock **413**. Also included in the system of FIG. **4**, is a cardholder **416** whose credit card account is held by the bank **410**. The cardholder **416** has a computing device **302** of the present invention to protect the cardholder's credit card account by providing encrypted CVV codes **114** for each transaction. The computing device **302** also includes a clock **306** used to validate transactions, as will be discussed. The system of FIG. **4** also includes a merchant **418** who supplies products or services to the cardholder **416**, and who presents authorized charges to the bank **410** to be charged to the cardholder's credit card account.

[0047] As illustrated in FIG. **4**, the merchant **418** presents at **420**, a bill for goods or services to the card holder **416** which includes the amount to be paid by the card holder **416**. The cardholder **416** enters the amount to be paid into the computing device **302**. The computing device **302** then calculates the encrypted CVV code **114**. The computing device may use, for example, a combination of the PIN of the card holder, the time on the clock **306**, and the amount to be paid, and the static CVV code **112** to compute the coded CVV **114**. The CVV code **114** is then displayed by the computing device. The cardholder then presents **422** the merchant with the cardholder's credit card information and the CVV code **114**.

[0048] The merchant **418** then sends the credit card number of the cardholder **416**, the amount charged, and the coded CVV **114**, along with any other information needed to complete the transaction, to the bank **410** at **424**. The bank **410** receives the data sent by the merchant **418**, finds the account information for the credit card number in the database **414** for the card holder **416**, and using the PIN from the database **414** and the amount reported by the merchant at **424**, together with the transaction time and original static CVV number **112**, validates the coded CVV **114**. If the transaction is approved, an approval is sent from the bank to the merchant **418** as shown at **428**, and the transaction is complete.

[0049] The cell phone clock **306** and bank clock **413** will normally be synchronized by the network, however, slight drift may occur if the cell phone is out of range of the network or for other similar reasons. The clock synchronization can be accomplished by analyzing the merchant's dollar value each time the credit card protection device is used. The merchant's

price will be presumed to be accurate and legitimate, thus the time can be set by those values unless they are in conflict with computing device **302** by a larger margin than expected by the banks computer **412**. During this synchronization process, the bank's computer **412** will keep a history on each computing device **302** and its model number in order to best predict its time drift at its next use.

[0050] If the cardholder **416** should lose the computing device **302**, the cardholder will call the bank and the credit cards in the computing device **302** may be invalidated in the banks database **414**. The bank may further send a message to the computing device **302** and disable credit card functions on the computing device **302**.

[0051] If someone finds the lost computing device **302**, the finder or attempted fraudulent user will be unable to access the credit card account since they must have knowledge of the PIN, and that PIN must be entered into the computing device prior to its use and acceptance by the bank's computer **412**. After some number of failed attempts to fraudulently use the computing device **302**, the bank's computer **412** will temporary disable or flag the account in the bank's computer database **414** until the rightful owner calls to report a loss or correct a mistake. If someone tries to fraudulently use the computing device **302** it will give no indication to the user until the banks processing center rejects the purchase back to the merchant which will take time and alert the bank to a possible fraudulent attempt.

[0052] FIG. **5** illustrates the face of an exemplary computing device in accordance with the present invention. The computing device **302** is preferably a networked computing device and preferably a cell phone or equivalent device. In one embodiment of the invention, the method is coded into a program that may be downloaded to one or more types of cell phones. Thus, the specific look of the face would be that of the cell phone and the look of the face and operation of the buttons may be somewhat different from the given example, yet embodying the teachings herein. The computing device of FIG. **5** comprises an LCD screen **310**, a numeric keypad **502**, at least two function buttons: the DTK button **510** and the Code button **512**, and a fingerprint reader **318**. The LCD screen **310** is shown displaying the credit card information in both barcode **504** format and numeric format **506**, **508**. A first numeric line **506** shows the credit card number. A second numeric line **508** shows the expiration date and CVV code **114**. The barcode information **504** includes the credit card number, the expiration date, and the CVV code **114**. The CVV code **114** is preferably the time dependent coded CVV **114** in accordance with the present invention. A scroll function **516** may be used to scroll through several available credit cards to select the desired credit card. The numeric keypad **502** is used for entering a PIN to enable the device or a particular credit card, or to enter a transaction amount, or other information. The Code key **512** initiates the calculation of the CVV code **114**. The DTK key **510** is used to signify a duplicate transaction, i.e., the same transaction reentered because of some problem or fault. In a preferred embodiment, a fingerprint reader **318** may be used to enable the device or a particular credit card as an alternative to the PIN. Reading the fingerprint is quicker and simpler than keying in a PIN and does not require the cardholder to remember the PIN.

[0053] FIG. **6** illustrates a process for using the computing device of FIG. **5** to execute a credit card transaction. Referring to FIG. **6**, the cardholder first activates the credit card module **602**. Activation may be done by entering the PIN or by pressing the finger against the fingerprint reader **318**. In addition, the computing device **302** may have a special key or menu required to select a credit card mode among the many modes of the computing device **302**. The next step is to select the mode of transaction **604**, whether the transaction is a card not present transaction, or an over the counter transaction. A card not present transaction includes telephone or WEB purchases or other situations where the computing device is not available to be scanned by the merchant. Over the counter transactions include transactions where the merchant may scan the computing device screen with a barcode scanner.

[0054] If card not present transaction mode is selected, the next step is to select the credit card or transaction type **606**. The screen will normally display the default credit card and no action is required to accept the default card. If another card is desired, the scroll function may be used to scroll through the available cards to select the desired one **608**. Next, the transaction amount is entered **610**. The code key, or equivalent function, may be pressed to generate the coded CVV **114**, and the resulting coded CVV **114** and credit card information may be provided to the merchant **612**. Entering the transaction amount enables the computing device to include information for validation of the transaction amount in the coded CVV **114**.

[0055] FIG. **7** illustrates a process for using the computing device of FIG. **5** to execute an over the counter credit card transaction. Referring to FIG. **7**, the cardholder first activates the credit card module **602** as previously described for FIG. **6**. The computing device **302** then computes the coded CVV **114** and the cardholder then provides the results to the merchant **612**. Merchants with a terminal equipped to read the barcode may simply scan the barcode to receive all of the credit card information. The numeric information may be transcribed manually or used to check the automatic barcode results. Since the cardholder will get a sales receipt **704** verifying the transaction amount, the step of entering the transaction amount to validate the transaction amount through the bank may add insufficient value to be worth the effort, however this may be done simply by selecting the card not present mode.

Generating A Time Dependent Coded CVV Code

[0056] FIG. **8** shows an exemplary method for calculating an encrypted time dependent CVV code **114**. Other methods may be used for encrypting the CVV **114** as are known in the art of data encryption. The encrypted CVV codel **14** should not be easily decoded to produce an altered transaction or a fraudulent transaction. In accordance with the invention, the encrypted code value **114** should preferably be computed separately for each transaction so that the CVV code **114** cannot be reused successfully for a fraudulent transaction. One exemplary method of ensuring a change in CVV code **114** is to use a time value as part of the data or part of the process for encryption. A further method of improving security is to use a different set of code variables for each device. The code variables would be known only to the processing center so that only the processing center could validate the transaction. A further feature which may be included, where needed, is to encode or encrypt data such as the selling price to further validate the transaction, preventing changes along the communication path from the original sales clerk to the bank processing center.

[0057] Referring to FIG. **8**, the current time is converted to coded time values **802**. The cardholder's PIN is then com-

pared to the coded minutes **804** and the static CVV number **112** is compared to the coded hour value **806**. The first two comparison results are compared **808** and a table index value is determined **810**. The index is used to find an algorithm multiplier from a unique table **810**. The algorithm multiplier is used with the transaction dollar amount to derive a product **812**. Then the time, date, PIN, static CVV number **112** and product **812** are summed **814**. The result is the time dependent encrypted CVV code **114** to be given to the merchant **816** in place of the conventional static CVV number **112**.

[0058] The present method utilizes a coded, or encrypted, clock, which is now described.

[0059] FIG. **9**A and FIG. **9**B illustrate an exemplary coded clock in accordance with the present invention. The clock of FIGS. **9**A and **9**B may be used, for example, for the exemplary VISAS card type shown displayed in FIG. **1**A, FIG. **1**B, FIG. **2**, and FIG. **5**. Referring to FIG. **9**A, the set of circles **902**, **904** represents a minute table. The inner circle **904** shows the minutes in an hour and the outer circle **902** shows a code minute value assigned to each respective minute. The set of sixty values corresponding to sixty minutes is different for each cell phone device and the values programmed into the computing device is known also by the bank transaction center. The radials **906** shown illustrate several exemplary minute values and corresponding code minute values. For the example calculation, the time is eight minutes after the hour, which has a corresponding code minute value of 1163. A PIN value of 3815 is compared with the code minute value of 1163.

[0060] The second set of circles, FIG. **9**B, represents an hour table. The inner circle **910** shows the hours in a day and the outer circle **908** shows a code hour value assigned to each respective hour. The set of twenty four values corresponding to twenty four hours is different for each cell phone device and is known by the bank transaction center. The radials **912** shown illustrate several exemplary hour values and corresponding code hour values. For the example calculation, the time is twenty-one hours after midnight, which has a corresponding code hour value of 4352. A static CVV number of 718 is compared with the code hour value of 4352.

[0061] Further details of the coding process may be observed by following an example using the following exemplary data:

Static CVV 112 printed on card	718
Cardholders PIN	3815
Merchant's Price	$ 673.00
Year	06
Month	04
Day	25
Hour	21
Minute	08

[0062] First, the coded minute is found using the minute table of FIG. **9**A. For eight minutes past the hour, the coded minute table value is 1163. To compare the coded minute value and the card holders PIN, subtract the smaller value from the larger value to arrive at a positive result.

[0063] 3815 PIN

[0064] −1163 Coded Minute Value

[0065] 2652 First Result

[0066] Second, the coded hour value is found using the hour table of FIG. **9**B. For twenty-one hours, the coded hour value is 4352. The coded hour value is compared with the static CVV number **112** by subtracting the smaller value from the larger. Thus,

[0067] 4352 Coded hour value

[0068] −718 CVV number

[0069] 3634 Second Result

[0070] The results are then compared by subtracting the smaller from the larger,

[0071] 3634 First Result

[0072] −2652 Second Result

[0073] 982 Final Comparison

[0074] The index algorithm value is found from the final comparison by selecting the smallest and largest two digits in the final comparison and keeping the order of the two digits reading from left to right. The index algorithm in this example is 92. The index is used to select a multiplier from an index algorithm table.

[0075] Each cell phone device includes a unique index algorithm table of 99 entries. The table entries are known only by the card processing center. Each cell phone device has a different set of entries to produce a unique coded CVV **114** result for each different cell phone. The table entries may be loaded upon issue of the cell phone device or downloaded over the network as discussed above. Table 1 shows an exemplary table of multiplier entries. A partial listing of table entries is shown to indicate the general structure of the table and show entries actually used in the example. Referring to Table 1, the index ranges from 1 to 99. Each corresponding entry may be any number, but preferably a number between 0.01 and 1.0. For this example, entry **92** in the table is equal to 0.1028. The transaction amount is $673.00. Multiplying the transaction amount times the multiplier results in 673×0.1028=69. Only the dollar portion of the transaction amount is used in this calculation.

TABLE 1

Index	Multiplier
1	.0200
2	.0233
. . .	. . .
14	.0701
15	.0381
. . .	. . .
92	.1028
. . .	. . .
99	.0810

[0076] Now the data can be summed. Thus:

718	CVV number 112 printed on card
38	first two digits of cardholder's PIN
15	second two digits of cardholder's PIN
69	price × multiplier from Table 1, =673 × 0.1028
06	year
04	month
25	day
21	hour
+08	minute
904	sum result used as new encrypted CVV code given to merchant.

[0077] The date and time from a conventional Julian calendar/clock based on Universal Time (GMT) to make the time the same worldwide. If the sum result has more than the

number of digits in the CVV number **112** used by the respective credit card company, the left digits may be deleted to truncate the number to the proper number of digits.

[0078] The bank transaction center may reverse the calculations to validate the total price.

[0079] Thus, the total of

718	CVV number 112 printed on card
38	first two digits of cardholder's PIN
15	second two digits of cardholder's PIN
06	year
04	month
25	day
21	hour
+08	minute
835	sum

[0080] The sum may be subtracted from the time dependent CVV of 904:

904	Time dependent CVV
−835	Sum from above
69	Remainder

[0081] Using the time to determine the coded time values and index algorithm as above gives the multiplier times the merchant's reported transaction dollar amount:

$$0.1028 \times \$673.00 = 69,$$

which agrees with the remainder above and validates the transaction.

[0082] Thus described is a coding method that may produce a new encrypted CVV code **114** for each transaction to prevent the CVV code **114** from being copied and used by another party for a fraudulent transaction.

Other Transaction Types

[0083] FIG. **10** through FIGS. **19**A and **19**B illustrate different types of transactions involving different types of accounts. Each type of account provides a PIN number, or equivalent, and a static CVV number or equivalent, to the code generation process of FIG. **8**. Each account may have a different associated clock table for use with the code generation process.

[0084] FIG. **10** illustrates the computing device of FIG. **5** with an E*Trade transaction selected. Note that a specific E*Trade PIN may be required and a coded login code may be computed in place of the coded CVV **114**.

[0085] FIGS. **11**A and **111**B illustrate the code minute and code hour tables for the E*trade transaction of FIG. **10**. Note that the clock tables are unique for E*Trade. The clock tables may further be unique for each cardholder or computing device.

[0086] FIG. **12** illustrates the computing device of FIG. **5** with a Bank transaction selected.

[0087] FIGS. **13**A and **133**B illustrate the code minute and code hour tables for the bank transaction of FIG. **12**. Note that the clock tables are unique for the bank.

[0088] FIG. **14** illustrates the computing device of FIG. **5** with a Virtual Credit Card (VCC) transaction selected. The virtual credit card is a credit card that exists only as a software object and has no plastic embodiment. The VCC may have sixteen digits with the last four being zero to prevent its use except by cell phone device. The virtual credit card may be downloaded over the network and validated by phoning a special number, just as today's credit cards are validated. Billing will be by any desired method, typically by mail as presently used for plastic credit cards.

[0089] FIGS. **15**A and **15**B illustrate the code minute and code hour tables for the VCC transaction of FIG. **14**. Note that the clock tables are unique for the VCC.

[0090] FIG. **16** illustrates the computing device of FIG. **5** with an ATM (Automatic Teller Machine) transaction selected.

[0091] FIGS. **17**A and **17**B illustrate the code minute and code hour tables for the ATM transaction of FIG. **16**. Note that the clock tables are unique for the ATM. The clock tables may further be unique for each cardholder or computing device.

[0092] FIG. **18** illustrates the computing device of FIG. **5** with a subway fare transaction selected. The computing device has particular benefits for subway fares and other small transactions as further described in this disclosure.

[0093] FIGS. **19**A and **19**B illustrate the code minute and code hour tables for the subway fare transaction of FIG. **18**. Note that the clock tables are unique for the subway fare.

Small Purchases

[0094] In one embodiment of the invention, small transactions may be made instantaneously by postponing bank validation. Bank validation and account reconciliation may be delayed and performed in a batch, for example, once each day for all transactions occurring during the previous twenty-four hours. Other time intervals may be selected. Since the trasaction is a small amount, bank and merchant risk is limited, permitting faster transaction time by delaying the validation and account reconciliation. Using the time dependent CVV code **114** as disclosed herein, the merchant records the account time along with the card number and time dependent CVV to have sufficient information for the bank to validate the time dependent CVV **114** and transaction. The recording of all information may be automatic by the merchant's terminal. Fast transactions speed sales and handling of customers through lines at such establishments as fast food restaurants, subway turnstiles, tollbooths and others.

[0095] As a further limitation on risk, the cell phone terminal may limit small transactions to some number, for example, ten per day. The small transaction amount may be limited to some predetermined value, for example, twenty-five dollars. Other numbers or values may be set. The number and value may be set in accordance with the purchaser's FICO score and/or past payment history or other factors. Because the device is networked, preferably to a cell phone network, the small transaction feature and limits may be set dynamically at anytime by the bank equipment calling the cell phone to automatically set feature limits and/or to enable and disable the feature. Further, if the small transaction feature were disabled, the device may still permit normal transactions requiring validation for each purchase.

Two Readings

[0096] The present invention may further speed sales transactions by allowing two readings of the credit card information. For example, for a subway payment, the cell phone's

credit card module may be activated and scanned by a barcode reader upon first entering the subway terminal. This may be done while walking past. The reader will send the information for processing, which may take ten seconds. By the time the turnstile is reached, the account will have been verified and a second scanning of the barcode may authorize entry.

[0097] In a second example at a grocery store, the cell phone's barcode may be scanned just prior to unloading food items at the checkout. By the time checkout is completed, the card may be activated and the cashier may provide the sales receipt without delay.

[0098] In a third example at fast food restaurant, the barcode may be read at order entry and may be fully approved before order pickup.

[0099] In a further embodiment, the barcode may be read upon entering an establishment to authorize the credit card to a certain credit limit. Upon checkout the flatbed scanner will automatically complete the transaction by interfacing with the cell phone. This process may be better understood by the following example:

[0100] When the cardholder enters a convenience store and runs the activated cell phones display over a barcode reader the card details will be sent to banks transaction center for activation. By the time the cardholder has completed shopping, the bank's transaction center will have returned an authorization with a credit limit to the merchants POS (Point of Sale) system. When the cardholder arrives at the checkout counter, the flatbed barcode scanner will recognize the cell phone device by the barcode displayed and cause the POS terminal to beep or light up a LED to notify the attendant that the cardholder has been approved with the dollar amount available. The flat bed scanner may include a CCD (charge coupled device) for reading the barcode.

[0101] After the store attendant has completed ringing up the items, the dollar amount from that purchase will be credited to the merchant's account and debited from the cardholder's account.

[0102] The flatbed scanner will then output a barcode containing the total dollar amount and store name, which will be read by the cell phones camera. The cell phones software will update the database including the dollar amount remaining in the credit or debit account and the merchant's name. This will allow the cardholder to keep track of the account. The process would work the same way in other situations, for example, in the subway where there is no attendant.

Account Payment Using Barcode Information Exchange

[0103] FIG. **20** illustrates an exemplary system having a direct optical interface between the merchant equipment and the customer's computing device. Two way communications is accomplished by displaying barcodes on the customers computing device **302***a*, (e.g. cell phone) to be read by the merchant's barcode scanner **418** and by displaying barcodes at the scanner to be viewed by the customer's cell phone camera. Referring to FIG. **20**, the merchant's terminal **418** includes a display that can display **2002** a barcode to the cell phone's camera in addition to the scanning mechanism that can read **2004** a barcode from an item to be purchased. The cell phone includes software that can analyze the camera image and decode the barcode. Thus, the scanner and cell phone can communicate in both directions **2002** and **2004** using barcode displays and readers in each corresponding device. This capability gives rise to several beneficial account processes.

[0104] In one embodiment, the cell phone **302***a* may communicate through the cell phone network **316** to a financial institution **410**, e.g., a bank, to establish an account. Account particulars may be stored in the cell phone **302***a*. In one embodiment, funds may be electronically transferred to the cell phone **302***a* by allocating funds at the bank **410** and storing the allocated amount in the cell phone **302***a*. At the merchant's location, the cell phone **302***a* may be used like a credit card or shopping card, except that instead of running the card through the card scanner, the cell phone **302***a* is placed on the merchant's adapted barcode scanner **418**. The merchant's scanner can read account information from the cell phone **302***a* and can then communicate with the bank **410**, as needed for authorization. In the case where funds are transferred to the cell phone, authorization from the bank would be unnecessary. When a purchase is made, the purchase price is subtracted from the cell phone's account in cell phone memory and a corresponding debit is generated by the merchant's terminal for a corresponding account at the customer's bank. As a further feature, the merchant's scanner can utilize security information collected by the cell phone, such as a PIN or password or fingerprint matching information, to further secure the transaction. Depending on established policies, the merchant's equipment may dispense with the need for further signatures by the purchaser based on fingerprint or other positive ID information collected by the cell phone.

[0105] In one embodiment, positive identification of the customer, such as by fingerprint matching, may enable customer age information to be conveyed to the merchant for age dependent purchases, such as for beer or cigarettes, or for senior discounts—potentially enabling self checkout of these items.

[0106] FIG. **21**A and FIG. **21**B illustrate two views of an exemplary barcode scanner including a barcode generator in accordance with the present invention. FIG. **21**A shows a side view and FIG. **21**B shows a front view. Referring to FIG. **21**A and FIG. **21**B, the barcode scanner **418** comprises a window **2106** and a scanning mechanism **2102** to scan barcodes. The scanning mechanism **2102** typically scans barcodes from merchandise placed on the window **2106**. The dotted lines represent the field of view of the scanning mechanism **2102** viewing the scanner window **2106**. The scanner of FIG. **21**A is shown scanning a cell phone **302***a* placed on the window **2106**. The cell phone **302***a* produces a barcode display on the cell phone display that is encoded with account information needed for the transaction. The merchant equipment **418** also includes a display **2104** which may display a barcode encoded with transaction amount, vendor name, and other information as needed or desired for the transaction. The merchant display **2104** may be read by the cell phone **302***a* using the cell phone camera to generate an electronic receipt or for debiting account balances in the cell phone memory, and/or recording transaction details. Dotted lines are also shown to indicate the field of view of the cell phone **302***a* camera reading the merchant display **2104**.

[0107] FIG. **21**A and FIG. **21**B show a single scan mechanism and a single window for scanning both the cell phone **302***a* and merchandise; however an alternative embodiment may dedicate a station for cell phone interface and a separate station for merchandise.

[0108] FIG. **22** illustrates an exemplary cell phone in accordance with the present invention. Referring to FIG. **22**, cell phone **302***a* includes the features of cell phone **302** of FIG. **3** with the addition of a camera **2202**. The cell phone **302***a* is

further adapted for account transactions by including software to read barcodes using the camera. The cell phone can generate barcodes for the display **310**. The display **310** is typically the same display used for normal cell phone applications. The software may also manage account information in memory **308** and may include necessary encryption technology to protect the account information. The software may also interface with the fingerprint reader **318** and/or keypad **312** for PIN numbers or passwords for positive user identification. It may be necessary to utilize a sequence of successive barcodes to accomplish the full communication where a single barcode is insufficient. It may be appreciated that many barcode standards are available which may be used with this invention. Standards include one dimensional and two dimensional barcodes, where information is encoded spatially along one or two dimensions. Any suitable barcode may be used. The cell phone **302***a* may utilize the cell phone network **316** for communication with the bank **410** to establish or replenish accounts, for viewing account status, or other account maintenance activities.

[0109] The invention is well suited for application to self checkout counters at grocery stores. The customer arrives at the checkout counter with one or more items. The customer then activates the mobile payment application in the cell phone **302***a*. The customer may then select the small payments option to use funds stored within the cell phone **302***a*, i.e., funds for which a funds available amount is maintained within the cell phone **302***a*. The customer then places the cell phone **302***a* on the stationary barcode reader **418**, where the account number and account details, including funds available may be read. Each item is then run over the merchandise barcode scanner **2102** to get item and price information. As each item is scanned, the funds are immediately transferred from the cell phone **302***a* and the cell phone account is updated by sending item and price information to the cell phone **302***a* through the merchant display **2104** to cell phone camera **2202** information path **2002**. This allows the customer to purchase a single item and walk out without delay. Additional items may be purchased, as long as the cell phone **302***a* is left on the scanner, **418** by simply continuing to scan items. When completed, the cell phone **302***a* is removed, and a merchant's supervisor station, if present, may be automatically notified that all items are paid for. The cell phone database and account information are now current.

[0110] In one embodiment, funds may be added to the account in the cell phone at the merchant location. The customer may pay cash or other acceptable funds to the merchant for the merchant to credit the funds to the cell phone account. The merchant equipment **418** reads the account number from the cell phone display **310** and sends the amount to the cell phone **302***a* using the merchant display **2104**. The cell phone **302***a* receives the amount by reading the barcode on the merchant display **2104** using the cell phone camera **2202** and updates the available amount in the cell phone memory **308**. The merchant terminal **418** may also send a copy of the transaction to the bank **410** associated with the account. The cell phone account may be established in one of two modes. One where the funds are an allocation of funds in a bank account. Another, where the funds are effectively in the cell phone with no corresponding bank account.

[0111] Alternatively, the customer may select credit card payment. In this scenario, the customer arrives, as before, with items to be purchased. The customer may scan all items and obtain a total for the sale. The customer then activates the mobile payment application in the cell phone **302***a* and then selects the credit card or VCC to be used and places the cell phone **302***a* on the barcode reader **418**. The merchant's POS system **418** then scans the cell phone barcode information on the cell phone display **310** to obtain the credit card number and sends the number to the bank **410** for authorization. A typical credit card number includes bank **410** identification. When authorization is received, the POS system **418** will send the transaction details to the cell phone **302***a* by displaying barcode information to the cell phone camera **2202**. The cell phone camera **2202** reads the barcode information and records the sale information in cell phone memory, updating any account information as necessary. The cell phone **302***a* may also respond by presenting receipt confirmation information as barcode information on the cell phone display **310** to be read by the merchant scanner **418**, thus completing the sale communications. The merchant system **418** may then beep, alerting the customer that the sale has been approved and completed. The customer may then remove the cell phone **302***a*. The cell phone **302***a* now contains the transaction amount, merchant date/time and item information.

CONCLUSION

[0112] The capabilities of the present invention can be implemented in software, firmware, hardware or some combination thereof. As one example, one or more aspects of the present invention can be included in an article of manufacture (e.g., one or more computer program products) having, for instance, computer usable media. The media has embodied therein, for instance, computer readable program code means for providing and facilitating the capabilities of the present invention. The article of manufacture can be included as a part of a computer system or sold separately. Additionally, at least one program storage device readable by a machine, tangibly embodying at least one progmm of instructions executable by the machine to perform the capabilities of the present invention can be provided.

[0113] The flow diagrams depicted herein are exemplary. There may be many variations to these diagrams or the steps (or operations) described therein without departing from the spirit of the invention. For instance, the steps may be performed in a differing order, or steps may be added, deleted or modified. All of these variations are considered a part of the claimed invention.

[0114] While particular embodiments of the invention have been described, it will be understood, however, that the invention is not limited thereto, since modifications may be made by those skilled in the art, particularly in light of the foregoing teachings. It is, therefore, contemplated by the appended claims to cover any such modifications that incorporate those features or those improvements that embody the spirit and scope of the present invention.

What is claimed is:

1. A system for generating a sales transaction comprising:

a merchant terminal for communicating with a customer computing device, said merchant terminal comprising:

an optical scanner, said optical scanner directed to said customer computing device for reading information displayed thereon; and

a merchant display device for displaying a first optically readable pattern, said optically readable pattern having merchant transaction information encoded thereon;

said customer computing device comprising:

a customer display device for displaying a second optically readable pattern, said second optically readable pattern having customer transaction information encoded thereon; and

an optical camera for reading said merchant transaction information from said merchant display device;

wherein said optical scanner reads customer account information from said customer display device, said merchant terminal communicates with a financial institution associated with said customer account information to obtain approval for said transaction; said merchant terminal displaying transaction receipt information on said merchant display device; said optical camera reading said transaction receipt information from said merchant display device.

2. The system of claim **1**, wherein said first optically readable pattern is a barcode.

3. The system of claim **1**, wherein said second optically readable pattern is a barcode.

4. The system of claim **1**, wherein said customer computing device is a cell phone.

5. The system of claim **1**, wherein said optical scanner also scans a barcode from an item of merchandise.

6. The system of claim **1**, wherein said customer computing device communicates with said financial institution to electronically store funds in said customer computing device.

7. The system of claim **1**, wherein said customer computing device further includes a fingerprint reader and fingerprint matching information is conveyed to said optical scanner using said customer display device.

8. The system of claim **1**, wherein said customer computing device further includes a fingerprint reader for positive user identification and after positive user identification is achieved, user age information is conveyed to said optical scanner using said customer display device.

9. A system for generating a sales transaction between a customer and a merchant comprising:

a merchant terminal for communicating with a customer computing device, said merchant terminal comprising:

a first optical scanner for scanning a barcode on an article of merchandise;

said merchant terminal generating a transaction price based on said scanning said barcode on said article of merchandise;

a second optical scanner, said optical scanner directed to said customer computing device for reading information displayed thereon; and

a merchant display device for displaying a first optically readable pattern, said first optically readable pattern having merchant transaction information encoded thereon;

said customer computing device comprising:

a customer display device for displaying a second optically readable pattern, said second optically readable pattern having customer transaction information encoded thereon; and

an optical camera for reading said merchant transaction information from said merchant display device;

a memory device for storing an account number and an amount of funds available, said customer computing device communicating over a cell phone network with a financial institution to allocate said amount of funds available;

wherein the second optical scanner reads said account number and said amount of funds available from said customer computing device;

said customer computing device reads said transaction amount from said merchant display device and subtracts said transaction amount from said amount of funds available;

said merchant terminal sends a debit note to a customer bank for payment to the merchant for the transaction amount from an account designated by the account number.

wherein said customer computing device stores an allocated fund amount in said customer computing device; said second optical scanner reads said account information from said customer display; said merchant terminal displays transaction information on said merchant display, said optical camera reads said transaction receipt information from said merchant display.

10. The system of claim **9**, wherein said first optically readable pattern is a barcode.

11. The system of claim **9**, wherein said second optically readable pattern is a barcode.

12. The system of claim **9**, wherein said customer computing device is a cell phone.

13. The system of claim **9**, wherein said first optical scanner and said second optical scanner comprise the same optical scanner.

14. The system of claim **9**, wherein said customer computing device communicates with said financial institution to electronically store funds in said customer computing device.

15. The system of claim **9**, wherein said customer computing device further includes a fingerprint reader and fingerprint matching information is conveyed to said merchant terminal using said customer display device.

16. The system of claim **9**, wherein said customer computing device further includes a fingerprint reader for positive user identification and after positive user identification is achieved, user age information is conveyed to said merchant terminal using said customer display device.

17. A method for purchasing an article of merchandise by a customer of a merchant comprising:

obtaining article information including price information based on barcode scanning of said article;

generating a transaction price based on said price information;

generating a first optically readable pattern on a display of a customer computing device, said optically readable pattern having customer account information encoded thereon;

said account information including account number and funds available as stored in said customer computing device;

reading said first optically readable pattern by a merchant optical scanner and decoding said customer account information;

generating a second optically readable pattern on a display associated with said merchant optical scanner, said second optically readable pattern having said transaction price encoded thereon;

reading said second optically readable pattern by said customer computing device and decoding said transaction price from said second optically readable pattern;

deducting said transaction price from said funds available as stored in said customer computing device;

generating a debit note for payment to said merchant by said account number directed to a bank associated with said account number.

18. The method of claim **17**, further including the step of:

repeating the steps of claim **17** for an additional item of merchandise.

19. The method of claim **17**, further including the step of:

adding additional funds to said finds available as stored in said customer computing device, said step of adding additional finds to said finds available comprising the steps of:

generating a third optically readable pattern on said display associated with said merchant optical scanner, said third optically readable pattern having said additional funds encoded thereon;

reading said third optically readable pattern by said customer computing device and decoding said funds available from said third optically readable pattern; and

updating said funds available by adding said additional funds as decoded from said third optically readable pattern.

* * * * *