for example, a user may enjoy a higher degree of integration such that a user may customize a level of detail provided on a receipt via mobile wallet 2802.

[0287] A payment receipt may, for example, be provided to mobile wallet 2802 as a proof-of-purchase object (e.g., a barcode) that may be provided to a display of mobile wallet 2802 and read by other computing equipment (e.g., a barcode scanner) for proof-of-purchase confirmation.

[0288] A mobile wallet (e.g., mobile wallet 2824) may, for example, include a contactless communication device (e.g., an RFID) that may initiate, sustain, and/or terminate contactless communication channel 228 with merchant terminal 2818. Accordingly, for example, mobile wallet 2824 may communicate payment information to merchant terminal 2818 to complete a financial transaction. In so doing, for example, mobile wallet 2824 may first receive payment information via a contactless communication channel from one or more contactless devices (e.g., a non-powered card), store the received payment information within a memory of mobile wallet 2824, and forward the payment information onto merchant terminal 2818 to complete a financial transaction. Accordingly, for example, payment information may be recalled from memory within mobile wallet 2824, optionally authenticated and authorized by a user of mobile wallet 2824 and communicated to merchant terminal 2818 via contactless communication channel 2828 to complete a financial transaction using merchant terminal 2818. An electronic receipt may, for example, be generated by merchant terminal 2818 and communicated to mobile wallet 2824 via contactless communication channel 2828.

GOOGLE EXHIBIT 1073 (Part 2 of 3)
Google LLC v. Cardware Inc.
IPR2025-01514

[0289] FIG. 29 shows system 2900, which may include mobile wallet 2902 and payment card 2904. Mobile wallet 2902 may, for example, be a laptop computer, a PDA, a mobile telephonic device (e.g., a smartphone), an MP3 player, a GPS, or any other mobile device. Display 2908 may be a touch-sensitive display (e.g., sensitive to a change in capacitance). Payment card 2904 may, for example, be a powered payment card or a non-powered payment card.

[0290] Mobile wallet 2902 and payment card 2904 may each include a contactless communication device (e.g., RFID) that may communicate via a contactless communication channel that may be formed between mobile wallet 2902 and payment card 2904 after coming into proximity to one another. Payment card 2904 may, for example, be tapped onto display 2908 of mobile wallet 2902 to establish a proximity relationship that forms a communication channel between payment card 2904 and mobile wallet 2902. As per another example, payment card 2904 may be brought within a proximity distance (e.g., up to two inches) of mobile wallet 2902 to establish a contactless communication channel between mobile wallet 2902 and payment card 2904.

[0291] A processor of mobile wallet 2902 may, for example, execute application code that may generate a graphical user interface (GUI) onto display 2908 of mobile wallet 2902. Message 2906 of such a GUI may invite a user of mobile wallet 2902 to begin storage of card information (e.g., payment card information) by tapping one or more cards (e.g., one or more payment cards) against display 2908. As per another example, by tapping a card (e.g., payment card 2904) against mobile wallet 2902, a processor of mobile wallet 2902

may autonomously determine that card information associated with the tapped card is to be stored within a memory of mobile wallet 2902 and a processor of mobile wallet 2902 may then generate a mobile wallet GUI onto display 2908 to autonomously download the card information and engage a user of mobile wallet 2902 to administer any other activities that may be associated with such an information download.

[0292] A processor of mobile wallet 2902 may, for example, autonomously determine a type of card that may be tapped against it. For example, a processor of mobile wallet 2902 may receive payment card data that may be indicative of a non-powered payment card (e.g., payment card data received from a non-powered card may not provide a security code associated with the card). As per another example, a processor of mobile wallet 2902 may receive data that may be indicative of a powered card (e.g., payment card data received may contain a dynamically generated security code). Payment card data received from a powered card may, for example, include a dynamic security code that may change depending upon a type of transaction being conducted (e.g., debit or credit transaction).

[0293] As per another example, payment card 2904 may be a powered payment card that may include electronics to simulate a human touch (e.g., payment card 2904 may generate a change in capacitance that may be sensed by display 2908). Through a series of simulated touches, payment card 2904 may communicate a series of data bits to display 2908, which may then be processed by a processor of mobile wallet 2902. In so doing, for example, a contactless communication channel may be established where data is transferred from payment card

2904 to mobile wallet 2902 via a series of simulated touches.

[0294] Payment card 2904 may, for example, include a light sensor. Accordingly, for example, payment card 2904 may be sensitive to light pulses generated within a region of display 2908. The light sensor of payment card 2904 may receive a series of light pulses, which may be construed by a processor of payment card 2904 as data generated by mobile wallet 2902. In so doing, for example, payment card 2904 may receive an optical data stream represented by a series of light pulses generated by display 2908. As such, a two-way communication channel may be formed, where simulated touches may generate a data stream from payment card 2904 to mobile wallet 2902 and light pulses may generate a data stream from mobile device 2902 to payment card 2904.

[0295] FIG. 30 shows GUI 3000, that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 3000 may, for example, provide a summary information screen that provides virtual card 3002 and associated identifying information. Virtual card 3002, for example, may be a virtual representation of a physical card that may have been tapped against a display of a mobile device to form a contactless communication channel between the physical card and a mobile device.

[0296] Card (e.g., payment card) information (e.g., track 1 and track 2 magnetic stripe data) may be communicated to the mobile device via a contactless communication channel and such information may be displayed within virtual card 3002 as summary information that may be associated with the physical

payment card. A payment card number communicated to a mobile device within a magnetic stripe message may, for example, include issuer identification as well as an issuing network identifier. Accordingly, for example, a processor of a mobile device may analyze the payment card number received from a physical payment card and may render a portion or all of the identifying information associated with the payment card number onto virtual card 3002. In so doing, for example, issuer identification 3004 as well as a logo representative of an issuing network identifier may be rendered onto virtual card 3002. Additionally, a portion or all of payment card number 3006 as well as cardholder's information (e.g., cardholder's name 3008) may be rendered onto virtual card 3002.

[0297] A portion or all of the card information received from a physical card may be stored within a memory of a mobile device. Alternately, for example, a portion or all of the card information received from a physical card may be collected by a mobile device and communicated by the mobile device to a remote server for storage and/or validation purposes. In so doing, for example, instead of storing payment card information within a memory of a mobile device, card identification 3010 may, for example, be stored within a mobile device and used as an index identifier to look up payment information that may be stored within a remote server. A processor of a mobile device may generate card identification 3010 and may display card identification 3010 within an alphanumeric entry box. In so doing, for example, a user of a mobile device may either accept, or change, card identification 3010 to a value that may later be used to remind the user of

which physical payment card is associated with card identification 3010 and to recall payment information associated with card identification 3010 that may be remotely stored.

[0298] FIG. 31 shows GUI 3100, that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 3100 may, for example, include a bank card validation screen as may be generated by a processor of a mobile device. GUI 3100 may, for example, challenge a user of the mobile device to enter a PIN that may be associated with a payment card (e.g., VISA credit 3102) that was previously presented to the mobile device so that payment information may be uploaded from the payment card to the mobile device via a contactless communication channel generated between the payment card and the mobile device. GUI 3100 may, for example, generate virtual pin pad 3106 that may include touch-sensitive buttons having alphanumeric indicia associated with each button. A user may touch one or more buttons of pin pad 3106 that may correspond to respective characters of a PIN and an indication of the user's selection may appear within area 3104. Characters displayed within area 3104 may, for example, be hidden for security purposes.

[0299] Activation of virtual button 3108 may, for example, cause a processor of a mobile device to compare a PIN entered by a user of the mobile device to a PIN that may be associated with the payment card presented to the mobile device for storage. The PIN may, for example, be stored within protected memory of the mobile device, so that a processor of the mobile device may locally determine the validity of the PIN

entered. Alternately, for example, the mobile device may communicate the PIN to, for example, the issuing bank for a remote validation of the PIN entered. Persons skilled in the art will appreciate that a user interface (e.g., a keypad or keyboard) of a mobile device may be used instead of virtual pin pad 3106 to enter the one or more characters of a PIN.

[0300] Upon validation that the correct PIN was entered, virtual card 3110 may be displayed. In particular, for example, account number 3112 may be fully populated within virtual card 3110 to indicate to a user of the mobile device that the PIN was correctly entered and to allow the user to compare account number 3112 against an account number printed on the physical payment card of which virtual card 3110 is a representation. Persons skilled in the art will appreciate that virtual payment cards may be stored within a mobile wallet without first requiring a user to validate the payment card using a PIN entry. An alternate form of validation (e.g., a security code) may, for example, be required for validation. As per another example, no validation may be required to store a virtual payment card onto a mobile wallet.

[0301] FIG. 32 shows system 3200, which may include mobile wallet 3202 and card 3206. Card 3206 may, for example, be a powered card (e.g., a powered payment card). Accordingly, for example, card 3206 may include a processor, display 3212, a battery, manual input interfaces (e.g., buttons 3208 and 3210) and other electronic components (e.g., a light source, a light sensor and a touch simulator). A user of powered card 3206 may, for example, interact with card 3206 to

select the information that may be communicated to mobile wallet 3202 from card 3206.

[0302] A user may, for example, press button 3208 and then tap card 3206 against display 3204 of mobile wallet 3202 to generate a contactless communication channel (an RFID communication channel) between card 3206 and mobile wallet 3202. Accordingly, for example, card 3206 may communicate payment information (e.g., one, two and/or three tracks of magnetic stripe data) that may be associated with a feature selected by pressing button 3208. In so doing, for example, card 3206 may communicate information (e.g., within a discretionary data field) associated with a selected feature (e.g., a VISA debit payment feature).

[0303] FIG. 33 shows GUI 3300, that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 3300 may, for example, include a bank card validation screen as may be generated by a processor of a mobile device. GUI 3300 may, for example, render virtual card 3310 so that a user of the mobile device may compare information 3312 and 3314 to information that the user intended to communicate to the mobile device.

[0304] Accordingly, for example, a user may have pressed a button on a powered payment card associated with a debit pay feature and may have communicated the debit pay feature (e.g., within a discretionary data field of a magnetic stripe message) to a mobile device via a contactless communication channel that may have been created between the powered payment card and the mobile device. In so doing, for example, a processor of a mobile device may analyze the debit pay feature received from the powered payment card and may render

an indication (e.g., "Pay Now" identifier 3314) onto virtual card 3310 to indicate that virtual payment card 3310 has been stored within the mobile device such that when used by a user of the mobile device to complete a payment transaction, authorizes an immediate deduction of funds from the user's payment account. Alphanumeric entry box 3316 may, for example, allow the user to tag stored virtual card 3310 with a card identifier that reminds the user of the debit functionality associated with virtual card 3310.

[0305] FIG. 34 shows GUI 3400, that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 3400 may, for example, render virtual card 3410 to allow a user to verify information previously communicated to a mobile device via a contactless communication channel that may be generated between a powered payment card and the mobile device. A user of a mobile device may, for example, press a button on a powered payment card that may be associated with a credit pay feature and may communicate the credit pay feature along with other payment information (e.g., payment account number 3412 and expiration date) via a contactless communication channel to the mobile device.

[0306] A processor of a mobile device may, for example, analyze information received from a powered payment card (e.g., information received via a discretionary data field) and may determine that payment information received from the powered payment card may be associated with a credit feature (e.g., "Pay Later" feature 3414). Accordingly, for example, a processor of a mobile device may use identifier 3414 of

virtual card 3410 to signify such a credit payment feature.

[0307] Virtual card identifier 3416 may, for example, be an editable card identifier to allow a user of a mobile device to store and recall virtual card 3410 to/from a memory of a mobile device. Card identifier 3416 may, for example, be used by a mobile device to access virtual card 3410 from a remote location (e.g., a remote server) such that the mobile device need not store sensitive information that may be associated with virtual card 3410 within the mobile device.

[0308] GUI 3400 may, for example, allow an additional card to be associated with virtual card 3410. A rewards card may, for example, be associated with a credit account that may be associated with virtual card 3410. Accordingly, for example, rewards card information may be communicated to a mobile device by tapping the rewards card against portion 3418 to generate a contactless communication channel (e.g., an RFID communication channel) between the rewards card and the mobile device. As per another example, an identification card (e.g., a driver's license) may be associated with virtual card 3410. Accordingly, for example, identifying information (e.g., date of birth and a picture) associated with the holder of the identification card may be communicated to a mobile device and stored within the mobile device. In so doing, for example, stored identification information may be recalled from a memory of the mobile device to provide authentication information while completing a purchase transaction using the mobile device.

[0309] A user may, for example, select option 3420 to allow card information to be scanned into a mobile device using a scanning device (e.g., a camera) of the mobile device. Accordingly, for example, a card (e.g., a driver's license) may be scanned into a mobile device by selecting radio button 3420 and holding the driver's license in front of the mobile device while a snapshot of the driver's license is taken by a camera of the mobile device and stored in a memory location of the mobile device. A mobile device may alternately, for example, access identifying information (e.g., name, address, phone number, and picture) from a database (e.g., a motor vehicle database) that may be accessible from a network. Such information may be rendered onto a virtual identification card (e.g., a driver's license) that may be stored within a mobile device. In so doing, for example, user identification data may be recalled from a memory of a mobile device and rendered onto a display of the mobile device, so that a merchant may verify the validity of the user identification data when virtual card 3410 is used to complete a purchase transaction in the presence of the merchant.

[0310] Card information may be communicated via programming portion 3422. A powered card may, for example, provide touch simulation electronics and a light sensor such that when the powered card is placed against portion 3422, a two-way contactless communication channel may be created. Accordingly, for example, information may be communicated from the powered card to the mobile device through a series of touch simulations generated by the powered card and sensed by a portion within portion 3422 that is touch sensitive. In so doing, for example, a processor of a

mobile device may construe a series of touch simulations as a series of data bits communicated by a powered card that may be indicative of information associated with the powered card. GUI 3400 may, for example, provide a series of light pulses within portion 3422 that may be received by a light sensor of the powered card and construed by a processor of the powered card as data communicated by the mobile device.

[0311] FIG. 35 shows GUI 3500 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 3500 may, for example, include upload area 3502 as generated by a processor of a mobile device. Upload area 3502 may, for example, include one or more data exchange areas (e.g., data exchange areas 3504 and 3506). Icon 3504 may, for example, be generated by GUI 3500 within an area of a display of a mobile device that may be sensitive to touch (e.g., an area that may be sensitive to a capacitance change). Area 3506 may, for example, be generated by GUI 3500 within an area of a display of a mobile device that may generate pulses of light.

[0312] Information associated with a powered payment card may be uploaded for use by a mobile device by exchanging data with the powered payment card via data exchange areas 3504 and 3506. For example, a powered payment card may be pressed against upload area 3502 so that a touch simulation device of the powered payment card aligns with data exchange area 3504 and a light sensing device of the powered payment card aligns with data exchange area 3506. Accordingly, for example, the powered payment card may communicate information to a processor of a mobile device by simulating a series of touches in data exchange area 3504 and data may be

communicated to the powered payment card by a processor of the mobile device by generating a series of light pulses in data exchange area 3506. In so doing, for example, a mobile device and a powered payment card may exchange information so that payment card information may be stored within the mobile device.

[0313] Once payment card information is uploaded into a mobile device, GUI 3500 of the mobile device may display a summary of the uploaded information in validation area 3510. Accordingly, for example, one, two or three tracks of magnetic stripe information may be uploaded from a payment card into a mobile device via data exchange area 3504 of upload area 3502. A portion or all of the uploaded data may, for example, be rendered within validation area 3510, so that a user of the mobile device may validate that the correct payment card information was uploaded and stored within the mobile device.

[0314] FIG. 36 shows GUI 3600 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 3600 may, for example, render virtual card 3610 and may display a portion of information that may be associated with virtual card 3610. Accordingly, for example, a payment card (e.g., a gift card) may be brought within a proximity or touch relationship with a mobile device such that a contactless communication channel may be generated between the payment card and the mobile device. In so doing, for example, payment account information may be communicated from the payment card to the mobile device and a portion or all of the payment card information may be rendered onto virtual card 3610.

[0315] A user of a mobile device may, for example, customize a visual appearance of virtual card 3610 by utilizing any number of graphical user interface objects (e.g., list 3604 and alphanumeric input box 3612) that may be rendered by GUI 3600. A user may, for example, drag-and-drop logos from list 3604 onto virtual card 3610 to more clearly identify virtual card 3610. Accordingly, for example, a user may identify virtual card 3610 as a gift card (e.g., a Walmart gift card), using drag-and-drop operation 3608, having a particular network brand (e.g., a VISA network brand), using drag-and-drop operation 3606. A user may, for example, annotate virtual card 3610 using alphanumeric input box 3612 with any identifying information that may be useful to the user (e.g., information that may be used to recall virtual card 3610 from a memory of a mobile device).

[0316] A mobile device may, for example, disallow certain customizations that may conflict with virtual card 3610. Accordingly, for example, a mobile device may prevent a user from applying a different network logo than was previously communicated by a physical card to the mobile device. In so doing, for example, a mobile device may prevent a user from customizing virtual card 3610 as, for example, a M/C network brand, when a payment card number previously communicated from a payment card to a mobile device indicated that the payment card was, for example, a payment card having a VISA network brand.

[0317] A credit balance, for example, may be communicated by a gift card to a mobile device via a contactless communication channel generated between the gift card and the mobile device and may be displayed as

account balance 3614 to represent an amount of credit that may be remaining on virtual card 3614. Virtual card 3610 may, for example, be used by a mobile device to complete a purchase transaction in which payment card information associated with virtual card 3610 may be communicated to a merchant terminal (e.g., communicated via an RFID communication channel) and an amount of the purchase may be communicated from the merchant terminal to the mobile device. Accordingly, for example, account balance 3614 may be updated (e.g., reduced) by the amount of the purchase and displayed so that a user of the mobile device may be updated as to an amount of credit remaining on virtual card 3610.

[0318] A user of a mobile device may, for example, purchase additional credit to be added to virtual card 3610. Accordingly, for example, account balance 3614 may be updated (e.g., increased) when an amount of credit is added to virtual card 3610. In so doing, for example, an amount of credit added to virtual card 3610 may be communicated (e.g., communicated via an RFID communication channel) to a mobile device by a merchant terminal and updated via account balance 3614 so that a user of the mobile device may receive up-to-date information relating to a credit balance that may be available on virtual card 3610. As per an example, a user may recall a virtual payment card from a memory of a mobile device, activate the payment card for use, and use the mobile device to purchase additional credit on virtual card 3610 using the activated payment card as the payment vehicle.

[0319] FIG. 37 shows GUI 3700 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 3700 may, for

example, provide a visual representation of all virtual cards that may be stored within a memory of a mobile device (or within a remote server) and may display each virtual card within one or more categories that may be associated with each virtual card. A processor of a mobile device may, for example, analyze information received from a physical card via a contactless communication channel (e.g., an RFID, electromagnetic, visible, audible, capacitive, or magnetic communication channel) to determine a card category that may be associated with the corresponding virtual card.

[0320] An account number may, for example, be communicated by a card to a processor of a mobile device that may identify the card as a particular card type (e.g., bank card, rewards card, identification card, healthcare card, travel card or airline card). Accordingly, for example, each virtual card stored within a memory of a mobile device may be assigned a category index by a processor of the mobile device and may then be rendered onto GUI 3700 in accordance with the category index assigned. As per another example, a user of a mobile device may assign a category index (e.g., card identification) to a virtual card after information associated with a corresponding physical card is communicated to the mobile device via a contactless communication channel.

[0321] One or more payment cards, for example, may be rendered onto GUI 3700 and each payment card may be aligned within category 3706. An ordering of each payment card in category 3706 may, for example, be established by a user of a mobile device via sort options 3702. A mobile device may, for example, maintain statistics (e.g., number of times each virtual

payment card is recalled from a memory of a mobile device and used to complete a purchase transaction via the mobile device). Accordingly, for example, upon selection of one of sort options 3702 (e.g., Most used), a processor of a mobile device may recall usage statistics that may be associated with each virtual payment card stored within a memory of a mobile device and may display each virtual payment card within category 3706 onto GUI 3700 in accordance with such usage statistics (e.g., the top virtual payment card displayed within category 3706 may have the most usages of all virtual payment cards stored within a memory of the mobile device).

[0322] A mobile device may, for example, maintain other information associated with virtual payment cards of category 3706. Accordingly, for example, a mobile device may access network devices (e.g., issuer servers) associated with each virtual payment card stored within the mobile device. In so doing, for example, a mobile device may collect information (e.g., credit limit and credit available) associated with each virtual payment card stored within a memory of the mobile device and may display each virtual payment card on GUI 3700 in accordance with sort options 3702 (e.g., the top card displayed within category 3706 may have the highest credit limit or may have the most credit available).

[0323] Category 3708 may, for example, be associated with all virtual gift cards that may be stored within a memory of a mobile device (or remote server). Information associated with each virtual gift card may, for example, include a merchant identifier, a merchant type identifier, and an amount of credit available.

Accordingly, for example, a user may select one of sort options 3704 (e.g., Most credit available) to display a list of virtual gift cards within category 3708 in a descending order, where the top virtual gift card of category 3708 may have the highest credit available.

[0324] A mobile device may, for example, be a locating device (e.g., a GPS) or may, for example, include location determination electronics. Accordingly, for example, a mobile device may determine its own location and may determine whether its location corresponds with a location of a merchant's place of business that may be associated with a virtual gift card of category 3708. In so doing, for example, a mobile device may determine that its location is within a Walmart store and if, for example, sort options 3704 is selected to "Location", then a processor of the mobile device may re-order the virtual gift cards of category 3706 such that a Walmart virtual gift card is displayed as the top card in the stack. Accordingly, for example, the Walmart virtual gift card may be conveniently located within GUI 3700 for selection by a user of a mobile device to use during a purchase transaction conducted between a contactless communication channel formed between the mobile device and a merchant terminal at the Walmart store.

[0325] Virtual cards may, for example, be autonomously sorted across categories depending upon a virtual card placement that may exist in a particular category. A virtual payment card may, for example, be selected to occupy a top card placement within category 3706. A virtual rewards card may, for example, be associated with the virtual payment card selected for top placement in category 3706. Accordingly, for

example, the associated virtual rewards card may be selected for top placement within category 3708 based upon its association with the virtual payment card selected for top placement within category 3706. As per another example, a virtual identification card (e.g., a virtual driver's license card) may be selected for top placement within category 3710 based upon its general association with any virtual payment card selected for top placement within category 3706 or its general association with any virtual gift card selected for top placement within category 3708.

[0326] FIG. 38 shows GUI 3800 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 3800 may, for example, provide a visual representation of all virtual cards that may be stored within a mobile device (or remote server) and may display each virtual card within one or more categories that may be associated with each virtual card. GUI 3800 may, for example, be rendered onto a touch-sensitive display of a mobile device, such that by touching a location of the display that corresponds to a location of a virtual card, that card may be selected for use. Accordingly, for example, a user may touch any area within virtual card 3804 to activate virtual card 3804 for use. In so doing, for example, indicia may be provided on GUI 3800 to indicate that virtual card 3804 has been selected for use (e.g., an outline of virtual card 3804 may be highlighted) and a copy of virtual card 3804 (e.g., virtual card 3802) may be rendered onto GUI 3800 to indicate to a user of the mobile device that virtual card 3802 has been selected for use.

[0327] FIG. 39 shows GUI 3900 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 3900 may, for example, allow a user of a mobile device to select (e.g., touch) one of the virtual cards rendered onto GUI 3900. Once selected, the virtual card may rise from its position (e.g., virtual card 3904 may be elevated above the neighboring virtual cards in category 3902) and may be highlighted to indicate the selection to a user. Once elevated, the selected virtual card (e.g., card 3904) may display relevant information associated with the virtual card (e.g., information displayed on a front surface of the virtual card such as account number and merchant affiliation) so that a user may verify that the selected virtual card is the virtual card that the user wishes to use. If the selected virtual card is not the virtual card that the user wishes to use, then the user may deselect (e.g., touch) the selected virtual card and the virtual card may fall back within the ranks of its neighboring virtual cards. If the selected virtual card is the virtual card that a user wishes to use, then the user may confirm (e.g., touch the selected virtual card twice) that the selected card is the desired virtual card for use.

[0328] FIG. 40 shows GUI 4000 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 4000 may, for example, allow a user of a mobile device to use selected virtual card 4002 in some manner. A user may, for example, wish to complete a purchase transaction using the mobile device and selected virtual card 4004. Accordingly, for example, upon selection of option

4004, information associated with selected virtual card 4002 may be communicated from a mobile device to, for example, a merchant terminal to complete a purchase transaction. In so doing, for example, a contactless communication channel (e.g., an RFID communication channel) may be formed between the mobile device and the merchant terminal and payment information (e.g., payment account number and expiration date) may be communicated from the mobile device to the merchant terminal via the contactless communication channel. As per another example, other information (e.g., one, two, or three tracks of magnetic stripe information) that may be associated with virtual card 4002 may be communicated by the mobile device to the merchant terminal when the mobile device detects the presence of an RFID communication channel formed between the mobile device and the merchant terminal.

[0329] A mobile device may, for example, request electronic receipts to be delivered to the mobile device after purchase transactions are completed. Accordingly, for example, receipts may be delivered to the mobile device via an electronic delivery method (e.g., text messaging or email) and may be stored within a memory of the mobile device for future use. In so doing, for example, a user may select option 4006 to view a list of one or more receipts that may be associated with purchases conducted via the mobile device and virtual card 4002.

[0330] A mobile device may, for example, request electronic bank statements to be delivered to the mobile device at the end of each billing cycle of virtual card 4002. Alternately, for example, a mobile device may access a network entity (e.g., an issuer's

server) to retrieve bank statement information that may be associated with virtual card 4002. Accordingly, for example, a user of a mobile device may review any and all bank statements associated with virtual card 4002 that a user's mobile device may have collected via its network access capabilities (e.g., a wireless access point or cellular network access infrastructure).

[0331] A mobile device may, for example, allow virtual card 4002 to be associated with one or more virtual cards stored within a memory of the mobile device (or remote server). For example, virtual card 4002 may be associated with one or more cards (e.g., a rewards card and a driver's license) and a user of a mobile device may view such associations using a GUI of the mobile device.

[0332] A mobile device may, for example, allow virtual card 4002 to be associated with one or more virtual cards that may be stored within a memory of another mobile device and/or may allow virtual card 4002 to be associated with one or more physical cards not stored within any mobile device. Virtual card 4002 may, for example, be one of many (e.g., two) cards issued against the same general account (e.g., a husband and wife joint charge account). Accordingly, for example, a mobile device may recognize that virtual card 4002 is one of a pair of cards associated with such a joint account and may provide information to the user of the mobile device about such associations.

[0333] FIG. 41 shows system 4100, which may include a mobile device (e.g., mobile wallet 4102), merchant terminal 4106 and GUI 4108 that may be executed by a processor of mobile wallet 4102. A user of mobile wallet 4102 may recall a virtual card (e.g., a virtual

payment card) from a memory of mobile wallet 4102 (or from a remote server) and use mobile wallet 4102 to communicate payment information associated with the virtual payment card to a merchant terminal. Accordingly, for example, a user of mobile wallet 4102 may have selected a virtual payment account from within a memory of mobile wallet 4102 (or remote server) to complete a payment transaction.

[0334] Once mobile wallet 4102 is brought within a communication distance (e.g., within approximately 2 inches) of merchant terminal 4106, a contactless communication channel (e.g., RFID communication channel 4104) may be generated between mobile wallet 4102 and merchant terminal 4106. Payment information associated with a virtual payment card selected by a user of mobile wallet 4102 may, for example, be autonomously communicated by a processor of mobile wallet 4102 to merchant terminal 4106 via contactless communication channel 4104 once a presence of merchant terminal 4106 is detected by the processor of mobile wallet 4102.

[0335] Contactless communication channel 4104 may, for example, be a two-way communication channel. Accordingly, for example, merchant terminal 4106 may communicate information to mobile wallet 4102 via contactless communication channel 4104. In so doing, for example, merchant terminal 4106 may communicate a total sale amount to mobile wallet 4102 and may wait for a user of mobile wallet 4102 to acknowledge that the total sale amount is correct (e.g., a user of mobile wallet 4102 may press an acknowledgment key that causes mobile wallet 4102 to communicate a confirmation message to merchant terminal via contactless communication channel 4104). Further communication

from merchant terminal 4106 may query mobile wallet 4102 as to whether a user of mobile wallet 4102 requires cash back.

[0336] Once a purchase transaction is completed, a user of mobile wallet 4102 may request a receipt to be delivered to mobile wallet 4102 via any one of a number of mediums. A user may, for example, request that a receipt be delivered to mobile wallet 4102 at a later time (e.g., receipt queued for delivery at a later time via text messaging or email). A user may, for example, request that a receipt be delivered to mobile wallet 4102 immediately. Accordingly, for example, an electronic receipt may be generated by merchant terminal 4106 and communicated to mobile wallet 4102 via contactless communication channel 4104.

[0337] An application executing on a mobile device (e.g., a receipt handler application associated with GUI 4108) may have its own address. Accordingly, for example, the receipt handler's address may be well known within a network (e.g., a payment network), such that a server (e.g., an email server associated with a merchant's payment server) may email an electronic receipt directly to the receipt handler application that may be running on the mobile device. In so doing, for example, one or more applications running on a mobile device may have well known addresses (e.g., email addresses and multimedia message addresses) associated with them, so that the applications may directly communicate with network entities to autonomously provide a user of the mobile device with up-to-date and valuable information.

[0338] FIG. 42 shows system 4200, which may include a mobile device (e.g., mobile wallet 4202), merchant

terminal 4212 and GUI 4204 that may be executed by a processor of mobile wallet 4202. Mobile wallet 4202 may, for example, complete a purchase transaction with merchant terminal 4212 by exchanging payment information with merchant terminal 4212 via a contactless communication channel (e.g., RFID communication channel 4214). Merchant terminal 4212 may, for example, communicate electronic receipt 4206 to mobile wallet 4202 after a purchase transaction completes. Electronic receipt 4206 may, for example, be displayed by a processor of mobile wallet 4202 onto GUI 4204 so that a user of mobile wallet 4202 may view electronic receipt 4206 and may execute certain options that may be associated with electronic receipt 4206.

[0339] Mobile wallet 4202 may, for example, allow a user of mobile wallet 4202 to annotate electronic receipt 4206 with a note that may be entered into alphanumeric entry box 4208. Mobile wallet 4202 may, for example, allow electronic receipt 4206 to be associated with a virtual card (e.g., virtual payment card VISA 3456 that was used to complete the purchase transaction) stored within a memory of mobile wallet 1602.

[0340] FIG. 43 shows GUI 4300 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 4300 may, for example, allow a user of a mobile device to view receipts that may be associated with a selected virtual card. Accordingly, for example, a user of a mobile device may select a virtual card (e.g., virtual payment card 4302) and may view a summary of receipts that may be associated with virtual payment card 4302. In so doing, for example, a user may select summary receipt

4304 (e.g., by touching portion 4304 on GUI 4300) and a processor of the mobile device may retrieve details of summary receipt 4304 from a memory of the mobile device and display them in receipt detail area 4306.

[0341] FIG. 44 shows GUI 4400 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 4400 may, for example, allow a user of a mobile device to view virtual cards stored within a memory of the mobile device (or remote server) that may be associated with a selected virtual card. Accordingly, for example, selected virtual card 4402 may have an association with virtual rewards card 4404 and selected virtual card 4402 may have an association with virtual identification card 4406.

[0342] A mobile device may, for example, access a user's rewards account by accessing a network entity (e.g., an issuer's server) to determine information associated with the rewards account (e.g., number of rewards points earned). A mobile device may, for example, access the network entity on a regularly scheduled basis and store the retrieved rewards account information within a memory location of the mobile device. A mobile device may, for example, access the network entity only upon demand to retrieve rewards account information and may only display the retrieved rewards account information without storing the retrieved rewards account information.

[0343] GUI 4400 may, for example, allow a user to obtain further information that may be associated with virtual cards 4404 and/or 4406. A user may, for example, touch a display of a mobile device in the vicinity of virtual card 4404 to obtain other

information (e.g., a rewards point balance) associated with virtual card 4404. Accordingly, for example, a user may obtain a rewards points total that may be associated with virtual card 4404 and may touch virtual card 4404 again to conduct a purchase transaction with rewards points that may be associated with virtual card 4404. In so doing, for example, a mobile device may, for example, establish a contactless communication channel (e.g., an RFID communication channel) with a merchant terminal and may communicate points information that may be associated with virtual card 4404 so that a purchase transaction may be completed using rewards points that may be associated with virtual card 4404.

[0344] GUI 4400 may, for example, provide other information to a user concerning virtual card 4406. For example, a processor of a mobile device may detect that an expiration date of virtual card 4406 is approaching. Accordingly, for example, a user may touch a display in the vicinity of virtual card 4406 to automatically renew the driver's license using the mobile device. In so doing, for example, a mobile device may contact a network entity (e.g., a driver's license renewal server) to order a renewal driver's license. The renewal driver's license may, for example, be delivered to the user as a physical card, in which case the user may upload information associated with the physical driver's license into the mobile device via a contactless communication channel formed between the physical driver's license and the mobile device. Alternately, for example, a mobile device may receive an electronic copy of a virtual driver's license and replace information associated

with virtual card 4406 with the updated information received from a driver's license renewal server.

[0345] FIG. 45 shows system 4500, which may include mobile wallet 4502 and a powered card (e.g., powered payment card 4506). Powered card 4506 may, for example, include a contactless communication device (e.g., an RFID) that may communicate with a contactless communication device (e.g., an RFID) of mobile wallet 4502. A GUI executed by a processor of mobile wallet 4502 may invite a user of powered card 4506 to tap powered card 4506 against display 4504 of mobile wallet 4502. Such contact with, or proximity to, mobile wallet 4502 may generate a contactless communication channel within which information may be exchanged between powered card 4506 and mobile wallet 4502.

[0346] As per another example, powered card 4506 may include circuitry that may simulate a touch. Display 4504 may be touch-sensitive. Accordingly, for example, powered card 4506 may communicate data to mobile wallet 4502 by simulating a series of touches that may be sensed by display 4504 and processed by a processor of mobile wallet 4502 as data received from powered card 4506. Powered card 4506 may include light sensor 4510. Accordingly, for example, a processor of mobile wallet 4502 may generate a series of light pulses on a portion of display 4504 that may be detected by light sensor 4510 of powered card 4506 and processed by a processor of powered card 4506 as data communicated by mobile wallet 4502. In so doing, for example, data may be communicated by powered card 4506 via a series of simulated touches and data may be communicated by mobile wallet 4502 via a series of light pulses.

[0347] Information communicated by powered card 4506 to mobile wallet 4502 may, for example, include payment information (e.g., payment account number, expiration date, and cardholder name). Information communicated by powered card 4506 to mobile wallet 4502 may, for example, include other information relating to a configuration of powered card 4506 including, for example, whether or not a display exists and if so, at what location; whether or not a manual input interface (e.g., one or more buttons) exists and if so, at what location; and whether or not a light sensor exists and if so, at what location. Accordingly, for example, configuration information relating to powered card 4506 may be communicated to mobile wallet 4502, so that when a virtual card relating to powered card 4506 is generated and stored within mobile wallet 4502, the virtual card may employ all of the features that may be employed by its physical counterpart.

[0348] Information communicated by powered card 4506 may, for example, be encrypted. Decryption may, for example, be executed within mobile wallet 4502 so that information communicated by powered card 4506 may be stored within a memory of mobile wallet 4502 in a decrypted format. Alternately, for example, information communicated by powered card 4506 may be stored within a memory of mobile wallet 4502 in an encrypted format. Mobile wallet 4502 may, for example, authenticate itself to a network entity (e.g., an issuer server) such that each time encrypted information is recalled from a memory of mobile wallet 4502, a decryption key may be communicated by the network entity to mobile wallet 4502 for decryption purposes.

[0349] FIG. 46 shows GUI 4600 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 4600 may, for example, display virtual card 4602 that may employ all of the features of its physical counterpart. Accordingly, for example, manual input interfaces (e.g., virtual buttons 4606 through 4614) may have the same functionality on virtual card 4602 as they do on the physical counterpart to virtual card 4602. In so doing, for example, virtual buttons 4606 through 4614 may be displayed on portions of GUI 4600 that may be touch-sensitive, such that when virtual buttons 4606 through 4614 are touched, a processor of the mobile device may impart a functionality to the mobile device just as if the mobile device itself was the physical card (e.g., a PIN may be entered into virtual card 4602 via one or more buttons 4606-4614 to unlock virtual dynamic portion 4618 of virtual payment card number 4616).

[0350] A mobile device may, for example, provide a light-sensitive display, such that when virtual card 4602 is rendered onto the light-sensitive display, light sensor 4604 may exhibit the same functionality as its physical counterpart. Accordingly, for example, virtual card 4602 may be rendered so that light sensor 4604 exists on a light-sensitive portion of a display of a mobile device. A processor of the mobile device may, for example, detect light pulses sensed at light sensor 4604 as data communicated to virtual card 4602. In so doing, for example, virtual card 4602 may receive information that changes the functionality of virtual card 4602 (e.g., an expiration date of virtual payment card 4602 may be updated via light sensor 4604).

[0351] A mobile device may, for example, provide a display that may simulate touch. Accordingly, for example, virtual card 4602 may be rendered onto a display of a mobile device so that touch-simulating portion 4620 aligns with a portion of the display that may be capable of simulating touch. In so doing, for example, virtual card 4602 may communicate information to another device (e.g., another mobile device) when touch-simulating portion 4620 of GUI 4600 is pressed against another device (e.g., a touch-sensitive display of another mobile device) and simulates a series of touches that may be construed by a processor of the other device as data communicated to the other device.

[0352] Virtual display 4618 may, for example, display a dynamic portion of payment card number 4616 just as it would be displayed on the physical counterpart to virtual card 4602. For example, virtual card 4602 may be disabled for use when virtual display 4618 does not display a valid portion of virtual card number 4616. Upon entry of a password (e.g., a PIN may be entered by touching one or more buttons 4606-4614 that corresponds to the PIN), virtual card 4602 may be activated for use. Accordingly, for example, once a valid PIN is entered, virtual display 4618 may be populated with a remaining portion of virtual payment card number 4616 thereby activating virtual card 4602 for use. In so doing, for example, a mobile device that displays activated virtual card 4602 via GUI 4600 may communicate payment information (e.g., virtual payment card number 4616 and expiration date) to a device (e.g., a merchant terminal) via a contactless communication channel (e.g., an RFID communication channel) so that a purchase transaction may be

completed between the mobile device and the merchant terminal.

[0353] FIG. 47 shows GUI 4700 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 4700 may, for example, display virtual card 4702 that may employ all of the features of its physical counterpart. For example, a powered card (e.g., a powered payment card) may establish a contactless communication channel (e.g., an RFID communication channel) with a mobile device and communicate configuration and payment information that may be associated with the powered card. Accordingly, for example, a powered card may provide a manual interface (e.g., buttons) to allow a user to select a method of payment (e.g., credit, debit, or points) at the point of sale and may communicate such methods of payment to a mobile device. In so doing, for example, a mobile device may render virtual payment card 4702 having a virtual manual interface (e.g., virtual buttons 4704 through 4708), which a user may select (e.g., touch) in order to select a method of payment to be used by the mobile device when the mobile device communicates payment information to complete a purchase transaction.

[0354] A mobile device may, for example, establish a contactless communication channel (e.g., an RFID communication channel) with a merchant terminal to communicate payment information to the merchant terminal to complete a purchase transaction. Accordingly, for example, a user may touch one of virtual buttons 4704-4708 just prior to placing the mobile device within a proximity to the merchant terminal. In so doing, for example, the mobile device

may communicate one, two, and/or three tracks of magnetic stripe data to the merchant terminal and may include additional information (e.g., within a discretionary data field) to communicate a method of payment (e.g., credit, debit, or points) to the merchant terminal. Persons skilled in the art will appreciate that payment information may be communicated by a mobile device to a network entity (e.g., a payment server) via a wireless interface (e.g., a cellular interface) such that a method of payment (e.g., credit, debit, or points) may be communicated by the mobile device to the payment server to complete a remote purchase transaction.

[0355] FIG. 48 shows GUI 4800 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 4800 may, for example, allow a user of a mobile device to break a payment up into multiple payment methods for a single purchase. For example, a user of a mobile device may have provided a mobile device within a proximity to a merchant terminal, such that the mobile device may have communicated a method of payment (e.g., credit) to the merchant terminal based upon a user selection made via a GUI displayed by the mobile device. A processor of the mobile device may, for example, recognize that a virtual card selected by the user for payment may offer additional payment methods (e.g., debit and points). Accordingly, for example, GUI 4800 may be rendered by a processor of the mobile device to allow the user of the mobile device the option to spread the payment across several accounts by entering amounts into alphanumeric entry boxes 4804-4808. In so doing, for example, a user may spread a purchase across multiple payment

methods by entering an amount desired to be charged to each payment method (e.g., $5 credit, $5 debit, and 1500 points for a $25 total purchase). The mobile device may, for example, settle the transaction as three separate financial transactions by communicating payment information to one or more network entities (e.g., a payment server) that corresponds to each of the three financial transactions.

[0356] FIG. 49 shows GUI 4900 that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 4900 may, for example, communicate a credit offer to a user of a mobile device that may have been communicated to the mobile device via any one of a number of electronic means (e.g., text messaging, email, or internet browser pop-up). A credit offer may, for example, be extended to a user of a mobile device to add a payment card to the user's mobile device. A credit offer (e.g., credit offer 4906) may, for example, be extended to a user of a mobile device to replace a virtual card (e.g., virtual payment card 4904) that already exists within the user's mobile device. Accordingly, for example, network entities may examine virtual cards and related information that may be stored within a memory of a mobile device and attempt to sway the user of the mobile device to opt into another virtual card offer that may be better for the user (e.g., the new virtual card may offer a lower interest rate than a user's current virtual payment card).

[0357] GUI 4900 may, for example, provide credit offer options 4908 to a user of a mobile device. Accordingly, for example, a user may elect to accept a new credit offer and cancel a current virtual payment

card with the same option. In so doing, for example, a mobile device may communicate with a network entity (e.g., an issuer of virtual payment card 4904) to cancel virtual payment card 4904 and may communicate with a network entity (e.g., an issuer for payment card offer 4906) to open the new payment account being offered.

[0358] Other options may be provided by GUI 4900. For example, a user may opt to accept the new credit offer, but keep virtual payment card 4904 as well. As per another example, a user may opt to accept the new credit offer, keep virtual payment card 4904, and transfer any balance that may be owing on virtual payment card 4904 to the new payment account now being offered.

[0359] FIG. 50 shows mobile application 5000 that may be executed by a processor of a mobile device and provided onto a display of the mobile device. Application 5000 may, for example, be any executable application that may reside within a memory of a mobile device. For example, application 5000 may be an internet browsing application that may allow a user of a mobile device to browse online for goods and/or services and may allow the user to purchase such goods and/or services from application 5000. As per another example, mobile application 5000 may be a gaming activity that may require a purchase transaction to continue on to a next level of play or to obtain gaming features for purchase.

[0360] Application 5000 may, for example, provide access to mobile wallet 5002 which may be another application running on a mobile device. Accordingly, for example, when application 5000 requires payment for

a particular function performed by application 5000 (e.g., a user wishes to purchase goods from an Amazon website), application 5000 may launch mobile wallet 5002 to allow a user to select a method of payment from mobile wallet 5002. A user may browse through each virtual card of mobile wallet 5002 by touching a virtual card to display the virtual card. Once a user has verified that a particular virtual card is the virtual card to be used to complete a purchase transaction, the user may touch the virtual card twice again to authorize a mobile device to complete a purchase transaction using payment information associated with the selected virtual card.

[0361] As per another example, a user may preselect payment options, such that mobile application 5000 need not launch mobile wallet 5002 to obtain a payment authorization. Instead, for example, a user may pre-authorize one virtual payment card within mobile wallet 5002 to be used by any other application running on a mobile device for purchase transactions. In so doing, for example, a user may pre-authorize payment information to be autonomously retrieved from mobile wallet 5002 without involving user interaction to authorize application 5000 for the purchase transaction.

[0362] FIG. 51 shows flow charts for process sequences 5110-5150. Process sequence 5110 may, for example, execute a mobile wallet application on a mobile device (e.g., as in step 5111) to request a user of the mobile device to present a card to the mobile device. In step 5112, a user may present a card to a mobile device (e.g., tap a card onto a display of a mobile device). In step 5113, a contactless

communication channel (e.g., an RF, capacitive, audible, visible, electromagnetic, or magnetic communication channel) may be generated between a card and a mobile device to communicate card information from the payment card to the mobile device. In step 5114, information may be stored within the mobile device or remote server (e.g., virtual cards may be generated, stored, and displayed by a GUI of the mobile device) for future use.

[0363] Process sequence 5120 may, for example, autonomously detect that a card is in a touching or a proximity relationship to a mobile device (e.g., as in step 5121). In step 5122, a contactless communication channel (e.g., an RF, capacitive, audible, visible, electromagnetic, or magnetic communication channel) may be generated between a card and a mobile device to communicate information from the card to the mobile device. In step 5123, information associated with each physical card presented to the mobile device may be stored within the mobile device for future use.

[0364] Step 5131 of sequence 5130 may include presenting a card to a mobile device. A card may, for example, be a powered card or a non-powered card. In steps 5132 and 5133, a contactless communication channel may be established between a card and a mobile device and information may be exchanged between the card and the mobile device.

[0365] A card may, for example, include a near-field communication device (e.g., an RFID) that may communicate with a contactless communication device of a mobile device to form a two-way communication channel between the card and the mobile device. A card may, for example, include circuitry to simulate touch (e.g.,

a capacitance change) in order to form a contactless communication channel with a mobile device. Accordingly, for example, a card may be pressed against a touch-sensitive display of a mobile device and information may be communicated by the card to the mobile device through a series of card-simulated touches that may be detected by the touch-sensitive display of the mobile device.

[0366] A card may, for example, include a light sensor to form a contactless communication channel with a mobile device. Accordingly, for example, a card may be pressed against a display of a mobile device and information may be communicated from the mobile device to the card through a series of light pulses generated by the display of the mobile device. A frequency, pulse width, and/or a pulse intensity of light pulses may, for example, be detected by a processor of a card as data communicated by a mobile device.

[0367] A card may, for example, include a light source (e.g., an LED) to form a contactless communication channel. Accordingly, for example, a card may emit varying light pulses from an LED that may be detected by a motion-capture device (e.g., a camera) of a mobile device as data communicated by the card. A card may, for example, include sound emission capabilities that may be detected by a microphone of a mobile device as data communicated by the card through a contactless communication channel. A mobile device may, for example, include sound emission capabilities that may be detected by a microphone of a card as data communicated by the mobile device through a contactless communication channel.

[0368] Step 5141 of sequence 5140 may include arranging information contained within a memory of a mobile device and/or a remote server and rendering the information on a display of a mobile device. The rendered information may, for example, be virtual cards that are representative of physical card counterparts previously presented to the mobile device for upload.

[0369] The virtual cards may, for example, be arranged according to category (e.g., payment cards, gift cards and identification cards). Within each category, virtual cards may be sorted according to any sort preference. For example, payment cards may be sorted in an order of most frequently used to least frequently used, in order of most available credit to least available credit, or in order of highest credit limit to lowest credit limit. Other cards (e.g., merchant gift cards) may be sorted in accordance with a user's location. For example, a mobile device may determine a location of its user and may sort virtual cards in response to the determined location (e.g., a virtual Walmart gift card may be displayed at the top of a gift card list based upon a user's location within a Walmart store).

[0370] Virtual cards displayed by a GUI of a mobile device may, for example, be selected for use (e.g., as in step 5142). A user may, for example, touch a virtual card among several virtual cards displayed by a mobile device to view information related to the touched virtual card. If desired for use, the touched virtual card may be touched twice again and activated for use (e.g., as in step 5143). An activated virtual card may, for example, be used to complete a purchase transaction via the mobile device. An activated

virtual card may, for example, be deleted from a memory of the mobile device. Documents associated with an activated virtual card, such as purchase transaction receipts and bank statements, may be viewed from a display of a mobile device. Virtual cards that may be associated with an activated virtual card may be viewed from a display of a mobile device and activated themselves to perform other functions (e.g., an activated virtual payment card may be associated with a virtual rewards card, where the virtual rewards card may be activated to obtain and view the total number of rewards points that may be associated with the virtual rewards card).

[0371] Step 5151 of sequence 5150 may include running an application on a mobile device. Such an application may be any executable application that may require purchase transactions to be completed while the application executes. As per one example, a user booking airline tickets using his or her mobile device may select their itinerary and may book their itinerary through a purchase transaction conducted by the mobile device. Accordingly, for example, the mobile application may request access to a mobile wallet application also running on the mobile device (e.g., as in step 5152), a user may grant access to the mobile wallet application (e.g., as in step 5153) by selecting a virtual payment card from within the mobile wallet and may authorize a purchase transaction to be conducted by the mobile application using the authorized virtual payment card. As per another example, a mobile application may autonomously request access to a mobile wallet application (e.g., as in step 5152) that has been pre-authorized by a user of the

mobile device (e.g., as in step 5153) such that the mobile application may autonomously conduct the purchase transaction without any further involvement with the user.

[0372] FIG. 52 shows mobile device 5200. Mobile device 5200 may be any mobile device, such as a mobile telephonic device (e.g., cell phone), a PDA, an electronic tablet, an MP3 player, or a locating device (e.g., a GPS device). Accordingly, mobile device 5200 may be operated in a mobile environment while a user of mobile device 5200 goes about his or her daily activities (e.g., driving, shopping, walking, dining, and exercising). In addition, for example, mobile device 5200 may perform multiple functions simultaneously (e.g., a person may carry on a conversation while at the same time browsing and authorizing purchases on the internet).

[0373] Mobile device 5200 may include audio processing devices (e.g., microphone 5208 and speaker 5210). Accordingly, for example, mobile device 5200 may receive voice commands from a user via microphone 5208 and may process such commands to perform a function. For example, a user may place mobile device 5200 into a desired operational mode by speaking a command into microphone 5208 that is associated with the desired operational mode. In so doing, for example, mobile device 5200 may engage in hands-free operation by receiving voice commands via microphone 5208 and performing functions associated with the received voice commands.

[0374] Mobile device 5200 may receive data input via microphone 5208. For example, a voice-band modem may generate signals in a voice-band frequency range that

may be received by microphone 5208. A processor of mobile device 5200 may interpret the received audible information as data signals and may process the data signals as, for example, data values and/or control data input.

[0375] Mobile device 5200 may include camera 5202. Camera 5202 may capture one or more frames of video data and store the video data within a memory of mobile device 5202. Accordingly, for example, a processor of mobile device 5200 may receive one or more frames of video information via camera 5202 and may process the video information as data values and/or control data input. In so doing, for example, mobile device 5200 may receive optical information that may be sensed by camera 5202 during a series of one or more video capture events that produce one or more frames of video information. The one or more frames of video information may contain one or more data elements (e.g., pixels) having properties (e.g., color, intensity, or contrast) that may be interpreted by a processor of mobile device 5200 as data values and/or control data.

[0376] Mobile device 5200 may include manual input interface 5212. Manual input interface 5212 may, for example, include keys and/or buttons that may be sensitive to manual input, such as a touch or an application of pressure. Accordingly, for example, a user of mobile device 5200 may enter information into mobile device 5200 via manual interface 5212 to cause a processor of mobile device 5200 to enter a particular mode of operation. Manual interface 5212 may, for example, be used for data entry (e.g., dialing a phone number or entering data as may be requested by mobile

device 5200) during a particular mode of operation of mobile device 5200.

[0377] Mobile device 5200 may include display 5204. Display 5204 may provide visible information that may be utilized by a user during interaction with mobile device 5200. A portion or all of display 5204 may be touch sensitive such that objects making contact with display 5204 or objects coming within a proximity of display 5204 may be detected by a processor of mobile device 5200. Accordingly, for example, mobile authorization graphical user interface 5206 may be provided by display 5204 so that graphical information may be displayed to solicit and/or receive data entry from a user. In so doing, for example, touch-sensitive graphical user interface devices such as radio buttons, alphanumeric input boxes, virtual buttons, pull-down menus, and navigational tools may be used for data entry to initiate, change, and/or support functions performed by mobile device 5200.

[0378] FIG. 52 shows architecture 5250. User interface 5252 may, for example, be included within architecture 5250 to allow user interaction with architecture 5250. For example, a dedicated key pad or keyboard may be included within user interface 5252 to allow alphanumeric data entry into architecture 5250.

[0379] Architecture 5250 may include one or more displays 5254. Display 5254 may, for example, be touch-sensitive. Accordingly, for example, display 5254 may be utilized for alphanumeric data entry using virtual buttons that may be rendered onto touch-sensitive portions of display 5254. In so doing, for example, touching virtual buttons that may be associated with alphabetic and numeric characters of

display 5254 may be detected by processor 5258 as alphanumeric data entry.

[0380] Alphanumeric entry boxes may, for example, be rendered onto display 5254. A user may, for example, activate a cursor within such an alphanumeric entry box by touching an area within the alphanumeric entry box. A user may utilize user interface 5252 and/or a virtual keypad rendered onto display 5254 to select alphanumeric characters to be placed within the alphanumeric entry box in accordance with a character position identified by an activated cursor within the alphanumeric entry box. In so doing, for example, processor 5258 may receive alphanumeric characters as typed into a alphanumeric entry box of display 5254 and may use such alphanumeric characters as data input.

[0381] Display 5254 may, for example, provide data output from architecture 5250. For example, display 5254 may communicate data using a series of light pulses. Accordingly, for example, processor 5258 may cause one or more portions of display 5254 to produce light pulses having varying characteristics (e.g., duration, intensity, and frequency) that may communicate information via such light pulses. In so doing, for example, a device that may be sensitive to light pulses may receive information communicated by display 5254 via light pulses having varying characteristics. Display 5254 may, for example, communicate data using visual information that may be substantially static (e.g., a barcode).

[0382] Architecture 5250 may include one or more transceivers 5256. Transceiver 5256 may communicate information to and/or may receive information from one or more devices. Transceiver 5256 may, for example,

communicate via a wireless interface with one or more cellular stations of a mobile network. Accordingly, for example, transceiver 5256 may allow a mobile device (e.g., mobile device 5200 of FIG. 52) to establish a communications channel with an associated cellular station. In so doing, for example, a mobile device (e.g., mobile device 5200 of FIG. 52) may exchange information (e.g., voice, text, data, or multimedia) with one or more terrestrial networks (e.g., the internet or a payment network) via an associated cellular station. As per another example, transceiver 156 may exchange information with one or more other mobile devices via one or more associated cellular stations.

[0383] Transceiver 5256 may, for example, communicate via a wireless interface with one or more mobile devices directly. Accordingly, for example, transceiver 5256 may communicate with another mobile device without first accessing a mobile network via a cellular station of the mobile network. As per another example, transceiver 5256 may, for example, communicate via a wireless interface with one or more network devices (e.g., a wireless access point) directly. Accordingly, for example, a mobile device (e.g., mobile device 5200 of FIG. 52) may directly connect to a wired and/or a wireless network via any one or more wireless standards (e.g., Bluetooth or Wi-Fi) to exchange information with other devices that may be connected to the wired and/or wireless network. In so doing, for example, a wired and/or wireless network may be accessed by a mobile device without first accessing a mobile network via a cellular station of a mobile network.

[0384] Architecture 5250 may include contactless communication device 5262, which may communicate via any one or more contactless communication methodologies, such as for example, near field communications (e.g., RFID), Bluetooth, touch simulation, light pulsing (e.g., via an LED), and electromagnetic data communication (e.g., via a dynamic magnetic stripe communications device). Accordingly, for example, contactless communication device 5262 may be compatible with any contactless device, such as for example, an RFID enabled payment card and a contactless reader (e.g., a magnetic stripe reader or an NFC reader).

[0385] A non-powered card may, for example, communicate with contactless communications device 5262. Contactless communication device 5262 may, for example, establish a carrier field (e.g., an RF field) that may be modulated by a device (e.g., an RFID tag) of a non-powered payment card. In so doing, for example, an RFID tag of a non-powered payment card may derive operational power from an RF field provided by contactless communications device 5262 and may communicate information (e.g., one, two, and/or three tracks of magnetic stripe data) to contactless communication device 5262 by modulating the RF field produced by contactless communications device 5262.

[0386] A powered card may, for example, communicate with contactless communication device 5262. A powered card may, for example, include a processor, a battery, a memory, wireless communication devices (e.g., a dynamic magnetic stripe communications device or RFID) and other electronics (e.g., buttons) that may allow a user to interact with the powered card to perform one

or more functions. Accordingly, for example, a powered card may be used to communicate specific information to contactless communication device 5262 by selective interaction with the buttons of the powered card. In so doing, for example, a powered card may be used to interactively communicate magnetic stripe information (e.g., one, two, and/or three tracks of magnetic stripe data) to contactless communication device 5262 by sending a signal to a processor of a powered card (e.g., by pressing a button on the powered card) to initiate such communications.

[0387] Contactless communication device 5262 may receive variable data sets from a powered card based upon, for example, manual input provided to a powered card. For example, a button associated with an on-line purchase may be pressed on the powered card that causes a variable data set (e.g., account number and expiration date) to be communicated from the powered card to contactless communication device 5262.

[0388] Discretionary data may, for example, be communicated by a powered card based upon which button was pressed on the powered card. In so doing, for example, a security code (e.g., "111") may be communicated within a discretionary data field when a button associated with a particular feature (e.g., pay with credit) is pressed on the powered card. As per another example, a different security code (e.g., "222") may be communicated within a discretionary data field when a button associated with a different feature (e.g., pay with debit) is pressed on the powered card. A powered card may, for example, communicate a different security code no matter what feature may be selected on the powered card. Accordingly, for

example, processor 5258 may identify what type of device may be in communication with contactless communication device 5262 by analyzing the data communicated to contactless communication device 5262.

[0389] Any device having contactless communication capability may communicate with contactless communication device 5262 to authorize functions that may be performed by a mobile device. An RFID enabled device (e.g., an RFID equipped automobile key) may, for example, communicate with contactless communication device 5262 to authorize functions that may be performed by a mobile device (e.g., mobile device 5200 of FIG. 52) on a device that may be controlled by the RFID enabled device (e.g., an automobile that corresponds to the RFID equipped automobile key). For example, processor 5258 may execute an automobile application that may wirelessly communicate with an automobile to perform remote functions (e.g., start an engine of the automobile or unlock the driver's door). Through use of an RFID equipped key, for example, such functions may be authorized to be performed by a mobile device (e.g., mobile device 5200 of FIG. 52) once the RFID equipped key has communicated the necessary security credentials (e.g., a key code) to an application running on a processor of the mobile device to establish that a one-to-one correspondence exists between the automobile and the RFID equipped key.

[0390] Architecture 5250 may include memory 5260 and/or processor 5258 may include internal memory. Accordingly, for example, application code may be stored within memory 5260 and/or processor 5258 and executed by processor 5258 in support of functions performed by architecture 5250. For example, an

application (e.g., a graphical user interface) may be executed by processor 5258 and displayed onto display 5254, which may be used to interact with a user of a mobile device (e.g., mobile device 5200 of FIG. 52). Persons skilled in the art will appreciate that executable application code may be communicated to architecture 5250 via any one or more interfaces of architecture 5250 (e.g., user interface 5252, display 5254, transceiver 5256, and/or contactless communication device 5262).

[0391] Application data (e.g., security credentials) may be stored within memory 5260 and accessed by processor 5258 during operation. For example, security credentials may be stored within memory 5260 and recalled by processor 5258 to authorize a function that may be performed by processor 5258 of a mobile device (e.g., mobile device 5200 of FIG. 52). Accordingly, for example, processor 5258 of a mobile device may challenge a user of the mobile device to produce security credentials to authorize any function that may be performed by the mobile device. A processor of the mobile device may, for example, validate the security credentials locally within the mobile device itself. Alternately, for example, security credentials may be forwarded to a network entity (e.g., an authorization server) for remote validation.

[0392] FIG. 53 shows network topology 5300 that may include, for example, mobile device 5302 (e.g., a mobile telephonic device, a PDA, an electronic tablet, a laptop, a GPS unit, or an MP3 player). Mobile device 5302 may, for example, include a contactless interface that may initiate, sustain, and/or terminate communication channel 5326 between contactless device

5304 and mobile device 5302. Contactless device 5304 and mobile device 5302 may communicate via channel 5326 using any number of contactless mediums, which may include for example, visible, audible, capacitive, electromagnetic, magnetic, and/or RF mediums.

[0393] Mobile device 5302 may provide one or more transceivers that may communicate with one or more wired networks (e.g., IP network 5312 and/or payment network 5314) and/or one or more wireless networks (e.g., mobile network 5310). Mobile device 5302 may, for example, communicate with a cellular station over a wireless radio interface (e.g., a GSM air interface) that may be used by mobile device 5302 to communicate information (e.g., voice and data) to cellular network access infrastructure 5306 (e.g., one or more GSM base transceiver stations, base station controllers, and mobile switching centers). Persons skilled in the art will appreciate that cellular network access infrastructure 5306 may utilize any multiple access architecture, such as for example, a code-division multiple access architecture and/or a time-division multiple access architecture.

[0394] Mobile device 5302 may, for example, communicate with wireless access point 5308 over a wireless interface (e.g., a Bluetooth interface or a Wi-Fi interface). Accordingly, for example, mobile device 5302 may access one or more wired networks (e.g., IP network 5312 and/or payment network 5314) and/or one or more wireless networks (e.g., mobile network 5310) without the need to first gain access to cellular network access infrastructure 5306.

[0395] Contactless device 5304 may, for example, be a powered card, a non-powered card (e.g., a powered

payment card or a non-powered payment card) or any contactless enabled device (e.g., an RFID enabled device). Accordingly, for example, security credentials may be communicated via a contactless communication channel from contactless device 5304 to mobile device 5302 to authenticate a purchase transaction that may be performed by mobile device 5302. In so doing, for example, items for purchase on IP network 5312 (e.g., the internet) may be accessed by a browser of mobile device 5302 via an access point (e.g., wireless access point 5308 or cellular network access infrastructure 5306), payment information may be retrieved from a memory of mobile device 5302, a user of mobile device 5302 may be challenged for security credentials (e.g., at least a portion of a payment account number and a card expiration date communicated to mobile device 5302 from a payment card corresponding to the payment information retrieved from a memory of mobile device 5302), such payment information may be authenticated by such security credentials, and such payment information may be communicated to network entities (e.g., issuer 5320) to complete the purchase transaction.

[0396] Issuer 5320 may, for example, contact authorization server 5316 via a network (e.g., payment network 5314) with payment information and security credentials received from mobile device 5302 for authorization of a purchase. Once authorized, payment transaction information may be recorded onto a receipt that may be delivered to mobile device 5302 via any one or more delivery options (e.g., via a short messaging service of mobile network 5310 or an email delivery service of IP network 5312). Mobile device 5302 may

allow a user to associate purchase categories (e.g., groceries, auto repair, or entertainment) to purchases transacted by the mobile device so that the user may receive a more detailed accounting of his or her expenditures on his or her receipt. Accordingly, for example, a user may enjoy a higher degree of integration such that a user may customize a level of detail provided on a receipt via mobile device 5302.

[0397] A payment receipt may, for example, be provided to mobile device 5302 as a proof-of-purchase object (e.g., a barcode) that may be provided to a display of mobile device 5302 and read by other computing equipment (e.g., a barcode scanner) for proof-of-purchase confirmation.

[0398] A processor of mobile device 5302 may, for example, authorize wireless device 5334 to perform functions that may be authenticated by contactless device 5304 (e.g., via security credentials communicated by contactless device 5304 to a processor of mobile device 5302). Accordingly, for example, a processor of mobile device 5302 may require security credentials to be communicated by contactless device 5304 via contactless communication channel 5326 and based upon a validity of the security credentials communicated, the processor may communicate instructions to wireless device 5334 via contactless communication channel 5336 to perform some function. As per another example, a processor of mobile device 5302 may communicate instructions (e.g., via wireless access point 5308 or cellular network access infrastructure 5306) to wireless device 5334 (e.g., a car or a home) to perform a function (e.g., start the

engine of the car) based upon a validity of security credentials communicated by contactless device 5304.

[0399] A processor of mobile device 5302 may, for example, locally validate security credentials communicated by contactless device 5304. Alternately, for example, mobile device 5302 may forward security credentials communicated by contactless device 5304 to a network entity (e.g., authorization server 5332) for remote validation.

[0400] A mobile device (e.g., mobile device 5324) may, for example, include a contactless communication device (e.g., an RFID device) that may initiate, sustain, and/or terminate contactless communication channel 5328 with merchant terminal 5318. Accordingly, for example, a processor of mobile device 5324 may communicate payment information to merchant terminal 5318 to complete a financial transaction. In so doing, for example, a processor of mobile device 5324 may receive payment information via contactless communication channel 5330 from contactless device 5322 (e.g., a powered or a non-powered card) and store the received payment information within a memory of mobile device 5324. To complete a purchase transaction, contactless device 5322 may, for example, be presented to mobile device 5324 and may communicate security credentials (e.g., at least a portion of a payment card number and a cardholder's name) via contactless communication channel 5330. A processor of mobile device 5324 may validate the security credentials and may forward the payment information onto merchant terminal 5318 to complete the purchase transaction.

[0401] FIG. 54 shows system 5400, which may include mobile device 5402 and contactless devices 5408-5414.

Mobile device 5402 may, for example, be a laptop computer, a PDA, a mobile telephonic device (e.g., a smartphone), an MP3 player, a GPS, or any other mobile device. Display 5404 may be a touch-sensitive display (e.g., sensitive to a change in capacitance). Contactless devices may, for example, include non-powered payment card 5408, identification card (e.g., driver's license 5410), powered payment card 5412, key 5414, and any other device capable of communicating security credentials to mobile device 5402 via a contactless communication channel that may be formed with mobile device 5402.

[0402] Mobile device 5402 and contactless devices 5408-5414 may each include a contactless communication device (e.g., an RFID device) that may communicate via a contactless communication channel that may be formed between mobile device 302 and contactless devices 5408-5414 after coming into proximity to one another. Contactless devices 5408-5414 may, for example, be tapped onto display 5404 of mobile device 5402 to establish a proximity relationship that forms a communication channel with mobile device 5402. As per another example, contactless devices 5408-5414 may be brought within a proximity distance (e.g., up to two inches) of mobile device 5402 to establish a contactless communication channel with mobile device 5402.

[0403] A processor of mobile device 5402 may, for example, execute application code that may generate a graphical user interface (GUI) onto display 5404 of mobile device 5402. Message 5406 of a GUI may invite a user of mobile device 5402 to begin a mobile authorization by tapping a contactless device against

display 5404. As per another example, by tapping a contactless device against mobile device 5402, a processor of mobile device 5402 may autonomously determine that a mobile authorization is desired and may then generate a mobile authorization GUI onto display 5404.

[0404] Mobile device 5402 may, for example, autonomously determine a type of contactless device that may be tapped against it. For example, a processor of mobile device 5402 may receive security credentials that may be indicative of a non-powered payment card (e.g., security credentials received from non-powered payment card 5408 may include at least a portion of a payment card number and a cardholder's name). As per another example, a processor of mobile device 5402 may receive security credentials that may be indicative of a powered card (e.g., security credentials received from powered card 5412 may contain a dynamically generated security code). Security credentials received from powered card 5412 may, for example, include a dynamic security code that may change for each function authorized by powered card 5412.

[0405] A contactless device (e.g., key 5414) may, for example, be a key that may start the ignition of a car, open a door to a home, or open a safe deposit box. Key 5414 may, for example, include a contactless communication device (e.g., an RFID device) that may communicate security credentials to a processor of mobile device 5402. Once security credentials received from key 5414 are validated, a processor of mobile device 5402 may effect an operation that may eliminate the need to physically use key 5414 to perform the

operation (e.g., a user of mobile device 5402 may remotely start the engine of the user's car by running an application on a processor of mobile device 5402 to validate security credentials received from key 5414 and wirelessly communicate with a wireless device of the user's car to start its ignition). As per an example, the user's physical key 5414 may, for example, be locked inside the user's car, in which case the user may select another contactless device (e.g., identification card 5410) to present to mobile device 5402. Identification card 5410 may, for example, communicate security credentials to a processor of mobile device 5402 and once the processor authorizes the identify of the user of mobile device 5402, mobile device 5402 may, for example, wirelessly communicate with the user's car to unlock its doors so that the user may retrieve key 5414 that may have been previously locked within the user's car.

[0406] Powered payment card 5412 may, for example, include electronics to simulate a human touch (e.g., powered payment card 5412 may generate a change in capacitance that may be sensed by display 5404). Through a series of simulated touches, powered payment card 5412 may communicate a series of data bits to display 5404, which may then be processed by a processor of mobile device 5402 as security credentials. In so doing, for example, a contactless communication channel may be established where data is transferred from powered payment card 5412 to a processor of mobile device 5402 via a series of simulated touches to authorize a function to be performed (or commanded to be performed) by a processor of mobile device 5402.

[0407] Powered payment card 5412 may, for example, include a light sensor. Accordingly, for example, powered payment card 5412 may be sensitive to light pulses generated within a region of display 5404. The light sensor of powered payment card 5412 may receive a series of light pulses, which may be construed by a processor of powered payment card 5412 as data generated by a processor of mobile device 5402. In so doing, for example, powered payment card 5412 may receive an optical data stream represented by a series of light pulses generated by display 5404. As such, a two-way communication channel may be formed, where simulated touches may generate a data stream from powered payment card 5412 to mobile device 5402 and light pulses may generate a data stream from mobile device 5402 to powered payment card 5412.

[0408] Mobile device 5402 may, for example, include a motion-capture device (e.g., a camera). Identification card (e.g., driver's license 5410) may, for example, include a barcode. Accordingly, for example, a contactless communication channel may be formed between identification card 5410 and mobile device 5402 where a camera of mobile device 5402 may capture an image of the barcode of identification card 5410. In so doing, for example, a processor of mobile device 5402 may analyze the barcode image and extract information from the barcode image that may be construed by the processor as security credentials that when validated, may authorize a processor of mobile device 5402 to perform (or cause to perform) any function.

[0409] As per another example, a user's photograph may appear on identification card 5410. Accordingly,

for example, a camera of mobile device 5402 may capture an image of the picture and a processor of mobile device 5402 may construe the captured image as a security credential. In so doing, for example, a processor of mobile device 5402 may compare a scanned image of a user's picture to an image contained within a memory of mobile device 5402 (or contained within a memory of a remote authorization server) for authorization. As per yet another example, a user may snap a picture of himself or herself with a camera of mobile device 5402 so that a processor of mobile device 5402 may scan the snapped picture for authorization purposes.

[0410] Mobile device 5402 may, for example, require authorization before being activated for use. Accordingly, for example, a processor of mobile device 5402 may require a password to be entered and verified before a processor of mobile device 5402 may unlock functions available to be performed by mobile device 5402. In so doing, for example, one or more contactless devices 5408-5414 may be presented to mobile device 5402 and security credentials may be communicated by the one or more contactless devices 5408-5414 in lieu of providing a password to mobile device 5402. Upon validation of the security credentials, a processor of mobile device 5402 may unlock those functions that may be available to be executed by the processor of mobile device 5402.

[0411] FIG. 55 shows GUI 5500, that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 5500 may, for example, provide a summary of each card that may be available for use within a memory of the mobile device

(e.g., each card may be displayed as virtual cards having visible and functional features that are substantially the same as their physical counterparts).

[0412] Physical card (e.g., payment card) information (e.g., track 1, track 2, and/or track 3 magnetic stripe data) may be communicated by the physical card to the mobile device via a contactless communication channel and such information may be displayed within a virtual card (e.g., virtual payment card 5502) as summary information that may be associated with the physical payment card. A payment card number communicated to a processor of a mobile device may, for example, include issuer identification as well as an issuing network identifier. Accordingly, for example, a processor of a mobile device may analyze the payment card number received from a physical payment card and may render a portion or all of the identifying information associated with the payment card number onto virtual payment card 5502. In so doing, for example, issuer identification as well as a logo representative of an issuing network identifier may be rendered onto virtual payment card 5502. Other virtual payment cards may, for example, be sorted behind virtual payment card 5502 in virtually any order (e.g., most popular to least popular, highest credit limit to lowest credit limit, or highest credit available to lowest credit available). Other virtual cards (e.g., virtual gift card 404 and virtual driver's license 5506) may be stored within a memory of a mobile device as well.

[0413] FIG. 56 shows GUI 5600, that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 5600 may, for

example, allow a selection of a virtual card contained within a memory of a mobile device to be authorized for use by its physical counterpart. Accordingly, for example, a user may touch anywhere within the vicinity of virtual card 5604 as it is being displayed by GUI 5600. Such a selection may be verified by highlighting attributes of a selected card (e.g., highlighting an outline of virtual card 5604) and by displaying the selected virtual card within verification region 502. In so doing, for example, a user of a mobile device may view a virtual card that is selected for authorization (e.g., as viewed within region 5602) so that the user may retrieve the physical card that corresponds to the virtual card that is to be authorized.

[0414] Once retrieved, a user may tap the physical card against region 5602. Accordingly, for example, a contactless communication channel (e.g., an RFID communication channel) may be formed between the physical card and the mobile device, such that security credentials may be communicated from the physical card to the mobile device via the contactless communication channel to authorize virtual payment card 5602 for use. In so doing, for example, a physical card may communicate security credentials (e.g., at least a portion of a payment card number of the physical card and/or a cardholder's name) to a processor of the mobile device and the processor may compare the received security credentials to security credentials stored within a memory of the mobile device that may be associated with virtual payment card 5602. If the processor of the mobile device determines that the received security credentials match at least a portion of the security credentials associated with virtual

payment card 5602, then virtual card 5602 may be authorized for use.

[0415] FIG. 57 shows GUI 5700, that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 5700 may, for example, allow the authorization of a virtual card via an alternate contactless communication channel. For example, GUI 5700 may display a virtual payment card (e.g., virtual payment card 5702) in a region within GUI 5700 that may provide a touch-sensitive area 5704 and area 5706 that may be capable of producing light pulses having varying characteristics (e.g., intensity, pulse width, and/or color).

[0416] A user's physical card that corresponds to virtual payment card 5702 may, for example, be a powered card having touch-simulation electronics and a light sensor. Accordingly, for example, the user's physical card may be pressed against region 5702, such that the touch simulation electronics of the physical card aligns with touch-sensitive portion 5704 and the light sensor of the physical card aligns with portion 5706. In so doing, for example, a contactless communication channel may be formed between the user's physical card and the mobile device, such that data may be communicated from the user's physical card to the mobile device through a series of simulated touches generated by the physical card and sensed at portion 5704 by a processor of the mobile device. Such communicated data may be construed by a processor of the mobile device as security credentials communicated by the user's physical card.

[0417] Security credentials that may be communicated (e.g., via a capacitive, visible, audible,

electromagnetic, magnetic, or RFID-based contactless communication channel) to a mobile device by a powered payment card may, for example, include a dynamic security code that may change with each use. Accordingly, for example, a network entity (e.g., an authorization server) may be synchronized with the user's powered payment card, such that when a dynamic security code of the powered payment card changes, so does the corresponding dynamic security code of the authorization server. In so doing, for example, a dynamic security code received by a mobile device from a powered payment card during authorization of virtual payment card 5702 may be communicated by a processor of the mobile device to an authorization server for verification that the dynamic security code matches the dynamic security code maintained by the authorization server. If so, virtual payment card 5702 may be authorized for use by the mobile device (e.g., payment information associated with virtual payment card 5702 may be communicated by the mobile device to complete a purchase transaction).

[0418] FIG. 58 shows system 5800 that may include mobile terminal 5802, payment card 5808, network 5814 and authorization server 5810. A processor of mobile device 5802 may, for example, execute an application (e.g., GUI 5804) that allows a user of mobile device 5802 to perform any financial account management function (e.g., change from paper statements to e-statements, transfer money from one account to another or open a checking account).

[0419] Prior to authorizing the financial account management function, GUI 5804 may challenge a user of mobile device 5802 to tap a card against mobile device

5802 that may be associated with the transaction. Accordingly, for example, a payment card (e.g., payment card 5808) that may be associated with the financial accounts used for the financial account management function may be used as a security credential to authorize the transaction. In so doing, for example, security credentials communicated by payment card 5808 to mobile device 5802 via contactless communication channel 5806 (e.g., an RFID communication channel) may be relayed by mobile device 5802 to authorization server 5810 via communication channel 5812 for authorization of the financial account management function. Once authorized, a processor of mobile device 5802 may receive the authorization from authorization server 5810 and may contact other network entities (e.g., a payment server of network 5814) to complete the financial account management function.

[0420] Payment card 5808 need not be directly related to the financial accounts involved with a financial account management function. Instead, authorization server 5810 may, for example, maintain links between various financial accounts that may be owned by a user of a mobile device. Accordingly, for example, while payment card 5808 may not be used as the source account from which money is to be transferred to an auto loan account, payment card 5808 may nevertheless be linked with the source account (e.g., M/C 1234). In so doing, for example, authorization server 5810 may recognize the link between payment card 5808 and the source account (e.g., M/C 1234) and may authorize the money transfer due to the recognized link.

[0421] Payment card 5808 may, for example, be a powered payment card. Accordingly, for example, a dynamic security code may be communicated from payment card 5808 to a processor of mobile device 5802 (e.g., via a discretionary data field of a magnetic stripe message communicated by payment card 5808) along with other identifying information (e.g., at least a portion of a dynamic payment card number or a cardholder's name). In so doing, for example, the dynamic security code and/or other optional identifying information may serve as the security credential that authorizes mobile device 5802 to perform the requested function. The dynamic security code and/or other optional identifying information may, for example, be relayed to authorization server 5810. Accordingly, for example, authorization server 5810 may analyze the security code and any other optional identifying information to determine whether the requested function is to be authorized. If so, the authorization may be communicated by authorization server 5810 to a processor of mobile device 5802 via communication channel 5812 so that the function may be completed.

[0422] FIG. 59 shows system 5900 that may include mobile terminal 5902, key 5908, network 5912 and car 5914. A processor of mobile device 5902 may, for example, execute an automobile application (e.g., GUI 5904) that may allow a user of mobile device 5902 to establish wireless link 5910 between car 5914 and mobile device 5902. Accordingly, for example, a user of mobile device 5902 may communicate wireless commands to car 5914 via wireless communication channel 5910.

[0423] A user may, for example, start his or her car from the convenience and warmth of the user's office at

work when temperatures outside may warrant a time period within which car 5914 may need to warm up. Accordingly, for example, a user may start his or her car via commands communicated by a processor of mobile device 5902 to car 5914 prior to leaving the office for the day. In so doing, for example, a processor of mobile device 5902 may require authorization to issue the command, in which case the user may be challenged to present key 5908 within a communication distance from mobile device 5902 to form contactless communication channel 5906. Security credentials may, for example, be communicated from key 5908 to a processor of mobile device 5902 via contactless communication channel 5906 and the processor may compare the received security credentials to security credentials stored within a memory of mobile device 5902 (or a remote authorization server). If a match is found, for example, a processor of mobile device 5902 may be authorized to issue one or more commands 5916 to car 5914.

[0424] A wireless device of car 5914 may, for example, communicate to a processor of mobile device 5902 via communication channel 5910. Accordingly, for example, once a command is authorized and sent to a wireless device of car 5914 by a processor of mobile device 5902, the wireless device of car 5914 may respond with an acknowledgment that the command (e.g., "Start car") was executed. A wireless device of car 5914 may, for example, provide status to a display of mobile device 5902. Accordingly, for example, a wireless device of car 5914 may report a gasoline level status to mobile device 5902 via communication channel 5910 so that the user of mobile device 5902 may know

that leaving car 5914 running for a length of time may deplete the car's gas reserves.

[0425] FIG. 60 shows GUI 6000, that may be generated by a processor of a mobile device and provided onto a display of the mobile device. GUI 6000 may, for example, allow a user of a mobile device to determine how certain functions that may be performed by the mobile device may be authorized. GUI 6000 may, for example, provide authorization options 6002 to determine how the mobile device itself may be authorized for use. A PIN, for example, may be required to be entered in order to activate the mobile device for use. As per another example, a memory of the mobile device may contain information associated with any physical card. Accordingly, for example, authorization to activate the mobile device may require that a user produce a physical card (e.g., a driver's license) that may correspond to a virtual card (e.g., a virtual driver's license) that may be stored within a memory of the mobile device. Alternately, for example, a physical card that corresponds to any virtual card or any virtual bank card stored within a memory of the mobile device may be used to authorize the mobile device for use.

[0426] Banking functions performed by a mobile device may, for example, be authorized as defined by options 6004. A mobile device may, for example, be equipped with scanning capability, such that biometrics (e.g., fingerprints) may be taken from the user of the mobile device and verified before banking functions may be authorized. As per another example, a dynamic security code communicated to a processor of a mobile device by a powered payment card via a contactless

communication channel may authorize banking functions to be performed by the mobile device.

[0427] Functions associated with remote operation of a car may, for example, be authorized as defined by options 6006. A mobile device may, for example, be equipped with a camera, such that only when a picture of an authorized user is taken with the camera and verified by a processor of the mobile device will that user be able to issue remote commands (e.g., unlock driver's door) to the user's car.

[0428] Other functions, such as remote house functions, may be authorized as defined by options 6008. For example, a garage door of a user's house may be commanded to be opened by the user's mobile device, but only if a house key communicates security credentials (e.g., a key code) to a processor of the user's mobile device via a contactless communication channel. Alternately, for example, a user may disable any house functions to be conducted by the user's mobile device.

[0429] FIG. 61 shows flow charts for process sequences 6110-6140. Process sequence 6110 may, for example, execute an authorization setup application (e.g., a GUI) on a mobile device that allows a user of the mobile device to select authorization options (e.g., as in steps 6111-6112) to be enforced by a processor of the mobile device (e.g., as in step 6113). For example, banking functions that may be performed by a mobile device may first require that a physical bank card be placed in proximity to the mobile device so that the physical bank card may communicate security credentials to a processor of the mobile device via a contactless communication channel that may be formed

between the physical banking card and the mobile device. In so doing, for example, a processor of the mobile device may compare the security credentials received from the physical card to security credentials stored within a memory of the mobile device (or remote authorization server). Upon a successful comparison, a processor of a mobile device may authorize banking functions to be performed by the mobile device.

[0430] A memory of a mobile device may, for example, contain a number of virtual cards that may correspond to information communicated to a processor of the mobile device via physical card counterparts to the virtual cards. Such virtual cards may, for example, be selected (e.g., as in step 6121 of sequence 6120) to perform a function in conjunction with the mobile device (e.g., payment information associated with a virtual payment card may be selected to complete a purchase transaction using the mobile device). In step 6122, a user of a mobile device may be required to produce a physical card that corresponds to the selected virtual card. A contactless communication channel (e.g., an RFID communication channel) may be formed between the physical card and the mobile device so that security credentials may be communicated from the physical card to a processor of the mobile device via the contactless communication channel (e.g., as in step 6123). In step 6124, a processor of a mobile device may compare the security credentials to security credentials stored within a memory of the mobile device (or remote authorization server) that corresponds to a physical card. Upon a favorable comparison, a processor of a mobile device may authorize the selected virtual card for use.

[0431] Any function (e.g., non-purchase transactions) that may be performed by a mobile device may be requested (e.g., as in step 6131 of sequence 6130) and challenged (e.g., as in step 6132 of sequence 6130). For example, a processor of a mobile device may be requested to perform any function (e.g., remotely start the engine of a user's car) and a processor of the mobile device may first require security credentials to be presented before the function may be performed. Security credentials may, for example, be any information that may be communicated to a mobile device by a contactless device (e.g., an RFID enabled ignition key) via a contactless communication channel. A processor of the mobile device may authorize the requested function if the security credentials are verified (e.g., as in step 6133) and may deny the requested function if the security credentials are not verified (e.g., as in step 6134).

[0432] In step 6141 of sequence 6140, a user of a mobile device may request a function to be performed by a mobile device. Upon receipt of security credentials communicated by a contactless communication device to a processor of the mobile device (e.g., as in step 6142), the security credentials may be forwarded (e.g., as in step 6143) to a remote authorization server for verification. In step 6144, the remote authorization server may communicate a message to a processor of the mobile device to either grant or deny authorization for the mobile device to perform the requested function.

[0433] FIG. 62 shows card 6200 that may include, for example, a dynamic number that may be entirely, or partially, displayed using a display (e.g., display 6206). A dynamic number may include a permanent

portion such as, for example, permanent portion 6204 and a dynamic portion such as, for example, dynamic portion 6206. Card 6200 may include a dynamic number having permanent portion 6204 and permanent portion 6204 may be incorporated on card 6200 so as to be visible to an observer of card 6200. For example, labeling techniques, such as printing, embossing, laser etching, etc., may be utilized to visibly implement permanent portion 6204.

[0434] Card 6200 may include a second dynamic number that may be entirely, or partially, displayed via a second display (e.g., display 6208). Display 6208 may be utilized, for example, to display a dynamic code such as a dynamic security code. Card 6200 may also include third display 6222 that may be used to display graphical information, such as logos and barcodes. Third display 6222 may also be utilized to display multiple rows and/or columns of textual and/or graphical information.

[0435] Persons skilled in the art will appreciate that any one or more of displays 6206, 6208, and/or 6222 may be implemented as a bi-stable display. For example, information provided on displays 6206, 6208, and/or 6222 may be stable in at least two different states (e.g., a powered-on state and a powered-off state). Any one or more of displays 6206, 6208, and/or 6222 may be implemented as a non-bi-stable display. For example, the display is stable in response to operational power that is applied to the non-bi-stable display. Other display types, such as LCD or electro-chromic, may be provided as well.

[0436] Other permanent information, such as permanent information 6220, may be included within card

6200, which may include user specific information, such as the cardholder's name or username. Permanent information 6220 may, for example, include information that is specific to card 6200 (e.g., a card issue date and/or a card expiration date). Information 6220 may represent, for example, information that includes information that is both specific to the cardholder as well as information that is specific to card 6200.

[0437] Card 6200 may accept user input data via any one or more data input devices, such as buttons 6210-6218. Buttons 6210-6218 may be included to accept data entry through mechanical distortion, contact, or proximity. Buttons 6210-6218 may be responsive to, for example, induced changes and/or deviations in light intensity, pressure magnitude, or electric and/or magnetic field strength. Such information exchange may then be determined and processed by a processor of card 6200 as data input. An RFID chip may, for example, include memory that may be populated with data to be communicated via RFID antenna 6224 when one or more buttons 6210-6218 are pressed. Accordingly, for example, once a button is pressed, RFID data may be loaded into an RFID chip memory and once an RFID communication channel is formed (e.g., once card 6200 is brought within an RFID communication distance of an RFID enabled device) the data in RFID chip memory may be communicated via an RFID communication channel using RFID antenna 6224. Once RFID data is communicated, or after a configurable delay period, the RFID chip memory may be erased.

[0438] FIG. 62 shows architecture 6250, which may include one or more processors 6254. One or more processors 6254 may be configured to utilize external

memory 6252, internal memory of processor 6254, internal memory of RFID chip 6262, or a combination of external memory 6252, internal memory of RFID chip 6262, and internal memory of processor 6254 for dynamically storing information, such as executable machine language, related dynamic machine data, RFID data and user input data values.

[0439] One or more of the components shown in architecture 6250 may be configured to transmit information to processor 6254 and/or may be configured to receive information as transmitted by processor 6254. For example, one or more displays 6256 may be coupled to receive data from processor 6254. The data received from processor 6254 may include, for example, at least a portion of dynamic numbers and/or dynamic codes. The data to be displayed on the display may be displayed on one or more displays 6256.

[0440] One or more displays 6256 may be, for example, touch sensitive and/or proximity sensitive. For example, objects such as fingers, pointing devices, etc., may be brought into contact with displays 6256, or in proximity to displays 6256. Detection of object proximity or object contact with displays 6256 may be effective to perform any type of function (e.g., transmit data to processor 6254). Displays 6256 may have multiple locations that are able to be determined as being touched, or determined as being in proximity to an object.

[0441] Persons skilled in the art will appreciate that a card (e.g., card 6200 of FIG. 62) may, for example, be a self-contained device that derives its own operational power from one or more batteries 6258. Furthermore, one or more batteries 6258 may be

included, for example, to provide operational power for a period of time (e.g., approximately 2-4 years). One or more batteries 6258 may be included, for example, as rechargeable batteries.

[0442] Input and/or output devices may be implemented on architecture 6250. For example, integrated circuit (IC) chip 6260 (e.g., an EMV chip) may be included on architecture 150 to communicate information to a chip reader (e.g., an EMV chip reader) via contacts that may be formed on a surface of a card (e.g., card 6200 of FIG. 62). Other input and/or output devices may be included on architecture 6250, for example, to provide any number of input and/or output capabilities within architecture 6250. For example, other input and/or output devices may include an audio device capable of receiving and/or transmitting audible information. Other input and/or output devices may include a device that exchanges analog and/or digital data using a visible data carrier. Alternately, for example, other input and/or output devices may include a device that is sensitive to a non-visible data carrier, such as an infrared data carrier or electromagnetic data carrier.

[0443] A dynamic magnetic stripe communications device may be included within architecture 6250 to communicate information to, for example, a read-head of a magnetic stripe reader via, for example, electromagnetic signals. For example, electromagnetic field generators 6270-6274 may be included to communicate one or more tracks of electromagnetic data to read-heads of a magnetic stripe reader. Electromagnetic field generators 6270-6274 may include, for example, a series of electromagnetic elements,

where each electromagnetic element may be implemented as a coil wrapped around one or more materials (e.g., a magnetic material and/or a non-magnetic material). Additional materials may be placed outside the coil (e.g., a magnetic material and/or a non-magnetic material).

[0444] Electrical excitation by processor 6254 of one or more coils of one or more electromagnetic elements via, for example, driving circuitry 6264 may be effective to generate electromagnetic fields from one or more electromagnetic elements. One or more electromagnetic field generators 6270-6274 may be utilized to communicate electromagnetic information to, for example, one or more read-heads of a magnetic stripe reader.

[0445] Timing aspects of information exchange between architecture 6250 and the various I/O devices implemented on architecture 6250 may be determined by processor 6254. Detector 6266 may be utilized, for example, to sense the proximity and/or actual contact, of an external device, which in turn, may trigger the initiation of a communication sequence. The sensed presence and/or touch of the external device may then be communicated to a controller (e.g., processor 6254), which in turn may direct the exchange of information with the external device. The sensed presence and/or touch of the external device may be effective to, for example, determine the type of device or object detected.

[0446] For example, the detection may include the detection of, for example, a read-head of a magnetic stripe reader. In response, processor 6254 may activate one or more electromagnetic field generators

6270-6274 to initiate a communications sequence with, for example, one or more read-heads of a magnetic stripe reader. The timing relationships associated with communications between one or more electromagnetic field generators 6270-6274 and one or more read-heads of a magnetic stripe reader may be provided through use of the detection of the magnetic stripe reader.

[0447] Persons skilled in the art will appreciate that processor 6254 may provide user-specific and/or card-specific information through utilization of any one or more of buttons 6210-6218, RFID chip 6262, RFID antenna 6268, IC chip 6260, electromagnetic field generators 6270-6274, and any other input and/or output device. RFID antenna 6268 may, for example, be brought within a communication distance of an RFID enabled device which may be generating a carrier field (e.g., an RF field). In so doing, RFID antenna 6268 may collect energy from the RF field which may then be detected by RFID chip 6262. RFID chip 6262 may, for example, communicate a presence of an RFID communication device to processor 6252. Processor 6252 may, in turn, populate a memory of RFID chip 6262 with user-specific and/or card-specific information (e.g., a payment account number, cardholder name, and a dynamic security code) that may then be communicated to the RFID enabled device via RFID antenna 168.

[0448] RFID antenna 6268 may be configured to receive data from an RFID device (e.g., an RFID tag). Accordingly, for example, RFID chip 6262 may interrogate the capabilities of an RFID device and may receive data from the RFID device upon a determination that the RFID device may communicate data. RFID antenna 6268 may, for example, be provided as two or

more RFID antennas that may be used to enhance RFID data communication and/or reception with an RFID enabled device.

[0449] FIG. 63 shows network topology 6300 that may include, for example, mobile device 6302 (e.g., a mobile telephonic device, a PDA, an electronic tablet, a laptop, a GPS unit, or an MP3 player). Mobile device 6302 may, for example, include a contactless interface that may initiate, sustain, and/or terminate communication channel 6326 between card 6304 and mobile device 6302. Card 6304 and mobile device 6302 may communicate via channel 6326 via a contactless communication medium (e.g., an RF medium).

[0450] Mobile device 6302 may provide one or more transceivers that may communicate with one or more wired networks (e.g., IP network 6312 and/or payment network 6314) and/or one or more wireless networks (e.g., mobile network 6310). Mobile device 6302 may, for example, communicate with a cellular station over a wireless radio interface (e.g., a GSM air interface) that may be used by mobile device 6302 to communicate information (e.g., voice and data) to cellular network access infrastructure 6306 (e.g., one or more GSM base transceiver stations, base station controllers, and mobile switching centers). Persons skilled in the art will appreciate that cellular network access infrastructure 6306 may utilize any multiple access architecture, such as for example, a code-division multiple access architecture and/or a time-division multiple access architecture.

[0451] Mobile device 6302 may, for example, communicate with wireless access point 6308 over a wireless interface (e.g., a Bluetooth interface or a

Wi-Fi interface). Accordingly, for example, mobile device 6302 may access one or more wired networks (e.g., IP network 6312 and/or payment network 6314) and/or one or more wireless networks (e.g., mobile network 6310) without the need to first gain access to cellular network access infrastructure 6306.

[0452] Card 6304 may, for example, be a powered card or a non-powered card (e.g., a powered payment card or a non-powered payment card). Accordingly, for example, payment information (e.g., a payment account number and a card expiration date) may be communicated from card 6304 to mobile device 6302 in support of a financial transaction being conducted by mobile device 6302. In so doing, for example, items for purchase on IP network 6312 (e.g., the internet) may be accessed by a browser of mobile device 6302 via an access point (e.g., wireless access point 6308 or cellular network access infrastructure 6306). Mobile device 6302 may, for example, complete a purchase transaction by first obtaining required payment information from card 6304 and then communicating such payment information to network entities (e.g., payment server 6316 and/or issuer 6320).

[0453] Payment server 6316 may, for example, contact issuer 6320 via a network (e.g., payment network 6314) with payment information received from mobile device 6302 for authorization of a purchase. Once authorized, payment transaction information may be recorded onto a receipt that may be delivered to mobile device 6302 via any one or more delivery options (e.g., via a short messaging service of mobile network 6310 or an email delivery service of IP network 6312). Mobile device 6302 may allow a user to associate purchase categories

(e.g., groceries, auto repair, or entertainment) to purchases transacted by the mobile device so that the user may receive a more detailed accounting of his or her expenditures on his or her receipt. Accordingly, for example, a user may enjoy a higher degree of integration such that a user may customize a level of detail provided on a receipt via mobile device 6302. A payment receipt may, for example, be provided to mobile device 6302 as a proof-of-purchase object (e.g., a barcode) that may be provided to a display of mobile device 6302 and read by other computing equipment (e.g., a barcode scanner) for proof-of-purchase confirmation.

[0454] A device (e.g., mobile device 6328 and/or card 6322) may, for example, include a contactless communication device (e.g., an RFID device) that may initiate, sustain, and/or terminate a contactless communication channel (e.g., an RFID communications channel) with merchant terminal 6318. Accordingly, for example, card 6322 and/or mobile device 6328 may communicate payment information to merchant terminal 6318 to complete a financial transaction. In so doing, for example, mobile device 6328 and/or card 6322 may first receive a request from a user to communicate payment information to merchant terminal 6318.

[0455] As per an example, a user of card 6322 may press a button on card 6322 that may cause payment information to be transferred to a memory of a processor (e.g., an RFID chip). An associated RFID antenna may, for example, sense the presence of merchant terminal 6318 by detecting an RF carrier field that may be generated by an RFID device of merchant terminal 6318. Once the presence of merchant terminal

6318 is sensed, payment information may be transferred from an RFID chip of card 6322 to an RFID antenna of card 6322 to communicate the payment information via an RFID communication channel to merchant terminal 6318 to complete a financial transaction.

[0456] As per another example, card 6322 may be a non-powered card (e.g., a non-powered payment card). Accordingly, for example, card 6322 may include an RFID chip and associated RFID antenna that may be brought within proximity to merchant terminal 6318. An RFID antenna of card 6322 may sense an RF carrier field generated by merchant terminal 6318 and may derive operational power from the RF carrier field. The operational power may, for example, be collected by an RFID antenna of card 6322 and provided to an associated RFID chip of card 6322 in order to energize the RFID chip of card 6322. Once energized, an RFID chip of card 6322 may modulate an RF carrier field generated by merchant terminal 6318 to, for example, communicate payment information from card 6322 to merchant terminal 218 to complete a purchase transaction.

[0457] Any computing device (e.g., desktop computer 6330) may, for example, provide contactless communication electronics (e.g., an RFID reader) that may communicate with a contactless communication device (e.g., card 6332 and/or mobile device 6334). Accordingly, for example, any information that may be communicated by card 6332 (e.g., payment information) may be received by computing device 6330 (e.g., received via an RFID communication channel established between card 6332 and computing device 6330) and forwarded onto a network entity (e.g., issuer 6320 and/or payment server 6316) to complete a purchase

transaction. Persons skilled in the art will appreciate that any RFID information may be exchanged between computing device 6330 and an RFID enabled device (e.g., card 6332 and/or mobile device 6334).

[0458] FIG. 64 shows mobile device 6400. Mobile device 6400 may be any mobile device, such as a mobile telephonic device (e.g., cell phone), a PDA, an electronic tablet, an MP3 player, or a locating device (e.g., a GPS device). Accordingly, mobile device 6400 may be operated in a mobile environment while a user of mobile device 6400 goes about his or her daily activities (e.g., driving, shopping, walking, dining, and exercising). In addition, for example, mobile device 6400 may perform multiple functions simultaneously (e.g., a person may carry on a conversation while at the same time browsing and purchasing products on the internet).

[0459] Mobile device 6400 may include audio processing devices (e.g., microphone 6408 and speaker 6410). Accordingly, for example, mobile device 6400 may receive voice commands from a user via microphone 6408 and may process such commands to perform a function. For example, a user may place mobile device 6400 into a desired operational mode by speaking a command into microphone 6408 that is associated with the desired operational mode. In so doing, for example, mobile device 6400 may engage in hands-free operation by receiving voice commands via microphone 6408 and performing functions associated with the received voice commands.

[0460] Mobile device 6400 may receive data input via microphone 6408. For example, a voice-band modem may generate signals in a voice-band frequency range that

may be received by microphone 6408. A processor of mobile device 6400 may interpret the received audible information as data signals and may process the data signals as, for example, data values and/or control data input.

[0461] Mobile device 6400 may include camera 6402. Camera 6402 may capture one or more frames of video data and store the video data within a memory of mobile device 6400. Accordingly, for example, a processor of mobile device 6400 may receive one or more frames of video information via camera 6402 and may process the video information as data values and/or control data input. In so doing, for example, mobile device 6400 may receive optical information that is sensed by camera 6402 during a series of one or more video capture events that produce one or more frames of video information. The one or more frames of video information may contain one or more data elements (e.g., pixels) having properties (e.g., color, intensity, or contrast) that may be interpreted by a processor of mobile device 6400 as data values and/or control data.

[0462] Mobile device 6400 may include manual input interface 6412. Manual input interface 6412 may, for example, include keys and/or buttons that may be sensitive to manual input, such as a touch or an application of pressure. Accordingly, for example, a user of mobile device 6400 may enter information into mobile device 6400 via manual interface 6412 to cause a processor of mobile device 6400 to enter a particular mode of operation. Manual interface 6412 may, for example, be used for data entry (e.g., dialing a phone number or entering data as may be requested by mobile

device 6400) during a particular mode of operation of mobile device 6400.

[0463] Mobile device 6400 may include display 6404. Display 6404 may provide visible information that may be utilized by a user during interaction with mobile device 6400. A portion or all of display 6404 may be touch sensitive such that objects making contact with display 6404 or objects coming within a proximity of display 6404 may be detected by a processor of mobile device 6400. Accordingly, for example, RFID operations graphical user interface 6406 may be provided by display 6404 so that graphical information may be displayed to solicit and/or receive data entry from a user. In so doing, for example, touch-sensitive graphical user interface devices such as radio buttons, textual input boxes, virtual buttons, pull-down menus, and navigational tools may be used for data entry to initiate, change, and/or support functions performed by mobile device 6400.

[0464] FIG. 64 shows architecture 6450. User interface 6452 may, for example, be included within architecture 6450 to allow user interaction with architecture 6450. For example, a dedicated key pad or keyboard may be included within user interface 6452 to allow alphanumeric data entry into architecture 6450.

[0465] Architecture 6450 may include one or more displays 6454. Display 6454 may, for example, be touch-sensitive. Accordingly, for example, display 6454 may be utilized for alphanumeric data entry using virtual buttons that may be rendered onto touch-sensitive portions of display 6454. In so doing, for example, touching virtual buttons that may be associated with alphabetic and numeric characters of

display 6454 may be detected by processor 6458 as alphanumeric data entry.

[0466] Alphanumeric entry boxes may, for example, be rendered onto display 6454. A user may, for example, activate a cursor within such an alphanumeric entry box by touching an area within the alphanumeric entry box. A user may utilize user interface 6452 and/or a virtual keypad rendered onto display 6454 to select alphanumeric characters to be placed within the alphanumeric entry box in accordance with a character position identified by an activated cursor within the alphanumeric entry box. In so doing, for example, processor 6458 may receive alphanumeric characters as typed into a alphanumeric entry box of display 6454 and may use such alphanumeric characters as data input.

[0467] Display 6454 may, for example, provide data output from architecture 6450. For example, display 6454 may communicate data using a series of light pulses. Accordingly, for example, processor 6458 may cause one or more portions of display 6454 to produce light pulses having varying characteristics (e.g., duration, intensity, and frequency) that may communicate information via such light pulses. In so doing, for example, a device that may be sensitive to light pulses may receive information communicated by display 6454 via light pulses having varying characteristics. Display 6454 may, for example, communicate data using visual information that may be substantially static (e.g., a barcode).

[0468] Architecture 6450 may include one or more transceivers 6456. Transceiver 6456 may communicate information to and/or may receive information from one or more devices. Transceiver 6456 may, for example,

communicate via a wireless interface with one or more cellular stations of a mobile network. Accordingly, for example, transceiver 6456 may allow a mobile device (e.g., mobile device 6400 of FIG. 64) to establish a communications channel with an associated cellular station. In so doing, for example, a mobile device (e.g., mobile device 6400 of FIG. 64) may exchange information (e.g., voice, text, data, or multimedia) with one or more terrestrial networks (e.g., the internet or a payment network) via an associated cellular station. As per another example, transceiver 356 may exchange information with one or more other mobile devices via one or more associated cellular stations.

[0469] Transceiver 6456 may, for example, communicate via a wireless interface with one or more mobile devices directly. Accordingly, for example, transceiver 6456 may communicate with another mobile device without first accessing a mobile network via a cellular station of the mobile network. As per another example, transceiver 6456 may, for example, communicate via a wireless interface with one or more network devices (e.g., a wireless access point) directly. Accordingly, for example, a mobile device (e.g., mobile device 6400 of FIG. 64) may directly connect to a wired and/or a wireless network via any one or more wireless standards (e.g., Bluetooth or Wi-Fi) to exchange information with other devices that may be connected to the wired and/or wireless network. In so doing, for example, a wired and/or wireless network may be accessed by a mobile device without first accessing a mobile network via a cellular station of a mobile network.

[0470] Architecture 6450 may include RFID chip 6464, RFID antenna 6462, and optional RFID antenna 6466 which may combine to communicate with an RFID enabled device via an RFID communication channel. Accordingly, for example, architecture 6450 may be compatible with any RFID device, such as for example, an RFID enabled card, an RFID reader, and an RFID enabled computing device (e.g., an RFID enabled desktop computer). RFID antenna 6466 may, for example, be provided to enhance RFID data communication and/or reception.

[0471] RFID antenna 6462 and/or RFID antenna 6466 may, for example, establish an RF carrier field that may be modulated by an RFID device (e.g., an RFID tag of a non-powered payment card). In so doing, for example, an RFID tag of a non-powered payment card may derive operational power from an RF field provided by RFID antenna 6462 and/or RFID antenna 6466 and may communicate information (e.g., one, two, and/or three tracks of magnetic stripe data) to RFID antenna 6462 and/or RFID antenna 6466 by modulating the RF field produced by RFID antenna 6462 and/or RFID antenna 6466.

[0472] A powered card may, for example, communicate with RFID antenna 6462 and/or RFID antenna 6466. A powered card may, for example, include a processor, a battery, a memory, a wireless communications device (e.g., a powered RFID device) and other electronics (e.g., buttons) that may allow a user to interact with the powered card to perform one or more functions. Accordingly, for example, a powered card may be used to communicate specific information to RFID antenna 6462 and/or RFID antenna 6466 by selective interaction with the buttons of the powered card. In so doing, for example, a powered card may be used to interactively

communicate magnetic stripe information (e.g., one, two, and/or three tracks of magnetic stripe data) to RFID antenna 6462 and/or RFID antenna 6466 by sending a signal to a processor of a powered card (e.g., by pressing a button on the powered card) to initiate such communications.

[0473] RFID chip 6464 may, for example, receive RFID data from processor 6458 and may store such RFID data temporarily. Accordingly, for example, once an RFID communication channel is formed with an RFID enabled device, RFID data contained within RFID chip 6464 may be communicated to the RFID enabled device via RFID antenna 6462 and/or RFID antenna 6466. RFID antennas 6462 and 6466 may, for example, communicate the same RFID data to an RFID enabled device. RFID antennas 6462 and 6466 may, for example, communicate different RFID data sets to an RFID enabled device and the differences between the RFID data sets communicated may provide multiple other channels of data that may be communicated (e.g., an amplitude difference between RFID data sets may be an RFID data channel and a phase difference between RFID data sets may be an additional RFID data channel).

[0474] Architecture 6450 may include memory 6460 and/or processor 6458 may include internal memory. Accordingly, for example, application code may be stored within memory 6460 and/or processor 6458 and executed by processor 6458 in support of functions performed by architecture 6450. For example, an application (e.g., a graphical user interface) may be executed by processor 6458 and displayed onto display 6454, which may be used to interact with a user of a mobile device (e.g., mobile device 6400 of FIG. 64).

Persons skilled in the art will appreciate that executable application code may be communicated to architecture 6450 via any one or more interfaces of architecture 6450 (e.g., user interface 6452, display 6454, transceiver 6456, and/or RFID antennas 6462 and/or 6466).

[0475] Application data (e.g., payment data) may be temporarily stored within RFID chip 6464 and communicated by RFID antenna 6462 and/or RFID antenna 6466 during operation. For example, payment data may be temporarily communicated to RFID chip 6464 by processor 6458 during a financial transaction being conducted via an RFID communication channel between a mobile device (e.g., mobile device 6400 of FIG. 64) and another RFID device (e.g., a merchant terminal). Once RFID data is communicated (or after a configurable delay period has expired), processor 6458 may cause the payment data stored within RFID chip 6464 to be erased so as to reduce an ability of an RFID skimmer to access data from RFID chip 6464.

[0476] FIG. 65 shows card 6500, which may be a powered card and may include, for example, board 6502, board 6504, dynamic magnetic communications device 6506, RFID chip 6518, board 6508, battery 6514, conductive leads 6520-6526 and RFID antenna 6516. Additional circuitry may be provided on board 6502, which may include, for example, processor 6530, an EMV chip, a display, a display driver, driver circuitry for dynamic magnetic stripe communications device 6506, light emitting diodes, light sensors, infrared sensors and transmitters, capacitive sensing contacts, and a user interface (e.g., one or more buttons).

[0477] All boards, circuitry, and other components of card 6500 may be laminated to form card assembly 6510. Such a lamination may, for example, be implemented using a series of lamination process steps, such that an electronics package containing boards 6502, 6504, and/or 6508 and associated electronics may be encapsulated by an injection molding process (e.g., a reaction injection molding process), whereby a silicon-based material or a polyurethane-based material may be injected and cured (e.g., using temperature and/or chemical reaction) to form the electronics package. The electronics package may then be sandwiched between layers of laminate (e.g., layers of polymer laminate). Accordingly, for example, both surfaces of card assembly 6510 may be formed by a layer of laminate such that no electrical contacts exist on either surface of card assembly 6510. Alternately, for example, a surface of card assembly 6510 may be formed by a layer of laminate such that electrical contacts may exist on a surface of card assembly 6510 to provide connectivity from a surface of card assembly 6510 to a processor (e.g., an EMV chip) of card 6500.

[0478] RFID antenna 6516 may, for example, be formed using an additive technique, whereby patterns of a conductive element (e.g., copper) may be applied to a PCB substrate (e.g., applied to either side of board 6508) according to a patterning mask definition layer. RFID antenna 6516 may, for example, be formed using a subtractive technique whereby patterns of a conductive element (e.g., copper) may be removed from a pre-plated PCB substrate (e.g., removed from either side of board 6508) according to an etching mask definition layer. Other non-PCB fabrication techniques may be used to

implement RFID antenna 6516 as may be required by a particular application.

[0479] Conductive leads 6520 and 6522 may, for example, provide electrical conductivity between board 6508 and board 6502. Accordingly, for example, RFID data signals received by RFID antenna 6516 may be communicated to RFID chip 6518 via conductive leads 6520 and 6522. RFID data signals to be communicated by RFID antenna 6516 (e.g., RFID data signals provided to RFID chip 6518 via processor 6530) may, for example, be received from RFID chip 6518 via conductive leads 6520 and 6522. Conductive leads 6524 and 6526 may, for example, provide electrical conductivity between board 6508 and board 6502 so that operational power may be provided to the active electrical components that may exist on board 6502 from battery 6514. Conductive leads 6520-6526, for example, may use conductive adhesive, soldering paste, or any other type of conductive applications to provide electrical conductivity between boards 6508 and 6502.

[0480] FIG. 66 shows card 6600, which may be a powered card and may include, for example, board 6602, board 6604, dynamic magnetic communications device 6606, RFID chip 6618, board 6608, battery 6614, conductive leads 6620-6626 and RFID antenna 6616. Additional circuitry may be provided on board 6602, which may include, for example, processor 6630, an EMV chip, a display, a display driver, driver circuitry for dynamic magnetic stripe communications device 6606, light emitting diodes, light sensors, infrared sensors and transmitters, capacitive sensing contacts, and a user interface (e.g., one or more buttons). All boards, circuitry, and other components of card 6600

may, for example, be encapsulated by an injection molding process and sandwiched between two layers of laminate to form card assembly 6610 having no exposed contacts. Alternately, for example, a surface of card assembly 6610 may be formed by a layer of laminate such that electrical contacts may exist on a surface of card assembly 6610 to provide connectivity from a surface of card assembly 6610 to a processor (e.g., an EMV chip) of card 6600.

[0481] RFID antenna 6616 may, for example, be formed using additive and/or subtractive techniques to define patterns of a conductive element (e.g., copper) to form RFID antenna 6616 (e.g., on either side of board 6604). Conductive leads 6620 and 6622 may, for example, provide electrical conductivity between board 6604 and board 6602. Accordingly, for example, RFID data signals received by RFID antenna 6616 may be communicated to RFID chip 6618 via conductive leads 6620 and 6622. RFID data signals to be communicated by RFID antenna 6616 (e.g., as may be provided to RFID chip 6618 by processor 6630) may be received from RFID chip 6618 via conductive leads 6620 and 6622. Conductive leads 6624 and 6626 may, for example, provide electrical conductivity between board 6608 and board 6602 so that operational power may be provided to the active electrical components that may exist on board 6602 from battery 6614.

[0482] FIG. 67 shows card 6700, which may be a powered card and may include, for example, board 6702, board 6704, dynamic magnetic communications device 6706, RFID chip 6718, board 6708, battery 6714, conductive leads 6722-6726 and RFID antenna 6716. Additional circuitry may be provided on board 6702,

which may include, for example, processor 6730, an EMV chip, a display, a display driver, driver circuitry for dynamic magnetic stripe communications device 6706, light emitting diodes, light sensors, infrared sensors and transmitters, capacitive sensing contacts, and a user interface (e.g., one or more buttons). All boards, circuitry, and other components of card 6700 may, for example, be encapsulated by an injection molding process and sandwiched between two layers of laminate to form card assembly 6710 having no exposed contacts. Alternately, for example, a surface of card assembly 6710 may be formed by a layer of laminate such that electrical contacts may exist on a surface of card assembly 6710 to provide connectivity from a surface of card assembly 6710 to a processor (e.g., an EMV chip) of card 6700.

[0483] RFID antenna 6716 may, for example, be formed using additive and/or subtractive techniques to define patterns of a conductive element (e.g., copper) to form RFID antenna 6716 (e.g., on either side of board 6704). One or more conductive leads 6722 may, for example, provide electrical conductivity between RFID chip 6718 of board 6704 and processor 6730 of board 6702. Accordingly, for example, while data exchanged between RFID chip 6718 and RFID antenna 6716 may remain on board 6704, one or more conduction paths 6722 may be provided so that data that is to be communicated by RFID antenna 6716 may first be communicated to RFID chip 6718 by processor 6730 that may exist, for example, on board 6702. Conductive leads 6724 and 6726 may, for example, provide electrical conductivity between board 6708 and board 6702 so that operational power may be provided to the active electrical

components that may exist on boards 6702 and 6704 from battery 6714.

[0484] FIG. 68 shows card 6800, which may be a powered card and may include, for example, board 6802, board 6804, dynamic magnetic communications device 6806, RFID chip 6818, board 6808, battery 6814, conductive leads 6824-6826 and RFID antenna 6816. Additional circuitry may be provided on board 6802, which may include, for example, processor 6830, an EMV chip, a display, a display driver, driver circuitry for dynamic magnetic stripe communications device 6806, light emitting diodes, light sensors, infrared sensors and transmitters, capacitive sensing contacts, and a user interface (e.g., one or more buttons). All boards, circuitry, and other components of card 6800 may, for example, be encapsulated by an injection molding process and sandwiched between two layers of laminate to form card assembly 6810 having no exposed contacts. Alternately, for example, a surface of card assembly 6810 may be formed by a layer of laminate such that electrical contacts may exist on a surface of card assembly 6810 to provide connectivity from a surface of card assembly 6810 to a processor (e.g., an EMV chip) of card 6800.

[0485] RFID antenna 6816 may, for example, be formed using additive and/or subtractive techniques to define patterns of a conductive element (e.g., copper) to form RFID antenna 6816 (e.g., on a top side of board 6802). Accordingly, for example, RFID antenna 6816 may be applied to board 6802 at a location proximate to a location of board 6804. In so doing, for example, RFID antenna 6816 may be applied to board 6802 below a location where board 6804 attaches to board 6802 and

conduction paths may be extended to RFID chip 6818 from RFID antenna 6816 (e.g., via conductive traces on board 6802). Conductive leads 6824 and 6826 may, for example, provide electrical conductivity between board 6808 and board 6802 so that operational power may be provided to the active electrical components that may exist on board 6802 from battery 6814. Persons skilled in the art will appreciate that RFID antenna 6816 may be placed anywhere on any board (e.g., around a perimeter of board 6802) so as to maximize an effectiveness of RFID antenna 6816.

[0486] Persons skilled in the art will further appreciate that any combination of processors, EMV chips, display drivers, dynamic magnetic stripe communications device drivers, RFID chips, and associated circuitry may be combined into one or more application specific integrated circuits (ASIC). Accordingly, for example, a core processor may interoperate with an ASIC that combines the functionalities of an RFID chip, a dynamic magnetic stripe communications device driver, and a display driver. Alternately, for example, a core processor, RFID chip, a dynamic magnetic stripe communications device driver, a display driver and associated electronics may be consolidated into a single ASIC. As per another example, a core processor and an RFID chip may be provided as discrete components that may interoperate with an ASIC that may be dedicated to dynamic magnetic stripe communications device driver functions and another ASIC that may be dedicated to display driver functions.

[0487] FIG. 69 shows card 6900, which may include multiple RFID antennas (e.g., RFID antennas 6902-6904)

and associated RFID chips (e.g., RFID chips 6906-6908). Additional circuitry may be provided on card 6900, which may include, for example, a processor, an EMV chip, a display, a display driver, driver circuitry for a dynamic magnetic stripe communications device, light emitting diodes, light sensors, infrared sensors and transmitters, capacitive sensing contacts, and a user interface (e.g., one or more buttons). All boards, circuitry, and other components of card 6900 may, for example, be encapsulated by an injection molding process and sandwiched between two layers of laminate to form card assembly 6912 having no exposed contacts. Alternately, for example, a surface of card assembly 6912 may be formed by a layer of laminate such that electrical contacts may exist on a surface of card assembly 6912 to provide connectivity from a surface of card assembly 6912 to a processor (e.g., an EMV chip) of card 6900.

[0488] Processor 6910 may, for example, provide data to RFID chips 6906 and/or 6908 that may be communicated by RFID antenna 6902 and/or RFID antenna 6904, respectively. Processor 6910 may, for example, receive data from RFID chips 6906 and/or 6908 that may be received by RFID antenna 6902 and/or RFID antenna 6904, respectively.

[0489] Card 6900 may, for example, be placed within a communication distance of one or more RFID devices (e.g., one or more RFID enabled merchant terminals) in order to conduct a purchase transaction. Accordingly, for example, processor 6910 may communicate track 1 and track 2 magnetic stripe data to the RFID enabled merchant terminal via RFID chip 6906 and associated RFID antenna 6902. Alternately, for example, processor

6910 may communicate track 1 and track 2 magnetic stripe data to the RFID enabled merchant terminal via RFID chip 6908 and associated RFID antenna 6904.

[0490] As per another example, processor 6910 may utilize both RFID antennas 6902 and 6904 and associated RFID chips 6906 and 6908, respectively, to increase communication efficiency. Accordingly, for example, processor 6910 may communicate track 1 magnetic stripe data to RFID chip 6906 and track 2 magnetic stripe data to RFID chip 6908, so that track 1 magnetic stripe data may be communicated to an RFID enabled merchant terminal via RFID antenna 6902 and track 2 magnetic stripe data may be communicated to an RFID enabled merchant terminal via RFID antenna 6904. In so doing, for example, two tracks of magnetic stripe data may be communicated in half the time.

[0491] As per yet another example, RFID data communicated to RFID chips 6906 and 6908 by processor 6910 may be communicated in a fashion such that multiple channels of information may be communicated in addition to the first and second channels of information communicated by RFID chips 6906 and 6908. For example, phase, frequency, and/or amplitude differences between data communicated by RFID chip 6906/RFID antenna 6902 and data communicated by RFID chip 6908/RFID antenna 6904 may be used to communicate multiple channels of information. Accordingly, for example, a first set of information may be communicated by RFID chip 6906/RFID antenna 6902, a second set of information may be communicated by RFID chip 6908/RFID antenna 6904, and a third set of information may be communicated as an amplitude difference between each data element of the first and second information sets.

A fourth set of information may be communicated, for example, as a phase difference between each data element of the first and second data sets. A fifth set of information may be communicated, for example, as a rate of change of the phase difference (e.g., frequency difference) between each data element of the first and second information sets. Persons skilled in the art will appreciate that any number of channels of information may be communicated by a pair of RFID communicators when differences between RFID data sets communicated by each RFID communicator are exploited as data channels.

[0492] A pair of RFID communicators may, for example, be used to increase accuracy of RFID data communicated. For example, the same RFID data may be communicated by RFID chip 6906/RFID antenna 6902 as is communicated by RFID chip 6908/RFID antenna 6904 so as to increase a probability that an RFID reader may receive RFID data that was intended to be communicated. Accordingly, for example, an RFID reader that may be spatially oriented such that data reception quality from a first RFID communicator is diminished in relation to a data reception quality from a second RFID communicator, may nevertheless receive a complete set of RFID data due to the redundant RFID communication configuration.

[0493] An RFID reader may, for example, employ collision avoidance algorithms, so that communications received from a first RFID communicator do not trump communications received from a second RFID communicator. Accordingly, for example, processor 6910 of card 6900 may communicate to such an RFID reader that dual RFID communicators may be present within card

6900. In so doing, for example, the RFID reader may activate its collision avoidance algorithm to accept RFID communications from both RFID communicators (e.g., RFID chip 6906/RFID antenna 6902 and RFID chip 6908/RFID antenna 6904) simultaneously.

[0494] RFID data may, for example, be received by RFID chip 6906/RFID antenna 6902 and RFID chip 6908/RFID antenna 6904. Accordingly, for example, card 6900 may be an RFID reader that may utilize a pair of RFID readers (e.g., a first RFID reader is provided by RFID chip 6906/RFID antenna 6902 and a second RFID reader is provided by RFID chip 6908/RFID antenna 6904). In so doing, for example, processor 6910 may impose an RFID communication protocol that accepts RFID data form each RFID reader simultaneously.

[0495] FIG. 70 shows card 7000 that may include, for example, configuration 7002. Configuration 7002 may include, for example, button 7004, button 7008, display 7006 and display 7010. Button 7004 may be associated with display 7006. Button 7004 may be pressed to utilize the option described by display 7006. Button 7008 may be associated with display 7010. Button 7008 may be pressed to utilize the option described by display 7010. A card may include additional buttons or displays or may not include the number of buttons or displays of card 7000. For example, a card may include only a single button (e.g., button 7004).

[0496] A user of card 7000 may, for example, select options 7006 or 7010 when card 7000 is to be used (e.g., when card 7000 is to be utilized at a point-of-sale terminal to complete a purchase transaction). Accordingly, for example, a user of card 7000 may press button 7004 to select option 7006 if the user wishes to

exchange RFID data between card 7000 and an RFID device. Alternately, for example, a user of card 7000 may press button 7008 to select option 7010 if the user wishes to communication information to a magnetic stripe reader.

[0497] A user may, for example, press button 7008 to prepare card 7000 for communications with a magnetic stripe reader. Accordingly, for example, a processor of card 7000 may initiate a mode of operation upon activation of option 7010, whereby the processor searches for the presence of a read-head housing of a magnetic stripe reader. Once option 7010 is activated, a user may bring card 7000 within a communication distance of a magnetic stripe reader (e.g., the user may swipe card 7000 through a magnetic stripe reader). Upon the detection of the read-head housing of the magnetic stripe reader, the processor may communicate one, two, and/or three tracks of magnetic stripe data to a read-head of the detected magnetic stripe reader via dynamic magnetic stripe communications device 7014.

[0498] Alternately, for example, a user may press button 7004 to prepare card 7000 for communication with an RFID device. Accordingly, for example, a processor of card 7000 may initiate a mode of operation upon activation of option 7006, whereby a processor of card 7000 provides magnetic stripe information (e.g., one, two, and/or three tracks of magnetic stripe data) to an RFID chip of card 7000. Once option 7006 is activated, a user may bring card 7000 within a communication distance of an RFID reader (e.g., the user may wave card 7000 within an RFID communication distance of an RFID reader) and an RFID communication sequence between card 7000 and an RFID reader may be completed where

RFID data may be provided to RFID antenna 7012 from an RFID chip on card 7000 and communicated from RFID antenna 7012 to the RFID reader.

[0499] Upon activation of option 7006, a processor of card 7000 may activate passive RFID communications or active RFID communications using RFID antenna 7012 and an associated RFID chip. Passive RFID communications, for example, may require little or no energy to be expended by card 7000. Instead, RFID antenna 7012 may collect energy from an RFID reader when a user of card 7000 brings card 7000 within a communication distance of the RFID reader. The energy collected by RFID antenna 7012 may, for example, provide power to an RFID chip of card 7000. In so doing, for example, an RFID chip of card 7000 may communicate with a processor of card 7000, so that the processor may populate a memory of the RFID chip with information (e.g., payment information) that may be needed to complete a transaction (e.g., a purchase transaction). Once populated with information, the RFID chip of card 7000 may communicate the information to RFID antenna 7012, which may then communicate the information to the RFID reader.

[0500] Active RFID communications from card 7000 may, for example, utilize battery power from within card 7000. Accordingly, for example, once card 7000 is brought within a communication distance of an RFID reader, RFID antenna 7012 may detect the RFID reader and may wake an RFID chip from a low-power state. In so doing, for example, an RFID antenna 7012 may detect energy from an RFID reader and an RFID chip of card 7000 may utilize battery power of card 7000 to receive information from a processor of card 7000 and to

provide the received information to RFID antenna 7012 for subsequent communication to an RFID reader.

[0501] Card 7000 may, for example, operate as an RFID reader, such that when brought within a communication distance of another RFID device, an RFID chip of card 7000 may interrogate the RFID device to determine whether the RFID device is to receive information from card 7000 (e.g., the RFID device is operating as an RFID reader) or whether the RFID device is to communicate information to card 7000 (e.g., the RFID device is operating as an RFID tag). Accordingly, for example, an RFID chip of card 7000 may interrogate the RFID device to determine that the RFID device is an RFID tag an that RFID data may be communicated from the RFID device to an RFID chip of card 7000. In so doing, for example, an RFID chip of card 7000 may receive information, such as executable machine code, payment information, or any other type of information that may be required by card 7000 to operate as intended and may forward such information to a processor of card 7000 to be stored within a memory of card 7000. As per one example, an RFID chip of card 7000 may receive personalization information (e.g., cardholder information and cardholder account information) to prepare card 7000 for use as a payment card.

[0502] FIG. 71 shows system 7100, which may include card 7102 and one or more RFID devices (e.g., mobile devices 7104 and 7106). Card 7102 may, for example, communicate with multiple RFID devices simultaneously. A user of card 7102 may, for example, enable RFID communications with card 7102 by pressing one of buttons 7112 or 7114. Accordingly, for example, payment information (e.g., payment account number and

cardholder name) may be communicated from a core processor within card 7102 and stored within one or more RFID chips of card 7102. Data indicative of which button was pushed (e.g., discretionary data indicative of either credit button 7112 or debit button 7114) may also be communicated and stored within the one or more RFID chips of card 7102.

[0503] As per one example, card 7102 may provide two RFID communication devices that may detect an RF carrier field that may be generated by each of mobile devices 7104 and 7106. Users of mobile devices 7104 and 7106 may, for example, be husband and wife who may wish to store payment information associated with card 7102 on respective memory locations of mobile devices 7104 and 7104 so that such payment information may be used to complete purchase transactions using mobile devices 7104 and 7106.

[0504] A first RFID communication device of card 7102 may establish RFID communication channel 7110 with an RFID reader of mobile device 7104 and a second RFID communication device of card 7102 may establish communication channel 7108 with an RFID reader of mobile device 7106. Accordingly, for example, the first and second RFID communication devices of card 7102 may communicate payment information temporarily stored within an RFID chip of each respective RFID communication device of card 7102. In so doing, for example, mobile devices 7104 and 7106 may store payment information communicated via RFID communication channels 7110 and 7108, respectively, within respective memory locations of mobile devices 7104 and 7106. Mobile devices 7104 and 7106 may later recall such payment information from their respective memory

locations, communicate the stored payment information via channels 7116 and 7118, respectively, of payment network 7120, and complete payment transactions with network entity 7122 using payment information received from card 7102.

[0505] FIG. 72 shows system 7200, which may include mobile device 7202, a stationary device (e.g., desktop computer 7204), payment network 7206, and network entity 7208. An application (e.g., RFID operations GUI 7212) may be executed by a processor of mobile device 7202 and may, for example, report a detection of an RFID device to a display of mobile device 7202. Such an RF device may, for example, include any device (e.g., desktop computer 7204) that may be RFID equipped. An RFID antenna and associated RFID chip may, for example, exist within desktop computer 7204 such that when mobile device 7202 is brought within an RFID communication distance of desktop computer 7204, an RFID antenna of mobile device 7202 may detect its presence, report the same to an RFID chip within mobile device 7202, which may then be reported to a processor of mobile device 7202 and reported to a user of mobile device 7202 via GUI 7212.

[0506] GUI 7212 may, for example, ask the user of mobile device 7202 whether he or she wishes to allow an RFID connection between mobile device 7202 and desktop computer 7204. The user may indicate his or her wish via radio buttons 7214 and may also indicate whether information (e.g., payment information) stored within a memory of mobile device 7202 is to be communicated to desktop computer 7204 via an RFID communication channel previously authorized by the user of mobile device 7202 (e.g., by selecting one of radio buttons 7216). If so,

then such information may be communicated to desktop computer 7204 by mobile device 7202 and stored within a memory of desktop computer 7204. In so doing, for example, payment information communicated by mobile device 7202 to desktop computer 7204 may subsequently be communicated by desktop computer 7204 via communication channel 7210 of payment network 7206 to complete a purchase transaction (e.g., an online purchase of items contained within a shopping cart generated by an internet browser of desktop computer 7204) via network entity 7208.

[0507] A flow diagram of communication sequences is shown in FIG. 73. Step 7311 of sequence 7310 may, for example, include activating an RFID search within a card. Accordingly, for example, a user interface (e.g., one or more buttons) of a card may be associated with a communication feature on the card, whereby pressing one of the buttons may activate an RFID communication device on the card. In step 7312, an RFID device may be detected by the card and an RFID connection may be established between the card and the RFID device. RFID data may, for example, be transferred to an RFID chip on the card (e.g., as in step 7313) and the RFID data contained within an RFID chip on the card may, for example, be communicated via an RFID antenna on the card to the RFID device (e.g., as in step 7314). Once RFID data is communicated, RFID data contained within an RFID chip on the card may be erased so as to reduce a likelihood of skimming RFID data from the RFID chip on the card.

[0508] Step 7321 of sequence 7320 may, for example, include activating an RFID search within a mobile device. Accordingly, for example, a user interface

(e.g., a GUI executing on a processor of the mobile device) may be associated with a communication feature on the mobile device, whereby interfacing with the GUI may activate an RFID communication channel between a detected RFID device and the mobile device (e.g., as in step 7322). In step 7323, RFID data may, for example, be transferred to an RFID chip on the mobile device and the RFID data contained within an RFID chip on the mobile device may, for example, be communicated via an RFID antenna on the mobile device to the RFID device (e.g., as in step 7324). Once RFID data is communicated, RFID data contained within an RFID chip on the mobile device may be erased so as to reduce a likelihood of skimming RFID data from the RFID chip on the mobile device.

[0509] Step 7331 of sequence 7330 may, for example, include transferring RFID data from a core processor to an RFID chip on a card or a mobile device in preparation for communicating the RFID data via an RFID antenna on the card or the mobile device. If a timeout period that may be set in step 7332 expires before the RFID data is communicated by the card or mobile device (e.g., as in step 7333), then RFID data previously transferred to the RFID chip may be erased from the RFID chip by the core processor.

[0510] Step 7341 of sequence 7340 may, for example, include transferring RFID data from a core processor to an RFID chip on a card or a mobile device in preparation for communicating the RFID data via two RFID antennas on the card or the mobile device. In step 7342, the same data may be transferred to both RFID antennas. Alternately, for example, different data may be transferred each RFID antenna. In step

7343, both RFID antennas may communicate data to an RFID reader. As per one example, the same data may be communicated by both RFID antennas so as to increase a reliability of data communication. As per another example, different data may be communicated by each RFID antenna in order to increase an efficiency of data communication. As per yet another example, different data may be communicated by each RFID antenna, where differences (e.g., phase, frequency, and/or amplitude) may be used to communicate multiple other data channels.

[0511] Persons skilled in the art will appreciate that the present invention is not limited to only the embodiments described. Instead, the present invention more generally involves mobile information and the exchange thereof. Persons skilled in the art will also appreciate that the apparatus of the present invention may be implemented in other ways than those described herein. All such modifications are within the scope of the present invention, which is limited only by the claims that follow.

What is claimed is:

1. A method, comprising:

accessing a network using a mobile device;

selecting an object for purchase from said network using said mobile device;

communicating payment information from a payment card to said mobile device using a contactless communication channel; and

communicating said payment information from said mobile device to said network to complete a purchase transaction for said object.

2. A method, comprising:

communicating source account information to a first mobile device using a first contactless communication channel;

communicating target account information to a second mobile device using a second contactless communication channel;

communicating said target account information from said second mobile device to said first mobile device; and

coordinating a money transfer from said source account into said target account using said first mobile device.

3. The method of claim 1, wherein said mobile device is a laptop computer.

4. The method of claim 1, wherein said mobile device is a PDA.

5. The method of claim 1, wherein said mobile device is a phone.

6. The method of claim 1, wherein said contactless communication channel is an RFID communication channel.

7. The method of claim 1, wherein said mobile device and said payment card are brought within a proximity distance of up to two inches to establish said contactless communication channel.

8. The method of claim 1, wherein said payment card is a powered card.

9. The method of claim 1, wherein said payment card is a non-powered card.

10. The method of claim 1, wherein said payment card simulates a series of touches to a display of said mobile device to establish at least a portion of said contactless communication channel.

11. The method of claim 1, wherein said mobile device communicates an optical data stream to said payment card to establish at least a portion of said contactless communication channel.

12. The method of claim 2, wherein a powered card communicates said target account information.

13. The method of claim 2, wherein a non-powered card communicates said target account information.

14. The method of claim 2, wherein a powered card communicates said source account information.

15. The method of claim 2, wherein a non-powered card communicates said source account information.

16. The method of claim 2, wherein said first mobile device is a laptop computer.

17. The method of claim 2, wherein said first mobile device is a PDA.

18. The method of claim 2, wherein said first mobile device is a phone.

19. The method of claim 2, wherein said second mobile device is a laptop computer.

20. The method of claim 2, wherein said second mobile device is a PDA.

21. The method of claim 2, wherein said second mobile device is a phone.

22. A method, comprising:

establishing a contactless communication channel between one or more physical cards and a mobile device;

communicating information from said physical card to said mobile device using said contactless communication channel;

creating a mobile wallet of virtual cards within a memory of said mobile device from said communicated information; and

selecting one of said virtual cards to complete a purchase transaction using said mobile device.

23. The method of claim 22, wherein said mobile device is a laptop.

24. The method of claim 22, wherein said mobile device is a PDA.

25. The method of claim 22, wherein said mobile device is a phone.

26. The method of claim 22, wherein said mobile device is an MP3 device.

27. The method of claim 22, wherein said mobile device is a GPS device.

28. The method of claim 22, wherein said physical card is a non-powered card.

29. The method of claim 22, wherein said physical card is a powered card.

30. The method of claim 22, wherein said contactless communication channel is an RFID communication channel.

31. The method of claim 22, wherein said mobile device and said physical card are brought within a proximity distance of up to two inches to establish said contactless communication channel.

32. The method of claim 22, wherein said physical card simulates a series of touches to a display of said mobile device to establish at least a portion of said contactless communication channel.

33. The method of claim 22, wherein said mobile device communicates an optical data stream to said physical card to establish at least a portion of said contactless communication channel.

34. The method of claim 22, wherein establishing said contactless communication channel comprises entering a PIN associated with said physical card to authorize said communicated information.

35. The method of claim 22, wherein said communicated information is selected based on manual input entered into said physical card.

36. The method of claim 22, wherein said communicated information includes payment information associated with a first payment account selected by pressing a first button of said physical card.

37. The method of claim 22, wherein said virtual cards include gift cards.

38. The method of claim 22, wherein said mobile device includes a graphical user interface to modify a visual appearance of said virtual cards as displayed by said mobile device.

39. The method of claim 22, wherein said communicated information is used to create a visual appearance of said virtual cards as displayed by said mobile device.

40. The method of claim 22, wherein said virtual cards are sorted onto a display of said mobile device based on manual input selection received by a graphical user interface of said mobile device.

41. The method of claim 22, wherein completing said purchase transaction includes establishing a second contactless communication channel between said mobile device and a merchant terminal and communicating payment information associated with said selected virtual card to said merchant terminal via said second contactless communication channel.

42. A method, comprising:

executing an application on a processor of a mobile device to perform a function;

communicating information to said mobile device from a contactless device using a contactless communication channel;

confirming said communicated information matches at least a portion of predetermined information; and

executing said function from said mobile device based on said confirmation.

43. The method of claim 42, wherein said mobile device is a laptop.

44. The method of claim 42, wherein said mobile device is a PDA.

45. The method of claim 42, wherein said mobile device is a phone.

46. The method of claim 42, wherein said mobile device is an MP3 device.

47. The method of claim 42, wherein said mobile device is a GPS device.

48. The method of claim 42, wherein said contactless device is a non-powered card.

49. The method of claim 42, wherein said contactless device is a powered card.

50. The method of claim 42, wherein said contactless device is an automobile key.

51. The method of claim 42, wherein said contactless device is a home door key.

52. The method of claim 42, wherein said contactless device is a key to a safe deposit box.

53. The method of claim 42, wherein said contactless communication channel is an RFID communication channel.

54. The method of claim 42, wherein a camera of said mobile device establishes said contactless communication channel.

55. The method of claim 42, wherein said contactless device is a powered card, said mobile device and said powered card being brought within a proximity distance of up to two inches to establish said contactless communication channel.

56. The method of claim 42, wherein said contactless device is a powered card, said powered card simulating a series of touches to a display of said mobile device to establish at least a portion of said contactless communication channel.

57. The method of claim 42, wherein said contactless device is a powered card, said mobile device communicating an optical data stream to said powered card to establish at least a portion of said contactless communication channel.

58. The method of claim 42, wherein said predetermined information exists on a memory of said mobile device.

59. The method of claim 42, wherein said predetermined information exists on a memory of a remote authorization server.

60. The method of claim 42, wherein said contactless device is a non-powered card, said non-powered card providing said communicated information to authorize a purchase transaction based on payment account information associated with said non-powered card.

61. The method of claim 42, wherein said function is executed by a device external to said mobile device.

62. A card, comprising:

a first board including a first RFID chip and a first RFID antenna; and

a second board including a processor, wherein first data is transferred from said processor to said first RFID chip via conductive terminals between said first and second boards and wherein said first data is communicated from said first RFID chip to a first RFID communication channel via said first RFID antenna.

63. A card, comprising:

a first board including a first RFID antenna; and

a second board including a first RFID chip and a processor, wherein first data is transferred from said processor to said RFID chip and wherein said first data is communicated from said first RFID chip to a first RFID communication channel via said first RFID antenna.

64. The card of claim 62, further comprising a second RFID antenna, wherein second data is transferred from said processor to a second RFID chip via conductive terminals between said first and second boards and wherein said second data is communicated from said second RFID chip to a second RFID communication channel via said second RFID antenna, said first and second data being the same.

65. The card of claim 62, further comprising a second RFID antenna, wherein second data is transferred from said processor to a second RFID chip via conductive terminals between said first and second boards and wherein said second data is communicated from said second RFID chip to a second RFID communication channel

via said second RFID antenna, said first and second data being different.

66. The card of claim 62, further comprising a second RFID antenna, wherein second data is transferred from said processor to a second RFID chip via conductive terminals between said first and second boards and wherein said second data is communicated from said second RFID chip to a second RFID communication channel via said second RFID antenna, wherein a difference between said first and second data forms information for a third RFID communication channel.

67. The card of claim 62, further comprising a second RFID antenna, wherein second data is transferred from said processor to a second RFID chip via conductive terminals between said first and second boards and wherein said second data is communicated from said second RFID chip to a second RFID communication channel via said second RFID antenna, wherein a first difference between said first and second data forms information for a third RFID communication channel and a second difference between said first and second data forms information for a fourth RFID communication channel.

68. The card of claim 62, wherein said first data is erased from said first RFID chip after said first data is communicated from said first RFID chip to said first RFID communication channel.

8. The card of claim 1, wherein said first data is erased from said first RFID chip after a delay period has expired.

69. The card of claim 62, wherein said first and second boards are encapsulated, said encapsulation being laminated between first and second lamination layers.

70. The card of claim 62, further comprising a dynamic magnetic stripe communications device.

71. The card of claim 63, further comprising a second RFID antenna, wherein second data is transferred from said processor to a second RFID chip and wherein said second data is communicated from said second RFID chip to a second RFID communication channel via said second RFID antenna, said first and second data being the same.

72. The card of claim 63, further comprising a second RFID antenna, wherein second data is transferred from said processor to a second RFID chip and wherein said second data is communicated from said second RFID chip to a second RFID communication channel via said second RFID antenna, said first and second data being different.

73. The card of claim 63, further comprising a second RFID antenna, wherein second data is transferred from said processor to a second RFID chip and wherein said second data is communicated from said second RFID chip to a second RFID communication channel via said second RFID antenna, wherein a first difference between said first and second data forms information for a third RFID communication channel.

74. The card of claim 63, further comprising a second RFID antenna, wherein second data is transferred from said processor to a second RFID chip and wherein said second data is communicated from said second RFID chip to a second RFID communication channel via said second RFID antenna, wherein a first difference between said first and second data forms information for a third RFID communication channel and a second difference between said first and second data forms information for a fourth RFID communication channel.

75. The card of claim 63, wherein said first data is erased from said first RFID chip after said first data is communicated from said first RFID chip to said first RFID communication channel.

76. The card of claim 63, wherein said first data is erased from said first RFID chip after a delay period has expired.

77. The card of claim 63, wherein said first and second boards are encapsulated, said encapsulation being laminated between first and second lamination layers.

78. The card of claim 63, further comprising a dynamic magnetic stripe communications device.

79. A method comprising:

communicating first data from a device to a reader via a first RFID communication channel;

communicating second data from said device to said reader via a second RFID communication channel;

receiving said first and second data via said reader; and

avoiding collisions between said first and second data within said reader.

80. The method of claim 79, wherein said first and second data are different.

81. A system, comprising:

means for accessing a network;

means for selecting an object for purchase from said network;

means for communicating payment information from a payment card to a mobile device; and

means for communicating said payment information from said mobile device to a network to complete a purchase transaction for said object.

82. A system, comprising:

means for communicating source account information to a first mobile device;

means for communicating target account information to a second mobile device;

means for communicating said target account information from said second mobile device to said first mobile device; and

means for coordinating a money transfer from said source account into said target account.

83. A system, comprising:

means for establishing a contactless communication channel between one or more physical cards and a mobile device;

means for communicating information from said physical card to said mobile device using said contactless communication channel;

means for creating a mobile wallet of virtual cards within a memory of said mobile device from said communicated information; and

means for selecting one of said virtual cards to complete a purchase transaction using said mobile device.

84. A system, comprising:

means for executing an application on a mobile device to perform a function;

means for communicating information to said mobile device from a contactless device;

means for confirming said communicated information matches at least a portion of predetermined information; and

means for executing said function from said mobile device based on said confirmation.

1/73

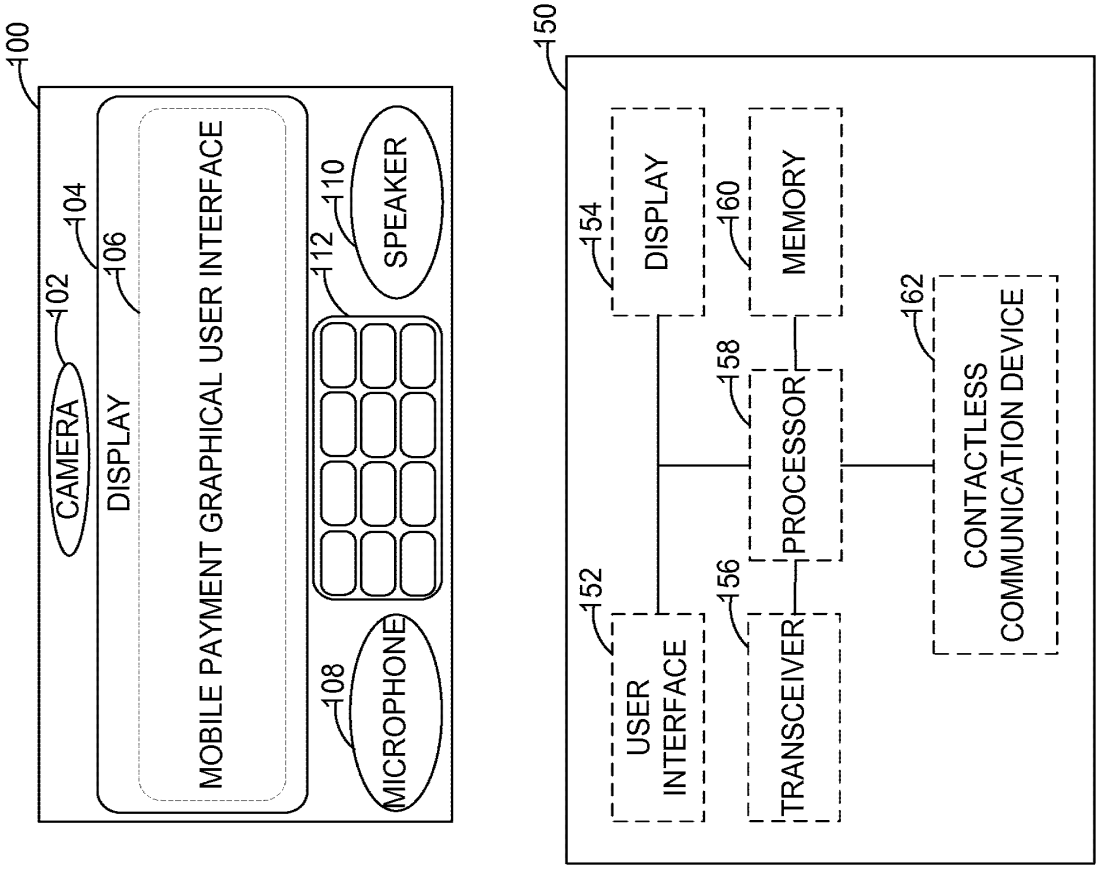

100
CAMERA
102
DISPLAY
104
MOBILE PAYMENT GRAPHICAL USER INTERFACE
106
MICROPHONE
108
SPEAKER
110
112
150
USER INTERFACE
152
TRANSCEIVER
156
PROCESSOR
158
DISPLAY
154
MEMORY
160
CONTACTLESS COMMUNICATION DEVICE
162

FIG. 1

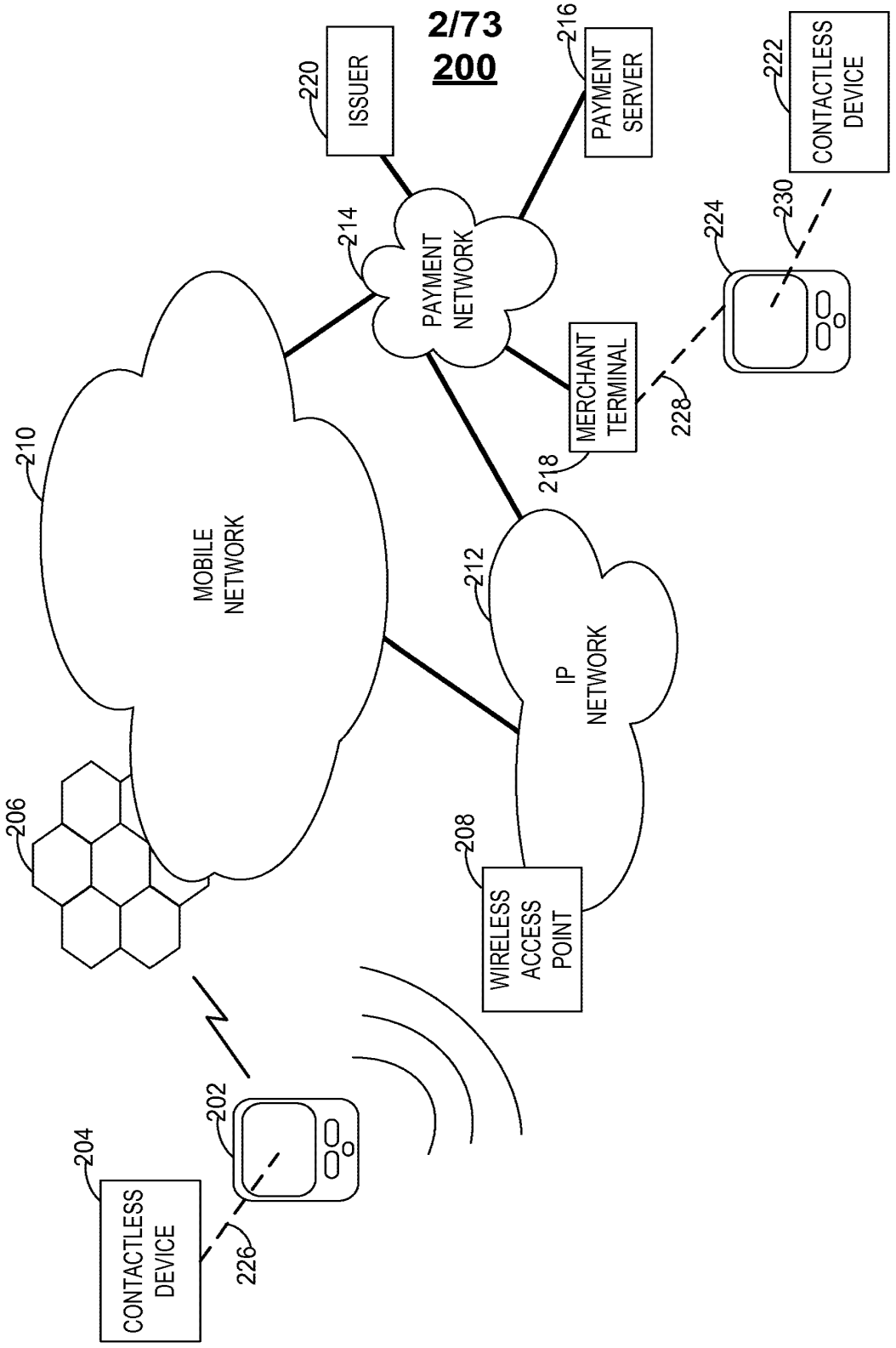

2/73
200
ISSUER
220
PAYMENT SERVER
216
CONTACTLESS DEVICE
222
PAYMENT NETWORK
214
MOBILE NETWORK
210
IP NETWORK
212
MERCHANT TERMINAL
218
228
224
230
206
208
WIRELESS ACCESS POINT
202
204
CONTACTLESS DEVICE
226

FIG. 2

3/73
300

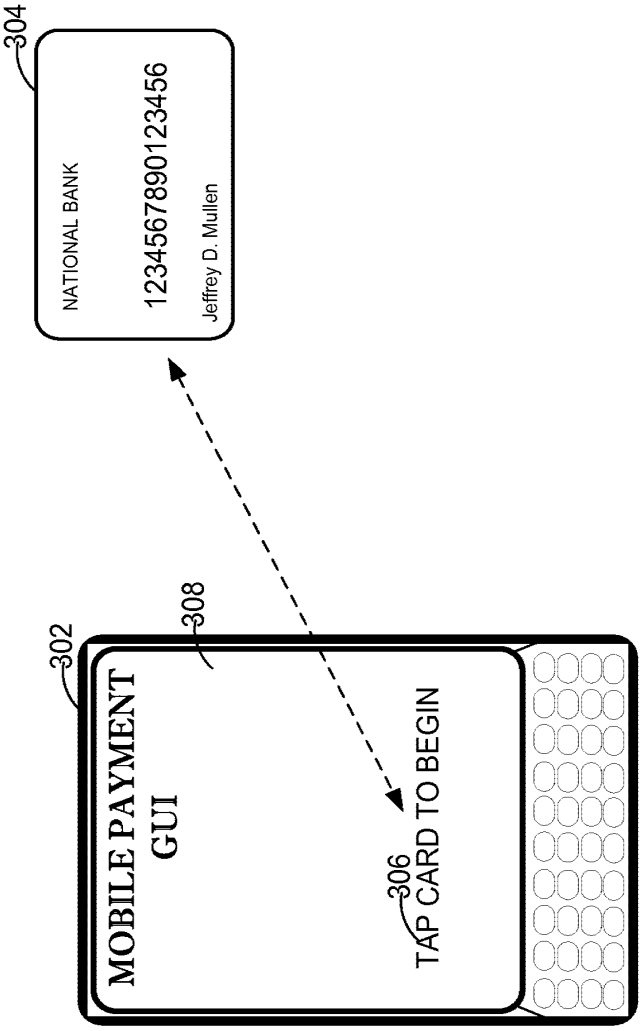

304
NATIONAL BANK
1234567890123456
Jeffrey D. Mullen
308
302
MOBILE PAYMENT
GUI
306
TAP CARD TO BEGIN

FIG. 3

4/73

400


CARD DETECTION
AIRLINE CARD
TRAVEL CARD
BANK CARD
404
HEALTHCARE CARD
IDENTIFICATION CARD
REWARDS CARD
BACK
406
CONTINUE
408

FIG. 4

5/73
500

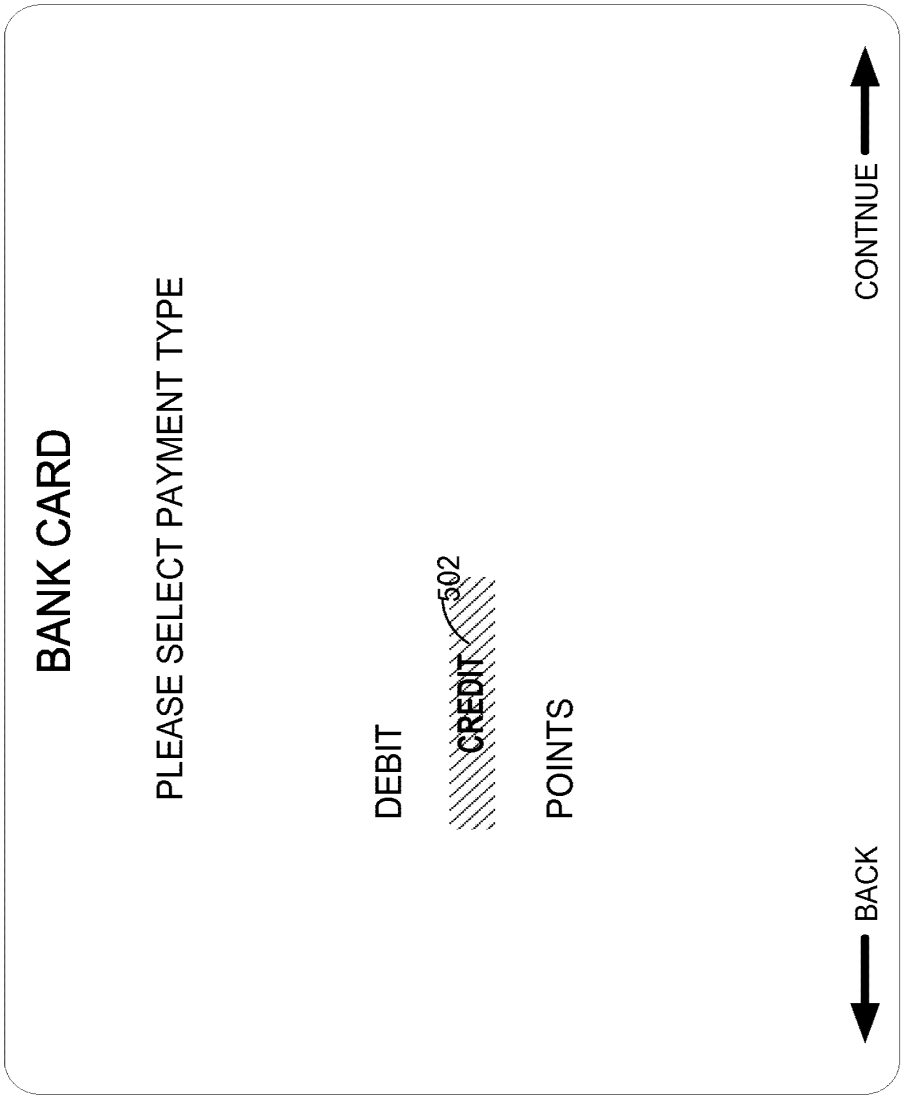

BANK CARD
PLEASE SELECT PAYMENT TYPE
DEBIT
CREDIT
502
POINTS
CONTNUE
BACK

FIG. 5

600

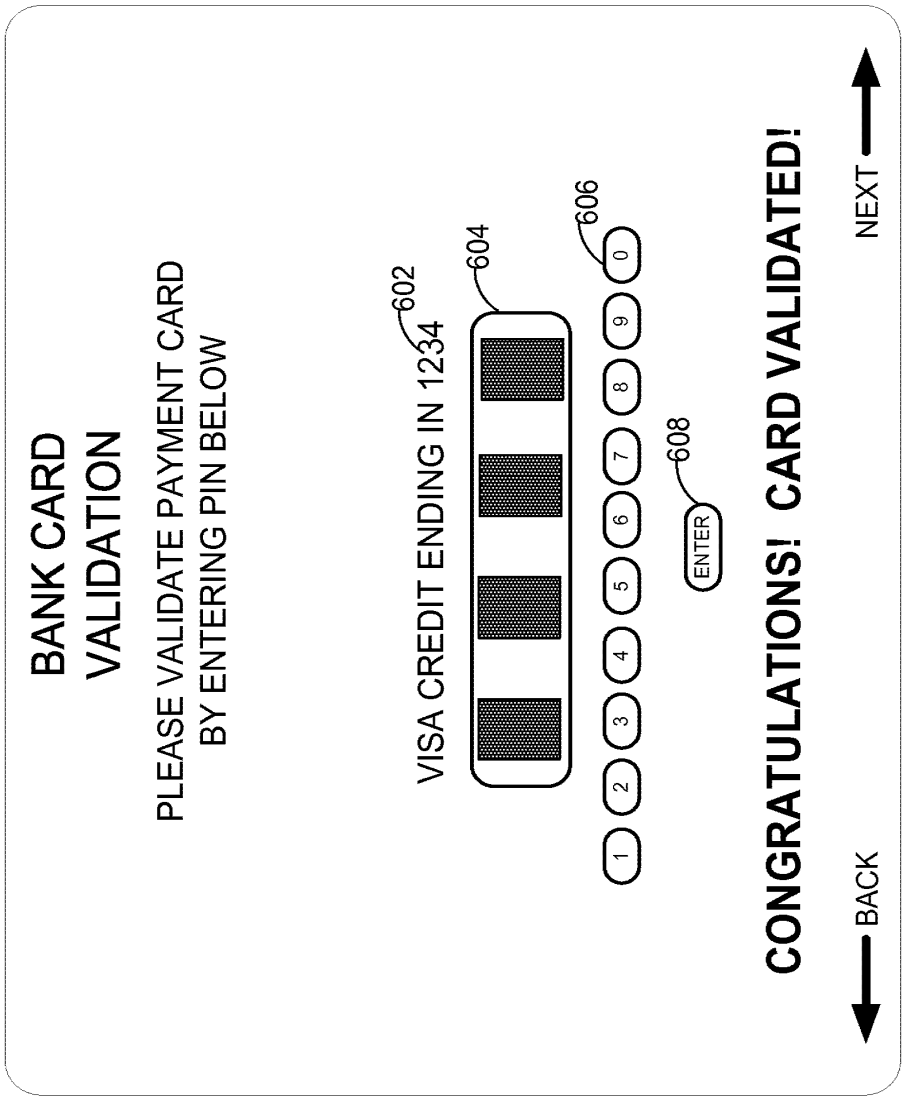

BANK CARD
VALIDATION
PLEASE VALIDATE PAYMENT CARD
BY ENTERING PIN BELOW
VISA CREDIT ENDING IN 1234
602
604
606
1
2
3
4
5
6
7
8
9
0
ENTER
608
CONGRATULATIONS! CARD VALIDATED!
BACK
NEXT

FIG. 6

7/73
700

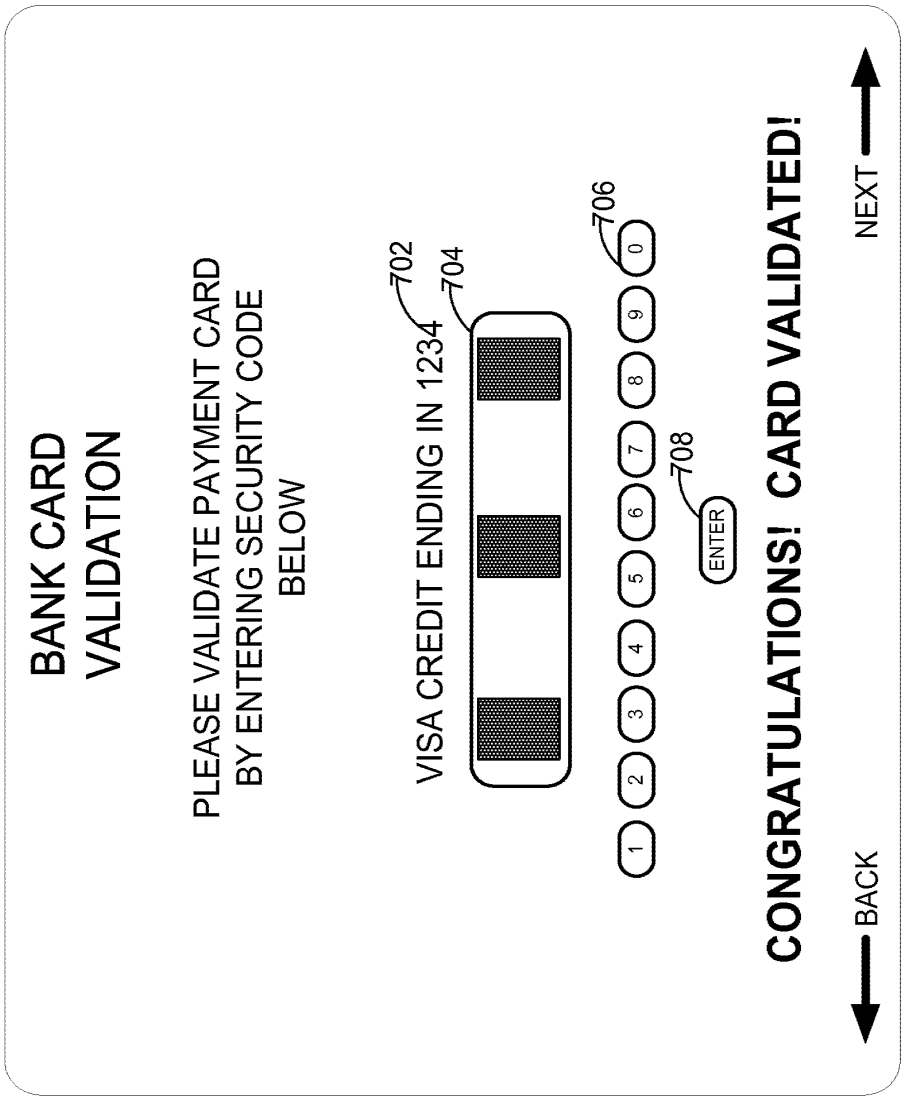

BANK CARD
VALIDATION
PLEASE VALIDATE PAYMENT CARD
BY ENTERING SECURITY CODE
BELOW
VISA CREDIT ENDING IN 1234
702
704
706
1
2
3
4
5
6
7
8
9
0
ENTER
708
CONGRATULATIONS! CARD VALIDATED!
BACK
NEXT

FIG. 7

8/73

800

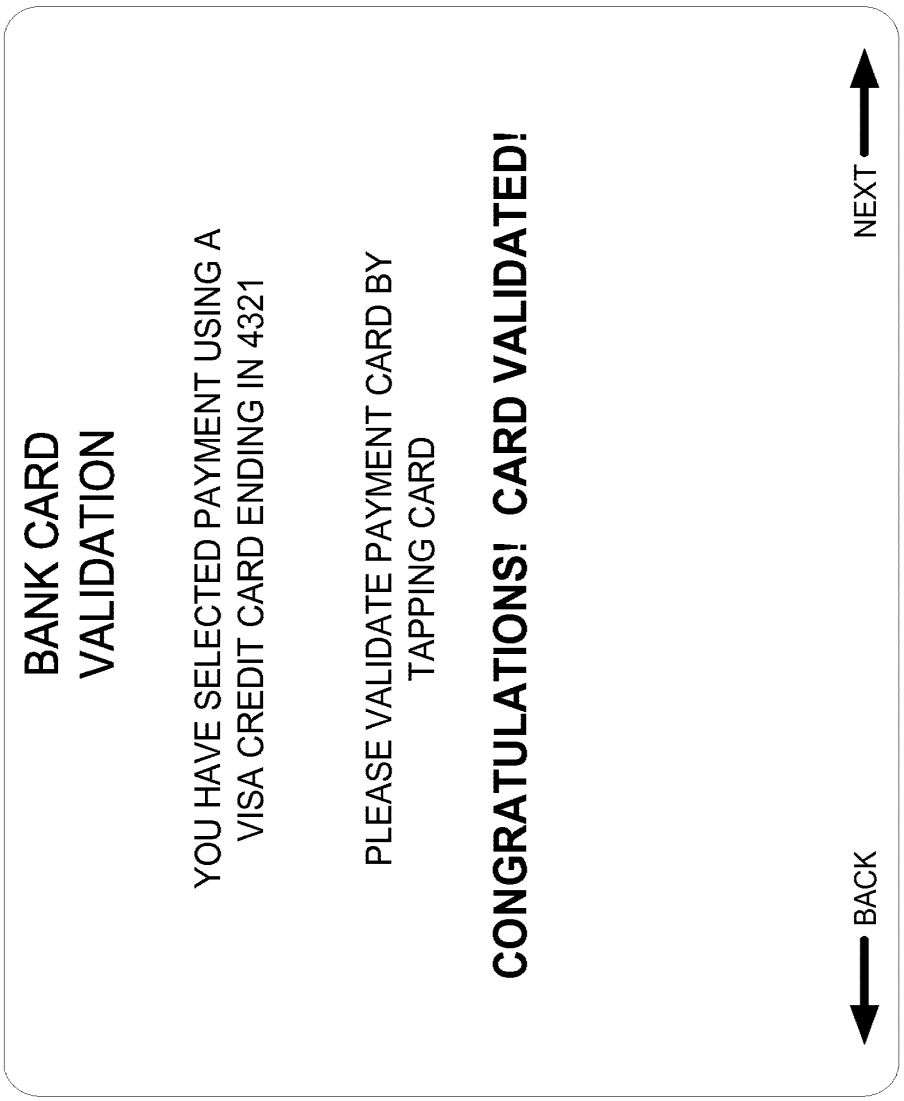

BANK CARD
VALIDATION
YOU HAVE SELECTED PAYMENT USING A
VISA CREDIT CARD ENDING IN 4321
PLEASE VALIDATE PAYMENT CARD BY
TAPPING CARD
CONGRATULATIONS! CARD VALIDATED!
BACK
NEXT

FIG. 8

900

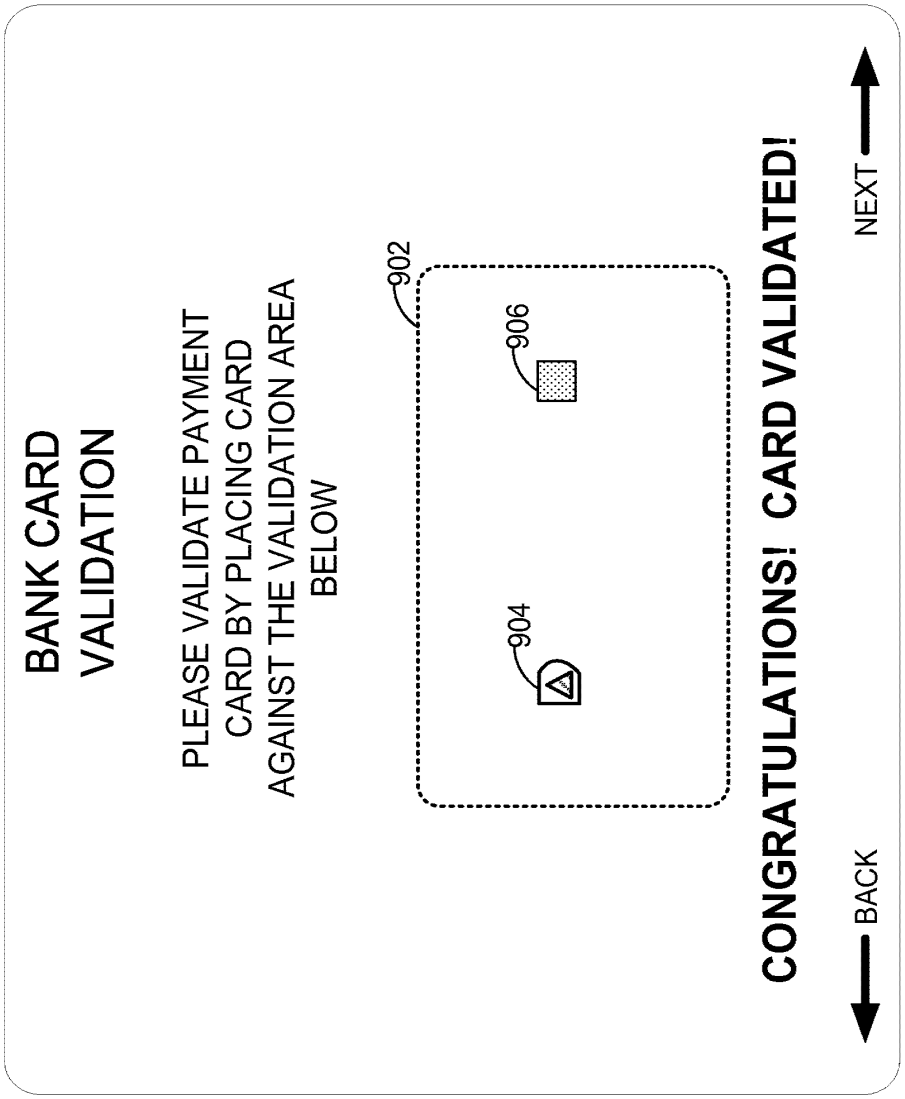

BANK CARD
VALIDATION
PLEASE VALIDATE PAYMENT
CARD BY PLACING CARD
AGAINST THE VALIDATION AREA
BELOW
902
906
904
CONGRATULATIONS! CARD VALIDATED!
BACK
NEXT

FIG. 9

10/73
1000

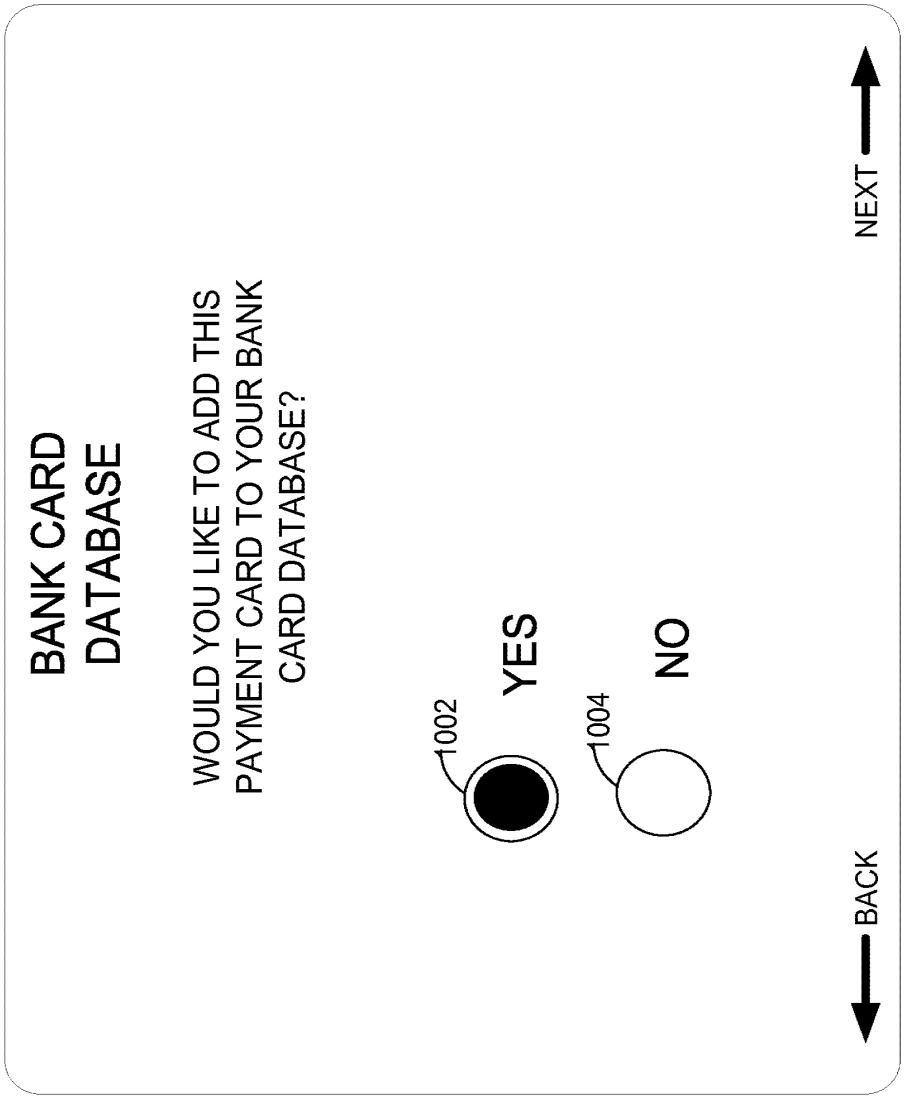


FIG. 10

11/73
1100

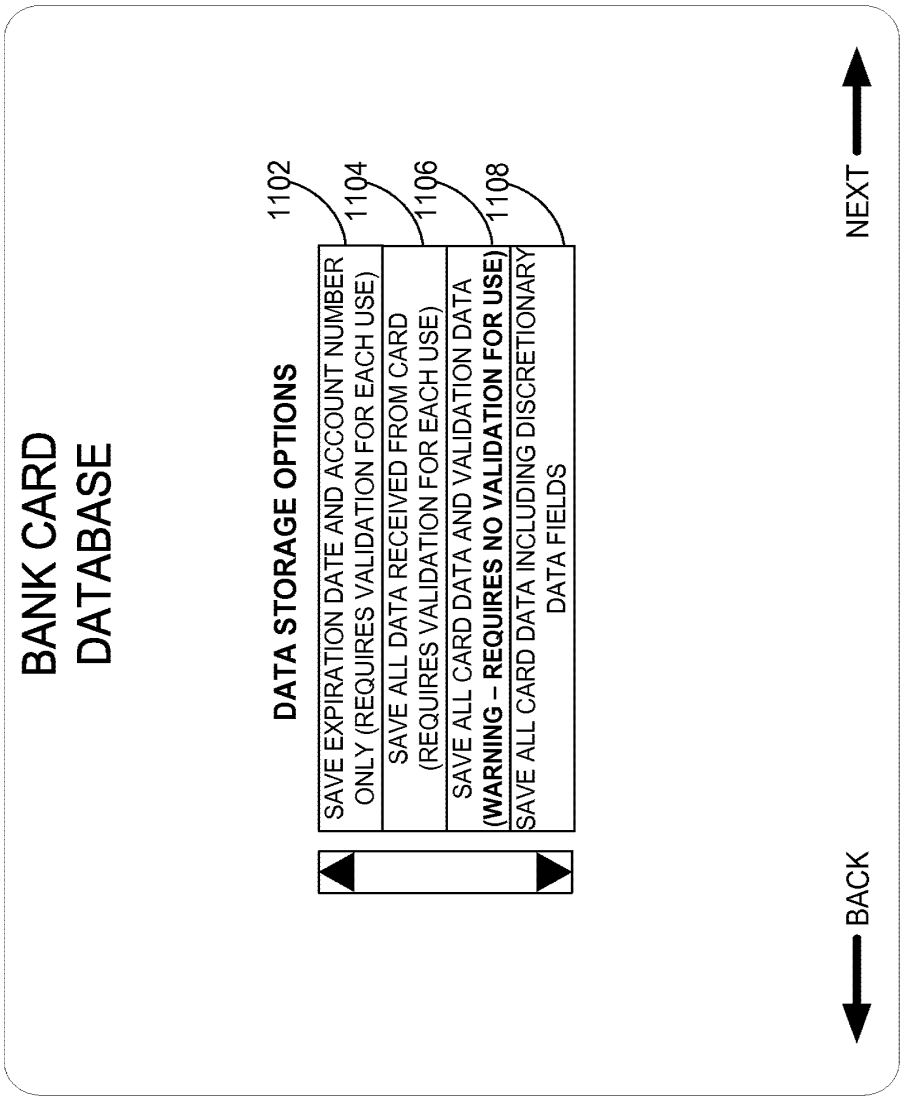


FIG. 11

12/73
1200

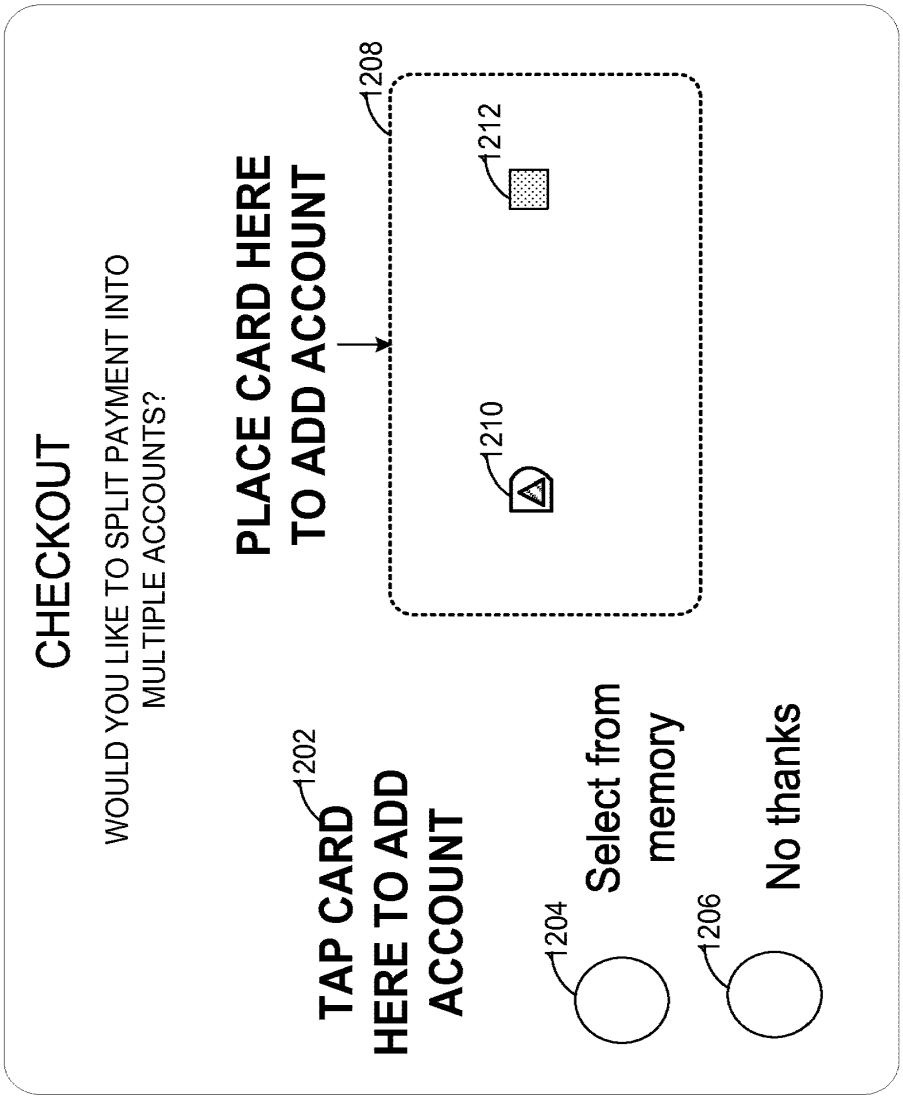


FIG. 12

13/73
1300

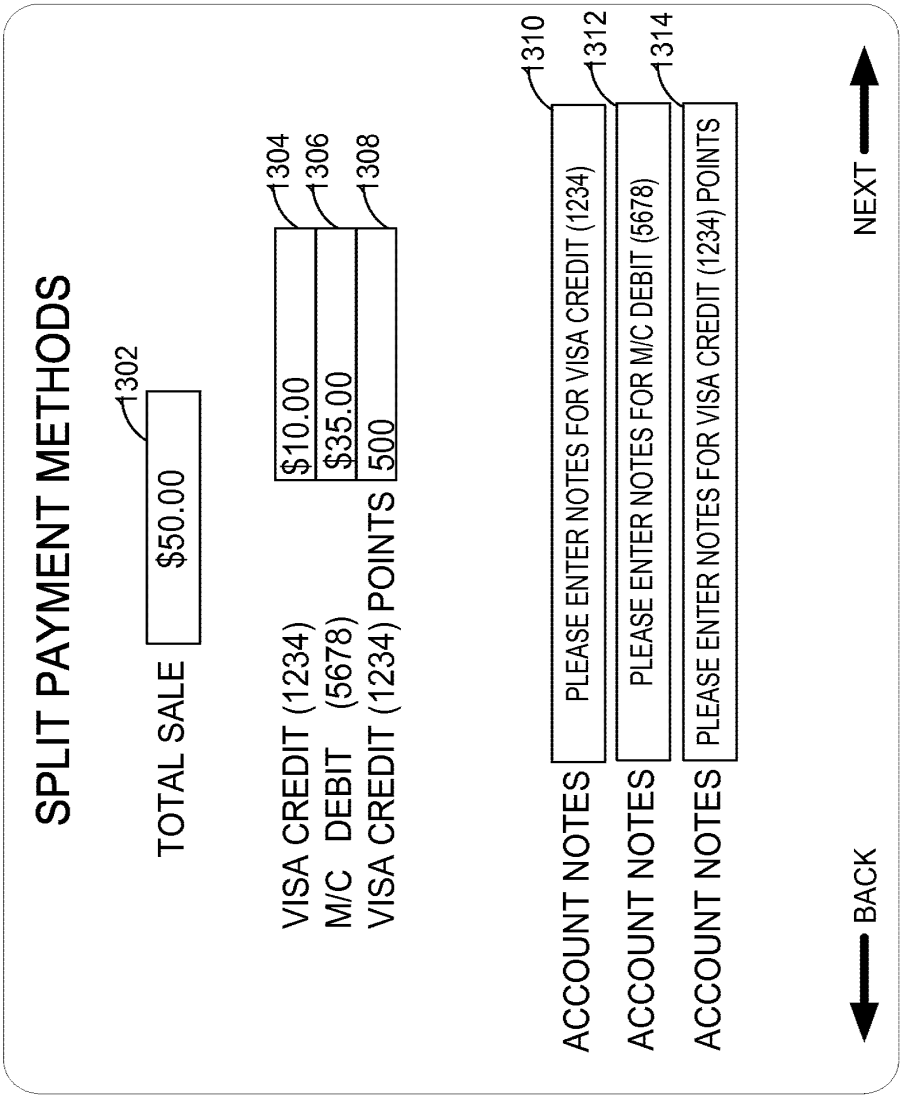


FIG. 13

14/73
1400

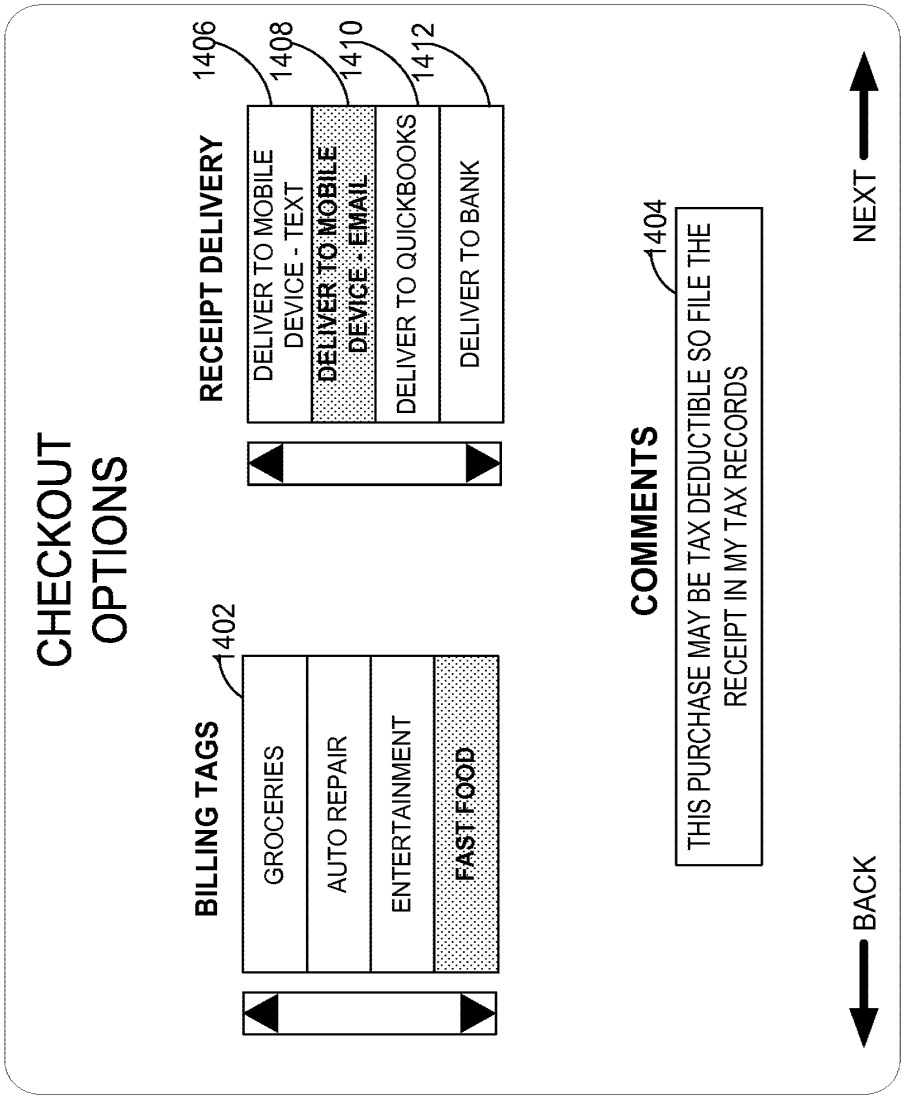


FIG. 14

15/73
1500

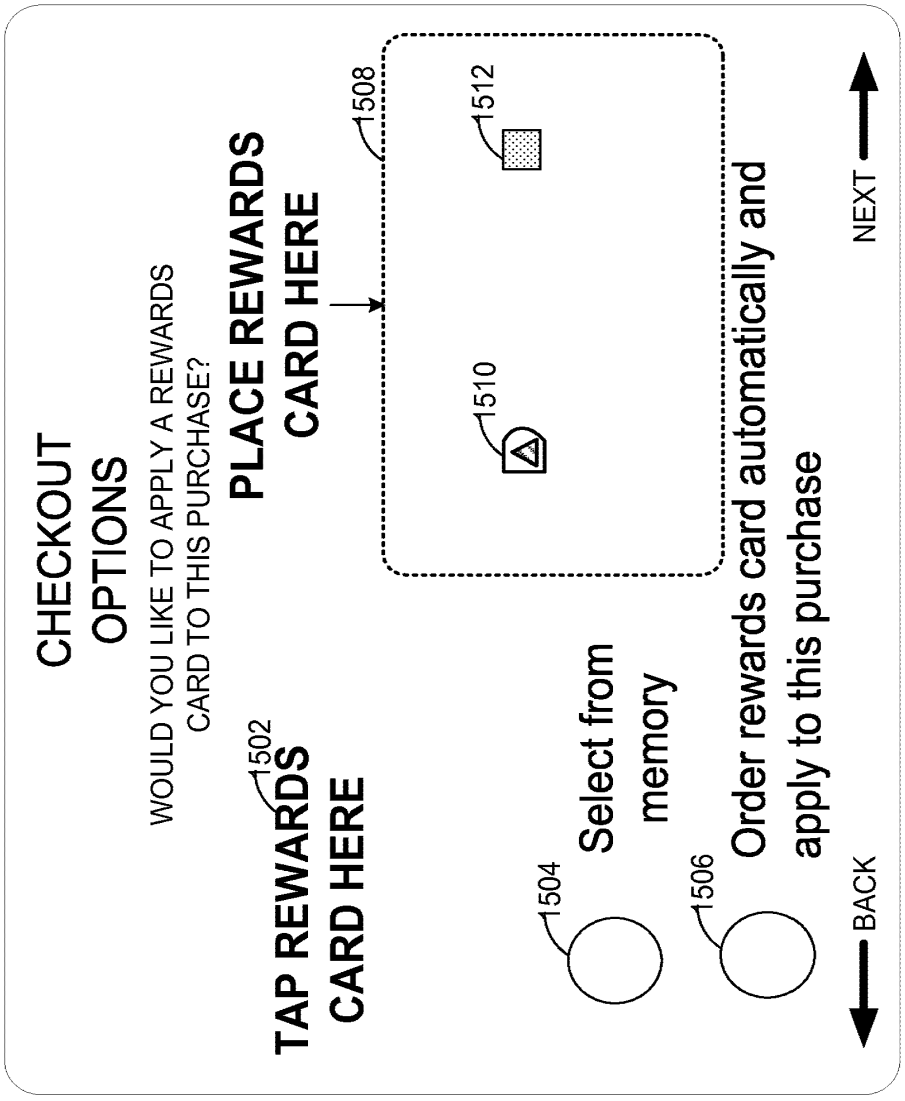


FIG. 15

16/73
1600

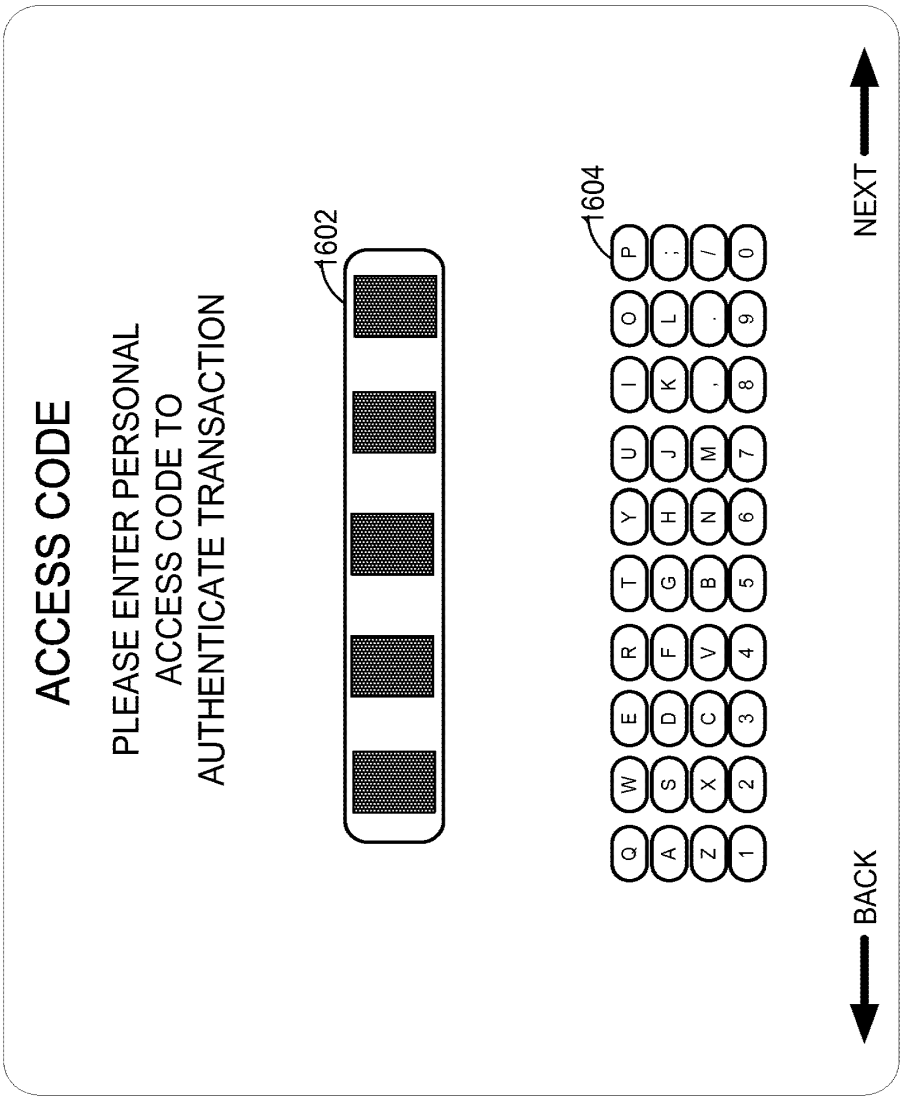


FIG. 16

17/73
1700

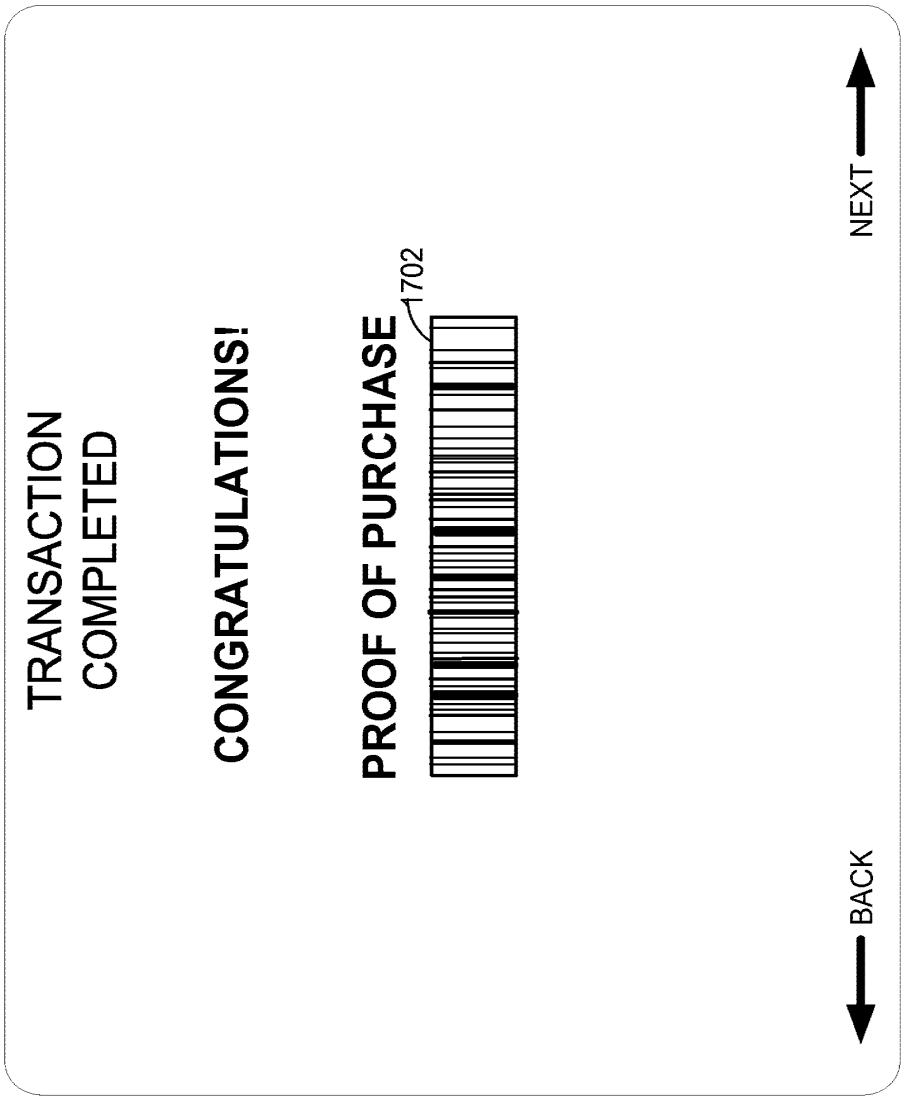


FIG. 17

1800

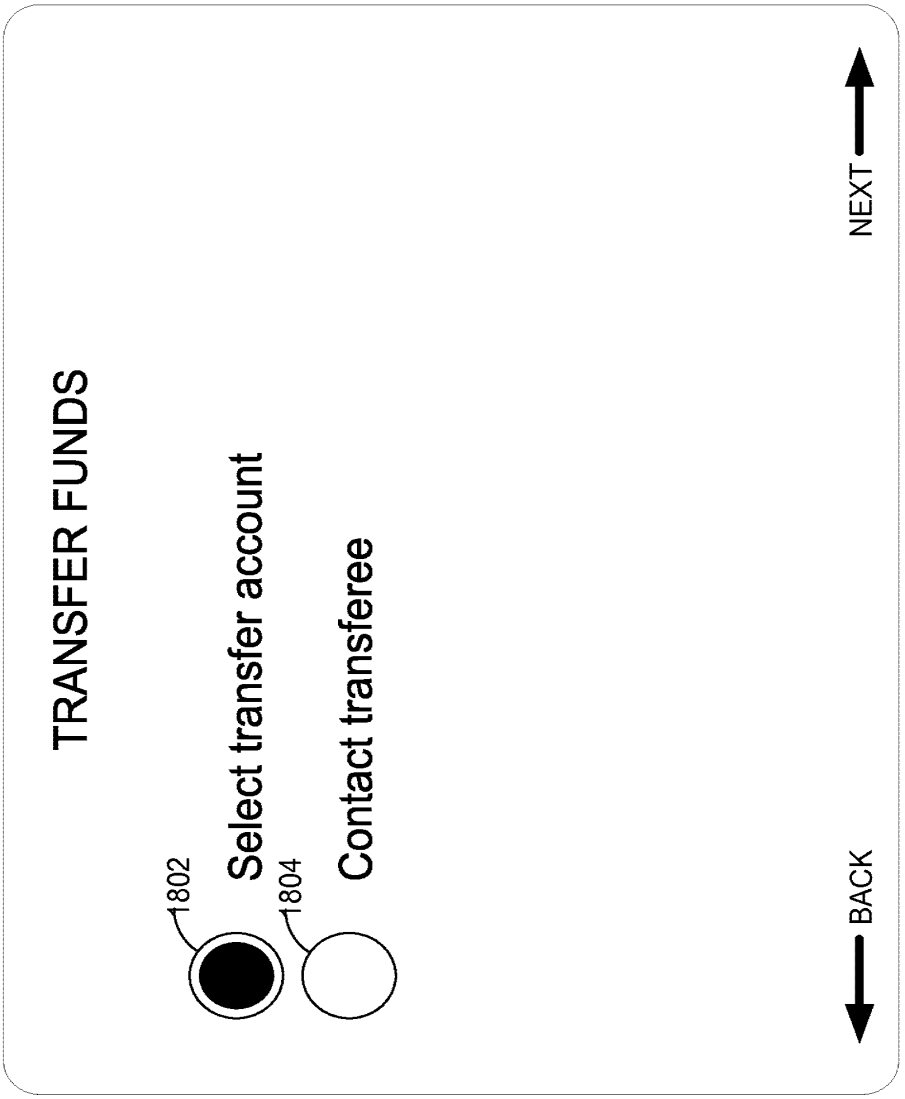

TRANSFER FUNDS
Select transfer account
Contact transferee
1802
1804
NEXT
BACK

FIG. 18

19/73
1900

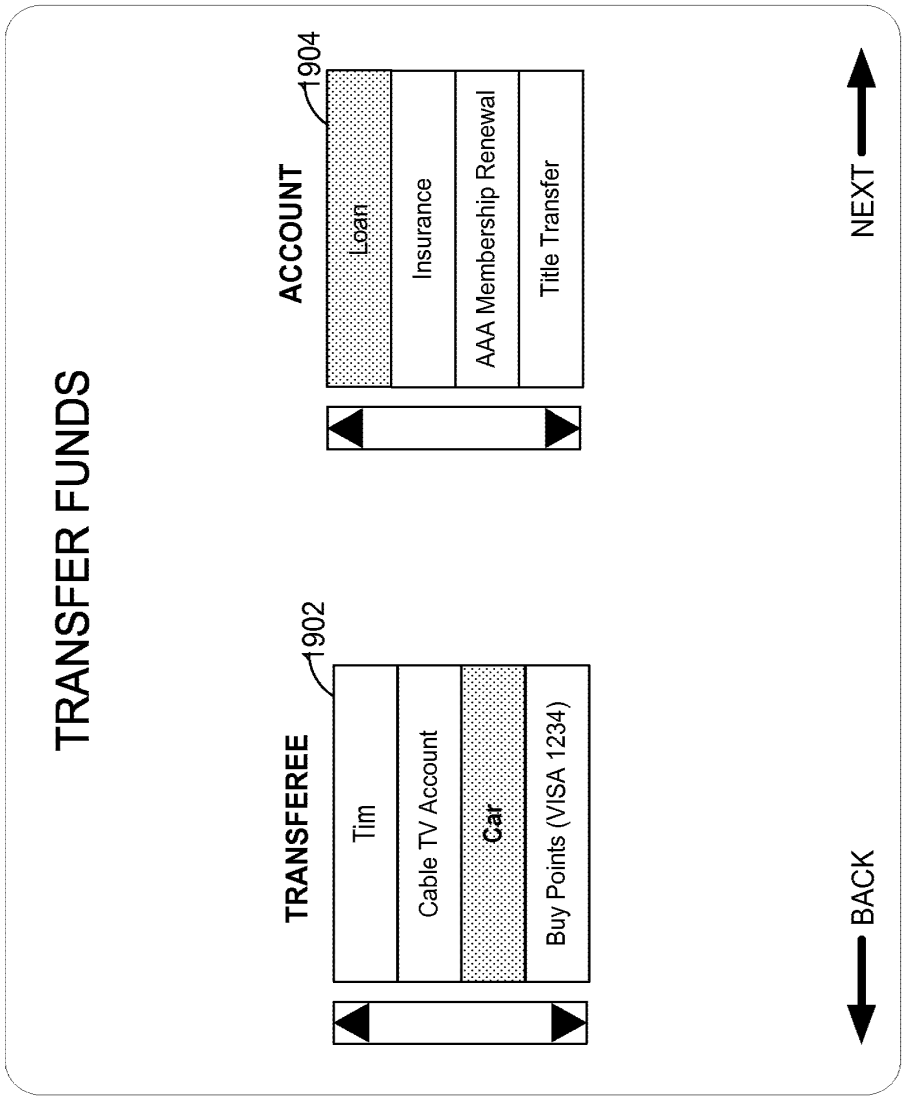


FIG. 19

20/73
2000

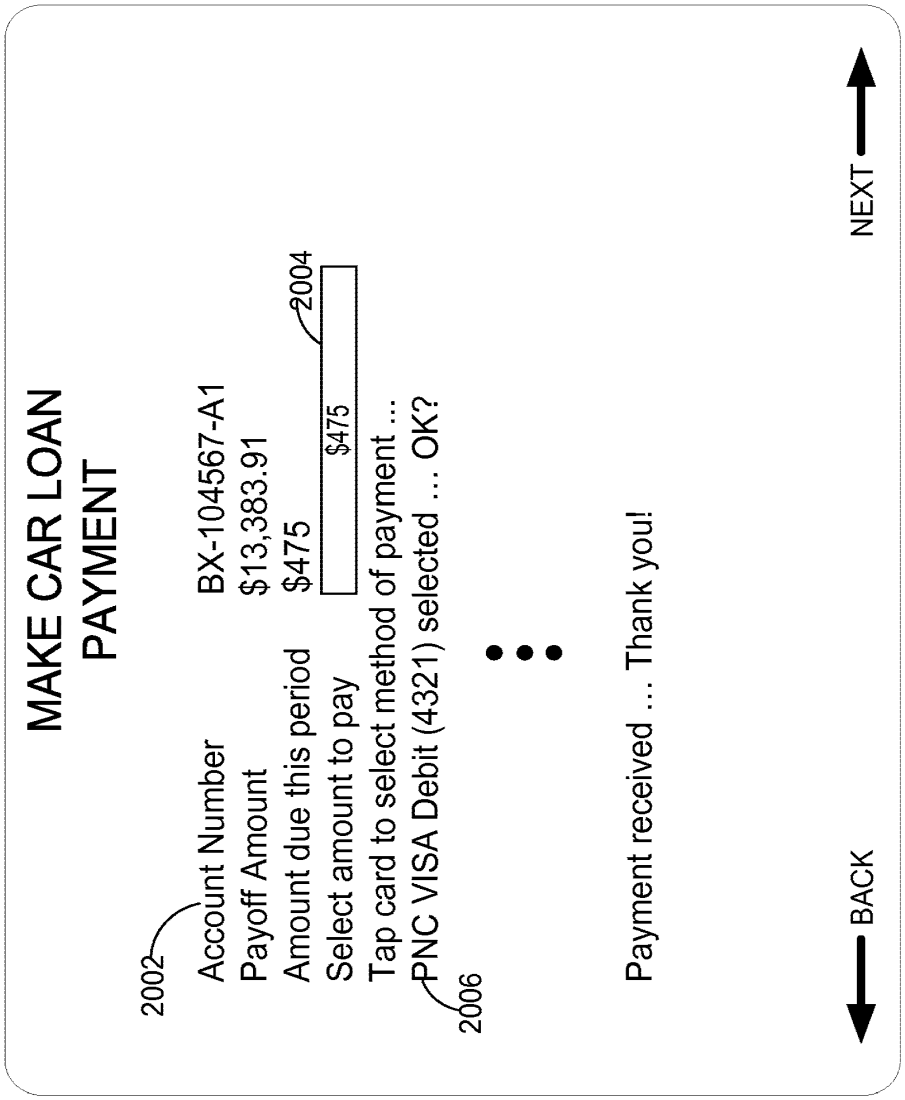


FIG. 20

2100

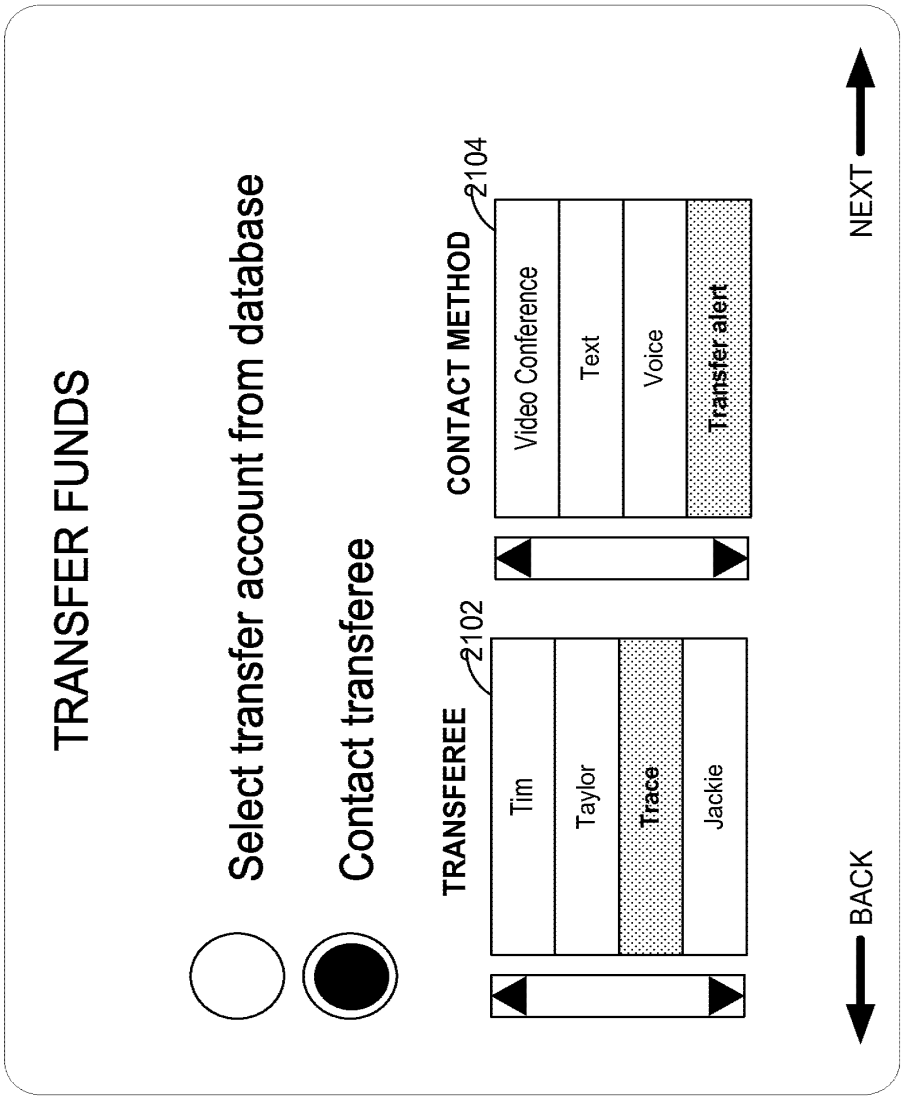

TRANSFER FUNDS
Select transfer account from database
Contact transferee
TRANSFEREE
2102
Tim
Taylor
Trace
Jackie
CONTACT METHOD
2104
Video Conference
Text
Voice
Transfer alert
BACK
NEXT

FIG. 21

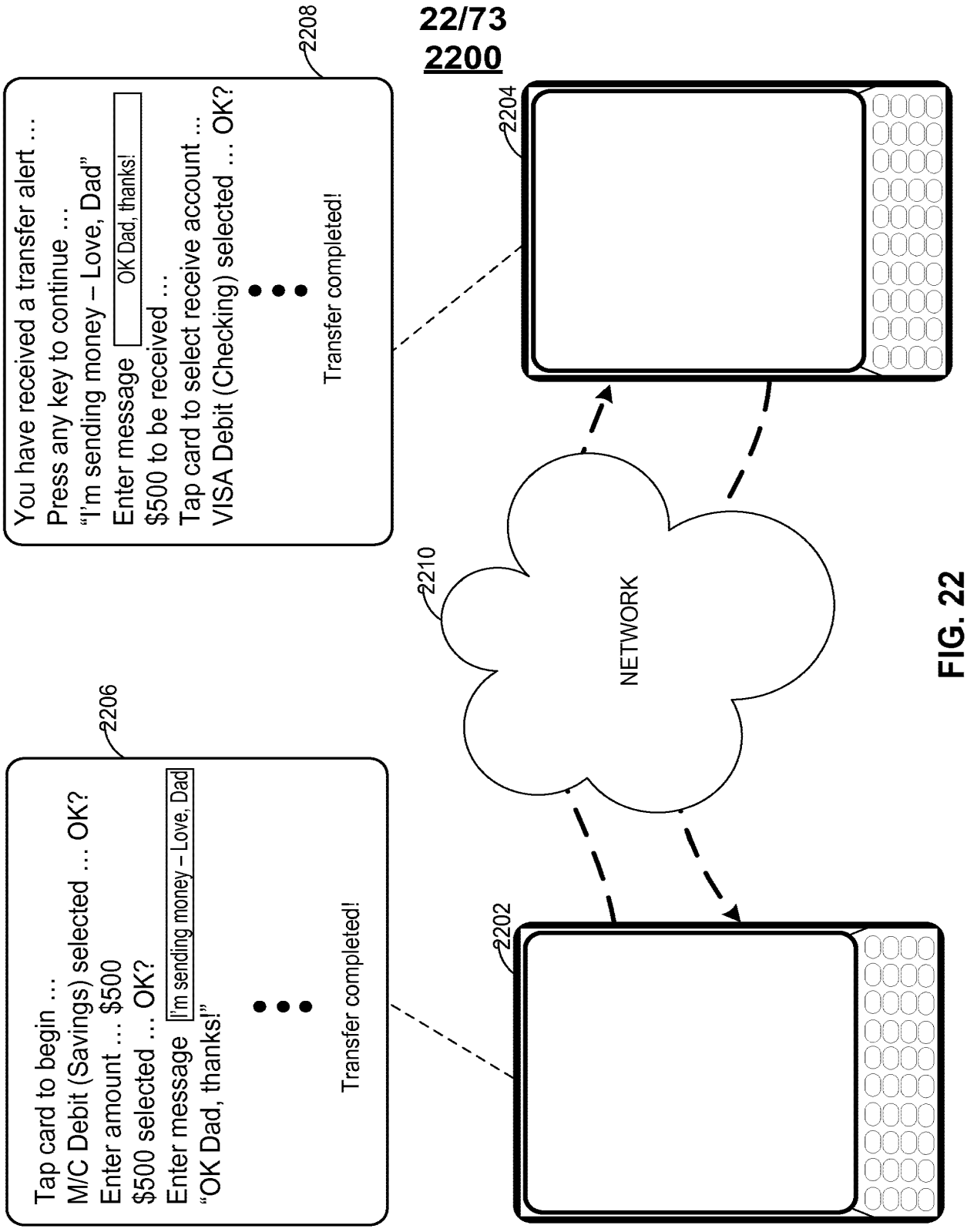

2200
2202
2204
2206
2208
2210
NETWORK
Tap card to begin …
M/C Debit (Savings) selected … OK?
Enter amount … $500
$500 selected … OK?
Enter message I'm sending money – Love, Dad
"OK Dad, thanks!"
Transfer completed!
You have received a transfer alert …
Press any key to continue …
"I'm sending money – Love, Dad"
Enter message OK Dad, thanks!
$500 to be received …
Tap card to select receive account …
VISA Debit (Checking) selected … OK?
Transfer completed!

FIG. 22

2300

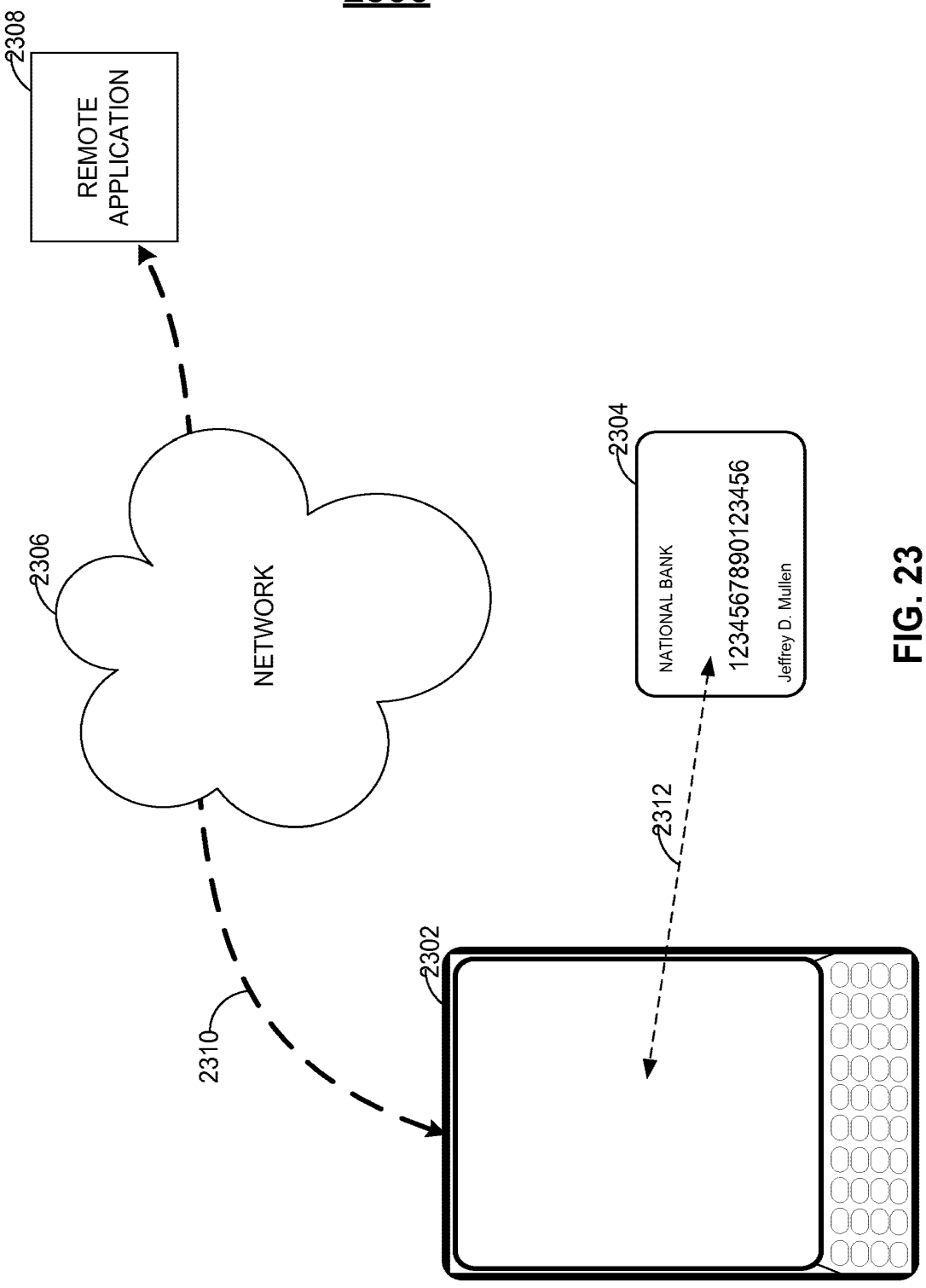

2308
REMOTE APPLICATION
2306
NETWORK
2304
NATIONAL BANK
1234567890123456
Jeffrey D. Mullen
2312
2302
2310

FIG. 23

2400

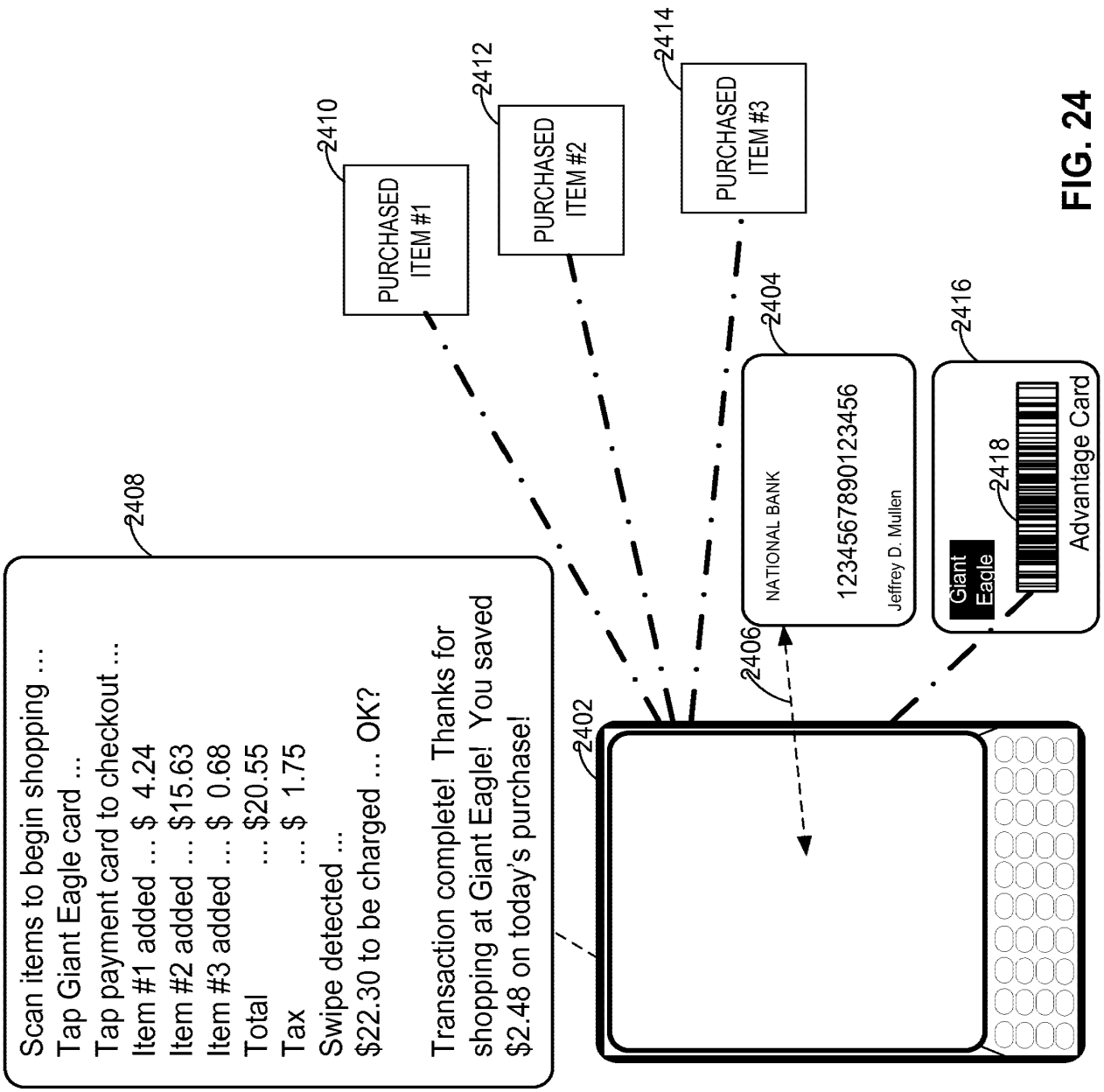

Scan items to begin shopping ...
Tap Giant Eagle card ...
Tap payment card to checkout ...
Item #1 added ... $ 4.24
Item #2 added ... $15.63
Item #3 added ... $ 0.68
Total ... $20.55
Tax ... $ 1.75
Swipe detected ...
$22.30 to be charged ... OK?
Transaction complete! Thanks for shopping at Giant Eagle! You saved $2.48 on today's purchase!
2408
2410
PURCHASED ITEM #1
2412
PURCHASED ITEM #2
2414
PURCHASED ITEM #3
2404
NATIONAL BANK
1234567890123456
Jeffrey D. Mullen
2416
Giant Eagle
2418
Advantage Card
2406
2402

FIG. 24

2500

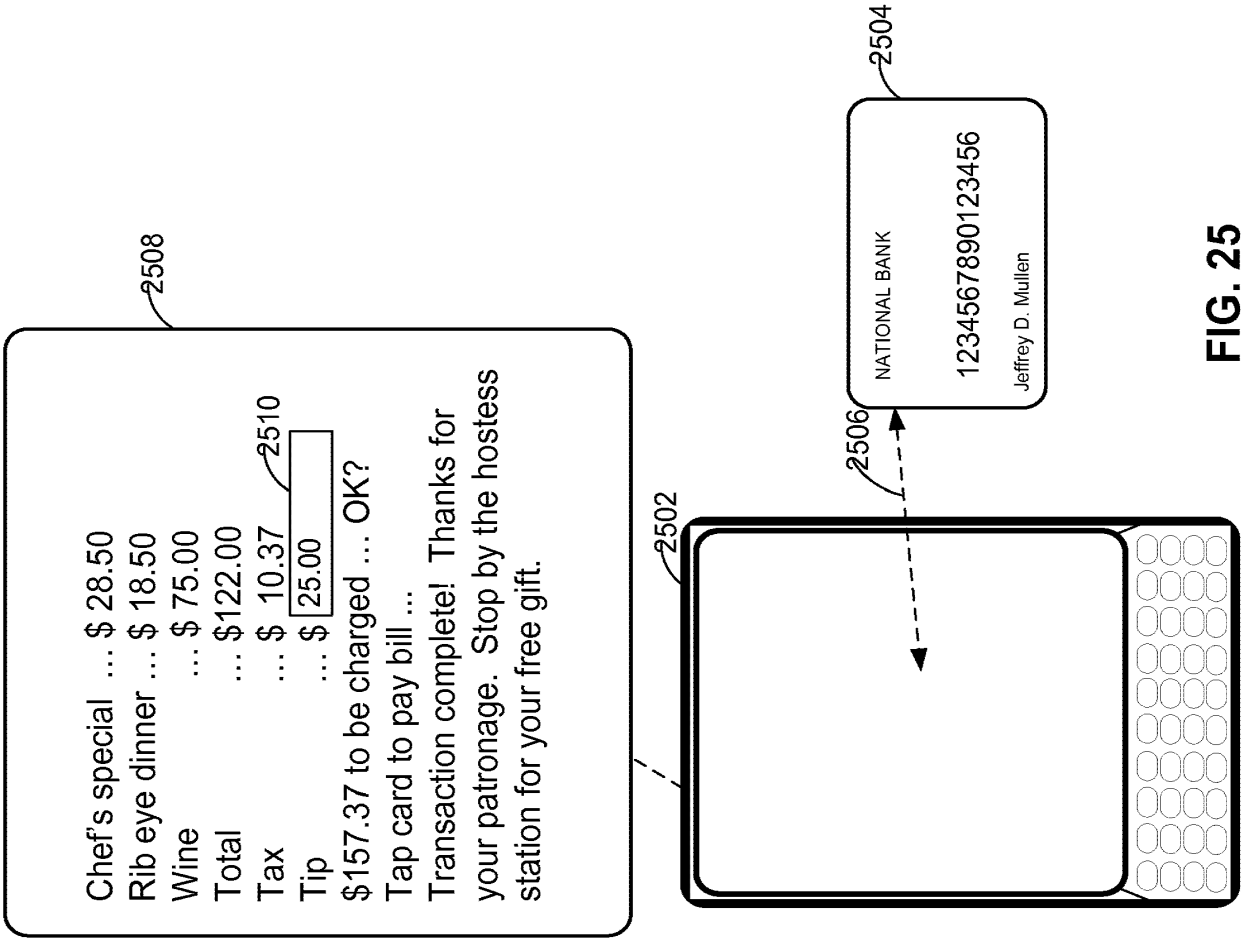

2508
Chef's special ... $ 28.50
Rib eye dinner ... $ 18.50
Wine ... $ 75.00
Total ... $122.00
Tax ... $ 10.37
2510
Tip ... $ 25.00
$157.37 to be charged ... OK?
Tap card to pay bill ...
Transaction complete! Thanks for your patronage. Stop by the hostess station for your free gift.
2502
2506
2504
NATIONAL BANK
1234567890123456
Jeffrey D. Mullen

FIG. 25

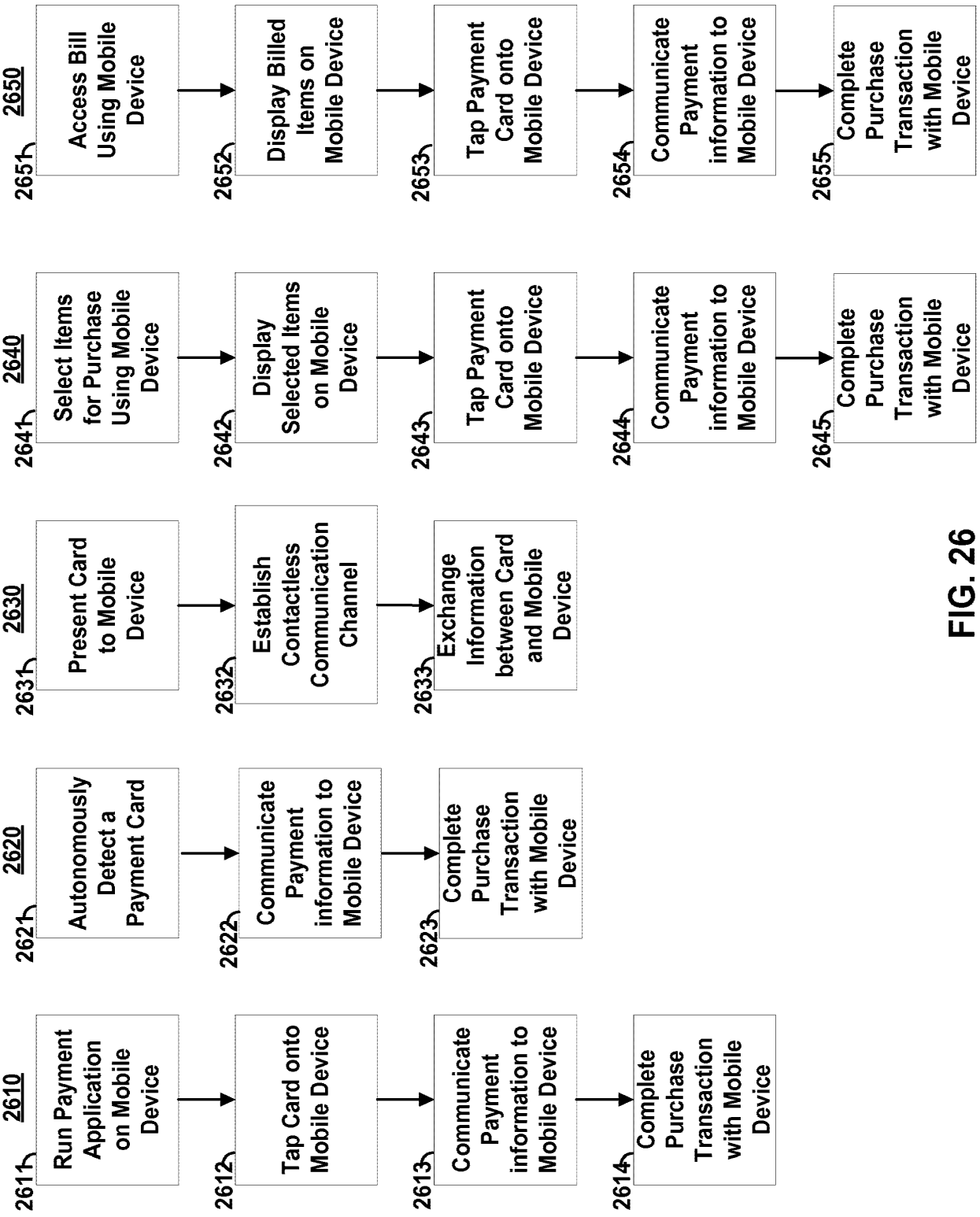

2610
2611 Run Payment Application on Mobile Device
2612 Tap Card onto Mobile Device
2613 Communicate Payment information to Mobile Device
2614 Complete Purchase Transaction with Mobile Device
2620
2621 Autonomously Detect a Payment Card
2622 Communicate Payment information to Mobile Device
2623 Complete Purchase Transaction with Mobile Device
2630
2631 Present Card to Mobile Device
2632 Establish Contactless Communication Channel
2633 Exchange Information between Card and Mobile Device
2640
2641 Select Items for Purchase Using Mobile Device
2642 Display Selected Items on Mobile Device
2643 Tap Payment Card onto Mobile Device
2644 Communicate Payment information to Mobile Device
2645 Complete Purchase Transaction with Mobile Device
2650
2651 Access Bill Using Mobile Device
2652 Display Billed Items on Mobile Device
2653 Tap Payment Card onto Mobile Device
2654 Communicate Payment information to Mobile Device
2655 Complete Purchase Transaction with Mobile Device

FIG. 26

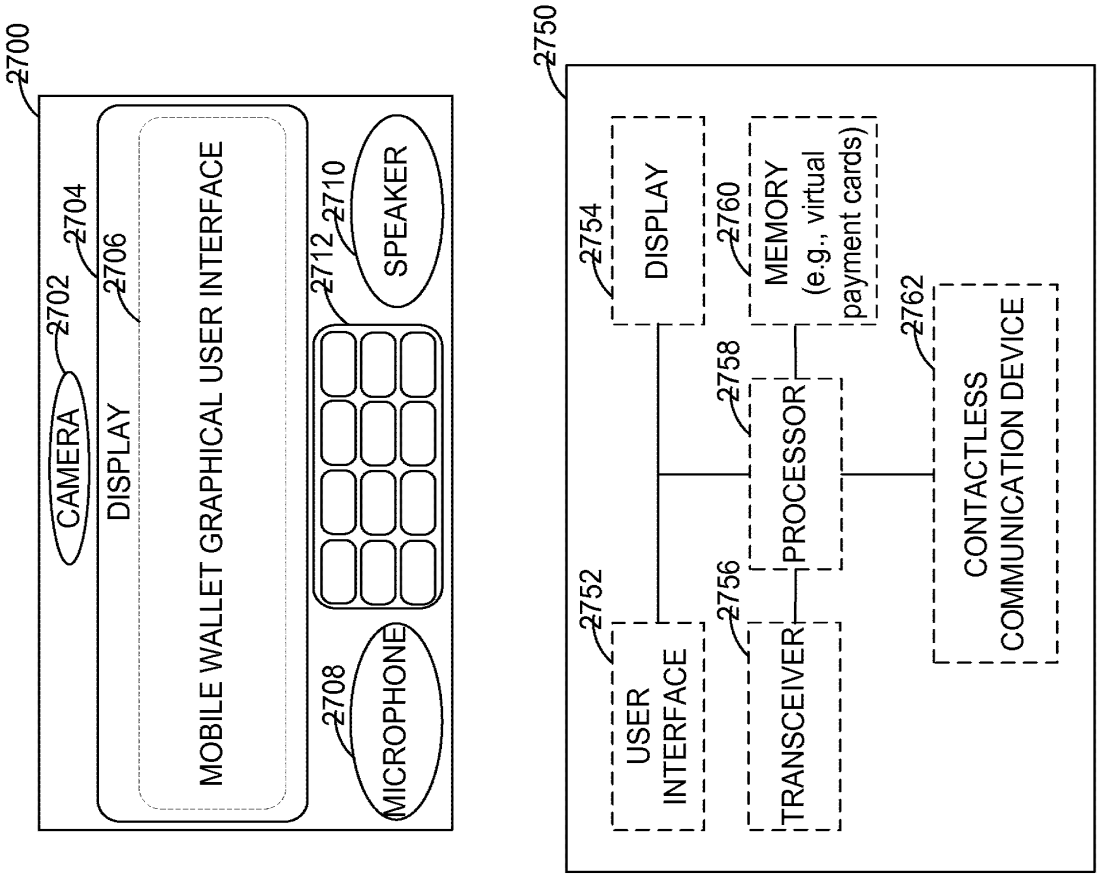

2700
CAMERA
2702
2704
DISPLAY
2706
MOBILE WALLET GRAPHICAL USER INTERFACE
2712
2710
SPEAKER
2708
MICROPHONE
2750
2754
DISPLAY
2760
MEMORY
(e.g., virtual
payment cards)
2752
USER
INTERFACE
2758
PROCESSOR
2756
TRANSCEIVER
2762
CONTACTLESS
COMMUNICATION DEVICE

FIG. 27

2800

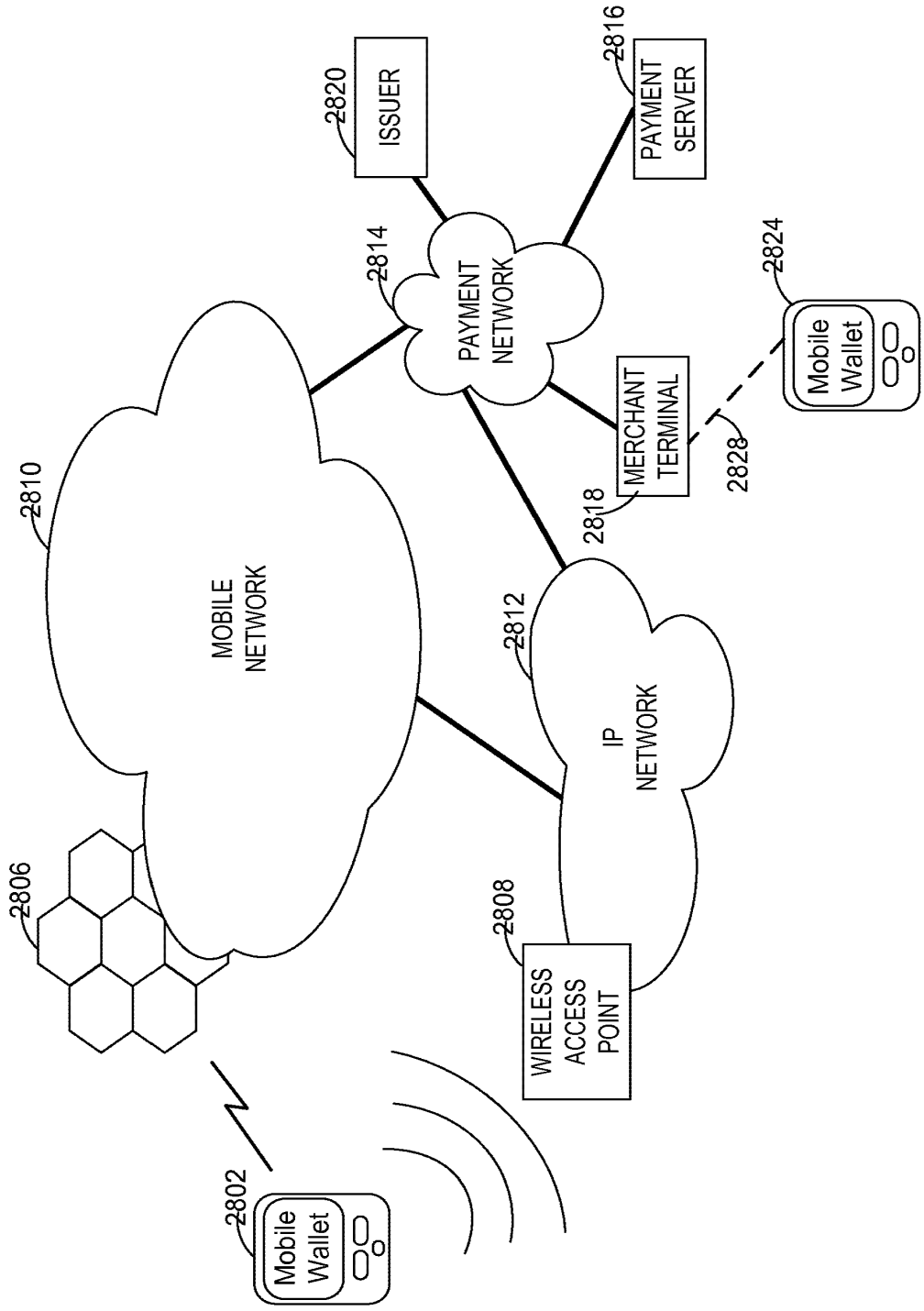

2820
ISSUER
2816
PAYMENT SERVER
2814
PAYMENT NETWORK
2824
Mobile Wallet
MERCHANT TERMINAL
2828
2818
2810
MOBILE NETWORK
2812
IP NETWORK
2806
2808
WIRELESS ACCESS POINT
2802
Mobile Wallet

FIG. 28

2900

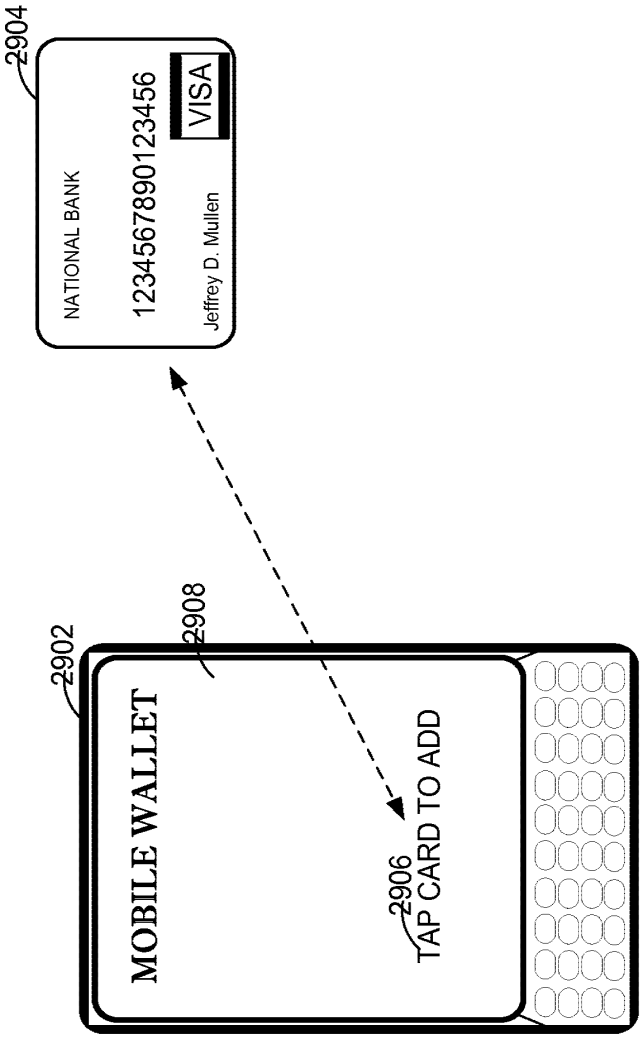

2904
NATIONAL BANK
1234567890123456
VISA
Jeffrey D. Mullen
2902
2908
MOBILE WALLET
2906
TAP CARD TO ADD

FIG. 29

3000

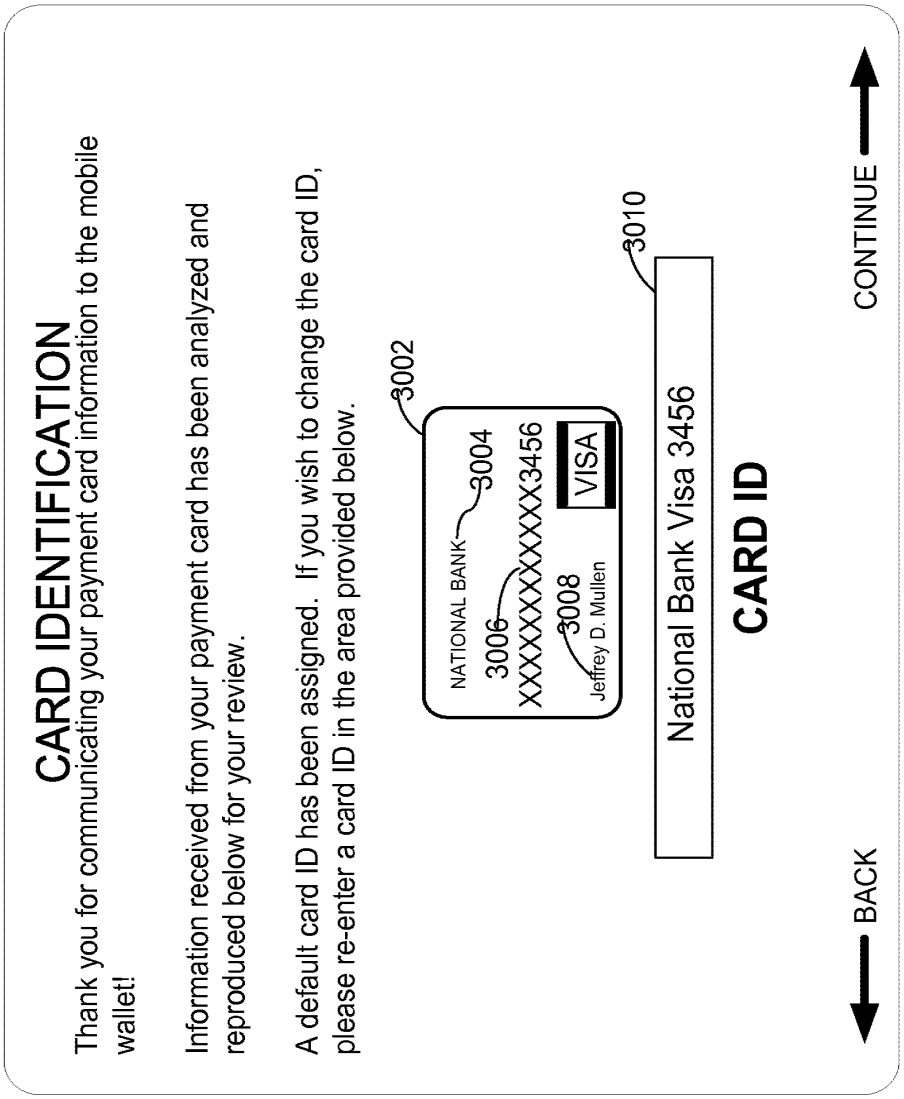

CARD IDENTIFICATION
Thank you for communicating your payment card information to the mobile wallet!
Information received from your payment card has been analyzed and reproduced below for your review.
A default card ID has been assigned. If you wish to change the card ID, please re-enter a card ID in the area provided below.
3002
NATIONAL BANK
3004
3006
XXXXXXXXXXXX3456
3008
Jeffrey D. Mullen
VISA
3010
National Bank Visa 3456
CARD ID
BACK
CONTINUE

FIG. 30

3100

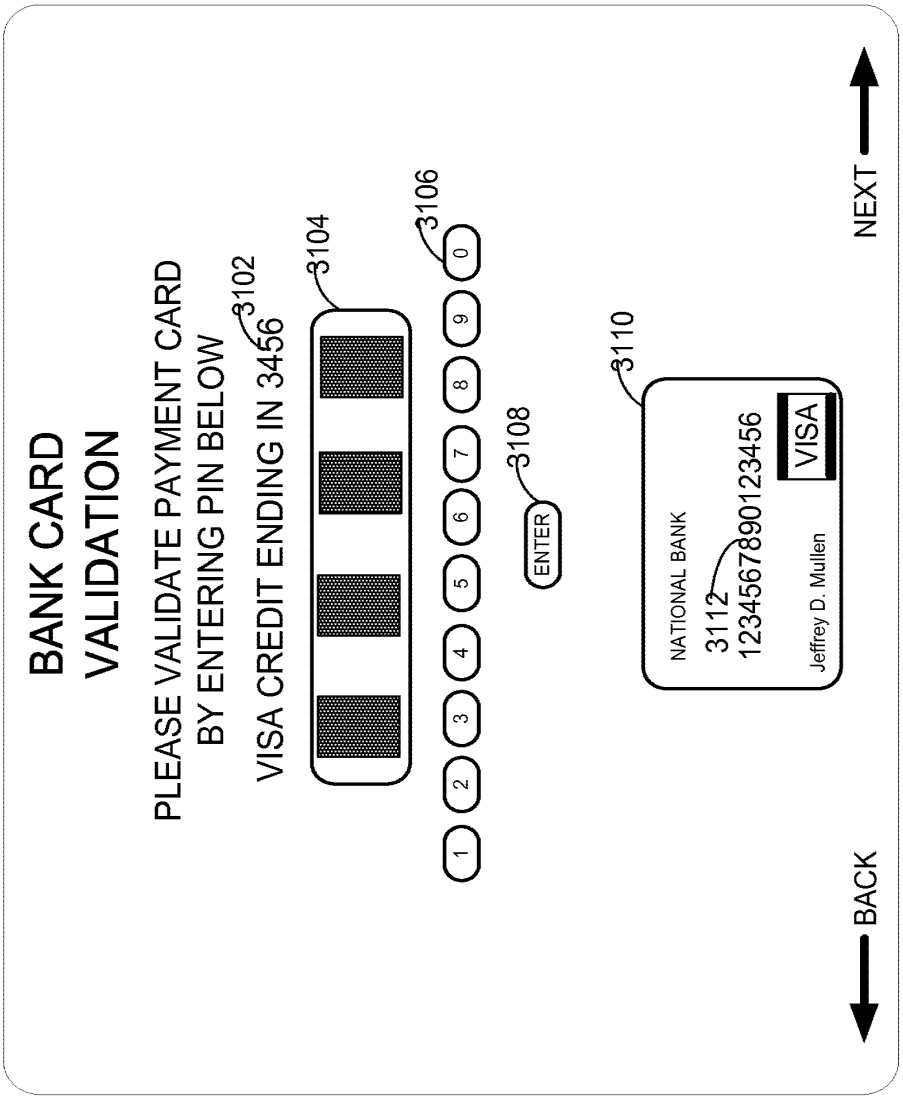

BANK CARD
VALIDATION
PLEASE VALIDATE PAYMENT CARD
BY ENTERING PIN BELOW
VISA CREDIT ENDING IN 3456
3102
3104
3106
1
2
3
4
5
6
7
8
9
0
ENTER
3108
3110
NATIONAL BANK
3112
1234567890123456
Jeffrey D. Mullen
VISA
BACK
NEXT

FIG. 31

3200

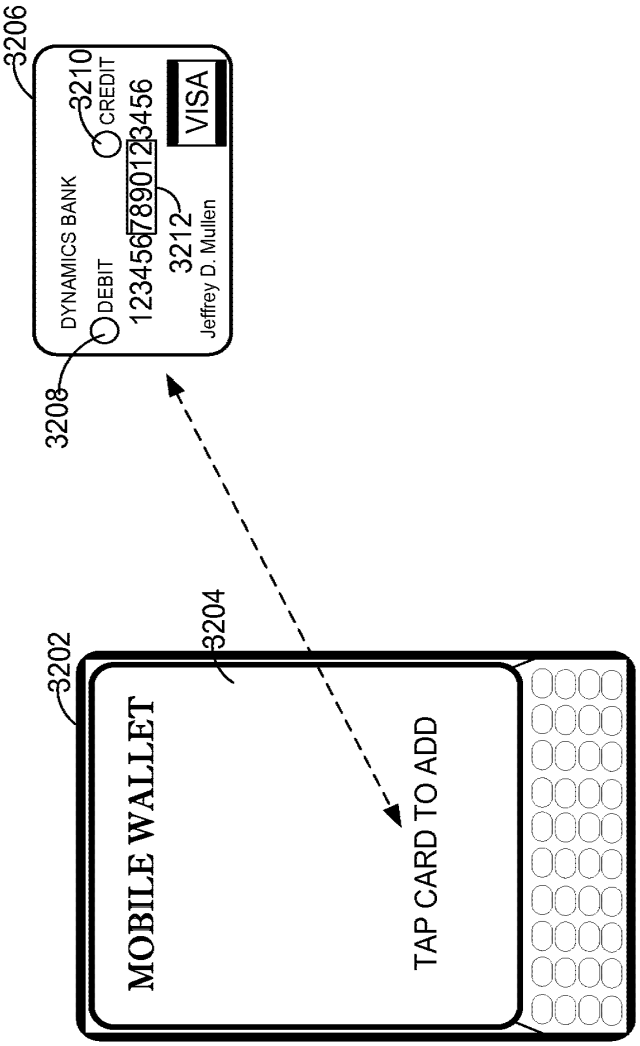

3206
3210
CREDIT
DYNAMICS BANK
DEBIT
123456789012 3456
VISA
3212
Jeffrey D. Mullen
3208
3202
3204
MOBILE WALLET
TAP CARD TO ADD

FIG. 32

3300

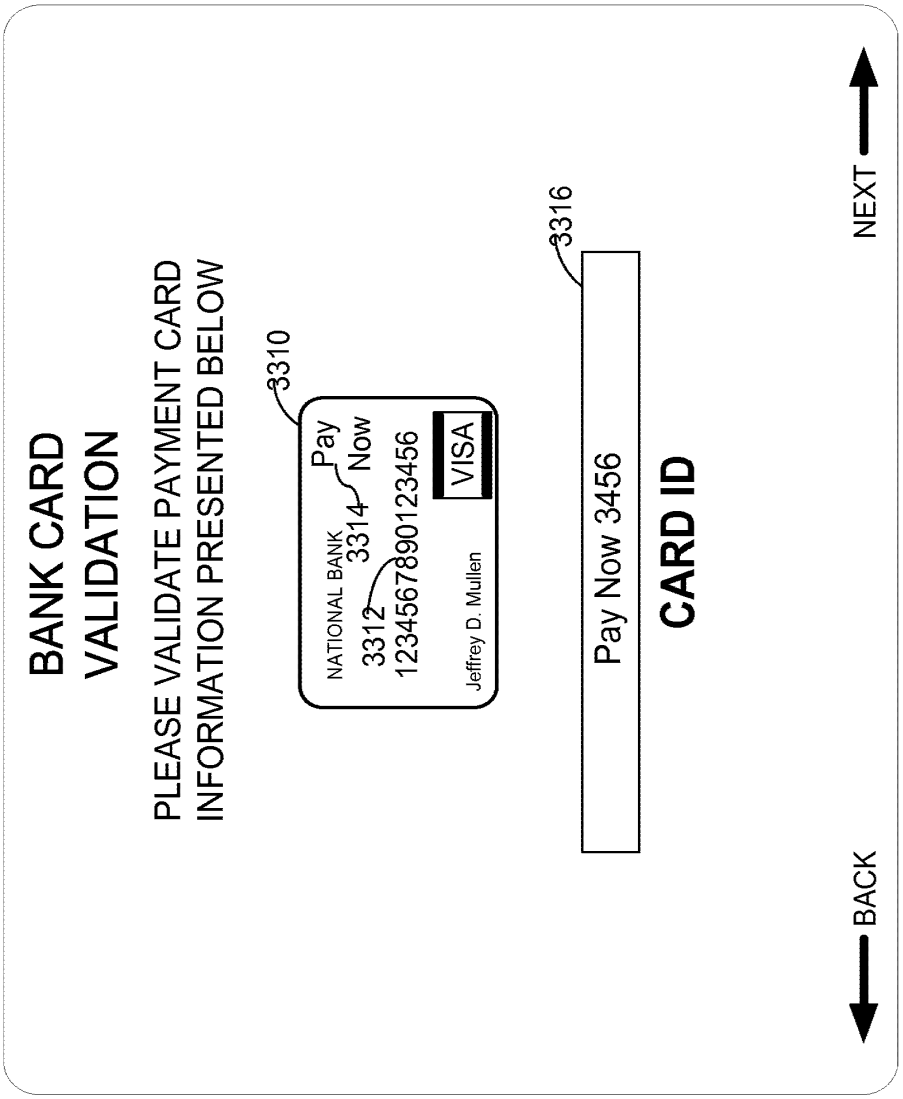

BANK CARD VALIDATION
PLEASE VALIDATE PAYMENT CARD INFORMATION PRESENTED BELOW
3310
NATIONAL BANK
3314
Pay Now
3312
1234567890123456
VISA
Jeffrey D. Mullen
3316
Pay Now 3456
CARD ID
BACK
NEXT

FIG. 33

34/73
3400

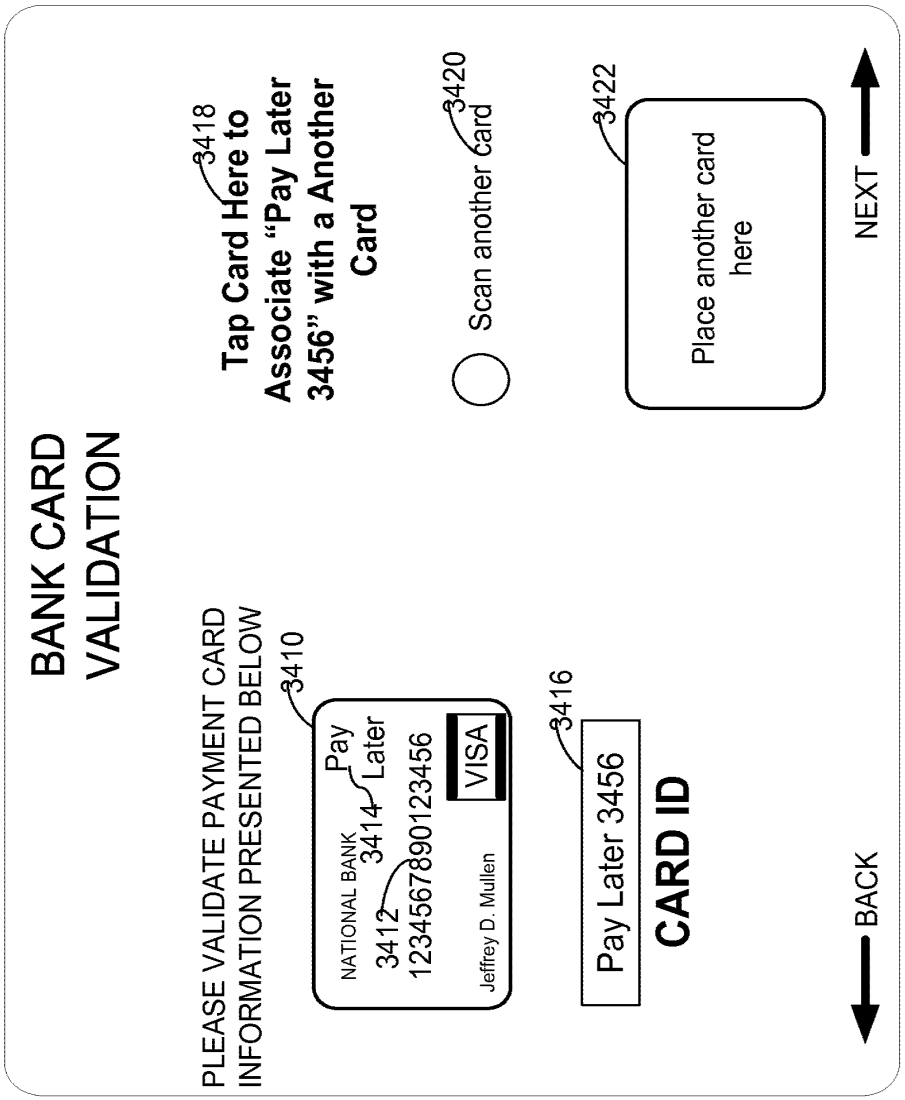


FIG. 34

35/73
3500

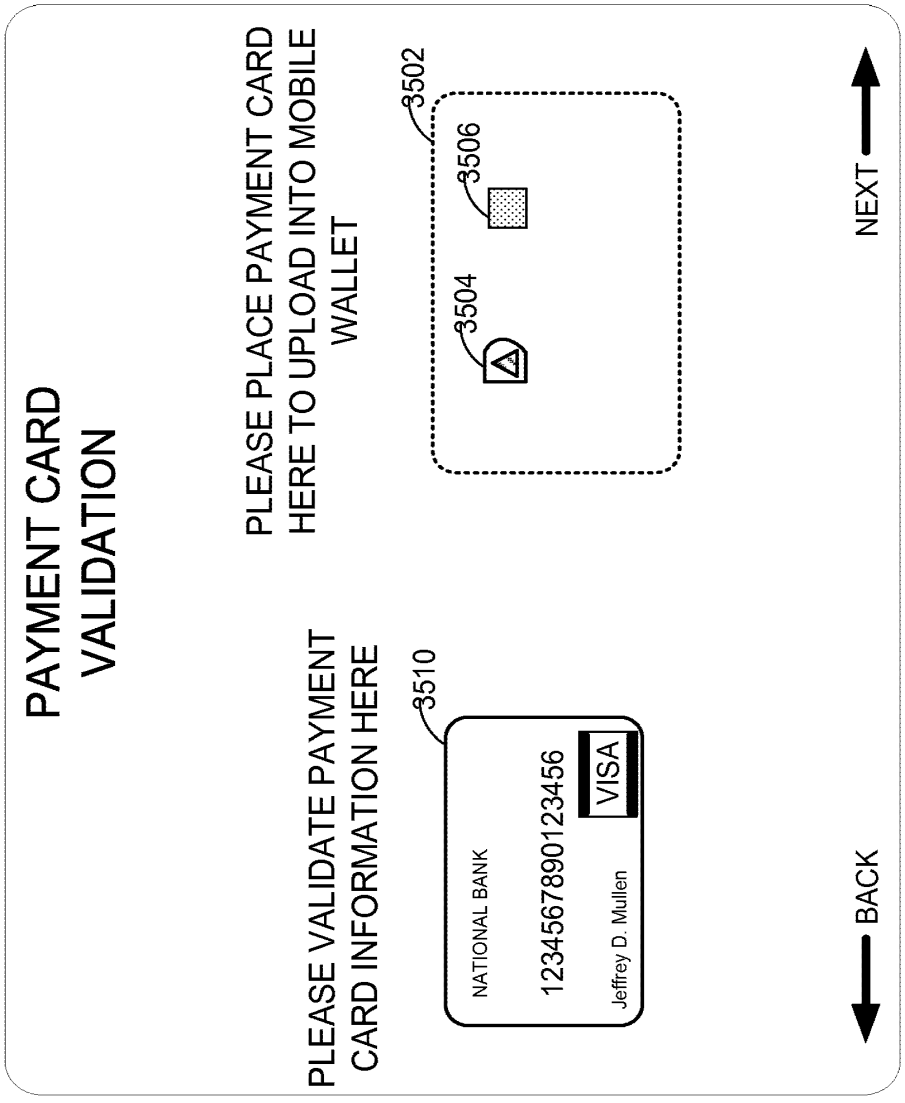


FIG. 35

36/73
3600

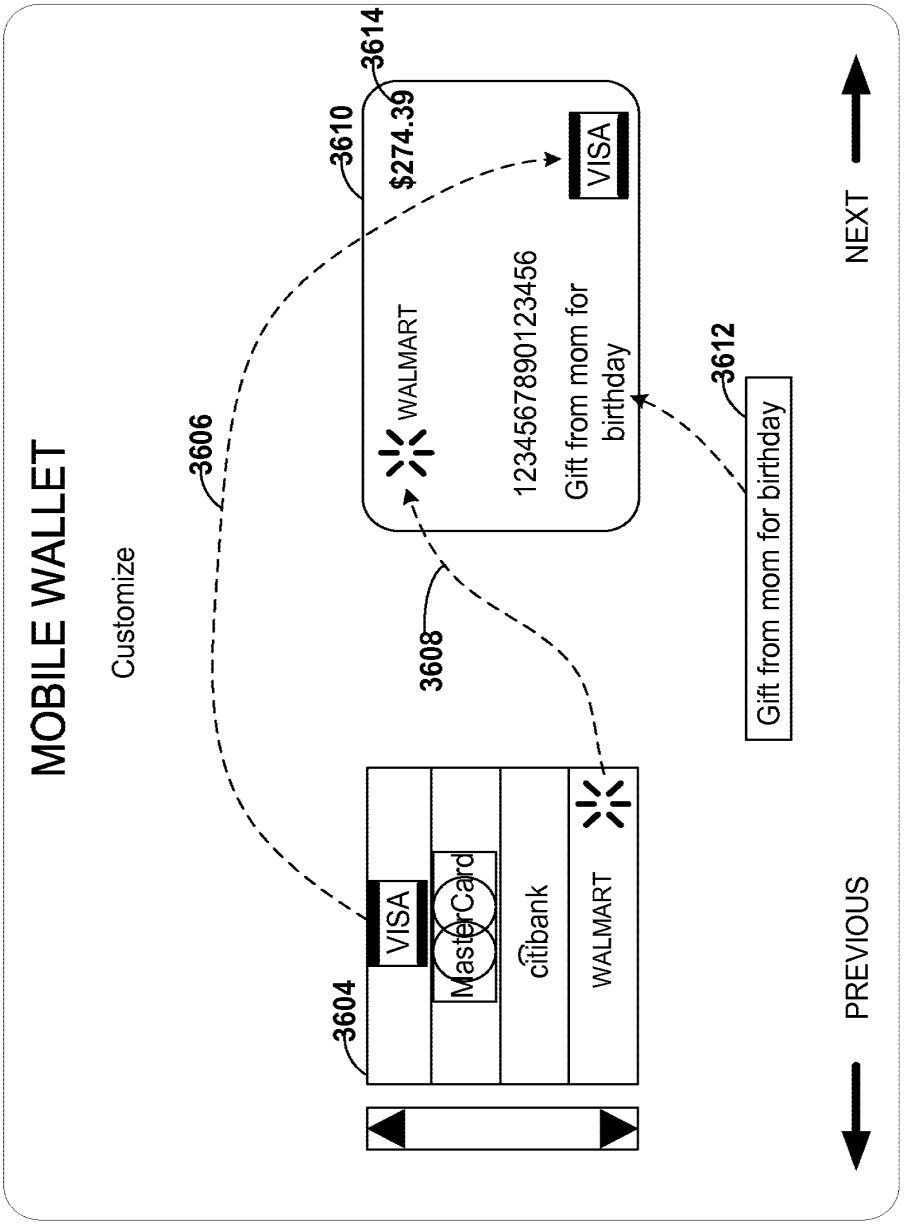


FIG. 36

37/73
3700

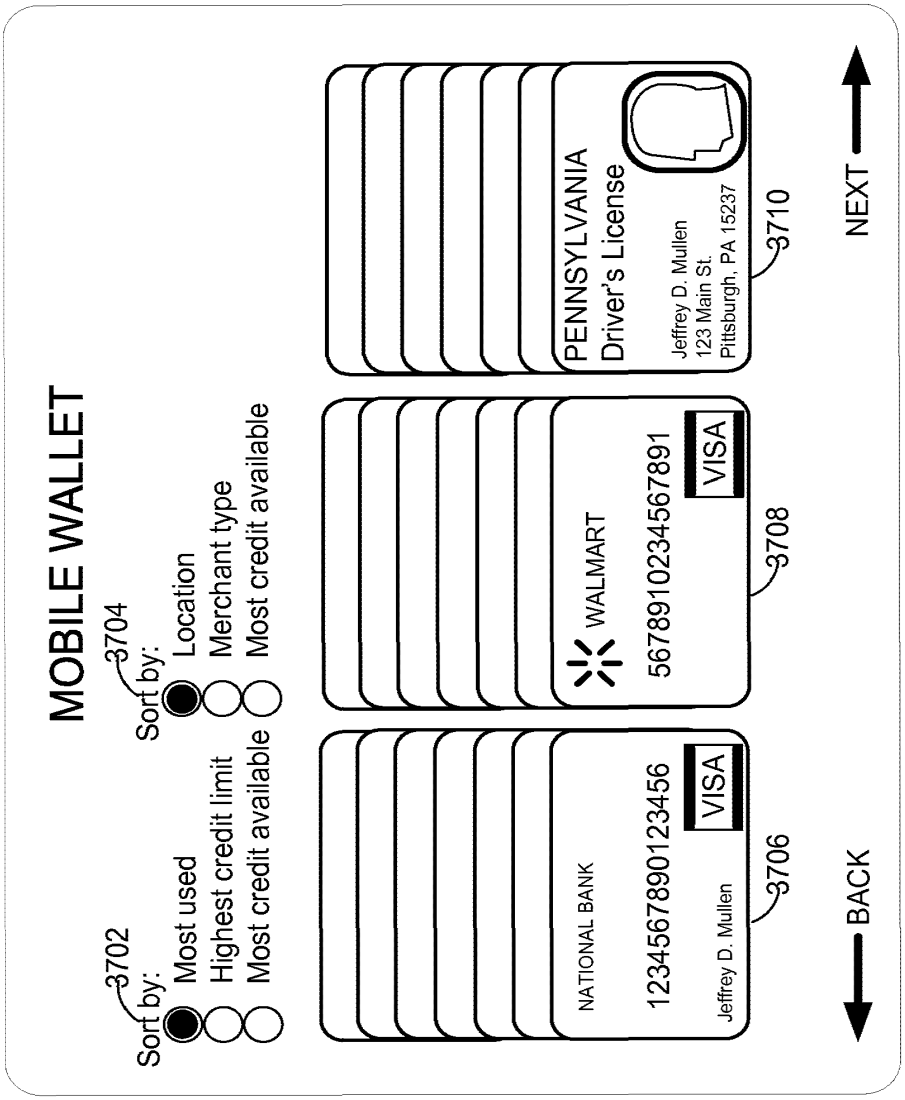


FIG. 37

3800

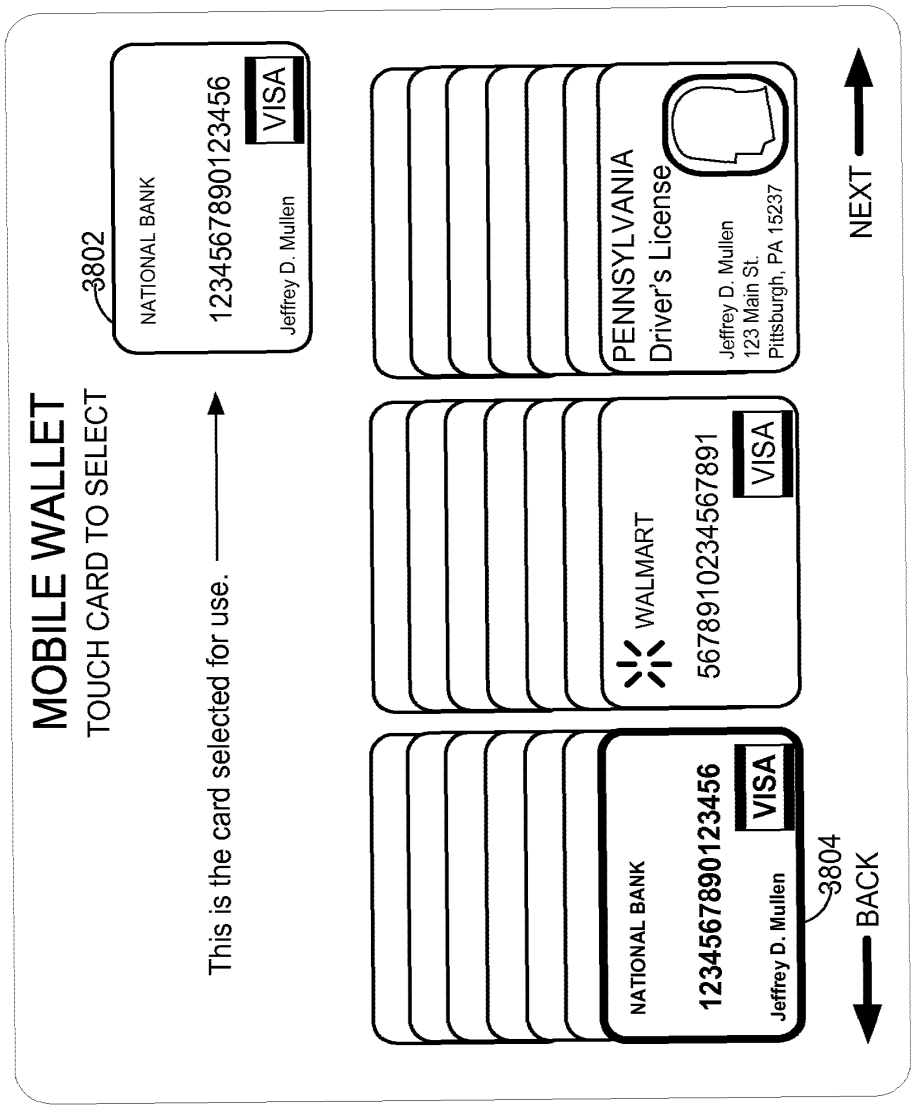

MOBILE WALLET
TOUCH CARD TO SELECT
This is the card selected for use.
3802
NATIONAL BANK
1234567890123456
Jeffrey D. Mullen
VISA
WALMART
5678910234567891
VISA
PENNSYLVANIA
Driver's License
Jeffrey D. Mullen
123 Main St.
Pittsburgh, PA 15237
NATIONAL BANK
1234567890123456
Jeffrey D. Mullen
VISA
3804
BACK
NEXT

FIG. 38

39/73
3900

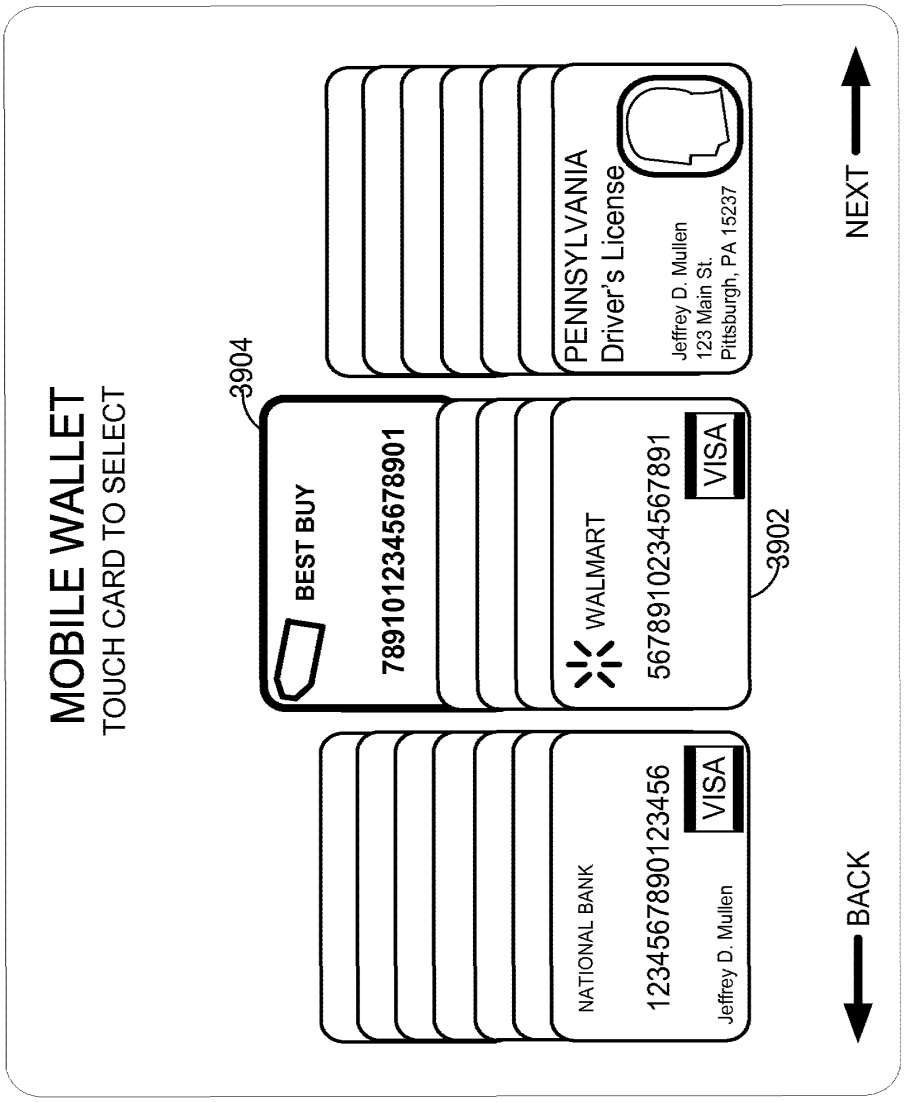


FIG. 39

40/73
4000

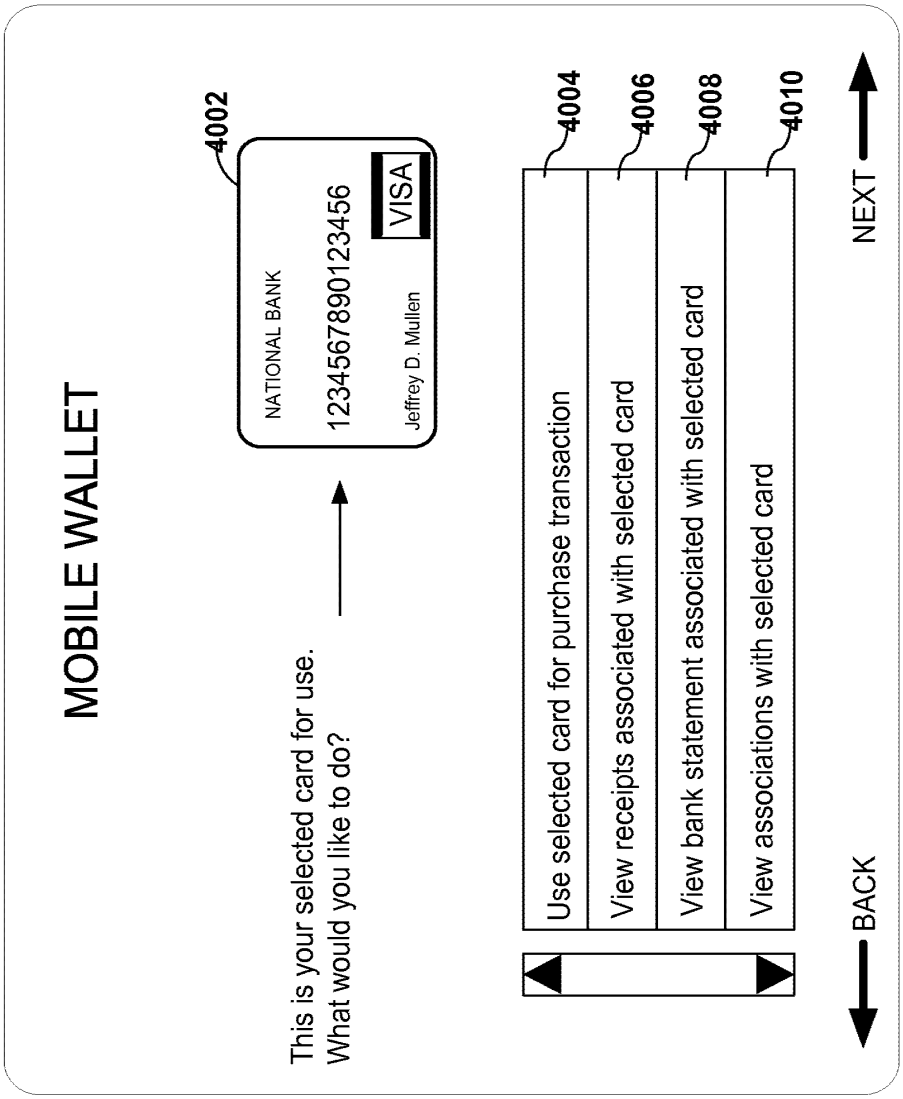


FIG. 40

41/73

4100

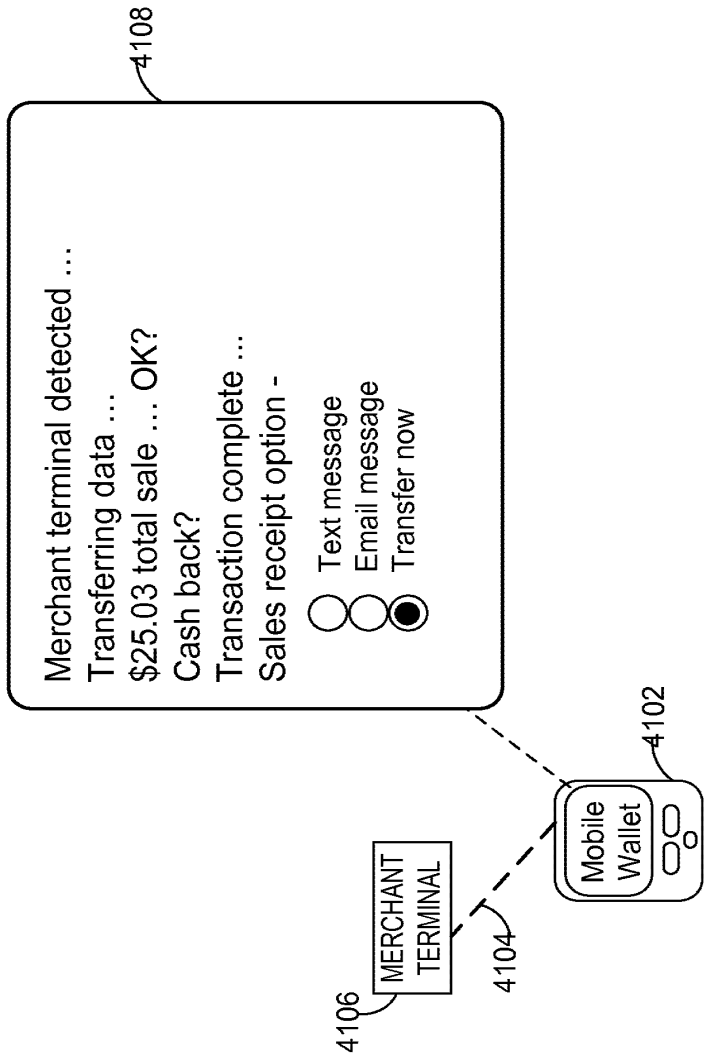


FIG. 41

4200

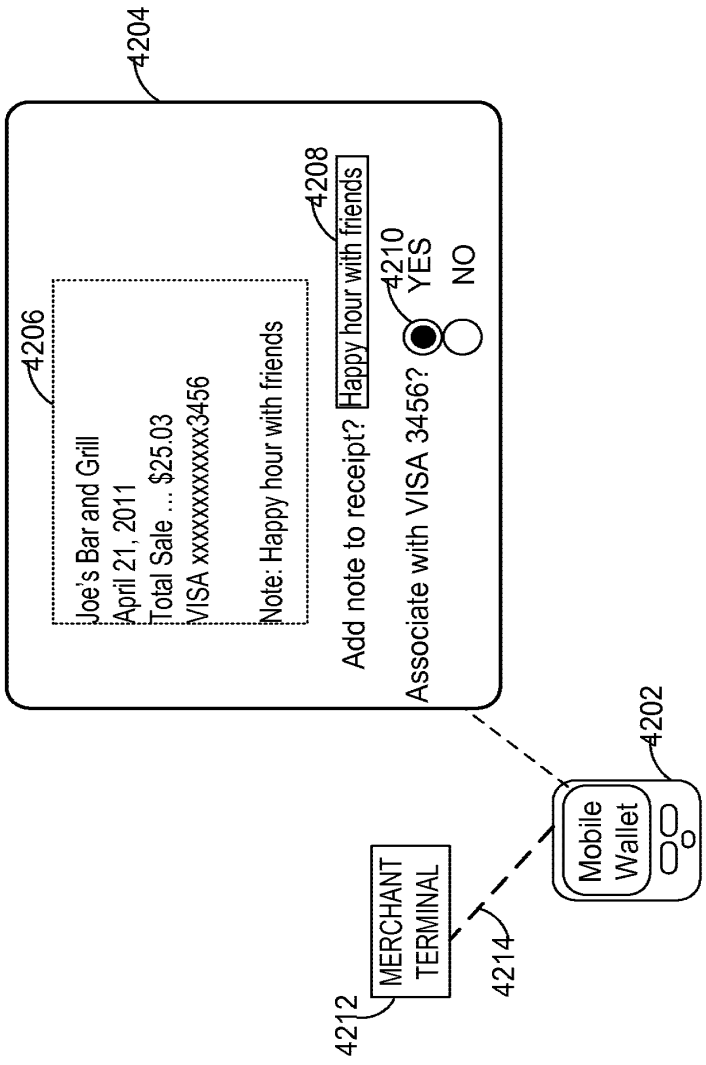

4204
4206
Joe's Bar and Grill
April 21, 2011
Total Sale ... $25.03
VISA xxxxxxxxxxx3456
Note: Happy hour with friends
4208
Add note to receipt? Happy hour with friends
4210
Associate with VISA 3456?
YES
NO
4202
Mobile Wallet
4212
MERCHANT TERMINAL
4214

FIG. 42

4300

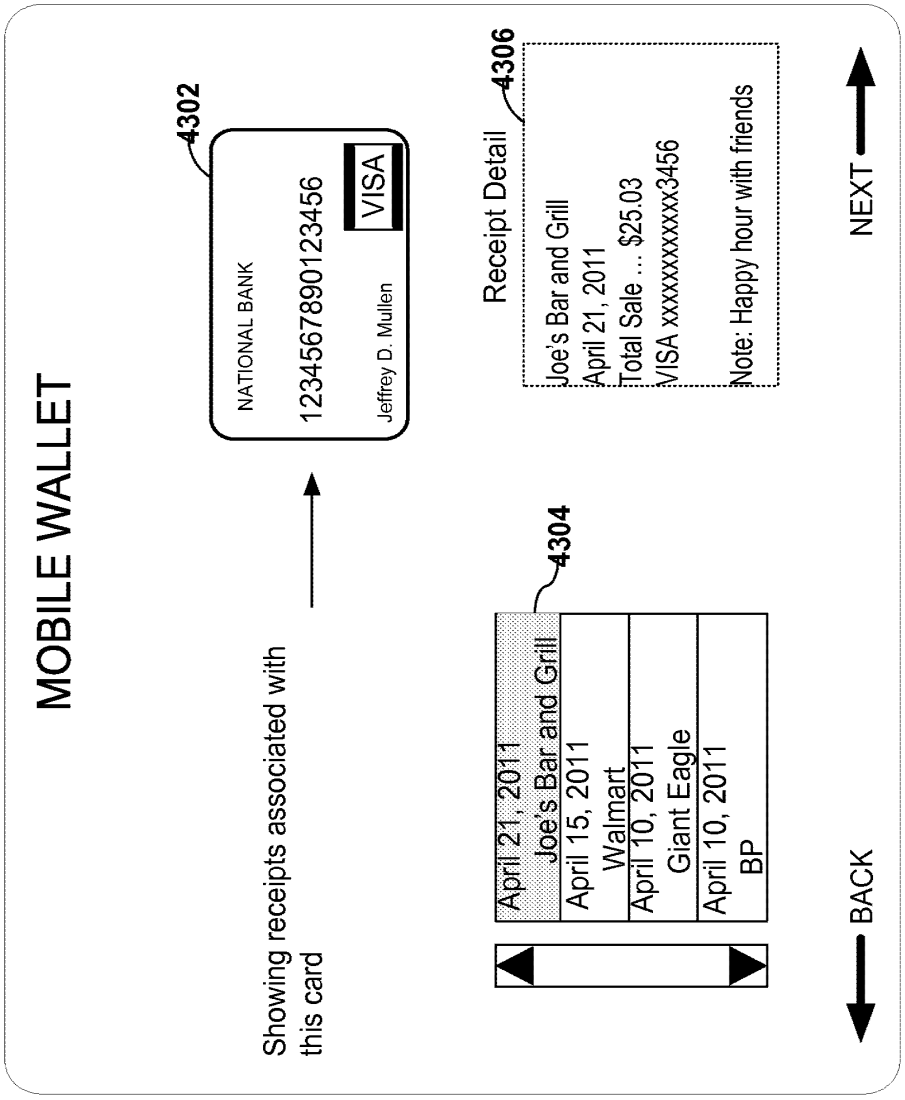

MOBILE WALLET
Showing receipts associated with this card
4302
NATIONAL BANK
1234567890123456
Jeffrey D. Mullen
VISA
4304
April 21, 2011
Joe's Bar and Grill
April 15, 2011
Walmart
April 10, 2011
Giant Eagle
April 10, 2011
BP
Receipt Detail
4306
Joe's Bar and Grill
April 21, 2011
Total Sale ... $25.03
VISA xxxxxxxxxxx3456
Note: Happy hour with friends
BACK
NEXT

FIG. 43

4400

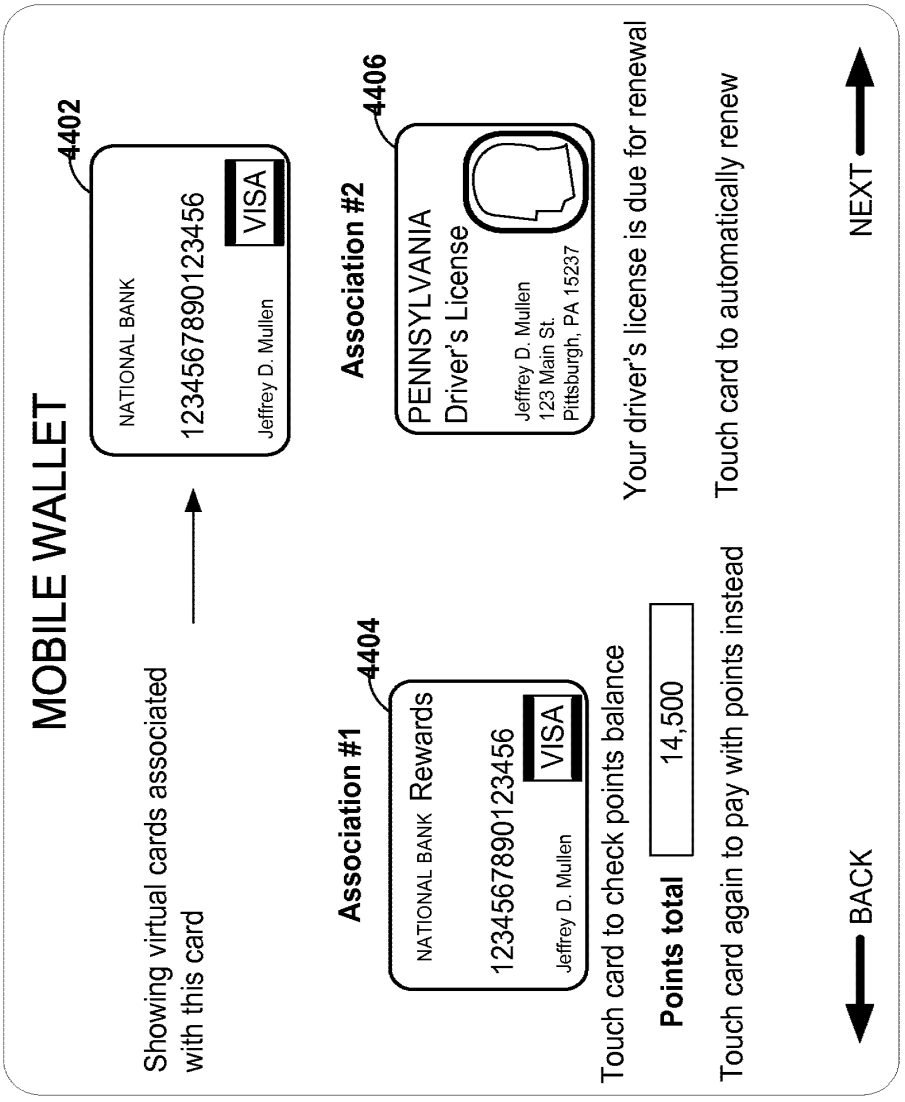

MOBILE WALLET
4402
NATIONAL BANK
1234567890123456
Jeffrey D. Mullen
VISA
Showing virtual cards associated with this card
Association #2
4406
PENNSYLVANIA
Driver's License
Jeffrey D. Mullen
123 Main St.
Pittsburgh, PA 15237
Your driver's license is due for renewal
Touch card to automatically renew
Association #1
4404
NATIONAL BANK Rewards
1234567890123456
Jeffrey D. Mullen
VISA
Touch card to check points balance
Points total
14,500
Touch card again to pay with points instead
BACK
NEXT

FIG. 44

4500

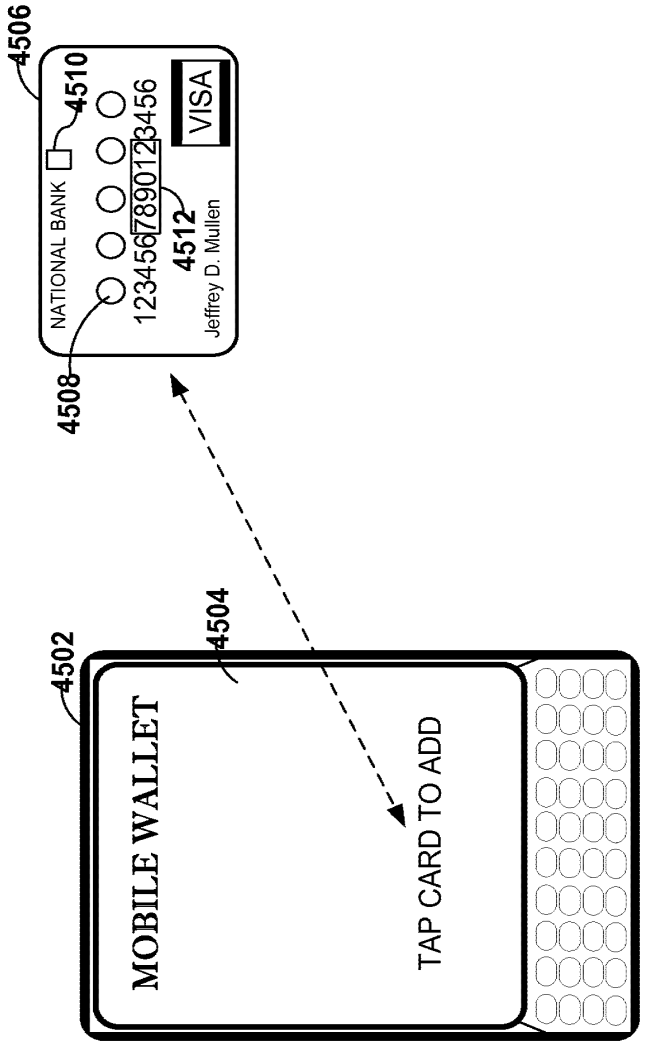

4506
4510
NATIONAL BANK
1234567890123456
VISA
4512
Jeffrey D. Mullen
4508
4502
4504
MOBILE WALLET
TAP CARD TO ADD

FIG. 45

4600

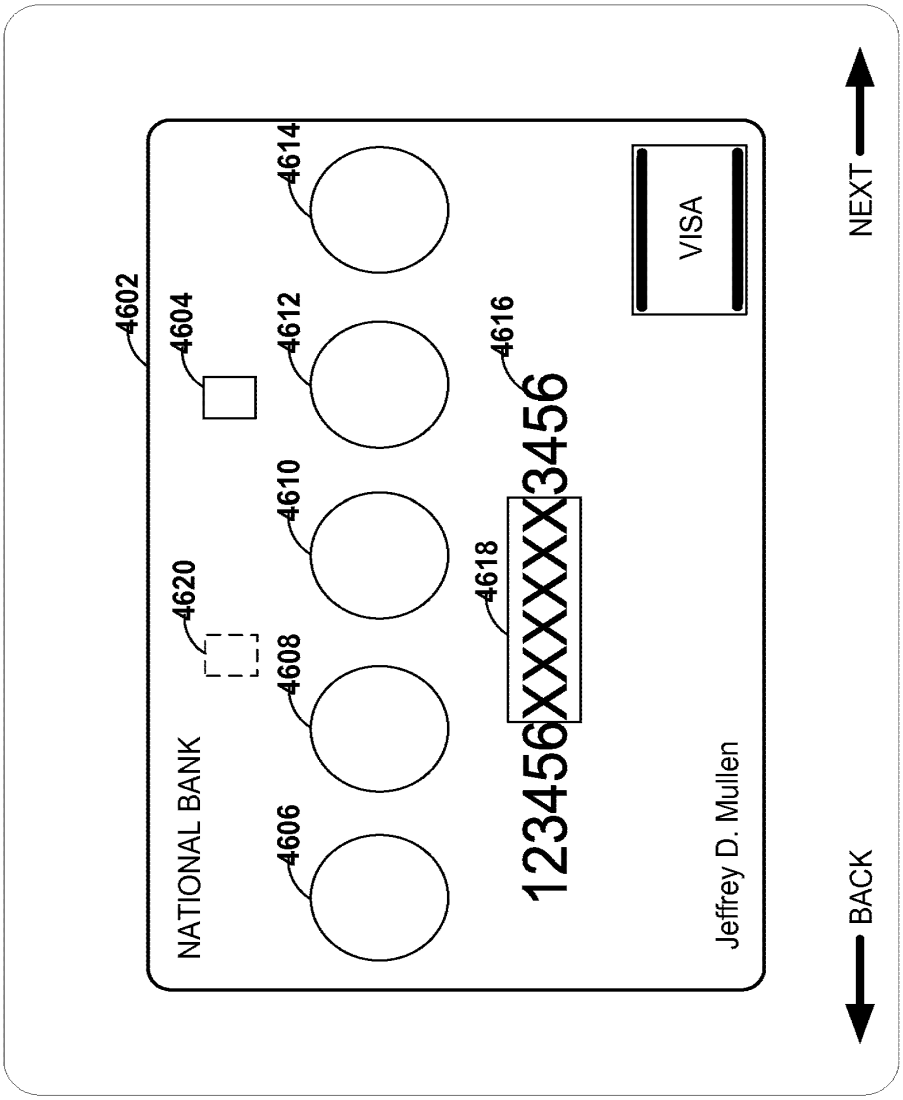

4602
4604
4606
4608
4610
4612
4614
4616
4618
4620
NATIONAL BANK
123456XXXXXX3456
Jeffrey D. Mullen
VISA
NEXT
BACK

FIG. 46

47/73
4700

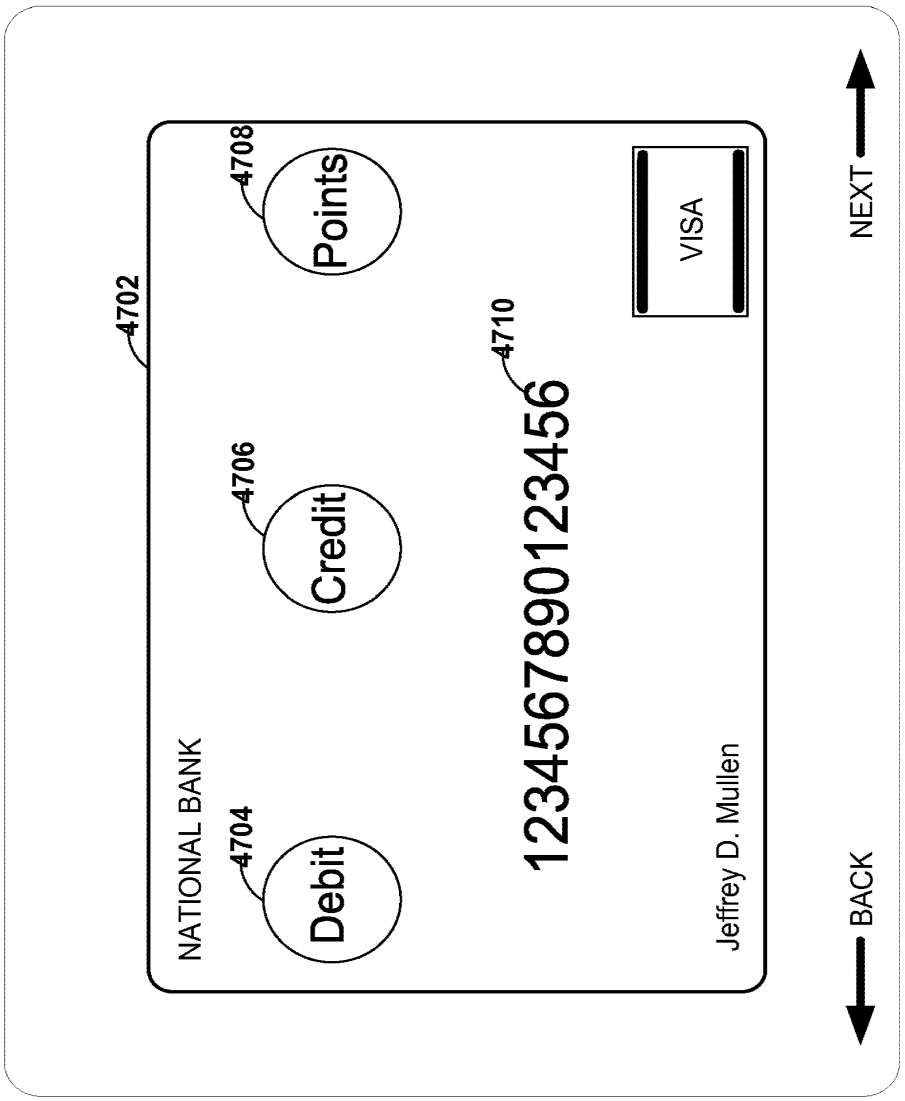


FIG. 47

4800

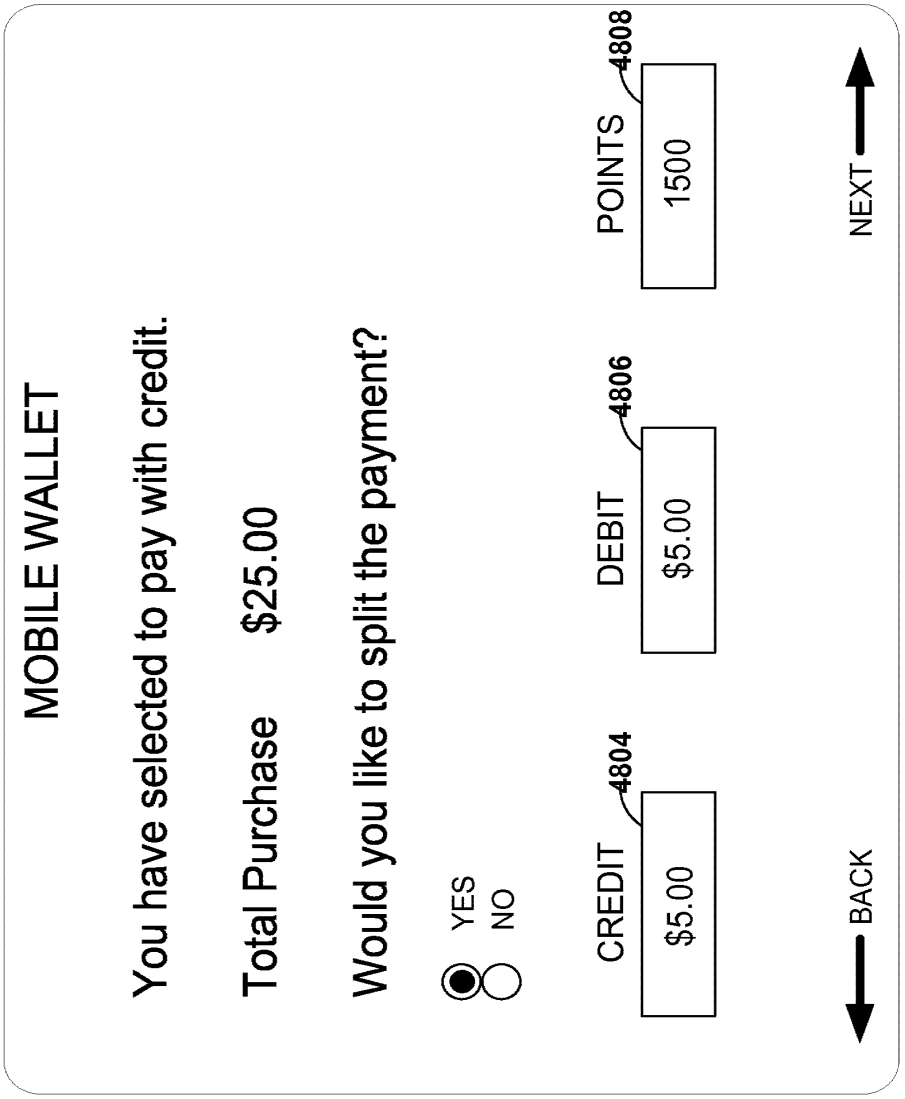

MOBILE WALLET
You have selected to pay with credit.
Total Purchase $25.00
Would you like to split the payment?
YES
NO
CREDIT
4804
$5.00
DEBIT
4806
$5.00
POINTS
4808
1500
BACK
NEXT

FIG. 48

4900

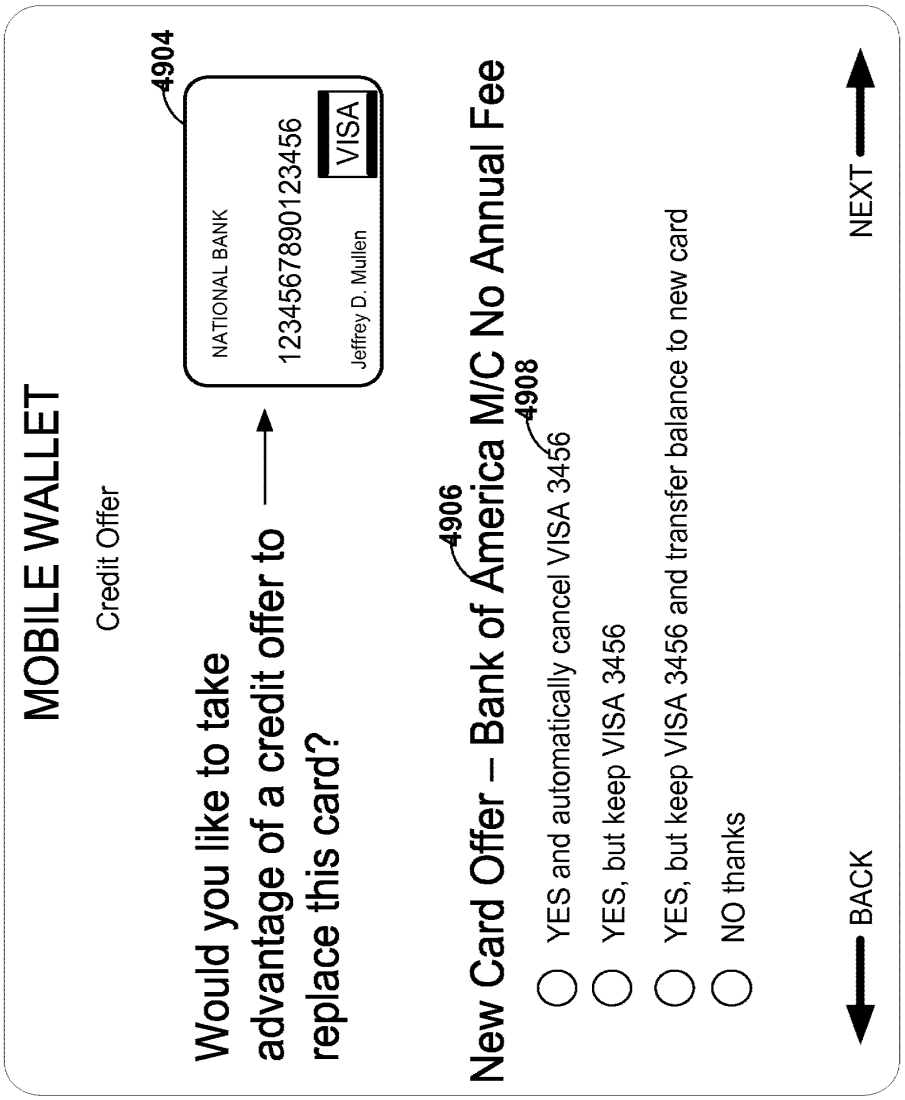

MOBILE WALLET
Credit Offer
Would you like to take advantage of a credit offer to replace this card?
4904
NATIONAL BANK
1234567890123456
VISA
Jeffrey D. Mullen
New Card Offer – Bank of America M/C No Annual Fee
4906
4908
YES and automatically cancel VISA 3456
YES, but keep VISA 3456
YES, but keep VISA 3456 and transfer balance to new card
NO thanks
BACK
NEXT

FIG. 49

5000

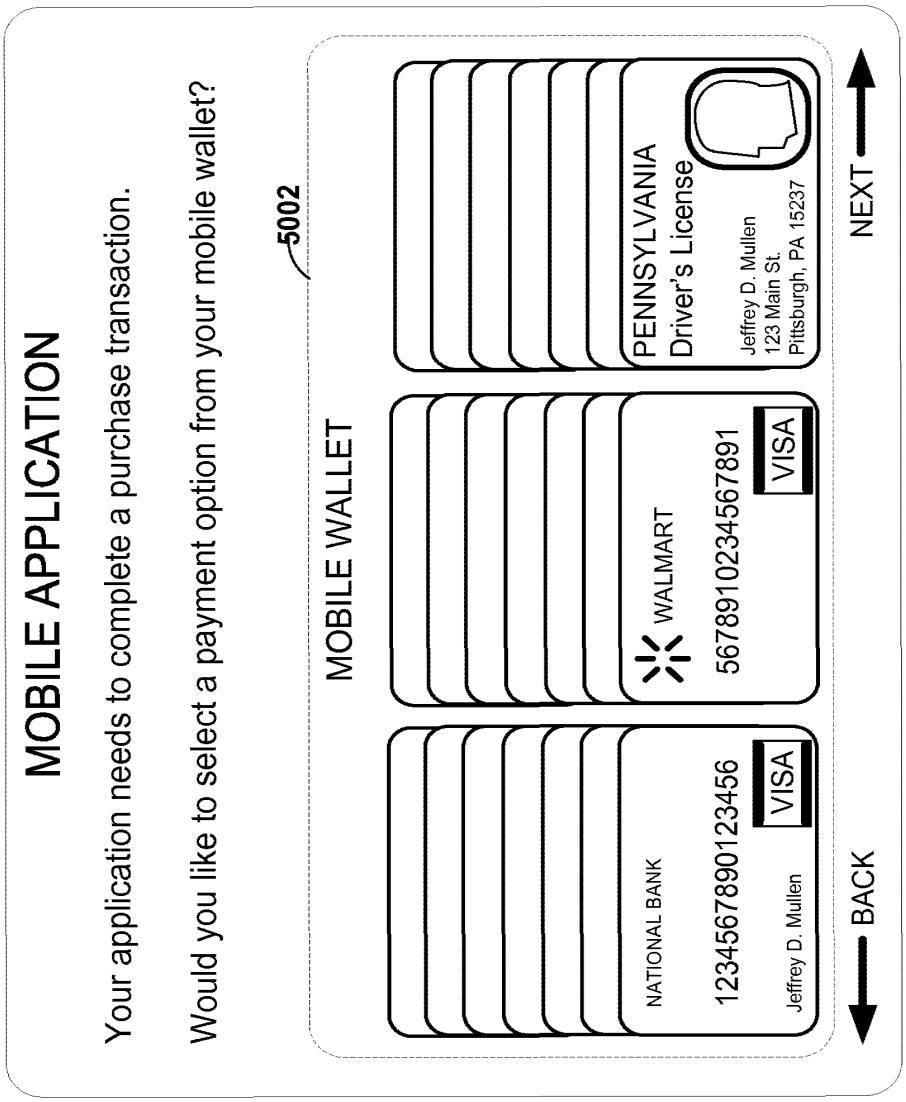

MOBILE APPLICATION
Your application needs to complete a purchase transaction.
Would you like to select a payment option from your mobile wallet?
5002
MOBILE WALLET
NATIONAL BANK
1234567890123456
Jeffrey D. Mullen
VISA
WALMART
5678910234567891
VISA
PENNSYLVANIA
Driver's License
Jeffrey D. Mullen
123 Main St.
Pittsburgh, PA 15237
BACK
NEXT

FIG. 50

51/73

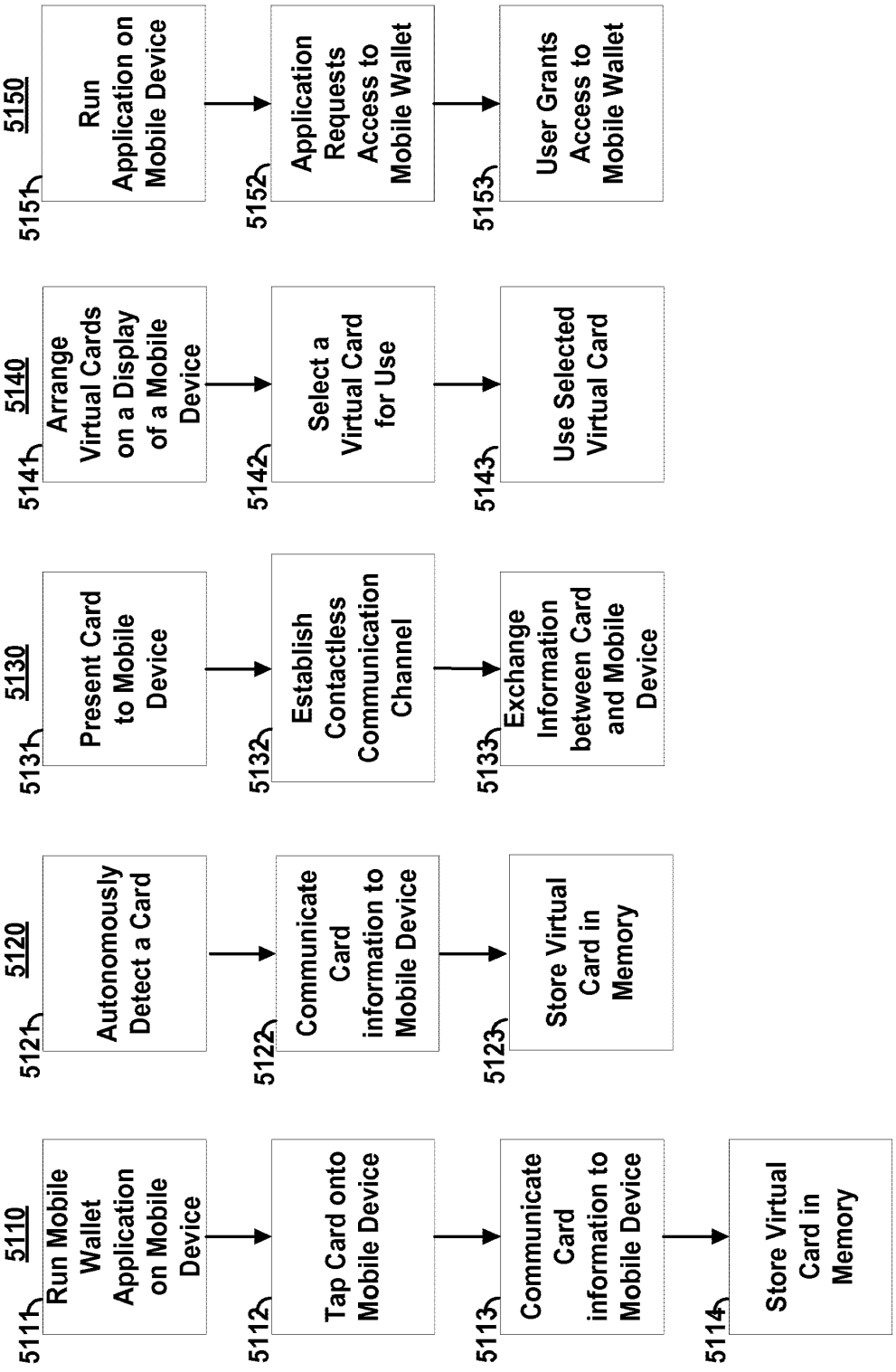

5110
Run Mobile Wallet Application on Mobile Device
5111
Tap Card onto Mobile Device
5112
Communicate Card information to Mobile Device
5113
Store Virtual Card in Memory
5114
5120
Autonomously Detect a Card
5121
Communicate Card information to Mobile Device
5122
Store Virtual Card in Memory
5123
5130
Present Card to Mobile Device
5131
Establish Contactless Communication Channel
5132
Exchange Information between Card and Mobile Device
5133
5140
Arrange Virtual Cards on a Display of a Mobile Device
5141
Select a Virtual Card for Use
5142
Use Selected Virtual Card
5143
5150
Run Application on Mobile Device
5151
Application Requests Access to Mobile Wallet
5152
User Grants Access to Mobile Wallet
5153

FIG. 51

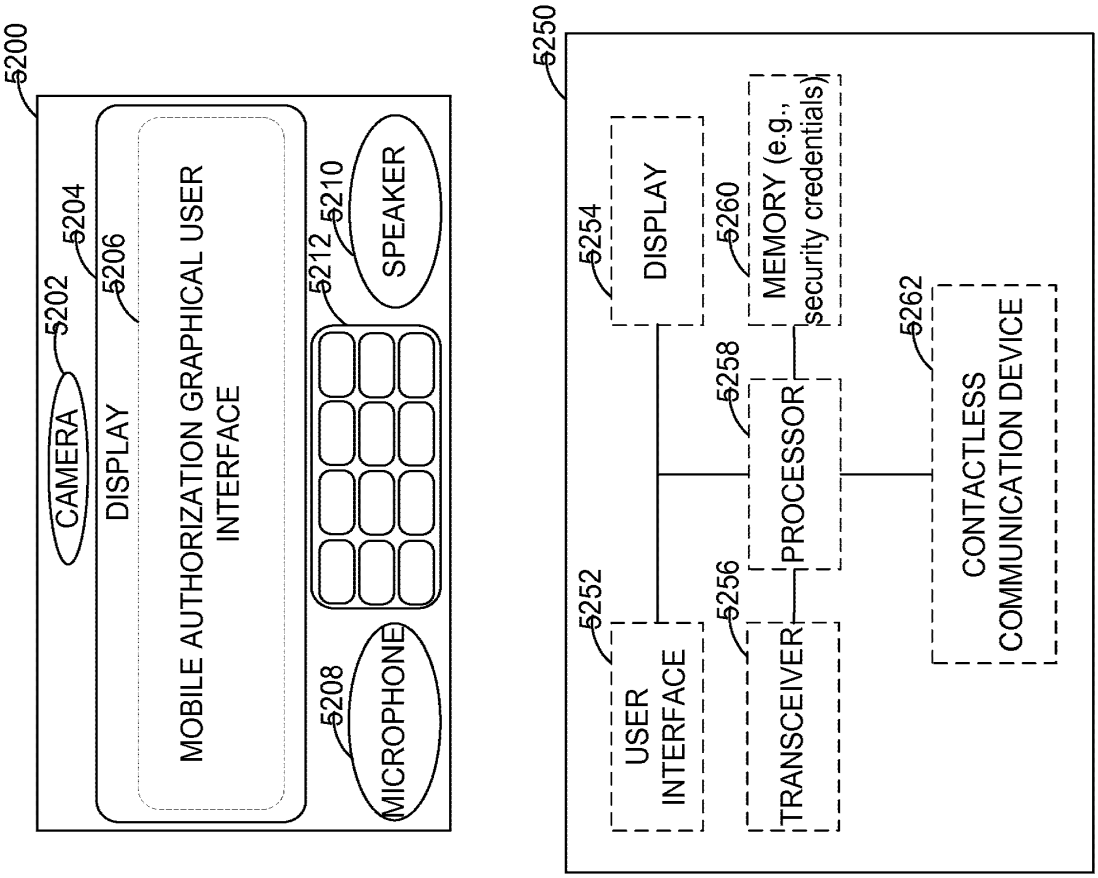

5200
CAMERA
5202
DISPLAY
5204
MOBILE AUTHORIZATION GRAPHICAL USER INTERFACE
5206
5212
SPEAKER
5210
MICROPHONE
5208
5250
USER INTERFACE
5252
DISPLAY
5254
TRANSCEIVER
5256
PROCESSOR
5258
MEMORY (e.g., security credentials)
5260
CONTACTLESS COMMUNICATION DEVICE
5262

FIG. 52

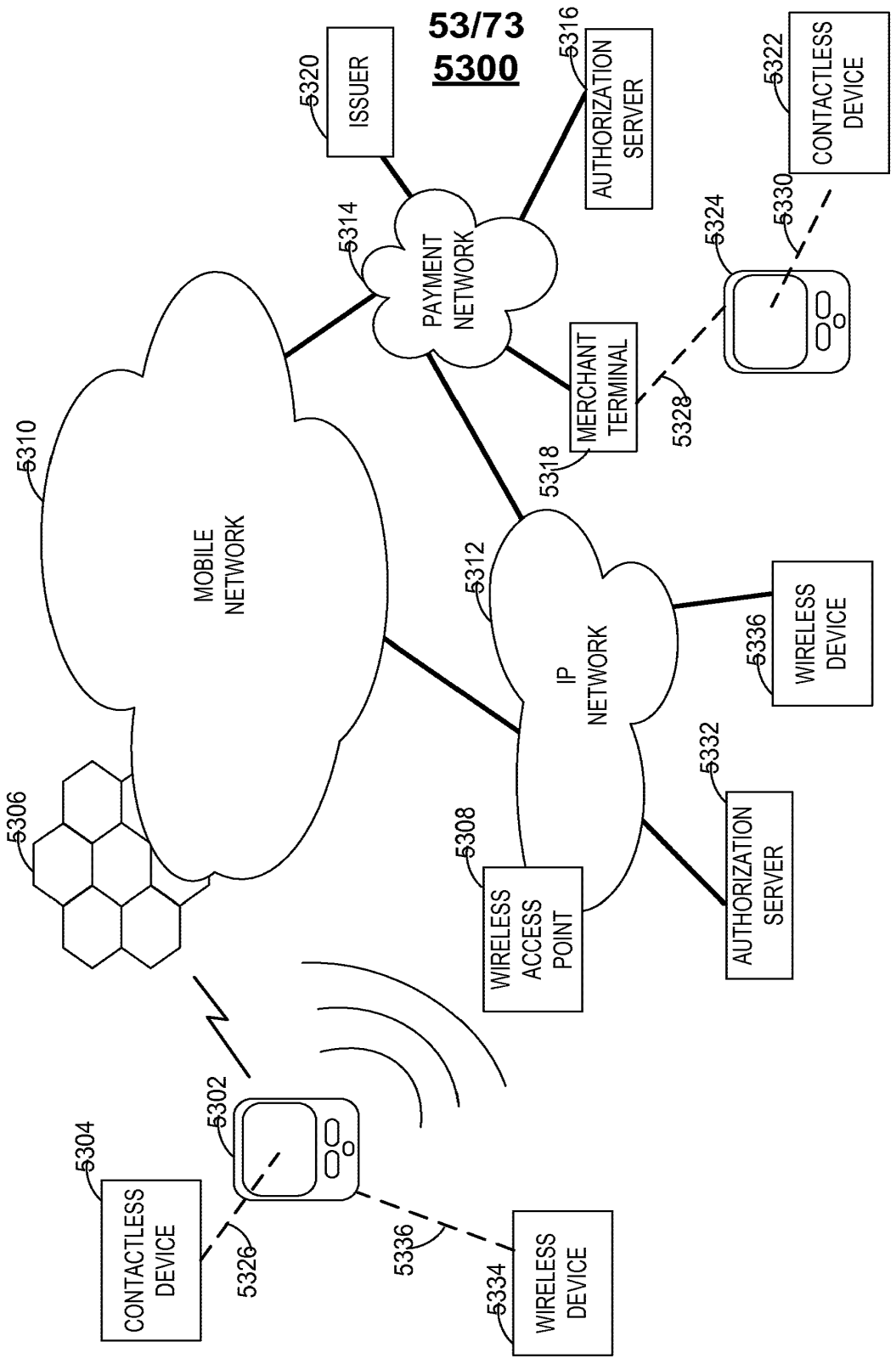

53/73
5300
ISSUER
5320
AUTHORIZATION SERVER
5316
CONTACTLESS DEVICE
5322
PAYMENT NETWORK
5314
5330
5324
MERCHANT TERMINAL
5318
5328
MOBILE NETWORK
5310
IP NETWORK
5312
WIRELESS DEVICE
5336
AUTHORIZATION SERVER
5332
5306
WIRELESS ACCESS POINT
5308
5302
5304
CONTACTLESS DEVICE
5326
5336
WIRELESS DEVICE
5334

FIG. 53

54/73
5400

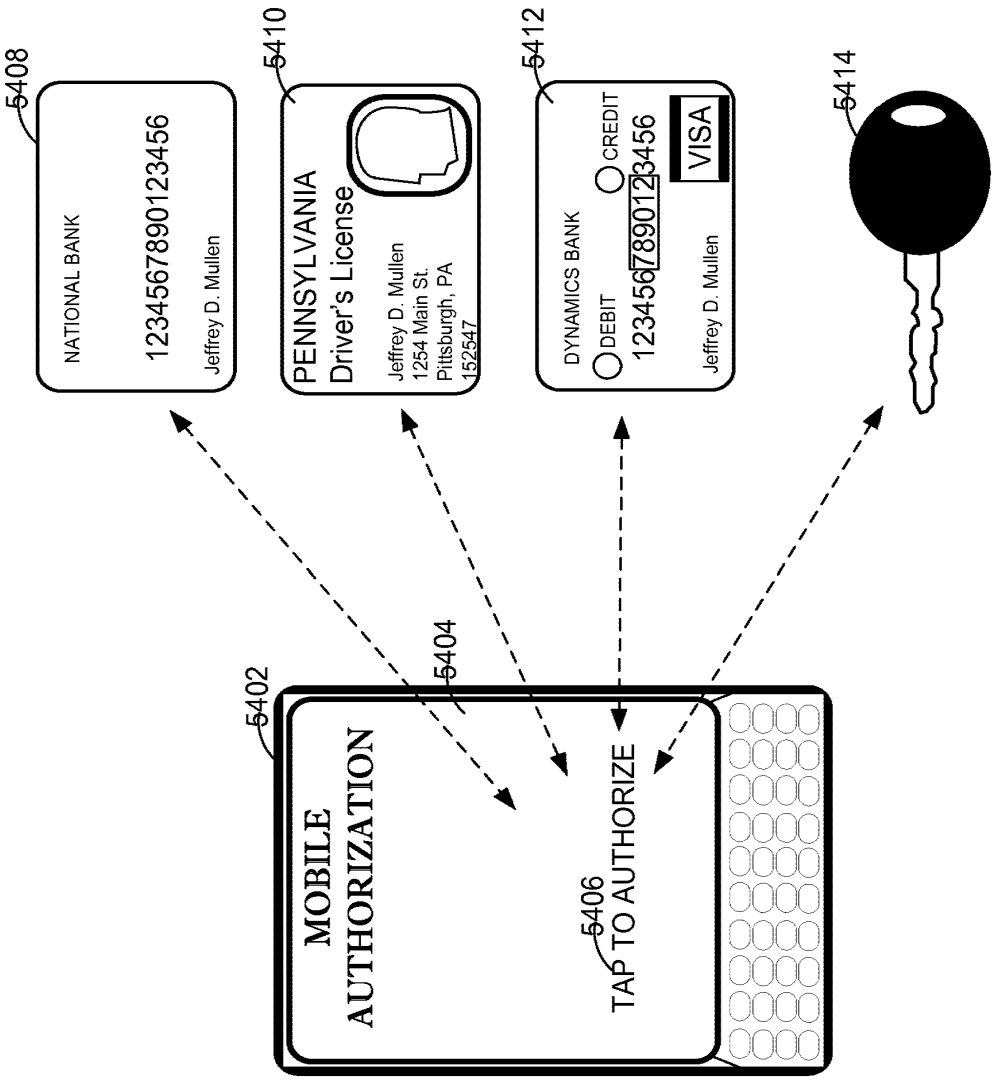


FIG. 54

5500

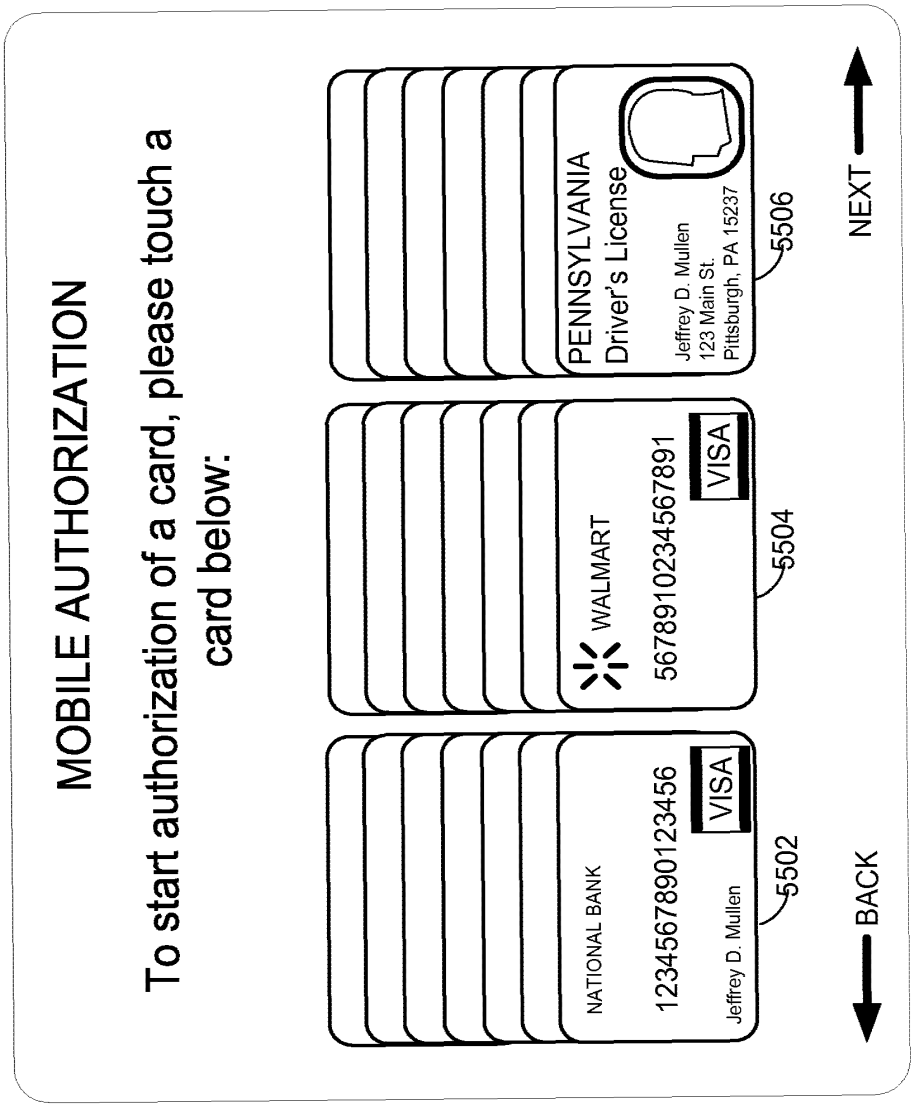

MOBILE AUTHORIZATION
To start authorization of a card, please touch a card below:
NATIONAL BANK
1234567890123456
Jeffrey D. Mullen
VISA
5502
WALMART
5678910234567891
VISA
5504
PENNSYLVANIA
Driver's License
Jeffrey D. Mullen
123 Main St.
Pittsburgh, PA 15237
5506
BACK
NEXT

FIG. 55

5600

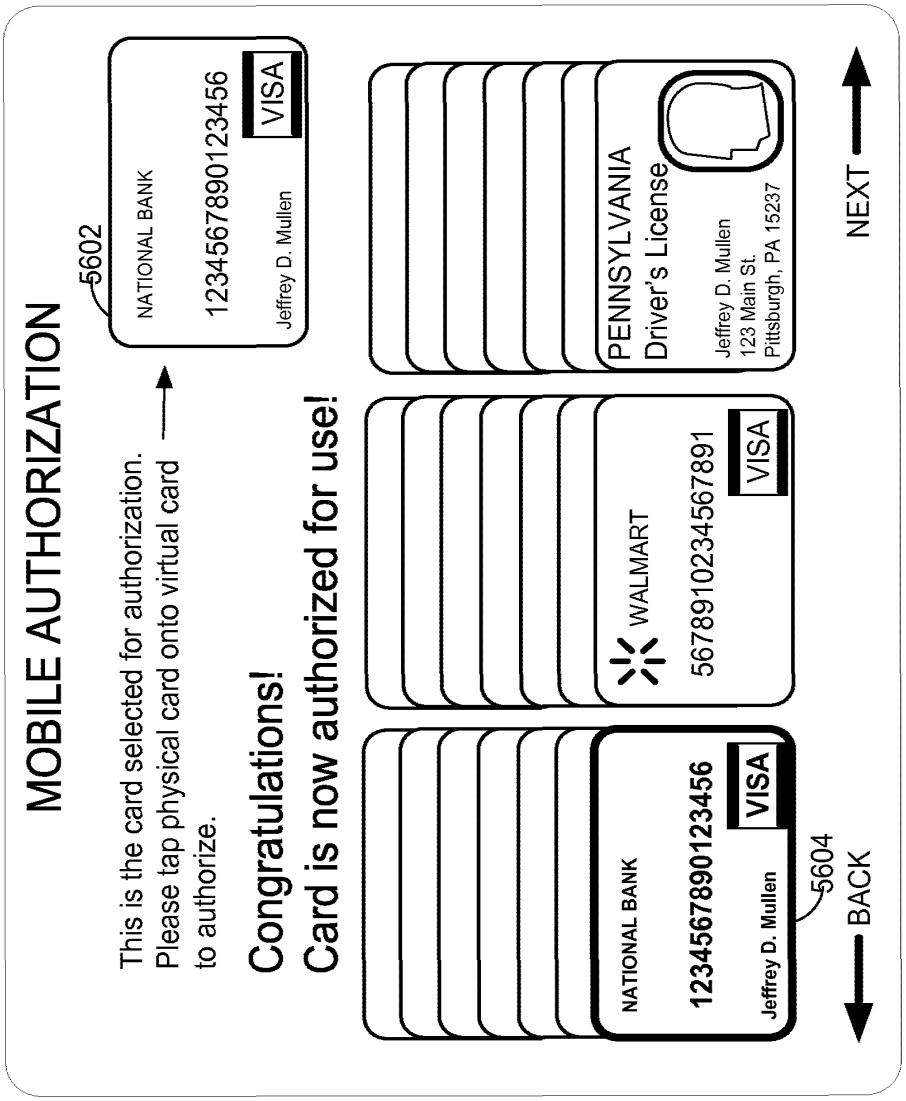

MOBILE AUTHORIZATION
This is the card selected for authorization.
Please tap physical card onto virtual card
to authorize.
Congratulations!
Card is now authorized for use!
5602
NATIONAL BANK
1234567890123456
Jeffrey D. Mullen
VISA
WALMART
5678910234567891
VISA
PENNSYLVANIA
Driver's License
Jeffrey D. Mullen
123 Main St.
Pittsburgh, PA 15237
NATIONAL BANK
1234567890123456
Jeffrey D. Mullen
VISA
5604
BACK
NEXT

FIG. 56

5700

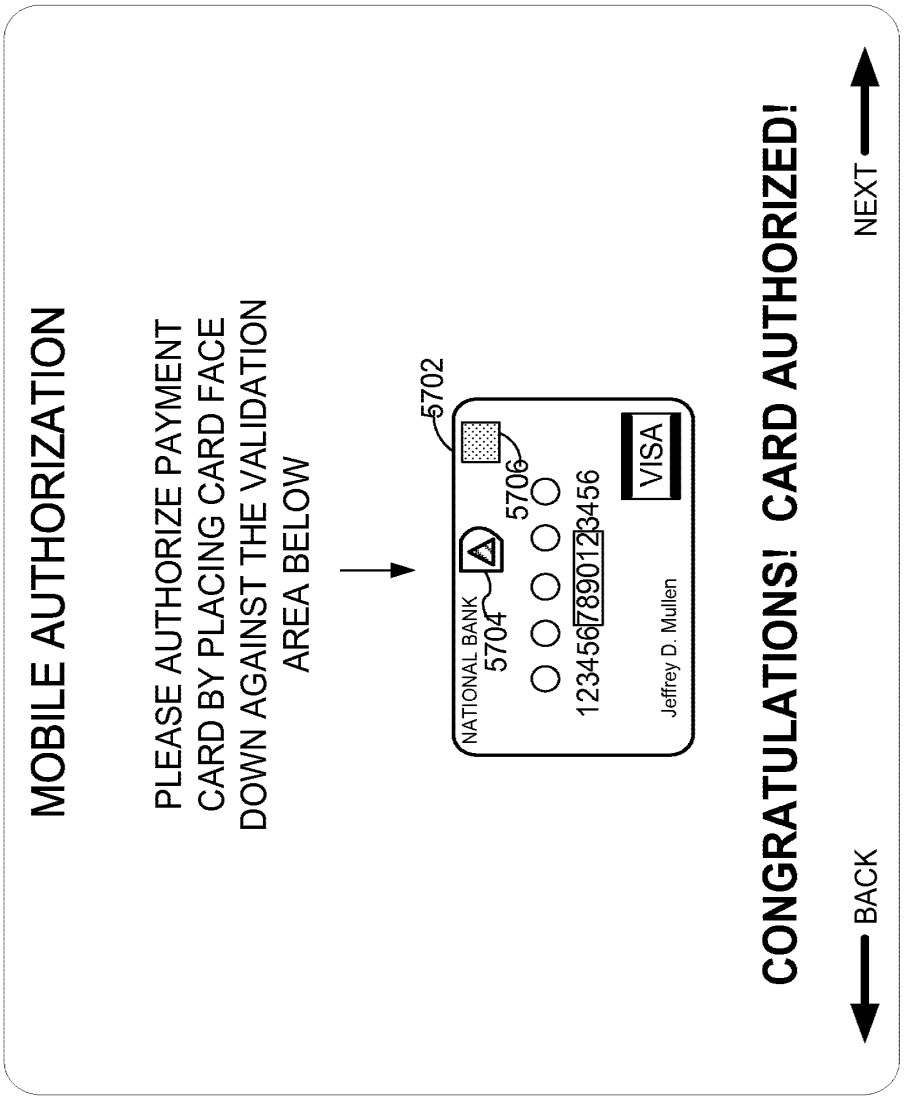

MOBILE AUTHORIZATION
PLEASE AUTHORIZE PAYMENT CARD BY PLACING CARD FACE DOWN AGAINST THE VALIDATION AREA BELOW
5702
NATIONAL BANK
5704
5706
123456789012 3456
VISA
Jeffrey D. Mullen
CONGRATULATIONS! CARD AUTHORIZED!
BACK
NEXT

FIG. 57

58/73

5800

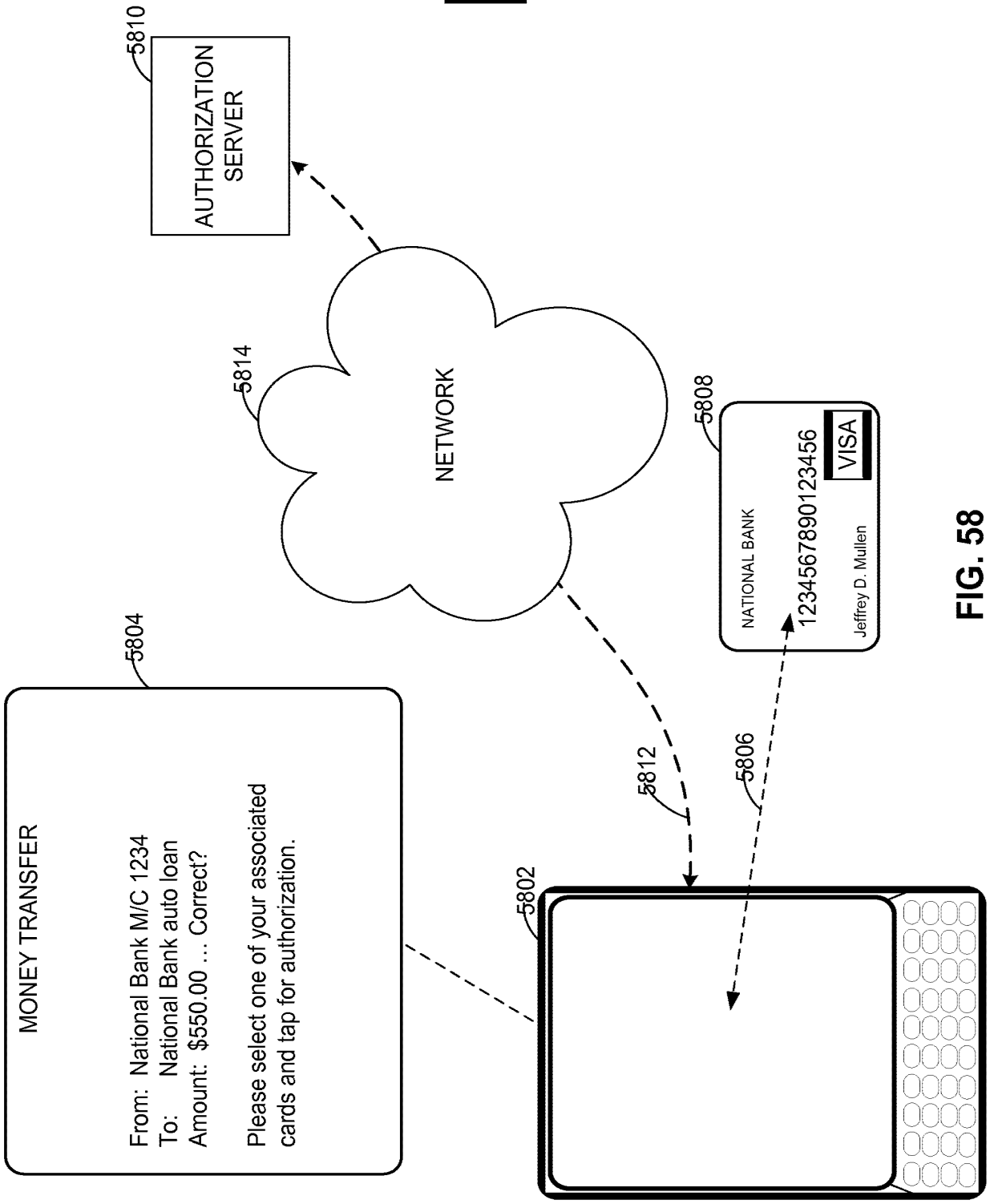


FIG. 58

5900

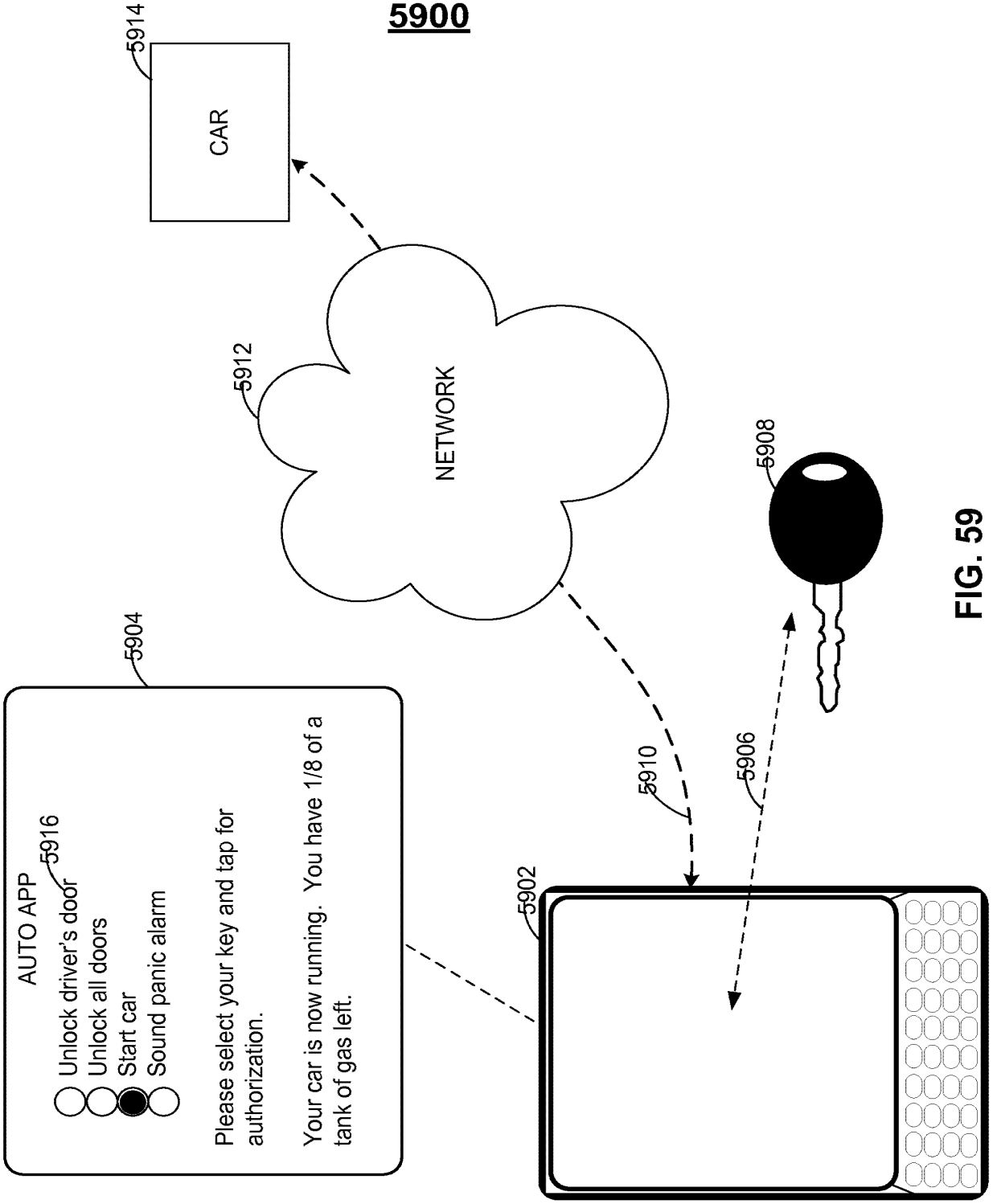

5914
CAR
5912
NETWORK
5908
5904
AUTO APP
5916
Unlock driver's door
Unlock all doors
Start car
Sound panic alarm
Please select your key and tap for authorization.
Your car is now running. You have 1/8 of a tank of gas left.
5910
5906
5902

FIG. 59

6000

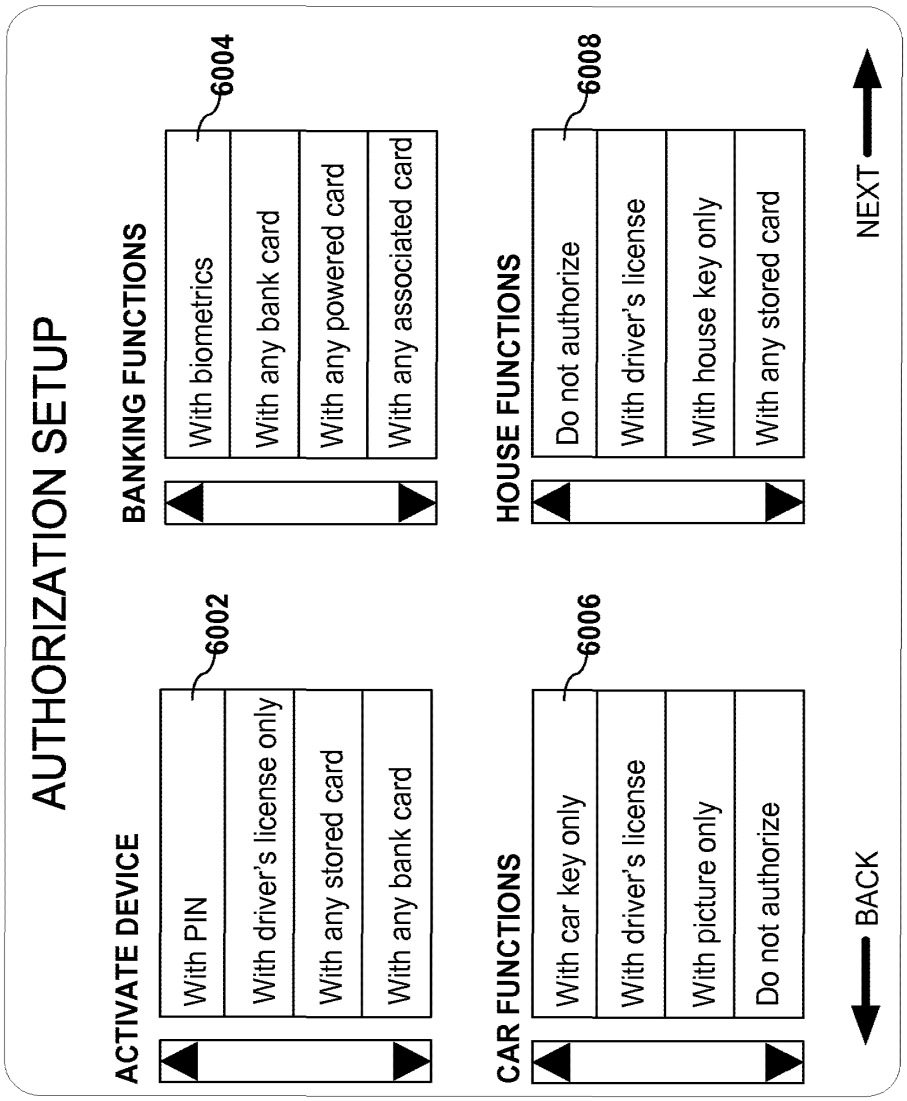

AUTHORIZATION SETUP
ACTIVATE DEVICE
With PIN
With driver's license only
With any stored card
With any bank card
6002
BANKING FUNCTIONS
With biometrics
With any bank card
With any powered card
With any associated card
6004
CAR FUNCTIONS
With car key only
With driver's license
With picture only
Do not authorize
6006
HOUSE FUNCTIONS
Do not authorize
With driver's license
With house key only
With any stored card
6008
BACK
NEXT

FIG. 60

61/73

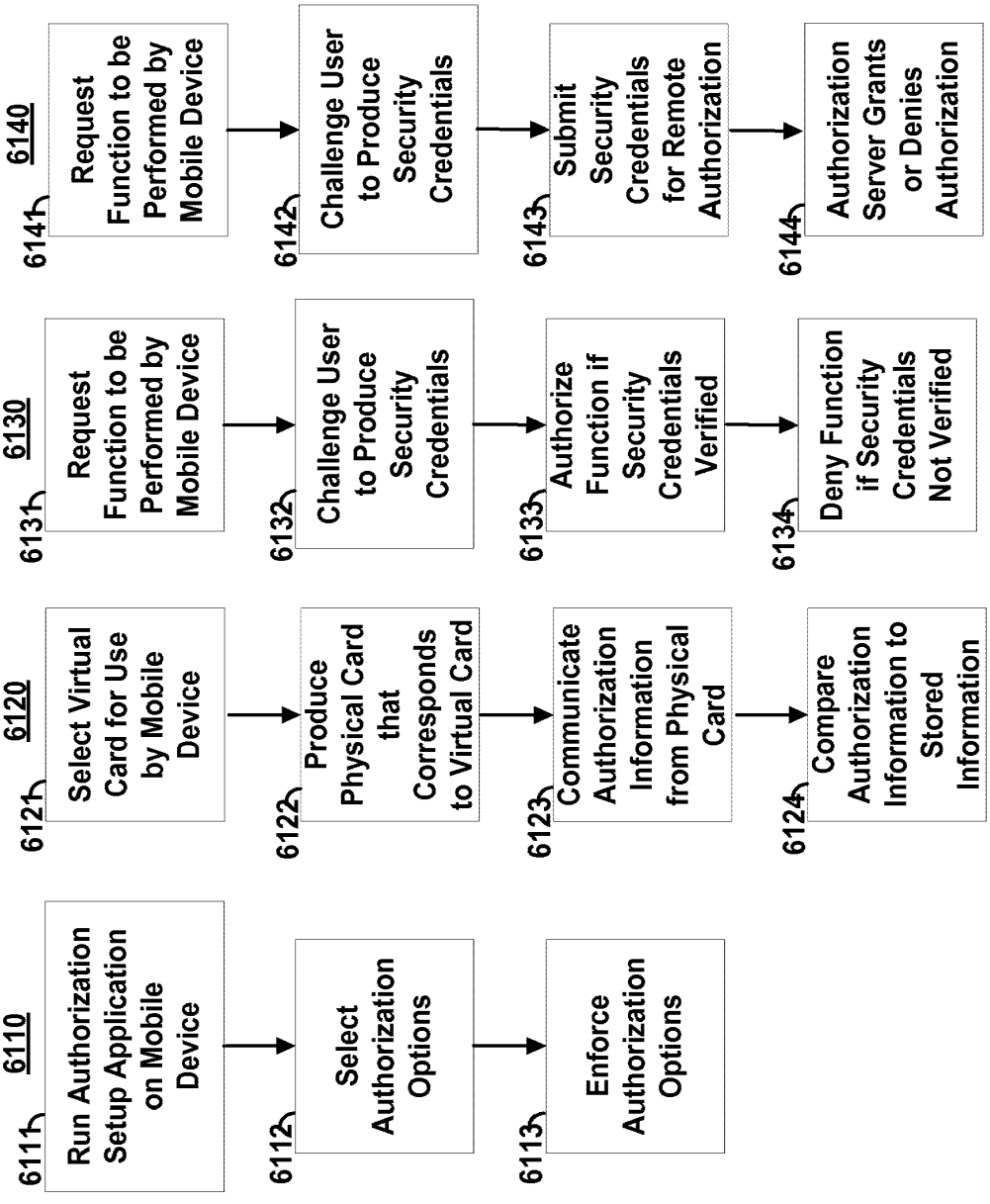

6110
6111
Run Authorization Setup Application on Mobile Device
6112
Select Authorization Options
6113
Enforce Authorization Options
6120
6121
Select Virtual Card for Use by Mobile Device
6122
Produce Physical Card that Corresponds to Virtual Card
6123
Communicate Authorization Information from Physical Card
6124
Compare Authorization Information to Stored Information
6130
6131
Request Function to be Performed by Mobile Device
6132
Challenge User to Produce Security Credentials
6133
Authorize Function if Security Credentials Verified
6134
Deny Function if Security Credentials Not Verified
6140
6141
Request Function to be Performed by Mobile Device
6142
Challenge User to Produce Security Credentials
6143
Submit Security Credentials for Remote Authorization
6144
Authorization Server Grants or Denies Authorization

FIG. 61

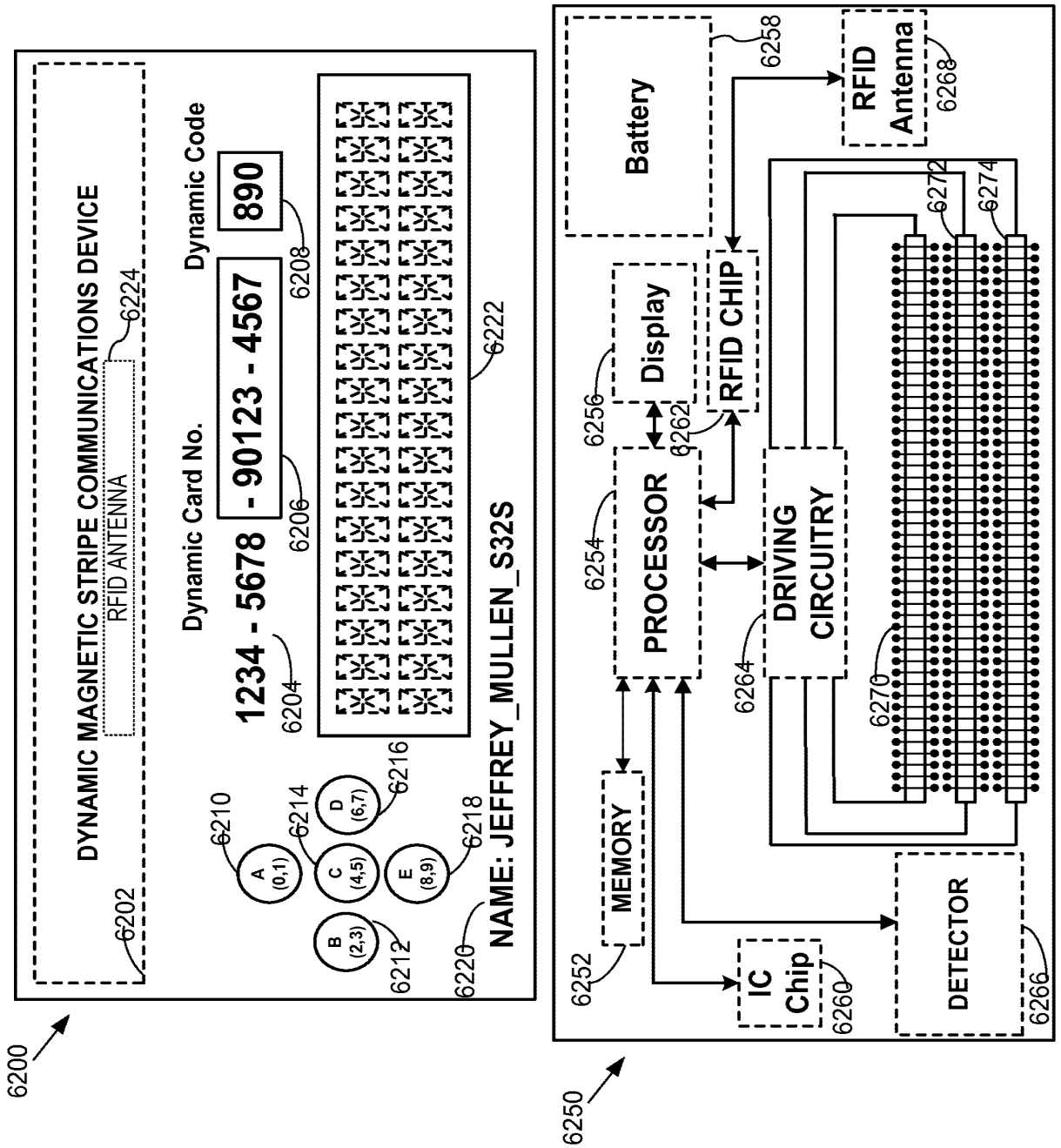

6200
DYNAMIC MAGNETIC STRIPE COMMUNICATIONS DEVICE
RFID ANTENNA
6224
6202
Dynamic Card No.
1234 - 5678 - 90123 - 4567
6204
6206
Dynamic Code
890
6208
6222
NAME: JEFFREY_MULLEN_S32S
6220
A (0,1)
B (2,3)
C (4,5)
D (6,7)
E (8,9)
6210
6212
6214
6216
6218
6250
Battery
6258
RFID Antenna
6268
Display
6256
RFID CHIP
6262
PROCESSOR
6254
DRIVING CIRCUITRY
6264
6270
6272
6274
MEMORY
6252
IC Chip
6260
DETECTOR
6266

FIG. 62

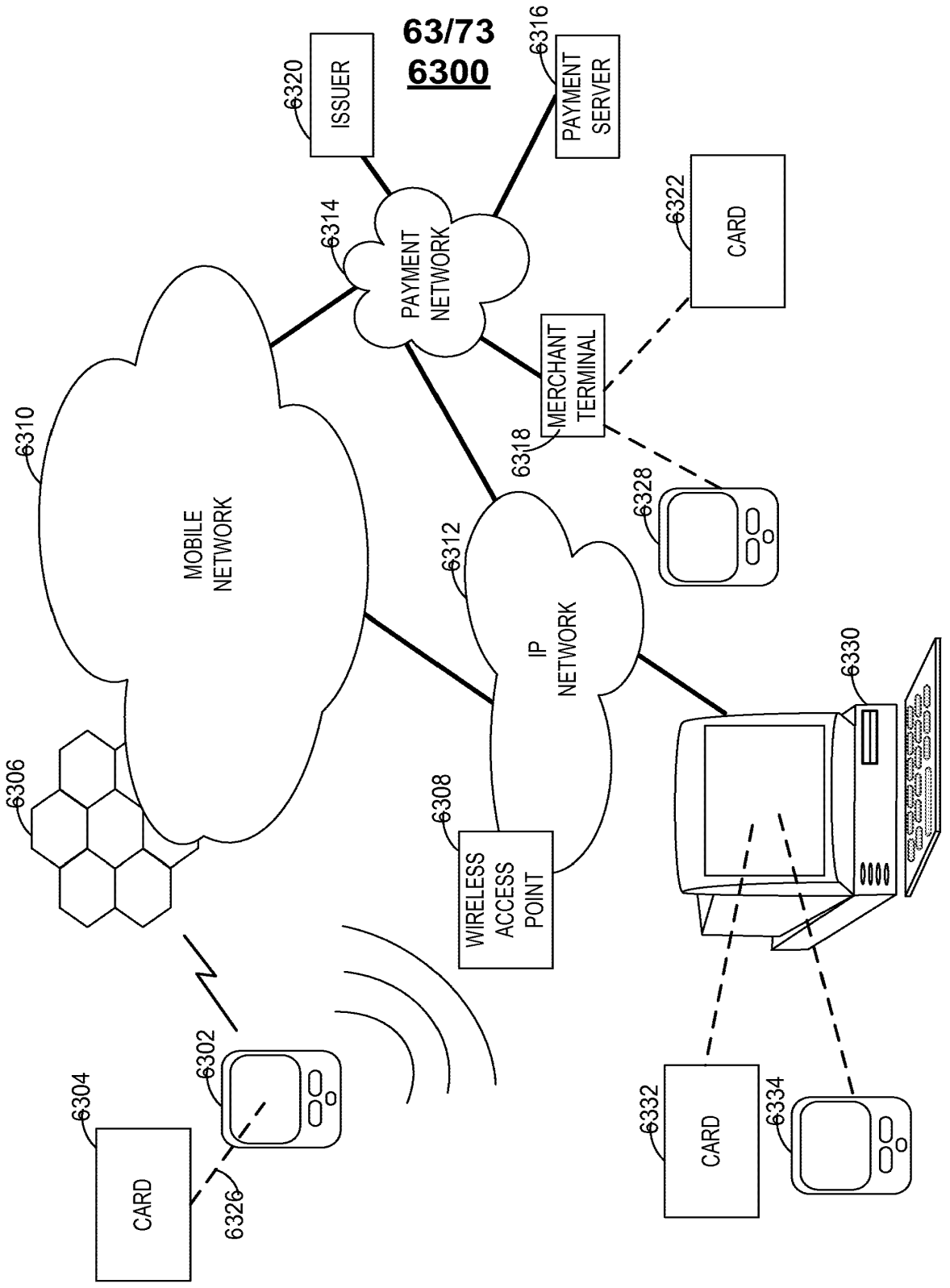

63/73
6300
6320
ISSUER
6316
PAYMENT SERVER
6314
PAYMENT NETWORK
6322
CARD
MERCHANT TERMINAL
6318
6328
6310
MOBILE NETWORK
6312
IP NETWORK
6330
6306
6308
WIRELESS ACCESS POINT
6302
6304
CARD
6326
6332
CARD
6334

FIG. 63

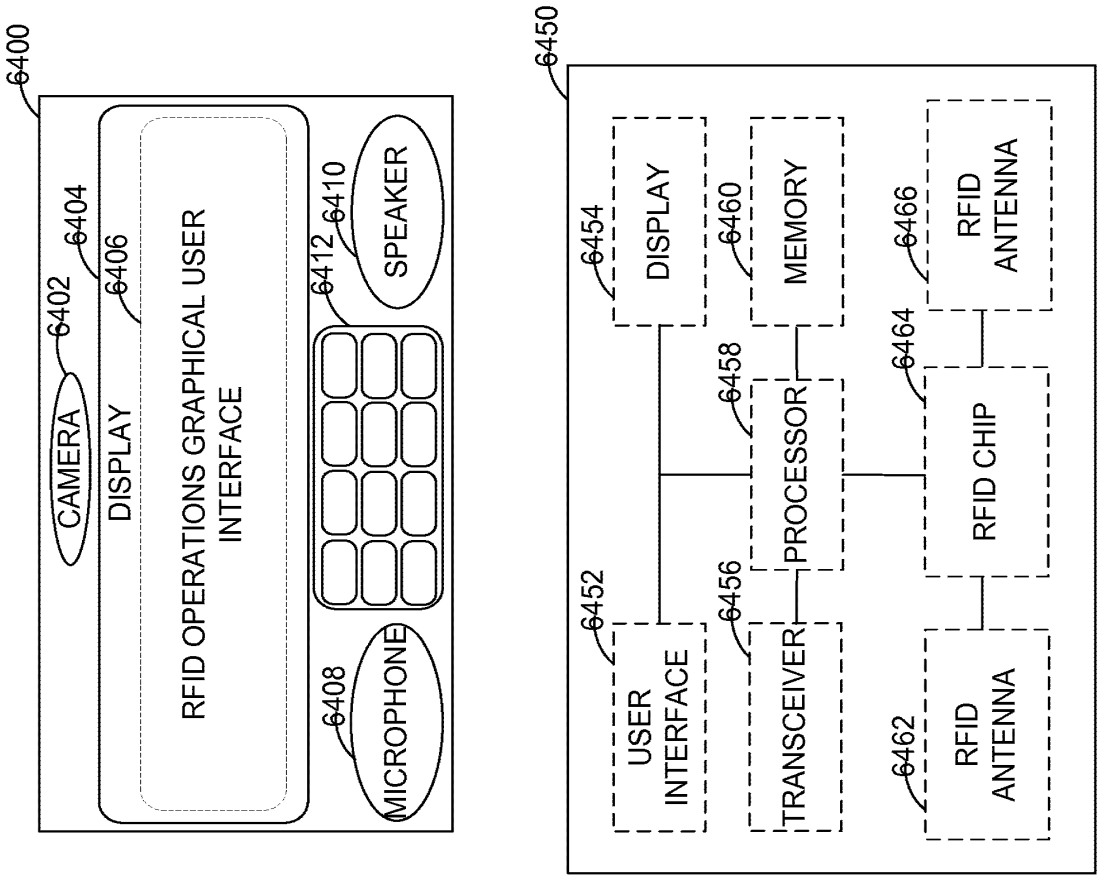

6400
CAMERA
6402
DISPLAY
6404
RFID OPERATIONS GRAPHICAL USER INTERFACE
6406
6408
MICROPHONE
6410
SPEAKER
6412
6450
USER INTERFACE
6452
DISPLAY
6454
TRANSCEIVER
6456
PROCESSOR
6458
MEMORY
6460
RFID ANTENNA
6462
RFID CHIP
6464
RFID ANTENNA
6466

FIG. 64

65/73
6500

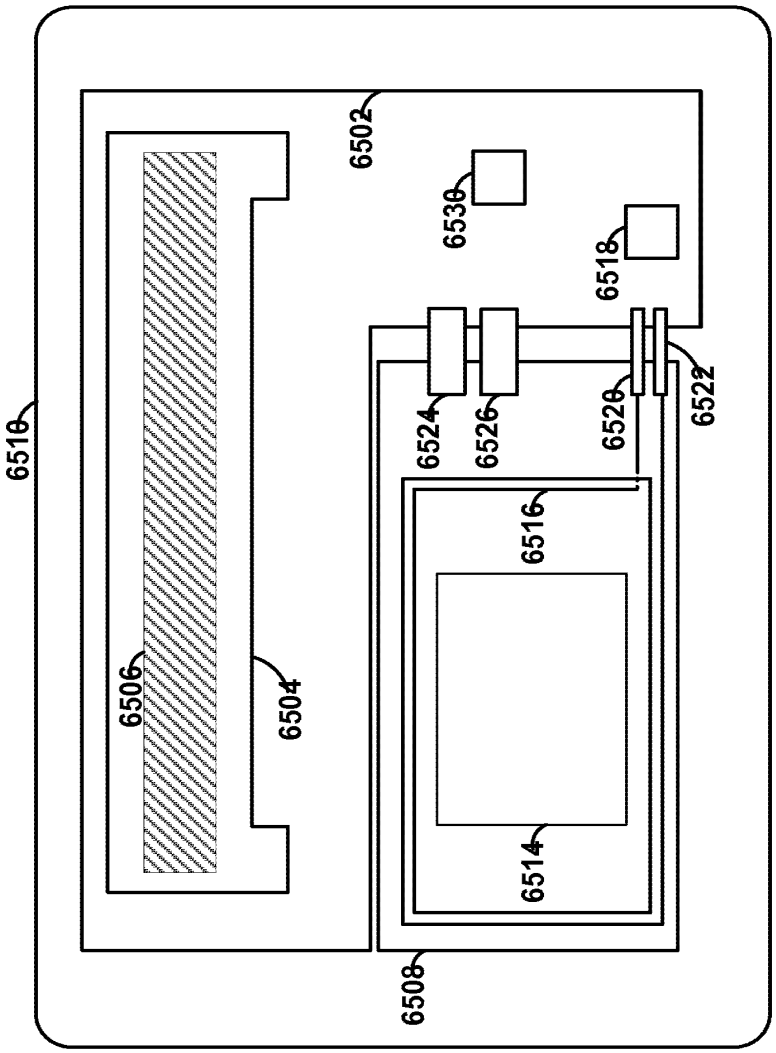


FIG. 65

66/73
6600

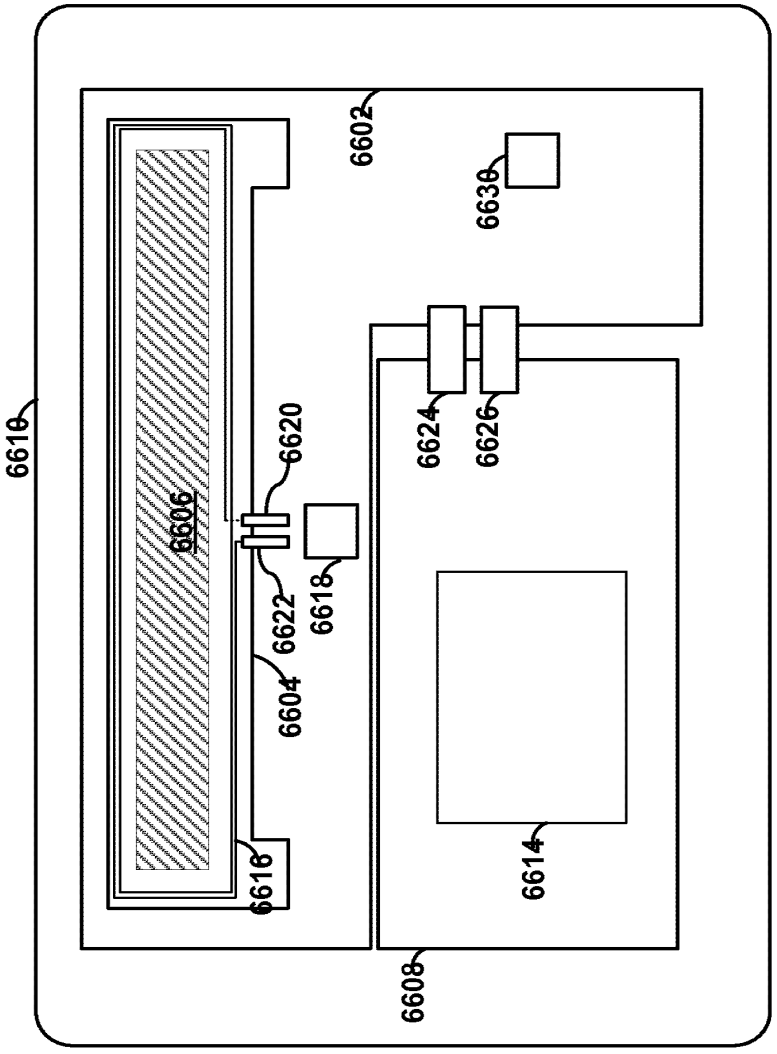


FIG. 66

67/73

6700

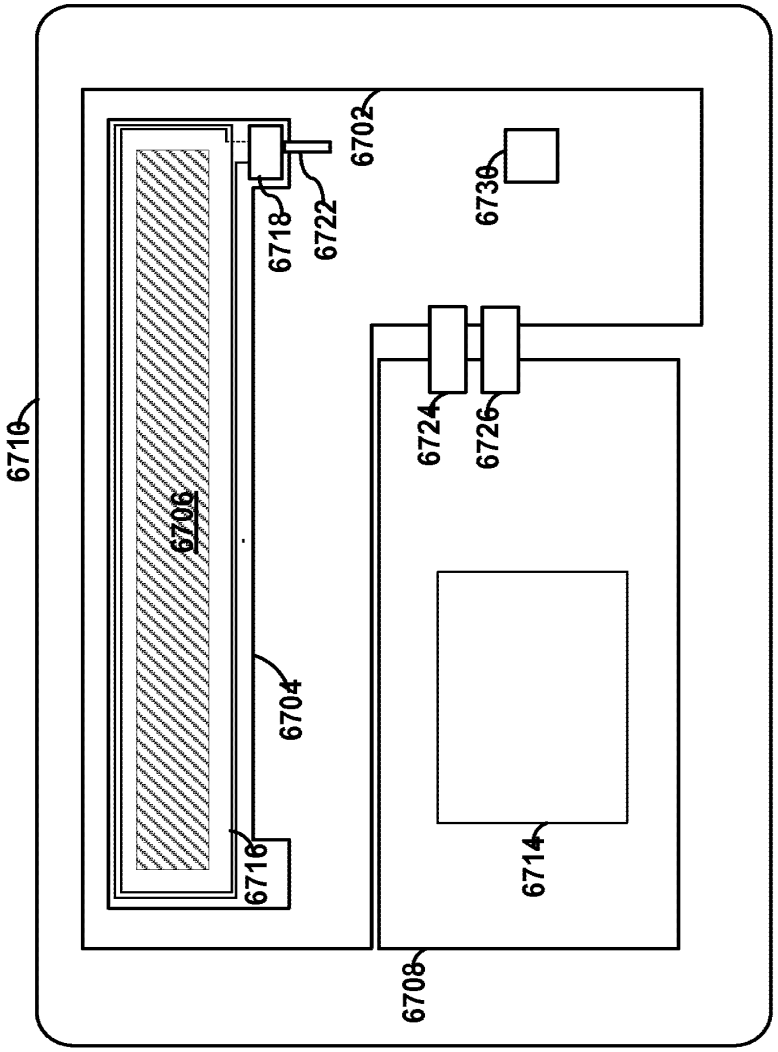


FIG. 67

68/73
6800

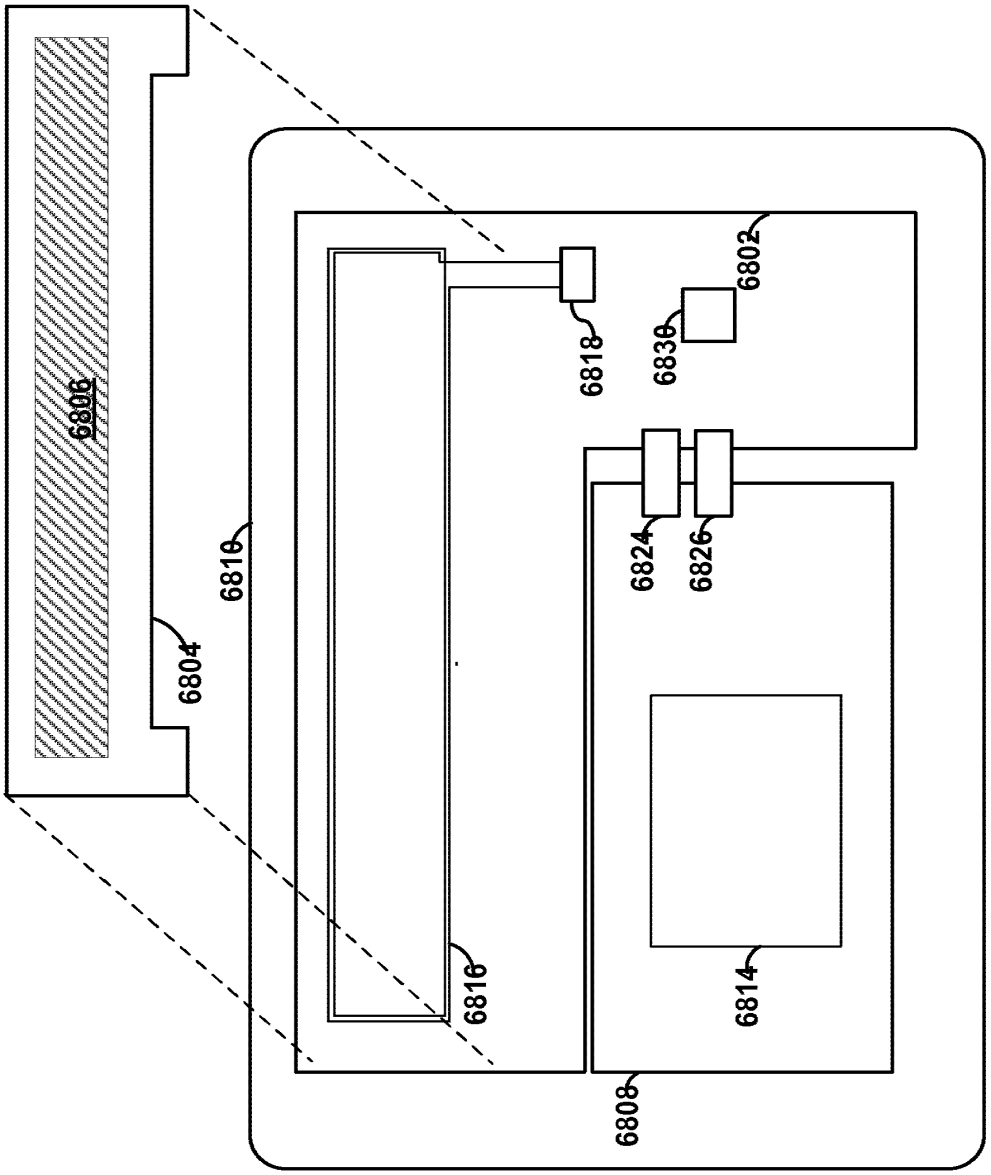


FIG. 68

6900

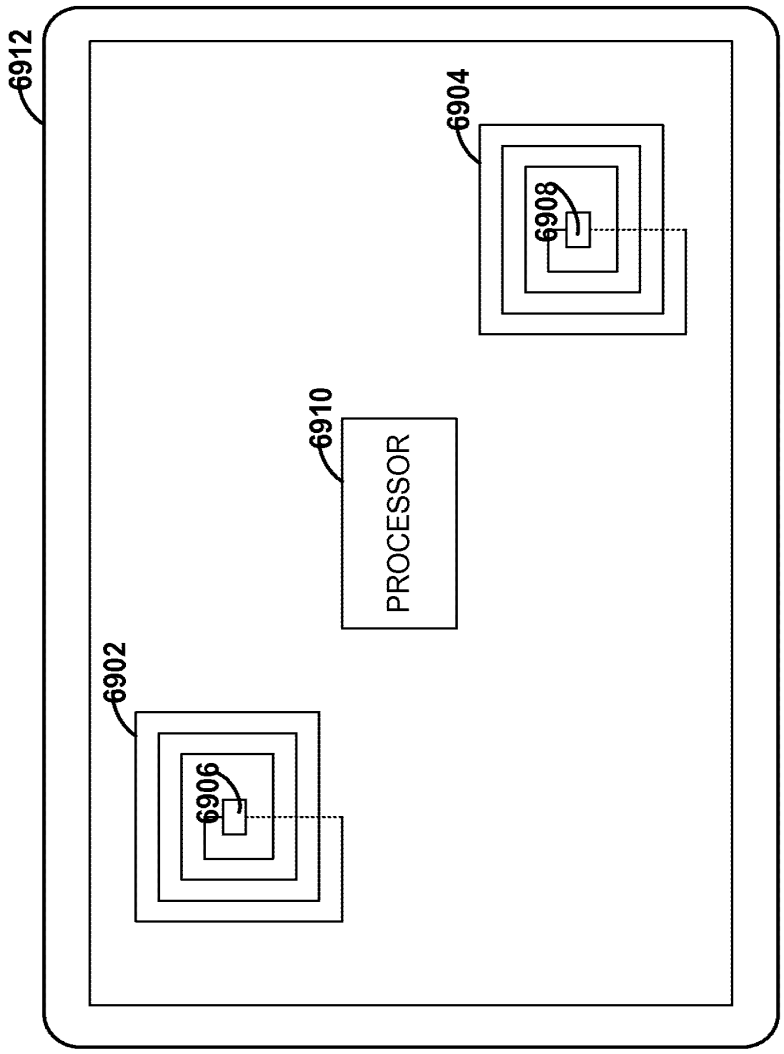


FIG. 69

70/73
7000

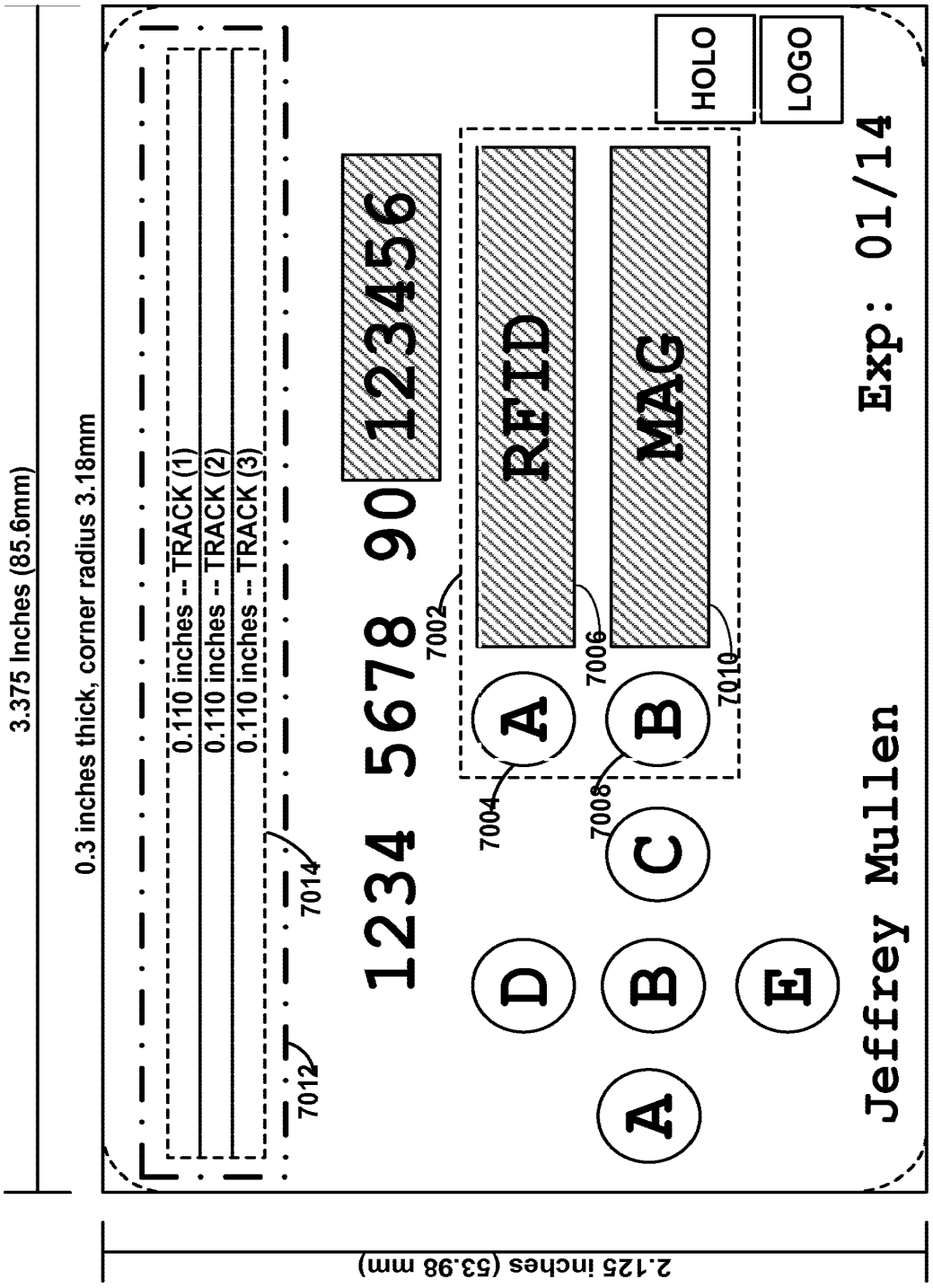


FIG. 70

71/73
7100

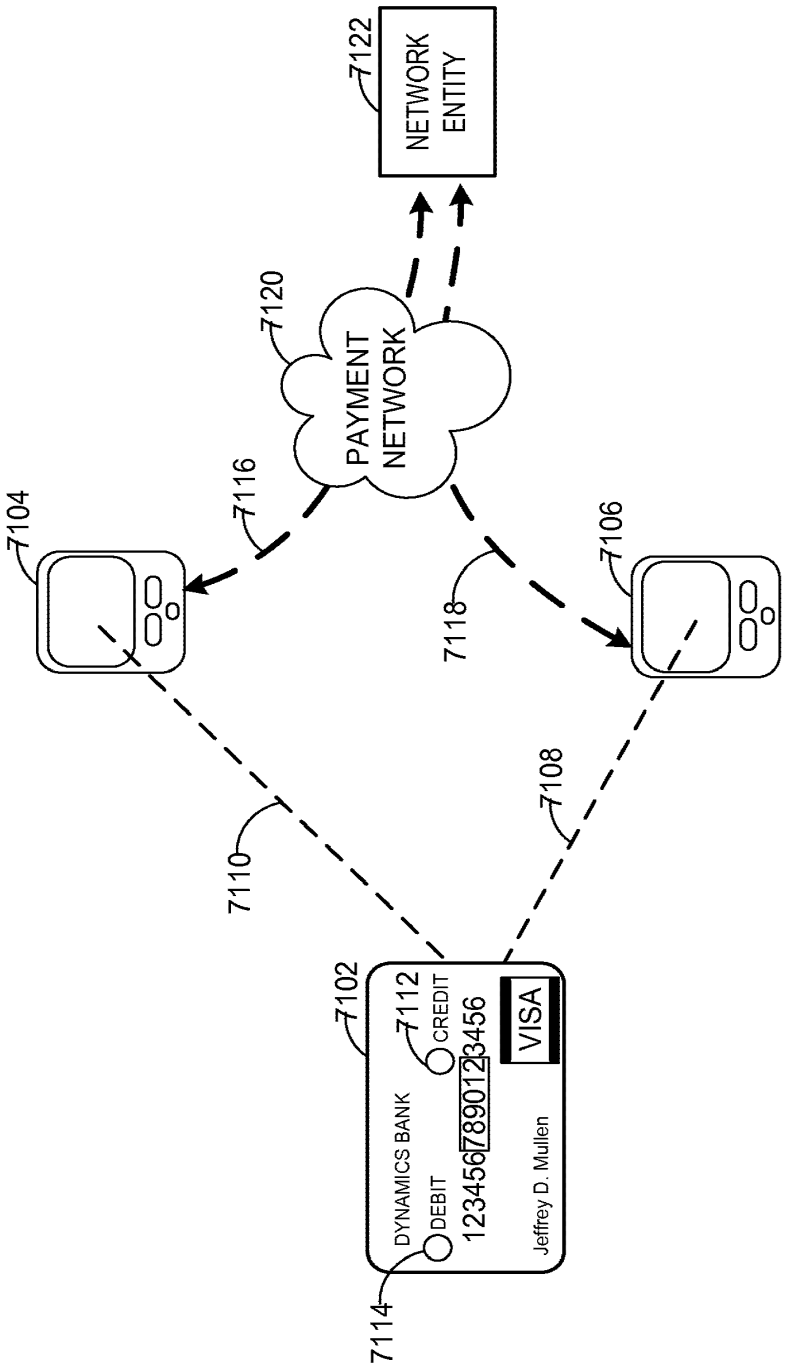


FIG. 71

7200

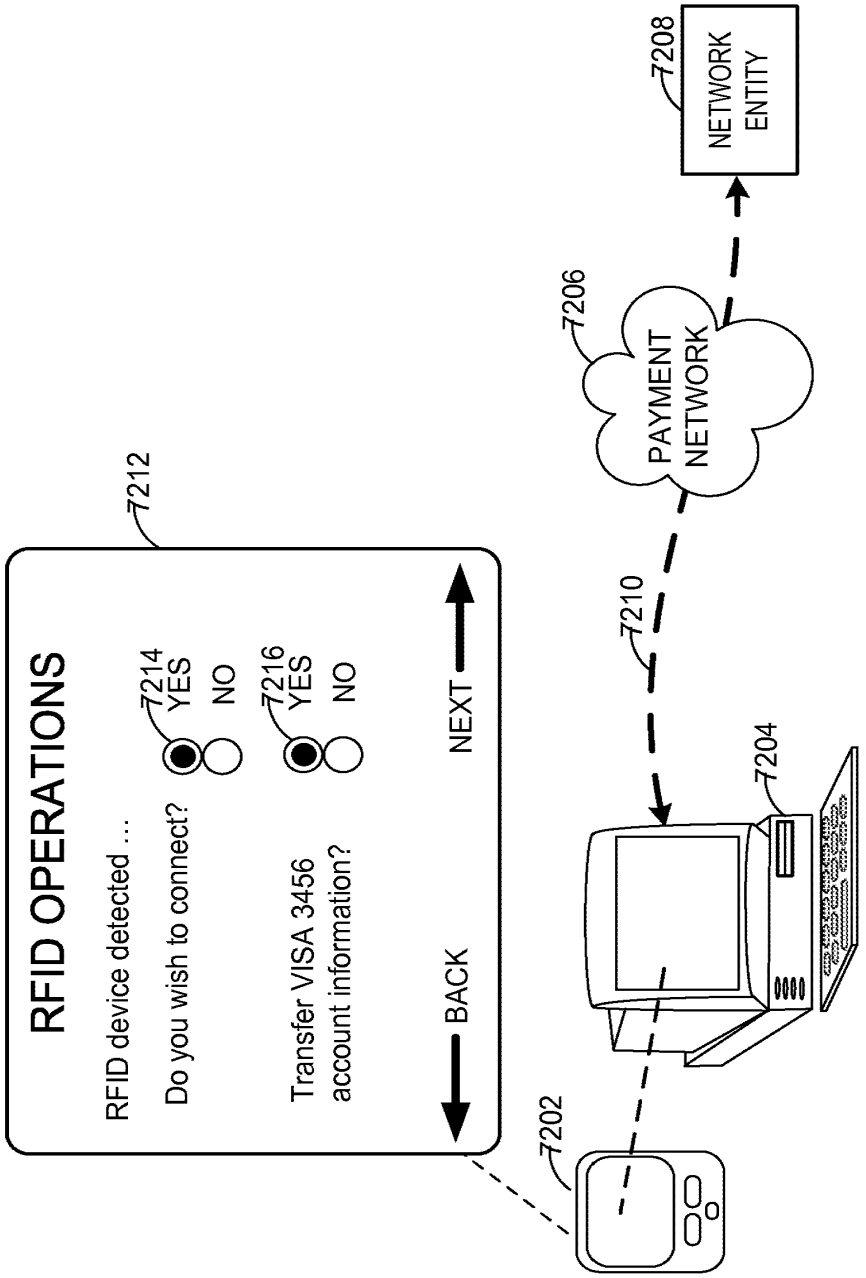

7208
NETWORK ENTITY
7206
PAYMENT NETWORK
7210
7204
7212
RFID OPERATIONS
RFID device detected ...
Do you wish to connect?
7214
YES
NO
Transfer VISA 3456 account information?
7216
YES
NO
NEXT
BACK
7202

FIG. 72

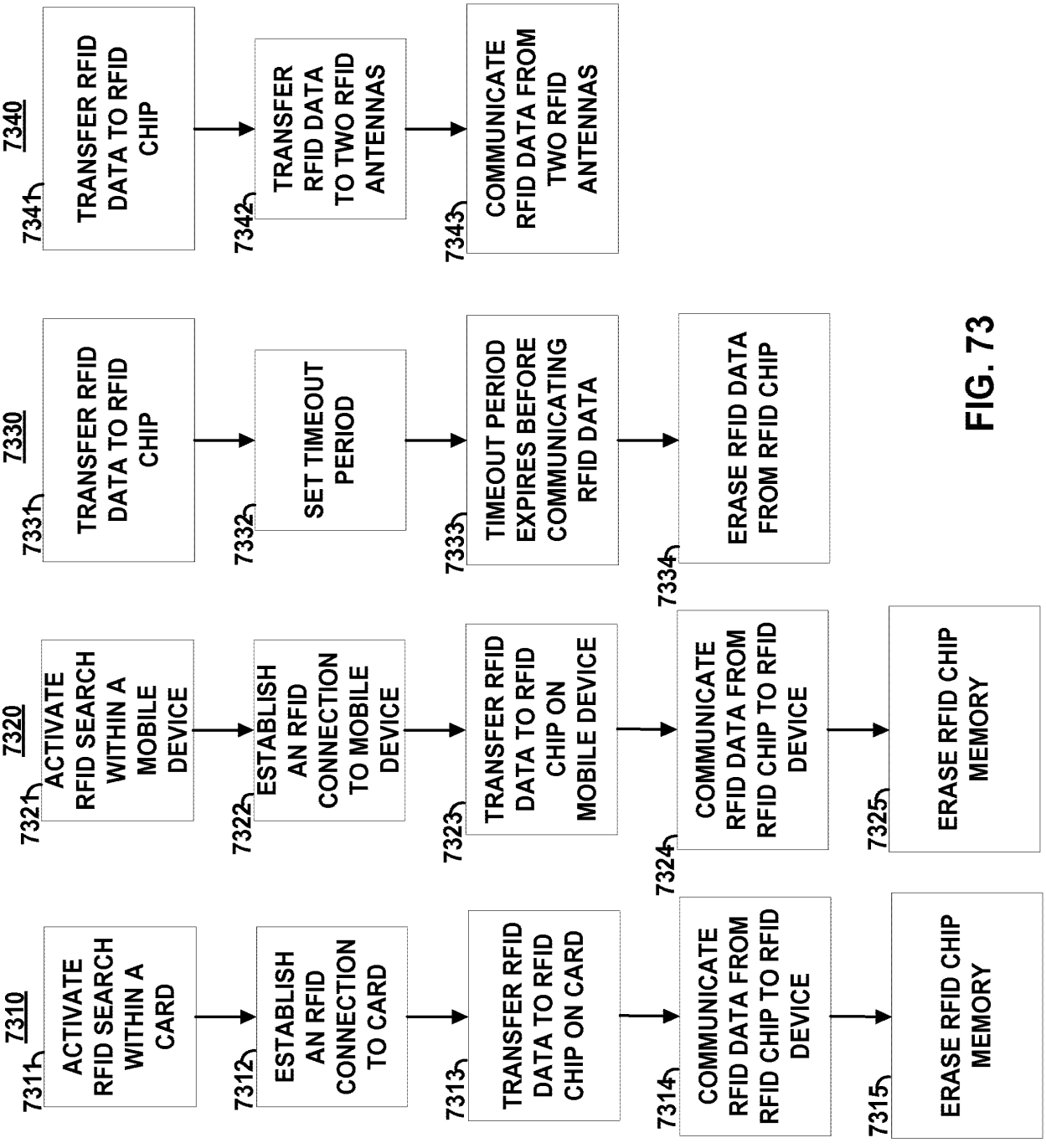

7310
7311
ACTIVATE RFID SEARCH WITHIN A CARD
7312
ESTABLISH AN RFID CONNECTION TO CARD
7313
TRANSFER RFID DATA TO RFID CHIP ON CARD
7314
COMMUNICATE RFID DATA FROM RFID CHIP TO RFID DEVICE
7315
ERASE RFID CHIP MEMORY
7320
7321
ACTIVATE RFID SEARCH WITHIN A MOBILE DEVICE
7322
ESTABLISH AN RFID CONNECTION TO MOBILE DEVICE
7323
TRANSFER RFID DATA TO RFID CHIP ON MOBILE DEVICE
7324
COMMUNICATE RFID DATA FROM RFID CHIP TO RFID DEVICE
7325
ERASE RFID CHIP MEMORY
7330
7331
TRANSFER RFID DATA TO RFID CHIP
7332
SET TIMEOUT PERIOD
7333
TIMEOUT PERIOD EXPIRES BEFORE COMMUNICATING RFID DATA
7334
ERASE RFID DATA FROM RFID CHIP
7340
7341
TRANSFER RFID DATA TO RFID CHIP
7342
TRANSFER RFID DATA TO TWO RFID ANTENNAS
7343
COMMUNICATE RFID DATA FROM TWO RFID ANTENNAS

FIG. 73

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2012/037237

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06Q 40/02 (2012.01)
USPC - 705/41
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC(8) - G06Q 30/06, 40/00, 40/02 (2012.01)
USPC - 455/41.1, 705/39, 40, 41, 42

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
PatBase, Google Patents, Google.com

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2009/0210308 A1 (TOOMER et al) 20 August 2009 (20.08.2009) entire document	1, 3-11, 81
X	US 2009/0191811 A1 (GRIFFIN et al) 30 July 2009 (30.07.2009) entire document	2, 12-21, 82
A	US 2010/0304670 A1 (SHUO) 02 December 2010 (02.12.2010) entire document	1-21, 81-82
A	US 2010/0023449 A1 (SKOWRONEK et al) 28 January 2010 (28.01.2010) entire document	1-21, 81-82
A	US 2009/0170432 A1 (LORTZ) 02 July 2009 (02.07.2009) entire document	1-21, 81-82
A	US 2010/0153269 A1 (MCCABE) 17 June 2010 (17.06.2010) abstract, Fig. 1-2, paragraphs 13, 15, 30-31, 36-40, 47.	1-21, 81-82

☐ Further documents are listed in the continuation of Box C. ☐

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 September 2012	16 OCT 2012
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2012/037237

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

See extra sheet.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:
1-21, 81-82

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2012/037237

This application contains the following inventions or groups of inventions which are not so linked as to form a single general inventive concept under PCT Rule 13.1. In order for all inventions to be examined, the appropriate additional examination fees must be paid.

Group I, claims 1-21, 81-82, drawn to a method and system comprising accessing a network using a mobile device, selecting an object for purchase from said network, communicating payment information/target account information to a second device, and completing a purchase transaction/coordinating a money transfer.
Group II, claims 22-41, 83, drawn to a method and system comprising creating a mobile wallet of virtual cards within a memory of a mobile device from communicated information, and selecting one of said virtual cards to complete a purchase transaction.
Group III, claims 42-61, 84, drawn to a method and system comprising executing an application on a processor of a mobile device to perform a function, communicating information to said mobile device, confirming said communicated information matches at least a portion of predetermined information, and executing said function from said mobile device based on said confirmation.
Group IV, claims 62-78, drawn to a card comprising a second board including a processor, wherein first data is transferred from a processor to a first RFID chip via conductive terminals between first and second boards and wherein said first data is communicated from said first RFID chip to a first RFID communication channel via said first RFID antenna.
Group V, claims 79-80, drawn to a method comprising communicating second data from a device to a reader via a second RFID communication channel, receiving first and second data via said reader and avoiding collisions between said first and second data within said reader.

The inventions listed as Groups I, II, III, IV and IV do not relate to a single general inventive concept under PCT Rule 13.1 because, under PCT Rule 13.2, they lack the same or corresponding special technical features for the following reasons: the special technical feature of the Group I invention: a method and system comprising accessing a network using a mobile device, selecting an object for purchase from said network, communicating payment information/target account information to a second device as claimed therein is not present in the invention of Groups II, III, IV or V. The special technical feature of the Group II invention: a method and system comprising creating a mobile wallet of virtual cards within a memory of a mobile device from communicated information, and selecting one of said virtual cards as claimed therein is not present in the invention of Groups I, III, IV or V. The special technical feature of the Group III invention: a method and system comprising executing an application on a processor of a mobile device to perform a function, confirming that communicated information matches at least a portion of predetermined information, and executing said function from said mobile device based on said confirmation as claimed therein is not present in the invention of Groups I, II, IV or V. The special technical feature of the Group IV invention: a card comprising a second board including a processor, wherein first data is transferred from a processor to a first RFID chip via conductive terminals between first and second boards as claimed therein is not present in the invention of Groups I, II, III or V. The special technical feature of the Group V invention: a method comprising communicating second data from a device to a reader via a second RFID communication channel, receiving first and second data via said reader and avoiding collisions between said first and second data within said reader as claimed therein is not present in the invention of Groups I, II, III or IV.

Groups I, II, III, IV and V lack unity of invention because even though the inventions of these groups require the technical feature of a method, system and card comprising establishing a contactless communication channel between a physical card and a mobile device through a first board including a first RFID chip and a first RFID antenna; communicating payment/source account information from a payment card to a mobile device using a contactless communication channel wherein first data is communicated from said first RFID chip to a first RFID communication channel visa said first RFID antenna; completing a purchase transaction/coordinating a money transfer, this technical feature is not a special technical feature as it does not make a contribution over the prior art in view of US 2010/0153269 A1 (MCCABE) 17 June 2010 (17.06.2010), abstract, Fig. 1-2, paragraphs 13, 15, 30-31, 36-40, 47.

Since none of the special technical features of the Group I, II, III, IV or V inventions are found in more than one of the inventions, unity of invention is lacking.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 April 2010 (22.04.2010)

PCT

(10) International Publication Number
WO 2010/043974 A1

(51) International Patent Classification:
G06Q 20/00 (2006.01) *H04L 9/32* (2006.01)
G06K 7/10 (2006.01) *H04K 3/00* (2006.01)

(21) International Application Number:
PCT/IB2009/007364

(22) International Filing Date:
16 October 2009 (16.10.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/136,945 16 October 2008 (16.10.2008) US

(72) Inventor; and
(71) Applicant : **RICHARD, Christian** [CA/CA]; 187 Dieppe, Pointe Claire, Quebec, H9R 1X8 (CA).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM,

[Continued on next page]

(54) **Title**: SYSTEM FOR SECURE CONTACTLESS PAYMENT TRANSACTIONS

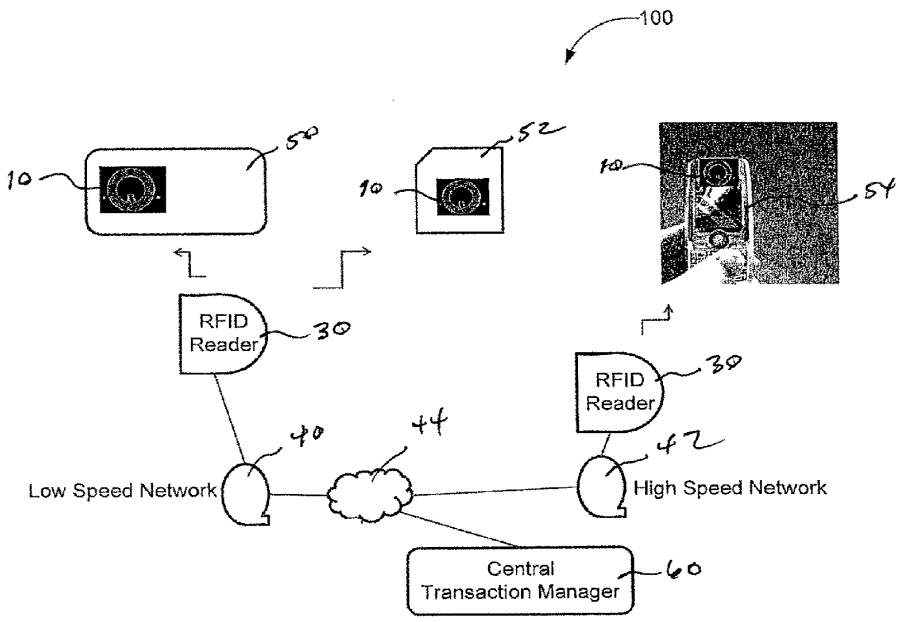


Figure 1

[Continued on next page]

WO 2010/043974 A1

TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to the identity of the inventor (Rule 4.17(i))*

Published:

— *with international search report (Art. 21(3))*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

(57) Abstract: The present invention is directed to a system that includes a transaction unit that includes a microchip having a computer readable medium configured to store a unit identifier (UI) and at least one one-time-password (OTP) therein. The UI and the at least one OTP comprising transaction authentication data. The transaction unit is configured to transmit the transaction authentication data in response to receiving a predetermined signal. A reader device is configured to transmit the predetermined signal to interrogate the transaction unit and read the transaction authentication data. The reader device is configured to generate at least one authentication indicia in response to receiving an authentication signal. A server is coupled to the reader device. The server includes a database having at least one server OTP related to at least one unit identifier stored therein, the at least one server OTP and the at least one unit identifier comprising transaction verification data. The server is configured to compare the transaction authentication data with the transaction verification data. The server also is configured to transmit the authentication signal to the reader device if the transaction authentication data matches the transaction verification data.

SYSTEM FOR SECURE CONTACTLESS PAYMENT TRANSACTIONS

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of priority under 35 U.S.C. §119(e) and 35 U.S.C. §365, to U.S. Provisional Patent Application Serial No. 61/136,945, filed on October 16, 2008, the content of which is relied upon and incorporated herein by reference in its entirety.

BACKGROUND OF THE INVENTION

1. Field of the Invention

[0002] The present invention relates generally to RFID systems, and particularly to a method and system for secure contactless payment transactions.

2. Technical Background

[0003] Contactless "smartcards" have been used for payment for many years. Smartcards and other such contactless payment schemes were originally promoted for use in a category of payment defined as micropayment. The smartcard typically included an RFID chip disposed therein. The RFID chip included memory for storing the payment information. The payment information was accessed by a reader. Micropayment was originally created for the purchase of products under a given price, e.g., $50, without any receipt. Micropayment was originally contemplated as a means for simplifying payment for small items such as newspapers, fast food and other similar purchases. The card may, for example, be issued by a merchant and include a $50 credit amount recorded in memory.

[0004] In another example, Paypass ™ is a smart credit card system adopted by various credit card companies. In fact, approximately 80 million credit cards with a contactless inlay using the ISO 14443A or B protocols were released into the stream of commerce. When the credit card is read through its RFID chip, the information that is transmitted to the bank is the same as the standard credit card track A and B data. The

system attempted to protect the sensitive financial data using the Texas Instruments ™ Digital Signal Transponder (DST) 24 to 40 bits protocol. One drawback with this method is that is vulnerable to "sniffing" attacks. *Sniffing* refers to a technique wherein a thief surreptitiously captures the transmissions between the smart card and the reader. This may be accomplished, for example, by hiding an unauthorized read in close proximity to the authorized reader. This technique often resulted in the fraudulent acquisition of many credit card numbers in a short span of time. For example, it was widely reported that one hacker was able to sniff thousands of credit cards using the contactless payment system over a span of a few hours using a $150 device.

[0005] What is needed, therefore, is a system for improving the security of contactless payment transactions.

SUMMARY OF THE INVENTION

[0006] The present invention addresses the needs described above by providing a system for improving the security of contactless payment transactions.

[0007] One aspect of the present invention is directed to a system that includes a transaction unit having a microchip that includes a computer readable medium. The computer readable medium is configured to store a unit identifier (UI) and at least one one-time-password (OTP) therein. The UI and the at least one OTP comprising transaction authentication data. The transaction unit is configured to transmit the transaction authentication data in response to receiving a predetermined signal. A reader device is configured to transmit the predetermined signal to interrogate the transaction unit and read the transaction authentication data. The reader device is configured to generate at least one authentication indicia in response to receiving an authentication signal. A server is coupled to the reader device. The server includes a database having at least one server OTP related to at least one unit identifier stored therein, the at least one server OTP and the at least one unit identifier comprising transaction verification data. The server is configured to compare the transaction authentication data with the transaction verification data. The server also is configured

to transmit the authentication signal to the reader device if the transaction authentication data matches the transaction verification data.

[0008] Another aspect of the present invention is directed to a system that includes a contactless transaction unit having an RFID assembly disposed therein. The RFID assembly includes an RFID coupler and a microchip having a computer readable medium configured to store transaction authentication data. The RFID coupler includes a detuned inlay, the detuned inlay including an LC circuit having a resonant frequency calculated to correspond to a sub-harmonic of the main frequency of a predetermined signal. The transaction unit is configured to transmit the transaction authentication data in response to receiving the predetermined signal. A contactless RFID reader device is configured to transmit the predetermined signal when the transaction unit is disposed within a predetermined distance from the reader device to thereby interrogate the contactless transaction unit and read the transaction authentication data. The contactless RFID reader device is configured to generate at least one authentication indicia in response to receiving an authentication signal. A server is coupled to the contactless RFID reader device. The server includes a database having transaction verification data stored therein. The server is configured to compare the transaction authentication data with the transaction verification data. The server is configured to transmit the authentication signal to the contactless RFID reader device if the transaction authentication data matches the transaction verification data.

[0009] Yet another aspect of the present invention is directed to a system that includes a transaction unit having an RFID assembly disposed therein. The RFID assembly includes an RFID coupler and a microchip having a computer readable medium. The computer readable medium is configured to store transaction authentication data. The transaction unit is also configured to transmit the transaction authentication data in response to receiving the predetermined signal. An RFID reader device is configured to transmit the predetermined signal when the transaction unit is disposed within a predetermined distance from the RFID reader device to thereby interrogate the transaction unit and read the transaction authentication data. The RFID reader includes a jammer coupler disposed proximate a reader coupler such that the

RFID reader device includes a sensing zone wherein the RFID reader device interrogates the transaction unit and a jamming zone wherein the RFID reader device transmits a jamming signal substantially outside of the sensing zone. The RFID reader device is also configured to generate at least one authentication indicia in response to receiving an authentication signal. A server is coupled to the RFID reader device, the server including a database having transaction verification data stored therein. The server is configured to compare the transaction authentication data with the transaction verification data. The server is configured to transmit the authentication signal to the RFID reader device if the transaction authentication data matches the transaction verification data.

[0010] Additional features and advantages of the invention will be set forth in the detailed description which follows, and in part will be readily apparent to those skilled in the art from that description or recognized by practicing the invention as described herein, including the detailed description which follows, the claims, as well as the appended drawings.

[0011] It is to be understood that both the foregoing general description and the following detailed description are merely exemplary of the invention, and are intended to provide an overview or framework for understanding the nature and character of the invention as it is claimed. The accompanying drawings are included to provide a further understanding of the invention, and are incorporated in and constitute a part of this specification. The drawings illustrate various embodiments of the invention, and together with the description serve to explain the principles and operation of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] Figure 1 is a block diagram of a secure contactless payment transaction according to an embodiment of the present invention

[0013] Figure 2 is a schematic view of a contactless payment card inlay;

[0014] Figure 3 is an example of a second harmonic of a signal having a main frequency of 13.56 MHz;

[0015] Figure 4 is a schematic view of a reader coupler with a concentric jammer; and

[0016] Figures 5A and 5B are schematic views of the reader coupler field and the reader coupler field combined with the concentric jammer field, respectively.

DETAILED DESCRIPTION

[0017] Reference will now be made in detail to the present exemplary embodiments of the invention, examples of which are illustrated in the accompanying drawings. Wherever possible, the same reference numbers will be used throughout the drawings to refer to the same or like parts. An exemplary embodiment of the system of the present invention is shown in Figure 1, and is designated generally throughout by reference numeral 100.

[0018] As embodied herein, and depicted in Figure 1, a diagrammatic depiction of a secure contactless payment transaction system 100 in accordance with one embodiment of the present invention is disclosed. System 100 may be configured as a hierarchical computer and software system implemented in the well known client-server model with at least one secure database for storing secure data. System 100 may include a server 60, middle layer computer processing nodes associated with the networks 40, 42 and RFID readers 30 at the lowest level. System 100 may also include an RFID card 50, an RFID token 52 and/or an RFID equipped electronic devices 54, e.g., a mobile near field communications (NFC) device 54. Each of these devices may be read by an RFID reader 30 in accordance with the present invention. These devices are coupled to a central transaction management server 60 by way of low speed network 40, high speed network 42, switched network 44, or some combination thereof. Secure data may include cytological keys used to authenticate computer processing nodes and sensors in the network. Of course, one-time passwords (OTPs) are used to authenticate and verify RFID cards 50, tokens 52 and NFC devices 54.

[0019] The switched network 44 may include the public switched telephony network (PSTN) or a packet switched network or a combination thereof. Network 44 may be, for example, the global packet data communication network now commonly

referred to as the "Internet." The World Wide Web (WWW) is a system of server computers that is supported and interconnected by the Internet. In the client-server model, the server computer(s) comprising the transaction manager server 60 may provide graphical "web pages" that are provided to a client computers that supports a given RFID reader 30 via the web. The client computer includes a graphical interface which provides an easily understood display that facilitates the POS transaction. Some of the information being served to the client is dynamically retrieved by the server from one or more databases. The graphical interface may allow the sales personnel to perform an identity check of the customer. The identification information may be provided to server along with the OTP data obtained by reader 30.

[0020] In one embodiment of the present invention, RFID reader 30 includes a secure contactless sensor that employs a 13.56 MHz microcircuit. The 13.56 MHz microcircuit is bidirectional and is characterized by a controllable range. Reader 30, therefore, exchanges data with the RFID device (50, 52, 54) at a reasonable speed. Reader 30 may be configured as a low power reader that employs the ISO 14443A protocol. Contactless payment cards are easily read at a range of 12 inches (30.48 cm). This range can be extended up to 3 feet (91.44 cm) when equipped with larger sensors. The RFID reader 30, depending on its sophistication at the point of sale (POS), may be include application programming configured to interact with POS personnel. The application programming may provide access to information retained in the Server databases and also to provide control over the RFID reader 30.

[0021] RFID reader 30 also includes a network interface to couple RFID reader 30 to external computer networks 40, 42, and/or 44. The communication interface may be of any suitable type such as a Universal Serial Bus (USB) interface, cable modem, a digital subscriber line (DSL) card or modem, an integrated services digital network (ISDN) card, a telephone modem, or any other communication interface to provide a data communication connection to a corresponding type of communication line. As another example, communication interface may be a local area network (LAN) or wide area network (WAN) card (e.g. for Ethernet™ or an Asynchronous Transfer Model (ATM) network) to provide a data communication connection to a compatible LAN or

WAN. Wireless links can also be implemented. In any such implementation, communication interface may send or receive electrical, electromagnetic, or optical signals that carry digital data streams representing various types of information.

[0022] The term "computer-readable medium" as used herein refers to any medium that participates in providing data and/or instructions to a processor associated with either the RFID reader 30 or the transaction manager server 60 for execution. Such media may take many forms, including but not limited to non-volatile media, volatile media, and transmission media. Common forms of computer-readable media include, for example, a floppy disk, a flexible disk, hard disk, magnetic tape, any other magnetic medium, a CD-ROM, CDRW, DVD, any other optical medium, punch cards, paper tape, optical mark sheets, any other physical medium with patterns of holes or other optically recognizable indicia, a RAM, a PROM, and EPROM, a FLASH-EPROM, any other memory chip or cartridge, a carrier wave, or any other medium from which a computer can read. Transmission media may include coaxial cables, copper wire and/or optical fiber. Transmission media can also take the form of acoustic, optical, or electromagnetic waves, such as those generated during radio frequency (RF) and infrared (IR) data communications. Any of the various forms of computer-readable media described above may be involved in providing instructions to the table computers 210 for execution.

[0023] The transaction manager server 60 refers to both the physical server computers configured to run and manage the various system applications, and the software that resides on the physical server computers. The server manages the proper reading and writing of data in the database. The server also manages the contactless payment sequence enabled by the RFID card 50. The server stores, receives and dispatches alarms over the networks to the clients in the event that an authentication fails.

[0024] One of the drawbacks associated with conventional smartcard systems relates to the use of customer tracking information during the data exchange. It is understood that the use of this data reduces the burden on the merchant by requiring

fewer changes to current conventional systems. However, this design makes it very easy and very attractive for thieves to hack these relatively unprotected smart cards.

[0025] The transaction manager server 60 may be configured to generate the one-time pass word and read/write to/from the database using symmetric security keys. The new OTP is written into the chip by the OTP module via the server. Client/server communications may be encrypted using a secure sockets layer (SSL). As will be explained in detail below, the OTP is a security system that changes a secret data key inside the RFID card 50 each time it is read. If the server validates the retrieved OTP, the transaction is written into the database, and a new OTP is retrieved in accordance with a predetermined sequence.

[0026] To generate the one-time password (OTP), a "seed" is provided by the transaction manager server 60 or by an authorized card issuing authority. The seed is combined with a static user password and a user card ID using a hash function. The hash value of the user's static password the session one-time password and the compressed data is used as input to the digital signature algorithm. This guarantees that the one-time password significantly determines the communication stream between the client and the server for each session. The transaction manager server 60 or the authorized card issuing authority computes a set S of independent one-time passwords that are stored in a password file in a database coupled to the transaction manager server 60.

[0027] The RFID card 50, token 52 or NFC device 54 stores the initial one time password word together with the corresponding index. In one embodiment, either the entire set (S) or a small subset (S') of S is stored on the card 50 before issuance in a secure way. At login time, upon presentation of the RFID tag, the transaction server issues a challenge to the tag. The challenge is merely one of the indices selected at random. Of course, the selected index is used by the card to retrieve the one-time password out of the subset S' of one-time passwords that corresponds to the selected index. Once retrieved, the RFID card (50, 52, 54) sends the one-time password stored in memory that corresponds to the challenge I, in response to the challenge. If this one-time password transmitted by the card matches the one stored in the password file at

index i, the transaction is authorized. If not, the authentication fails. This approach is not vulnerable to over-the-shoulder attacks since the passwords are stored in the RFID tag. Further, since the one-time passwords are selected at random and the subset S' can be chosen to be small enough to allow frequent refresh of the passwords stored in the RFID tag, a passive eavesdropper that monitors the communication between the RFID tag and the central controller will not be able to predict the next one-time password that the card will send.

[0028] In another embodiment, card 50, token 52 or device 54 is equipped with computing power, and the initial OTP is employed to generate additional passwords by applying a series of iterations of the cryptographic functions f to the initial OTP. In one embodiment, the memory of the contactless payment card would include a 64 bit permanent unique identifier (UIO) and at least one 16 to 63 bit one-time password (OTP) in the read/write memory using a fast encryption algorithm based on, for example, an exponential *Certicom* keying system. The memory would also include a class of service bits and optional challenge complement bits. In order to authenticate to the system, the user applies an iteration of the cryptographic function (f) to the initial OTP. The encrypted information is transmitted to the server 60 via the reader 30. The server 60 verifies the correctness of the information by decoding the encrypted data provided by the RFID card 50, token 52 or device 54. The decoded result is compared to the value previously stored in the server 60. If there is a match, authentication succeeds and the new value of i together with the next iteration of the cryptographic function (f) are stored in the controller. Otherwise, authentication fails and the value of i is discarded.

[0029] In both implementations, the one-time password can be used to secure subsequent communications between the client and the transaction manager server 60. The user password is never transmitted in plain text to the central controller. A slight modification of this approach allows also for server authentication to the client card 50, token 52 or NFC device 54. The set of one-time passwords computed by the client or the server can be either based on Elliptic Curves or on the RSA scheme or on any other pseudo random function.

[0030] The present invention envisions several classes of OTP service. The first class (Class 1 OTP) is referred to as close loop fast access. In this embodiment, an OTP server is on site and it facilitates a full OTP exchange. In other words, if the RFID card 50 includes one OTP, the server may cryptographically generate a new OTP and write it into the inlay 10 memory. This approach requires a relatively high speed central server to be efficient. Thus, this approach is particularly efficient in environments such as shopping centers, airports and subways in which the speed of the connection to a central server is not a issue. The second class (Class 2 OTP) is referred to as fast access OTP. In this embodiment, an OTP server may be easily accessible but is not required for every transaction. The third class of service (Class 3 OTP) does not have immediate access to the transaction manager server 60 and relies on the hand shaking key to secure the transaction. It is envisioned that Class 3 OTP would be employed in remote locations. The "hand shaking sequence" would require the reader 30 to have a key to access the data in the RFID card (50, 52, 54), based on the specific time of the transaction. Thus, only an authorized reader can read the RFID card 50, token 52 or NFC device 54 based on the authentication process described. To complement the transaction, human interaction may be required to complete the secure transaction, for example a cashier asking for a picture identification.

[0031] Accordingly, the present system eliminates the drawbacks associated with existing contactless payment systems whereby the RFID microchip can be read at a distance by an unauthorized sensor. Further, an unauthorized sensor placed within or underneath a counter, or within a doorway gate cannot be used to illegally read the data in the RFID card (50, 52, 54) of the present invention. For example, recently conducted tests showed that on low power reader using the ISO 14443A protocol can easily read conventional contactless payment cards at a range of 12 inches (30.48 cm). As noted, this range can be up to 3 feet (91.44 cm) with larger sensors. The OTP of the present invention eliminates this threat. As another example, the 40 bit key used in certain conventional cards has been broken and made public on the Internet. In fact, a group of students from the University of Baltimore, and sponsored by RSA, showed that a

particular algorithm could be broken in a few minutes. Again, the OTP of the present invention eliminates this threat.

[0032] One benefit of the present invention relates to the use of a 13.56 MHz RFID reader 30 that is based on the ISO 14443 protocol. Most payment or secure transaction contactless systems commonly use the 13.56 MHz reader. The ISO 14443 protocol (or its ISO 18000 equivalent) was created for secured RF transaction at 13.56 MHz. Thus, the present invention presents certain advantages vis á vis certain conventional systems such as conventional systems employing 125 KHz tokens. At a 6 Kbits/sec throughput, these tokens do not provide for bidirectional exchanges of data at a sufficient speed. There are higher frequency range systems but they also suffer from various deficiencies. For example, the Wall Mart ™ EPC 915 MHz system and the upcoming 915 MHz from EM Marin do not include enough memory capacity. Another issue in the 915 MHz frequency systems relates to the relative inability to control the range and the cross talk. In view of these drawbacks, many security experts prefer the 13.56 MHz system as the frequency of choice for secure applications.

[0033] As noted above, the present invention includes RFID equipped electronic devices 54, such as those configured in accordance with *near field communications* (NFC) technologies. Those of ordinary skill in the art will understand that NFC employs short-range high frequency wireless communication technology for contactless bidirectional transmission of data between devices separated by approximately 10 centimeters, which is about 4 inches. NFC may be thought of as an application or extension of the ISO/IEC 14443 RFID proximity-card standard (described above) in that it incorporates a so-called smart card into a hand held electronic device. NFC is primarily aimed at usage in mobile phones and may be employed in *blackberries* and other such devices. NFC may also combine the interface of a smartcard and a reader into a single device. An NFC device of this type can, therefore, communicate with both existing ISO/IEC 14443 smartcards and readers, as well as with other NFC devices. One of the benefits of NFC devices is that they are compatible with existing contactless infrastructure already in use for public transportation and payment. For example, NFC devices communicate by way of magnetic field induction over the globally available

and unlicensed RF-ISM band of 13.56 MHz, with a bandwidth of 14 kHz. As alluded to above, the RFID devices (50, 52, 54) may operate in a passive mode or in an active mode. In the passive RFID mode the RFID reader 30 provides a near magnetic field to interrogate the RFID Device (50, 52, 54). The RFID Device (50, 52, 54) typically employs an LC circuit that is excited by the near field such that the RFID device obtains its operating power from the near field. In the active mode, both the RFID device (50, 52, 54) and the reader 30 communicate by generate their own near field to transmit and deactivate their near field during the receive portion of the communication cycle. As noted above, the RFID device (50, 52, 54) requires a power supply to operate in this mode. Thus, the NFC RFID device 54 is well suited for this application.

[0034] It should be noted that conventional NFC devices may employ the ISO 14443 standard or newer 13.56 MHz implementations, e.g., the SONY™ FELICA™ system. There may be other private protocols being used in the U.S. Each of these protocols recognize the benefits of attaching a NFC chip to a mobile device. Cell phones are ubiquitous and one so equipped would essentially function as an electronic wallet, or an "*e-wallet*." However, the conventional devices briefly described above have drawbacks because the "sniffing" problem remains. Further, the "near field" is not specifically defined. As a matter of fact, this umbrella specification makes it very difficult for RFID chip makers because of the various protocols (e.g., NFC, ISO 14443 and ISO 15693) that must be supported in the same die. The sniffing issue is substantially eliminated by the present invention by use of the OTP, hardware range reduction and jamming of the chips beyond specific reading zone.

[0035] As embodied herein and depicted in Figure 2, a schematic view of a contactless payment card 10 is disclosed. In this embodiment, the inlay 10 is an LC circuit composed of the chip (microchip) and mainly its capacitance (C1) and the inductance (L_1) of the winding 12 attached to the die 14. This combination creates a resonant circuit resonating at a particular frequency. The basic ISO specification is very narrow at 13.56 MHz, +/- 500 KHz. This also applies to the NFC or any radio frequency (RF) payment system.

[0036] An effective technique for providing a sorter reading range without affecting the data rate is to detune the inlay of the contactless payment card. To detune the inlay 10, the resonance frequency of the LC circuit is calculated on one of the secondary harmonics of the main frequency, namely:

$$F_{detuned} = 1/2\pi \sqrt{L_1 C_1}. \qquad \text{(Equation 1)}$$

[0037] As previously discussed, controlling the range at which contactless payment cards may be read is one of the features of the present invention that eliminates the sniffing problem. As noted, the operating frequency of the device may be in the HF RFID band at 13.56 MHz, employing inductive coupling to communicate with the RFID reader 30. RFID inlay 10 may include a read/write memory of at least 500 bits. In another embodiment, the memory size is about 2 K bits.

[0038] Referring to Figure 3, an example of a near field signal 20 in accordance with the present invention is depicted. Note that signal 20 includes a second harmonic 22 that has a main frequency of 13.56 Mhz. By detuning the inlay 10 in accordance with Equation 1, only the secondary harmonic will be used in the near field RFID communications between the RFID device (50, 52, 54) and the RFID reader 30. This drastically reduces the range of the reader 30 because only a fraction of the power is transmitted to the LC circuit in RFID card inlay 10. This range may be controlled with a relatively high precision at 13.56 MHz. One benefit of this technique is that is simple to realize. Only the inlay 10 must be detuned for the resultant RFID cards (50, 52, 54) to operate with existing readers. If the OTP is employed in conjunction with the range reduction features described immediately above, the probability of sniffing being an issue is quite low.

[0039] If the present invention is employed in higher frequency range systems (e.g., at 915 MHz or Wi-Fi), the RFID reader 30 may require redesign. Further, the OTP would be required. Another technique that may be employed in high frequency systems employs a predetermined geometric configuration of RFID readers 30. The geometric arrangement of readers 30 provides a means for physically locating the RFID card (50,

52, 54). If the RFID card (50, 52, 54) is deemed to be in an authorized location, the transaction is authorized to proceed.

[0040] As embodied herein and depicted in Figure 4, a schematic view of a reader coupler 30 with a concentric jammer is disclosed. In this embodiment, the RFID reader 30 includes a jammer coupler 32 disposed within a perimeter formed by the reader coupler 34. The jammer coupler 32 is shown slightly offset from the center of the reader coupler 34 to compensate for various factors, such as the presence of metal or other conductors, and to provide separation from the reader power input 36. Jamming is a technique whereby potential communications between the contactless RFID card (50, 52, 54) and an unauthorized reader disposed outside of the reading zone of an authorized reader 30 are disturbed and/or interrupted. This is implemented in accordance with the present invention by the jamming coupler 32 which is configured to generate white noise centered around 13.56 MHz. This technique substantially prevents sniffers or hackers from monitoring RFID signals within the reading zone of reader 30.

[0041] Figures 5A and 5B are schematic views of the reader coupler field and the reader coupler field combined with the concentric jammer field, respectively. In Figure 5A, a field 35 generated by the reader coupler 35 is depicted. Figure 5B shows the combination of the field 35 generated by the reader coupler 34 and the field 33 generated by the jammer coupler 32. Figure 5B, therefore, illustrates the coverage of the jammer coupler field 33 relative to the reading zone of RFID reader 30. For example, a reader coupler 34 with a diameter of 6" will have a range of approximately 8.5". If the RFID reader 30 employs a jammer coupler 32 having a diameter of about 70% of that of the reader coupler 34, i.e. 4.2", reader 30 will have a range of about 6".

[0042] The above described techniques may be applied individually or collectively to contactless payment transaction systems in order to enhance the security of such transactions. These techniques may also be applied to any wireless transactions but particularly to payment transactions such as the NFC token system used in cellular phones. As for the OTP technique, it may also be applied to contact payment card

systems or to other type of transaction system such as M-commerce, ticket purchase or payment at video terminals.

[0043] All references, including publications, patent applications, and patents, cited herein are hereby incorporated by reference to the same extent as if each reference were individually and specifically indicated to be incorporated by reference and were set forth in its entirety herein.

[0044] The use of the terms "a" and "an" and "the" and similar referents in the context of describing the invention (especially in the context of the following claims) are to be construed to cover both the singular and the plural, unless otherwise indicated herein or clearly contradicted by context. The terms "comprising," "having," "including," and "containing" are to be construed as open-ended terms (i.e., meaning "including, but not limited to,") unless otherwise noted. The term "connected" is to be construed as partly or wholly contained within, attached to, or joined together, even if there is something intervening.

[0045] The recitation of ranges of values herein are merely intended to serve as a shorthand method of referring individually to each separate value falling within the range, unless otherwise indicated herein, and each separate value is incorporated into the specification as if it were individually recited herein.

[0046] All methods described herein can be performed in any suitable order unless otherwise indicated herein or otherwise clearly contradicted by context. The use of any and all examples, or exemplary language (e.g., "such as") provided herein, is intended merely to better illuminate embodiments of the invention and does not impose a limitation on the scope of the invention unless otherwise claimed.

[0047] No language in the specification should be construed as indicating any non-claimed element as essential to the practice of the invention.

[0048] It will be apparent to those skilled in the art that various modifications and variations can be made to the present invention without departing from the spirit and scope of the invention. There is no intention to limit the invention to the specific form or forms disclosed, but on the contrary, the intention is to cover all modifications, alternative constructions, and equivalents falling within the spirit and scope of the

invention, as defined in the appended claims. Thus, it is intended that the present invention cover the modifications and variations of this invention provided they come within the scope of the appended claims and their equivalents.

What is claimed is:

1. A system comprising:

a transaction unit including a microchip having a computer readable medium configured to store a unit identifier (UI) and at least one one-time-password (OTP) therein, the UI and the at least one OTP comprising transaction authentication data, the transaction unit being configured to transmit the transaction authentication data in response to receiving a predetermined signal;

a reader device configured to transmit the predetermined signal to interrogate the transaction unit and read the transaction authentication data, the reader device being configured to generate at least one authentication indicia in response to receiving an authentication signal; and

a server coupled to the reader device, the server including a database having at least one server OTP related to at least one unit identifier stored therein, at least one server OTP and the at least one unit identifier comprising transaction verification data, the server being configured to compare the transaction authentication data with the transaction verification data, the server being configured to transmit the authentication signal to the reader device if the transaction authentication data matches the transaction verification data.

2. The system of claim 1, wherein transaction unit includes an RFID assembly disposed therein, the RFID assembly including an RFID coupler configured to operate at a predetermined frequency, and wherein the reader device is configured as an RFID reader operating at the predetermined frequency.

3. The system of claim 2, wherein the transaction unit is configured as a card, a token or as a mobile communications device.

4. The system of claim 3, wherein the mobile communications device includes a graphical user interface (GUI) coupled to at least one microprocessor, the mobile communications device being configured to transmit the transaction authentication data to the server via at least one network by manipulating the GUI.

5. The system of claim 2, wherein the contactless RFID reader includes a jammer coupler disposed proximate a reader coupler such that the RFID reader includes a sensing zone wherein the RFID reader interrogates the contactless payment unit and a jamming zone wherein the RFID reader transmits a jamming signal substantially outside of the sensing zone.

6. The system of claim 1, wherein the predetermined signal is carried by a near field magnetic field, and wherein the RFID coupler includes a detuned inlay, the detuned inlay including an LC circuit having a resonant frequency calculated to correspond to a sub-harmonic of the main frequency of the predetermined signal such that the predetermined distance is less than or equal to approximately eight (8) inches.

7. The system of claim 1, wherein the transaction unit and the reader device are configured to communicate at a frequency substantially equal to 13.56 MHz in accordance with an ISO 14443 standard.

8. The system of claim 1, wherein the transaction authentication data includes timing authentication data and the transaction verification data includes timing verification data.

9. The system of claim 1, wherein the at least one authentication indicia includes a visual indicator or an aural indicator, the visual indicator including an LED indicator configured to provide a color coded response indicative of authentication or authentication denial, or wherein the visual indicator is transmitted by way of a graphical user interface coupled to the RFID reader.

10. The system of claim 1, wherein the server is configured to generate the at least one OTP using a predetermined encryption algorithm, the predetermined encryption algorithm is selected from a group of methods that include an Elliptical Curve Cryptography (ECC) encryption method, an Advanced Encryption Standard (AES) encryption method, a Temporal Key Integrity Protocol (TKIP) method, or a Counter-Mode/CBC-Mac protocol (CCMP) method.

11. The system of claim 1, wherein the at least one OTP includes a plurality of one time passwords, each one time password of the plurality of one time passwords being associated with a corresponding index number, and wherein the computer readable medium is configured as a first in first out memory that is configured to store either the plurality of one time passwords or a subset of the plurality of one time passwords.

12. A system comprising:

a contactless transaction unit including an RFID assembly disposed therein, the RFID assembly including an RFID coupler and a microchip having a computer readable medium configured to store transaction authentication data, the RFID coupler including a detuned inlay, the detuned inlay including an LC circuit having a resonant frequency calculated to correspond to a sub-harmonic of the main frequency of a predetermined signal, the transaction unit being configured to transmit the transaction authentication data in response to receiving the predetermined signal;

a contactless RFID reader device configured to transmit the predetermined signal when the transaction unit is disposed within a predetermined distance from the reader device to thereby interrogate the contactless transaction unit and read the transaction authentication data, the contactless RFID reader device being configured to generate at least one authentication indicia in response to receiving an authentication signal; and

a server coupled to the contactless RFID reader device, the server including a database having transaction verification data stored therein, the server being configured to compare the transaction authentication data with the transaction verification data, the server being configured to transmit the authentication signal to the contactless RFID reader device if the transaction authentication data matches the transaction verification data.

13. The system of claim 12, wherein the computer readable medium is configured to store a unit identifier (UI) and at least one one-time-password (OTP) therein, the UI and the at least one OTP comprising the transaction authentication data.

14. The system of claim 12, wherein the transaction verification data comprises at least one server OTP related to at least one unit identifier.

15. The system of claim 12, wherein the contactless RFID reader includes a jammer coupler disposed proximate a reader coupler such that the RFID reader includes a sensing zone wherein the RFID reader interrogates the contactless payment unit and a jamming zone wherein the RFID reader transmits a jamming signal substantially outside of the sensing zone.

16. The system of claim 12, wherein the predetermined distance is less than or equal to approximately eight (8) inches.

17. A system comprising:

a transaction unit including an RFID assembly disposed therein, the RFID assembly including an RFID coupler and a microchip having a computer readable medium configured to store transaction authentication data, the transaction unit being configured to transmit the transaction authentication data in response to receiving the predetermined signal;

an RFID reader device configured to transmit the predetermined signal when the transaction unit is disposed within a predetermined distance from the RFID reader device to thereby interrogate the transaction unit and read the transaction authentication data, the RFID reader includes a jammer coupler disposed proximate a reader coupler such that the RFID reader device includes a sensing zone wherein the RFID reader device interrogates the transaction unit and a jamming zone wherein the RFID reader device transmits a jamming signal substantially outside of the sensing zone, the RFID reader device being configured to generate at least one authentication indicia in response to receiving an authentication signal; and

a server coupled to the RFID reader device, the server including a database having transaction verification data stored therein, the server being configured to compare the transaction authentication data with the transaction verification data, the server being configured to transmit the authentication signal to the RFID reader device if the transaction authentication data matches the transaction verification data.

18. The system of claim 17, wherein the RFID coupler includes a detuned inlay, the detuned inlay including an LC circuit having a resonant frequency calculated to correspond to a sub-harmonic of the main frequency of the predetermined signal.

19. The system of claim 17, wherein the predetermined distance is less than or equal to approximately eight (8) inches.

20. The system of claim 17, wherein the computer readable medium is configured to store a unit identifier (UI) and at least one one-time-password (OTP) therein, the UI and the at least one OTP comprising the transaction authentication data, and wherein the transaction verification data is comprised of at least one server OTP related to at least one unit identifier.

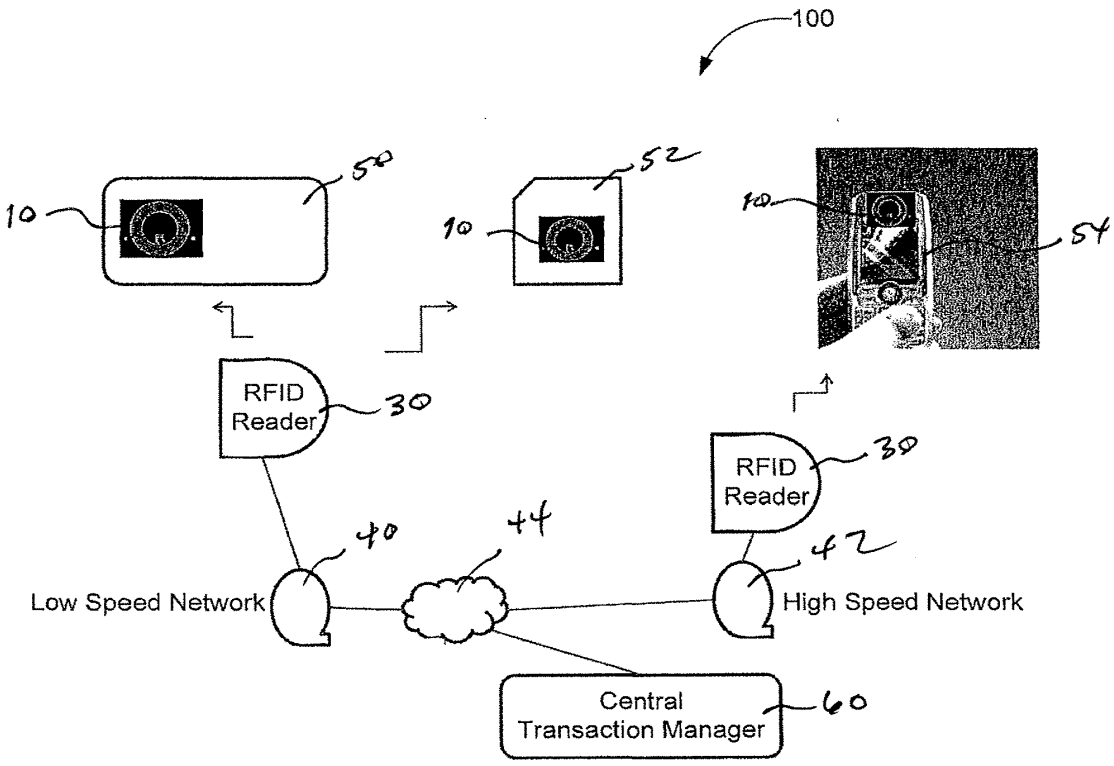

100
10
50
10
52
10
54
RFID Reader
30
RFID Reader
30
40
44
42
Low Speed Network
High Speed Network
Central Transaction Manager
60

Figure 1

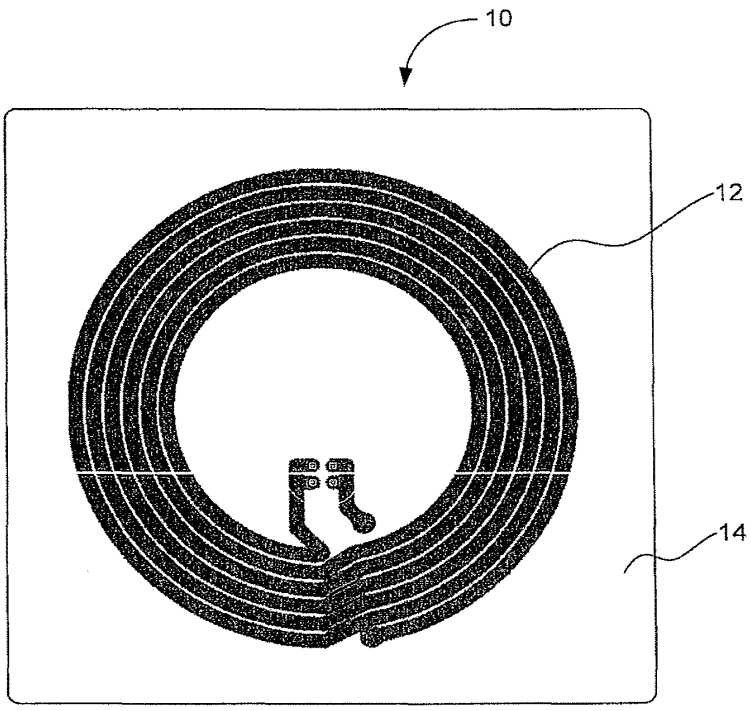


Figure 2

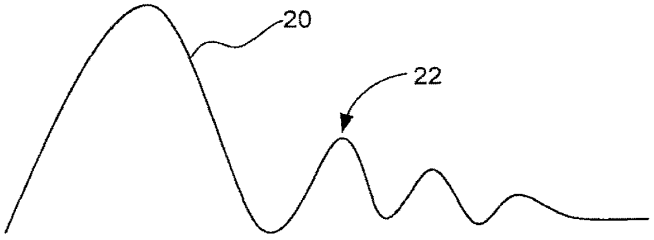


Figure 3

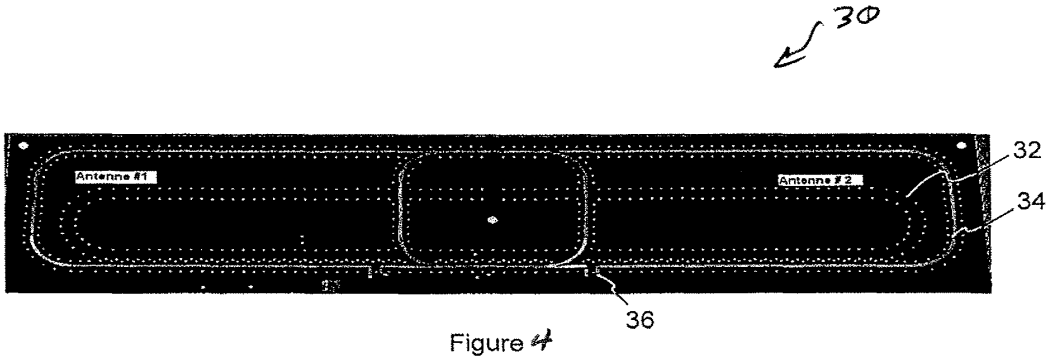


Figure 4

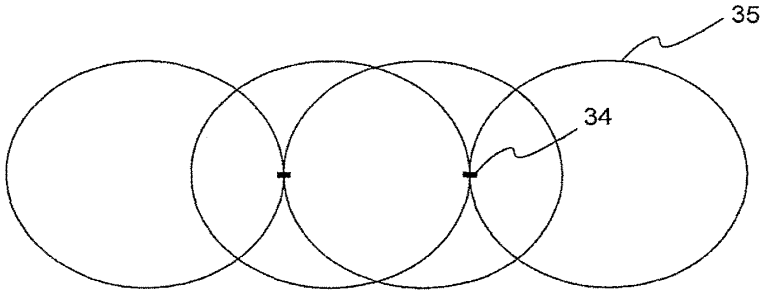


Figure 5A

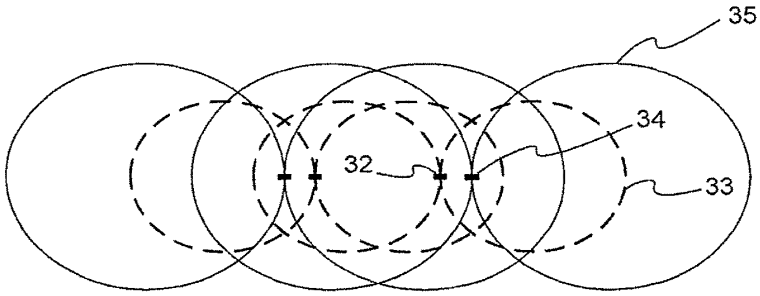


Figure 5B

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB2009/007364

A. CLASSIFICATION OF SUBJECT MATTER
IPC: ***G06Q 20/00*** (2006.01) , ***G06K 7/10*** (2006.01) , ***H04L 9/32*** (2006.01) , ***H04K 3/00*** (2006.01)
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC: ***G06Q*** (2006.01) , ***G06F*** (2006.01), ***G06K*** (2006.01), ***H04B*** (2006.01), ***H04L*** (2006.01), ***H04Q*** (2006.01)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic database(s) consulted during the international search (name of database(s) and, where practicable, search terms used)
EPOQUE, DELPHION, Canadian Patent Database, Google™, Google™ Scholar,
& keywords: RFID reader, one-time password*, authentication, jammer, LC, sub-harmonic* and similar terms.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2006/037220 A1 (RICHARD, C.) 13 April 2006 (13-04-2006) * pages 1, 3, 4, 6, 8, 9 and 11 *	1 - 3, 10, 11
Y		4 - 9, 12 - 20
X	US 2007/0194889 A1 (BAILEY, D.V. et al.) 23 August 2007 (23-08-2007) * paragraphs [0030] to [0037], [0040] to [0047], [0053] to [0060] and [0075] *	1 - 3, 7
Y		4 - 6, 8 - 20
Y	US 2007/0194931 A1 (MILLER, R.N. et al.) 23 August 2007 (23-08-2007) * paragraphs [0012] to [0016] *	5, 15, 17 - 20
Y	US 2002/0140215 A1 (BREED, D.S.) 3 October 2002 (03-10-2002) * paragraph [0275] *	6, 12 - 16, 18
Y	US 2008/0014867 A1 (FINN, D.) 17 January 2008 (17-01-2008) * paragraphs [0018], [0057], [0058], [0063], [0082] to [0084] and [0095] *	6, 8, 9, 16, 19
A	* paragraphs [0118], [0145], [0146] and [0184] to [0185] *	1 - 5, 7, 10 - 18, 20

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents :	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier application or patent but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search	Date of mailing of the international search report
25 February 2010 (25-02-2010)	4 March 2010 (04-03-2010)

Name and mailing address of the ISA/CA	Authorized officer
Canadian Intellectual Property Office Place du Portage I, C114 - 1st Floor, Box PCT 50 Victoria Street Gatineau, Quebec K1A 0C9 Facsimile No.: 001-819-953-2476	Jennifer Guerra (819) 934-2628

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 2007/057786 A2 (FINN, D.) 24 May 2007 (24-05-2007) * pages 2, 8, 14, 15, 32, 37, 39, 43, 44, 46, 47, 48, 61, 62 and 67 *	4, 9
A	* pages 77 and 79 *	1 - 3, 5 - 8, 10 - 20
Y	WO 2005/125078 A1 (KAMENDJE, G) 29 December 2005 (29-12-2005) * pages 3 and 9 *	11
P, X	WO 2009/075434 A1 (CHOI, D.H.) 18 June 2009 * entire document *	1 - 3, 10
P, Y		4 - 9, 11 - 20
P, X	US 2009/0200371 A1 (KEAN, B.) 13 August 2009 (13-08-2009) * paragraphs [0009], [0012], [0017], [0055] and [0059] *	1 - 3
P, Y		4 - 20
P, Y	US 7,387,260 B1 (MACKENZIE, J.D.) 17 June 2008 (17-06-2008) * column 1, lines 56 to 65 and column 22, lines 57 to 62 *	6, 12, 18
P, Y	US 2009/0224058 A1 (SAVRY, O.) 10 September 2009 (10-09-2009) * paragraph [0032] *	6, 12, 18
A	WO 2007/123895 A2 (HALLAM-BAKER, P.M.) 1 November 2007 (01-11-2007) * paragraphs [0020] to [0039] and [0050] to [0067] *	1 - 20
A	US 2008/0238676 A1 (DHILLON, P.S. et al.) 2 October 2008 (02-10-2008) * paragraphs [0019] and [0025] *	1 - 20
A	WO 2007/149775 A2 (HAMMAD, A. et al.) 27 December 2007 (27-12-2007) * pages 2, 6 to 8, 12, 14, 20 and 21 *	1 - 20
A	WO 2007/073609 A1 (ROLLIER, A. et al.) 5 July 2007 (05-07-2007) * pages 3 to 5, 8, 9, 12 and 13 *	1 - 20

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/IB2009/007364

Patent Document Cited in Search Report	Publication Date	Patent Family Member(s)	Publication Date
WO2006037220A1	13-04-2006	AU2005291797A1	13-04-2006
		CA2578983A1	13-04-2006
		CN101031940A	05-09-2007
		EP1805735A1	11-07-2007
		US2008214312A1	04-09-2008
US2007194889A1	23-08-2007	NONE	
US2007194931A1	23-08-2007	CA2678423A1	23-08-2007
		US7612675B2	03-11-2009
		WO2007093038A1	23-08-2007
US2002140215A1	03-10-2002	US6820897B2	23-11-2004
US2008014867A1	17-01-2008	NONE	
WO2007057786A2	24-05-2007	EP1883892A2	06-02-2008
		US2006219776A1	05-10-2006
		US7597250B2	06-10-2009
WO2005125078A1	29-12-2005	CA2471055A1	16-12-2005
		CA2570878A1	29-12-2005
		CN101015163A	08-08-2007
		EP1759479A1	07-03-2007
		US2008172713A1	17-07-2008
WO2009075434A1	18-06-2009	KR20090061118A	16-06-2009
US2009200371A1	13-08-2009	US2009104888A1	23-04-2009
		WO2009052196A1	23-04-2009
US7387260B1	17-06-2008	US7152804B1	26-12-2006
US2009224058A1	10-09-2009	EP2098981A1	09-09-2009
		FR2928475A1	11-09-2009
		JP2009211696A	17-09-2009
WO2007123895A2	01-11-2007	AU2007240903A1	01-11-2007
		CA2649584A1	01-11-2007
		CN101569130A	28-10-2009
		EP2016699A2	21-01-2009
		GB0707939D0	30-05-2007
		GB2437639A	31-10-2007
		JP2009535900T	01-10-2009
		KR20080112395A	24-12-2008
		US2007250704A1	25-10-2007
US2008238676A1	02-10-2008	NONE	

(Continued on extra sheet, page 6)

(Continued from patent family annex, page 5)

WO2007149775A2	27-12-2007	AU2007261072A1	27-12-2007
		CA2655015A1	27-12-2007
		CN101473344A	01-07-2009
		EP2041714A2	01-04-2009
		KR20090023491A	04-03-2009
		MX2008016173A	26-01-2009
		US2008005037A1	03-01-2008
WO2007073609A1	05-07-2007	AU2006331310A1	05-07-2007
		CA2650063A1	05-07-2007
		CN101336436A	31-12-2008
		EA200870122A1	27-02-2009
		EA012094B1	28-08-2009
		EP1811421A1	25-07-2007
		EP1966737A1	10-09-2008
		KR20080087021A	29-09-2008
		US2009320118A1	24-12-2009

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB2009/007364

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of the first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons :

1. [ ] Claim Nos. :
because they relate to subject matter not required to be searched by this Authority, namely :

2. [ ] Claim Nos. :
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically :

3. [ ] Claim Nos. :
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows :

see extra sheet, page 7

1. [ ] As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. [X] As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. [ ] As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claim Nos. :

4. [ ] No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claim Nos. :

Remark on Protest

[ ] The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

[ ] The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

[ ] No protest accompanied the payment of additional search fees.

Continued from Box III, page 2

The international application relates to multiple inventions not linked to form a single general inventive concept. The multiple inventions are as follows:

Group A: Claims 1 to 11 are directed to a system comprising a transaction unit, a reader device, and a server wherein the reader transmits an authentication signal to the transaction unit, which in turn transmits a unit identifier (UI) and one-time-password (OTP) to the reader for authentication purposes. The reader communicates with a server to verify the authentication information.

Group B: Claims 12 to 16 are directed to a system comprising a transaction unit having an RFID assembly with LC circuit thereon, a contactless reader device and a server. The reader transmits an authentication signal to the transaction unit, which in turn transmits authentication data to the reader for authentication purposes. The reader communicates with a server to verify the authentication.

Group C: Claims 17 to 20 are directed to a system comprising a transaction unit having an RFID assembly, a RFID reader device and a server, wherein the RFID reader includes a jammer. The reader transmits a signal to the transaction unit when it is within a predetermined distance from the RFID reader, which in turn transmits authentication data to the reader. The reader communicates with a server to verify the authentication data.

The common features between the groups of claims are known. Specifically, WO 2006/037220 (D1) and US 2007/0194889 (D2) teach the following features:

- a transaction unit (D1 - tag 302, page 8; D2 - Tag, paragraph [0053]), a reader device (D1 - reader 301, page 8; D2 - Reader, paragraph [0053]) and a server (D1 - host 305 and security server, page 8; D2 - paragraph [0036]);
- the reader device sends an authentication signal to the transaction unit (D1 - page 8, lines 22 to 25; D2 - paragraph [0054]);
- the transaction unit responds with authentication data (D1 - page 8, lines 25 to 27; D2 - paragraph [0055]);
- the reader verifies the authentication data with a server (D1 - page 8, line 27 to page 9, line 1; D2 - paragraph [0036]).

As the common features between the groups of claims are known, the claims are considered to lack unity.

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
17/528,073	**01/12/2023 12:46:29 AM ET**	**WYAT-0002.USD1C1C1C1C1C**

Title of Invention

MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	4809	FILED BY	Jose Garcia
PATENT CENTER #	61424590	FILING DATE	11/16/2021
CUSTOMER #	136197	FIRST NAMED INVENTOR	David WYATT
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	-

Documents

TOTAL DOCUMENTS: 10

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
WYAT-0002-13C12US_IDS_transmittal_form.pdf	12	Information Disclosure Statement (IDS) Form (SB08)	1236 KB
WYAT-0002-13C12US_RCE_transmittal_sb0030efs.pdf	3	Request for Continued Examination (RCE)	1628 KB
WO0062214A1.pdf	50	Foreign Reference	3712 KB
WO0157620A2.pdf	165	Foreign Reference	13790 KB
GB2478712A.pdf	33	Foreign Reference	1829 KB

GB2485442A.pdf	55	Foreign Reference	3691 KB
WO2010043974A1.pdf	32	Foreign Reference	1935 KB
WO2005119607A2.pdf	52	Foreign Reference	2732 KB
WO2007145687A1.pdf	116	Foreign Reference	8227 KB
WO2012154915A1.pdf	292	Foreign Reference	14237 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
WYAT-0002-13C12US_IDS_transmittal_form.pdf	A1DCCC49E010C972B8DA039B97AD768C924D75104D82341DD15D00514387B5428A82E16EDB5E46FDE9AF4B0C121A9C4444C3AAB4AF212CF19698B3F2F74535F0
WYAT-0002-13C12US_RCE_transmittal_sb0030efs.pdf	5A47D147BF3F4D153AB91045FBEC5786F3DCE68AE5ECD2BA94EE2B394BC27BF0C53EE5FF3AE6D7BCB0C6EFBA5CA373654D02B0B7CCD985C94F1918670777F806
WO0062214A1.pdf	DDABC100FBD99C5C2F1307B97ADAFDC42462C2F8E0A9EC08BF4DB93A3284DB009B21554EB4E4075C1982C64BCDA34ABABD069F983983ADB16719B4102F372C9C
WO0157620A2.pdf	180EBC78F4CC75B078186E3A497C95A442BC876B63C20EA5B2ACD32EF886AEEF91E5D3D51D1601CAAC89E00E66B25CB04122092207BEB9E98658F0C35EC9CA2B
GB2478712A.pdf	8FEF0EF3995674C591E9DF1668886F0633A19CF86756C6E406A54250C819993EEA54B56D8A7747698A55352B0C83FDE463BE4283E73E89340EC72BEC1C5A80F9
GB2485442A.pdf	1A2A993084C17AD07871B330FC849EF279D41D3ADD1533B418BC28A5AA9F71F623C8B1A672A909C468E9EACFBF5A704E7EA064390D0EEEF17B6F1448EFECD140

WO2010043974A1.pdf	1286E404C4D2D6FADECD924104DEFAEC9E36C84A8D2A2EA EB2BF8D92C0FF78FC7C1E94943BAB2B5068D741F166D7D90A 0B78EB3110238CF343F754C6383CA509
WO2005119607A2.pdf	F8CB44647999039A2B9B267DDA24D9B1C602EF693973B5F94 ADE9EB117CC0A6490CA09551374E915889481A8AB1ABAF5DF 22962178D89D90E69C7E5CA52A3E95
WO2007145687A1.pdf	A2ADDB624C035AAC00F247824B6AD54B06A15A36EE4B1B5E FA1BE459D3DE0BC5E781ECF631EF543EB85D53AE13B902697 CA72D63A3334618B25123D2FDE04363
WO2012154915A1.pdf	A734A15C2B5EA2E2E7A65BBDFED9D06E720BA873F1E1958B 33B89AC6941E2D48D9775F93B3FDCEE3B6CAE6AC75862E8A 0E05E1D0728AC941EE393B2FEBEA7BAF

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC PAYMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
17/528,073	01/12/2023 12:46:29 AM ET	WYAT-0002.USD1C1C1C1C1C

Title of Invention

MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	4809	FILED BY	Jose Garcia
PATENT CENTER #	61424590	AUTHORIZED BY	-
CUSTOMER #	136197	FILING DATE	11/16/2021
CORRESPONDENCE ADDRESS	-	FIRST NAMED INVENTOR	David WYATT

Payment Information

PAYMENT METHOD	PAYMENT TRANSACTION ID	PAYMENT AUTHORIZED BY
EFT / 9055	E20231B147333454	Jose Garcia

FEE CODE	DESCRIPTION	ITEM PRICE($)	QUANTITY	ITEM TOTAL($)
2801	REQUEST FOR CONTINUED EXAMINATION (RCE) - 1ST REQUEST (SEE 37 CFR 1.114)	544.00	1	544.00
			TOTAL AMOUNT:	$544.00

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

(12) UK Patent Application (19) GB (11) 2478712 (13) A

(43) Date of A Publication 21.09.2011

(21) Application No: 1004246.3

(22) Date of Filing: 15.03.2010

(51) INT CL:
G06Q 20/00 (2006.01) *G07C 9/00* (2006.01)
G07F 7/08 (2006.01)

(56) Documents Cited:
US 20080222048 A US 20080210754 A1
US 20050211771 A1

(58) Field of Search:
INT CL G06Q, G07C, G07F
Other: Online: WPI & EPODOC

(71) Applicant(s):
David Jackson
18 Feltham Avenue, EAST MOLESEY, KT8 9BL, United Kingdom

(72) Inventor(s):
David Jackson

(74) Agent and/or Address for Service:
Mathys & Squire LLP
120 Holborn, LONDON, EC1N 2SQ, United Kingdom

(54) Title of the Invention: **Authorisation system**
Abstract Title: **Authorisation system**

(57) An authorisation system 1 which comprises a transaction processing terminal 20 for processing transactions; and a mobile user device 10, the user device 10 comprising means for receiving information relating to a particular transaction from the processing terminal 20, and means for generating a user code to authorise a transaction in dependence upon the received information, wherein the user code is adapted to be received by the processing terminal 20 thereby to enable the processing terminal 20 to process the transaction. The invention extends to a corresponding method, a point-of-sale terminal POS, and a mobile device. The process for card holder present transactions comprises the merchant scanning goods and presenting via a barcode the transaction reference, merchant id and amount. The customer scans the barcode and depending on the amount enters a PIN into the smart phone. The smartphone generates a one time activation code and card number via an on screen barcode and the merchant scans the barcode and processes the transaction. A dynamic activation code may be generated based on a clock signal and a preinstalled random seed key. The system may also be used to control access or authorize provision of service.

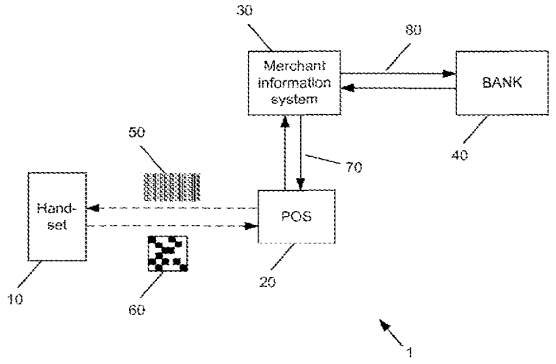


Fig. 1

GB 2478712 A

At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

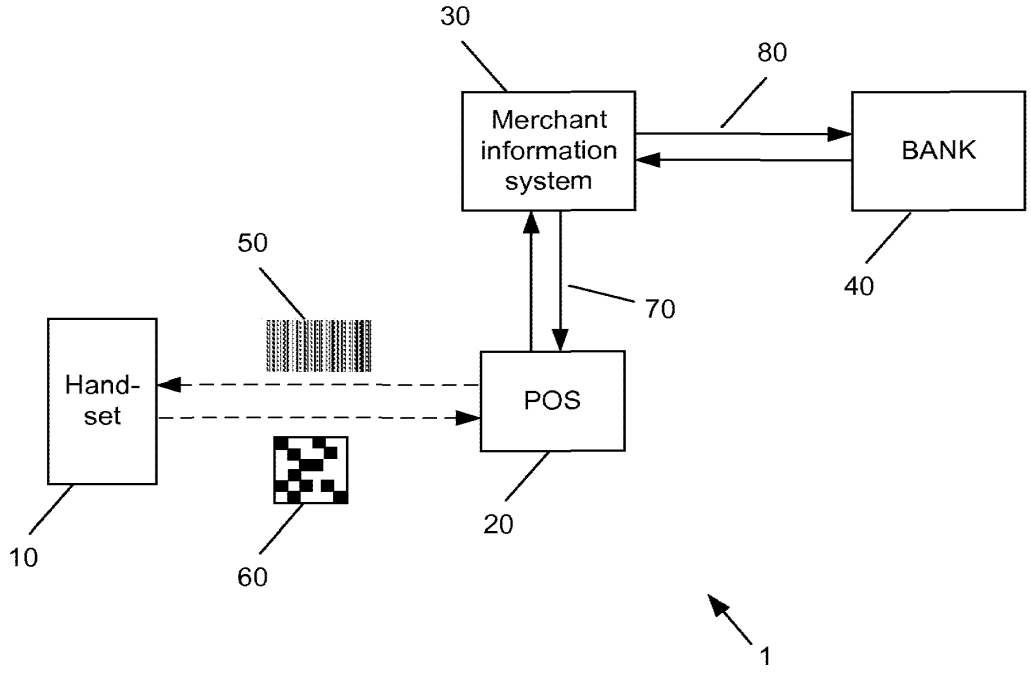

30
80
Merchant information system
BANK
40
50
70
Hand-set
POS
10
60
20
1

Fig. 1

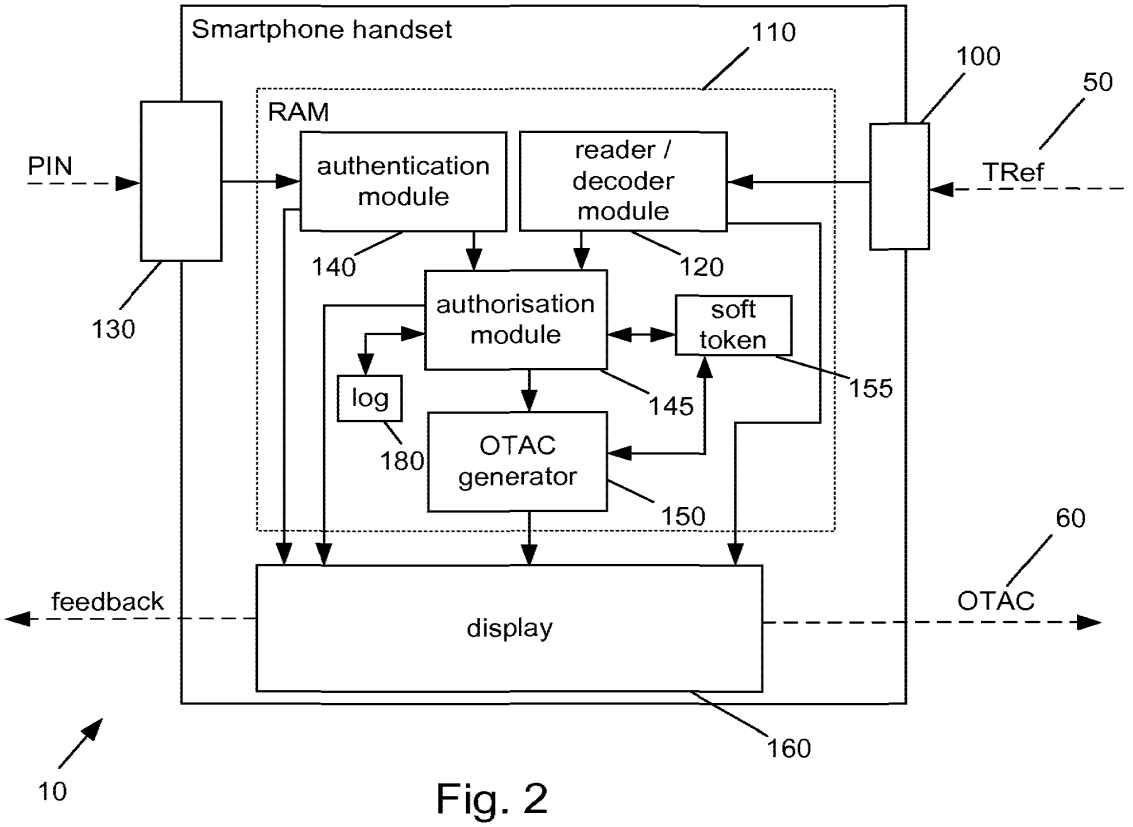

Smartphone handset
110
100
50
RAM
PIN
authentication module
reader / decoder module
TRef
140
120
130
authorisation module
soft token
log
145
155
180
OTAC generator
150
60
feedback
display
OTAC
160
10

Fig. 2

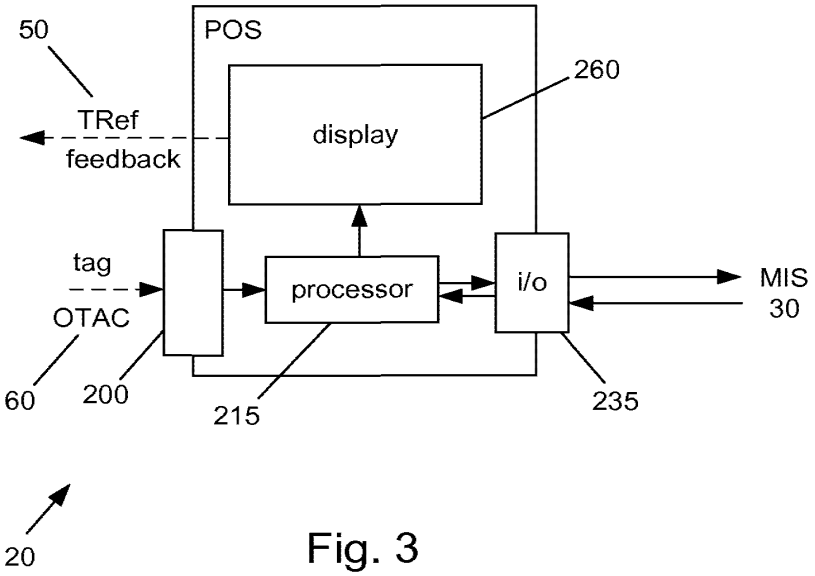

50
POS
260
TRef
feedback
display
tag
processor
i/o
MIS
30
OTAC
60
200
215
235
20

Fig. 3

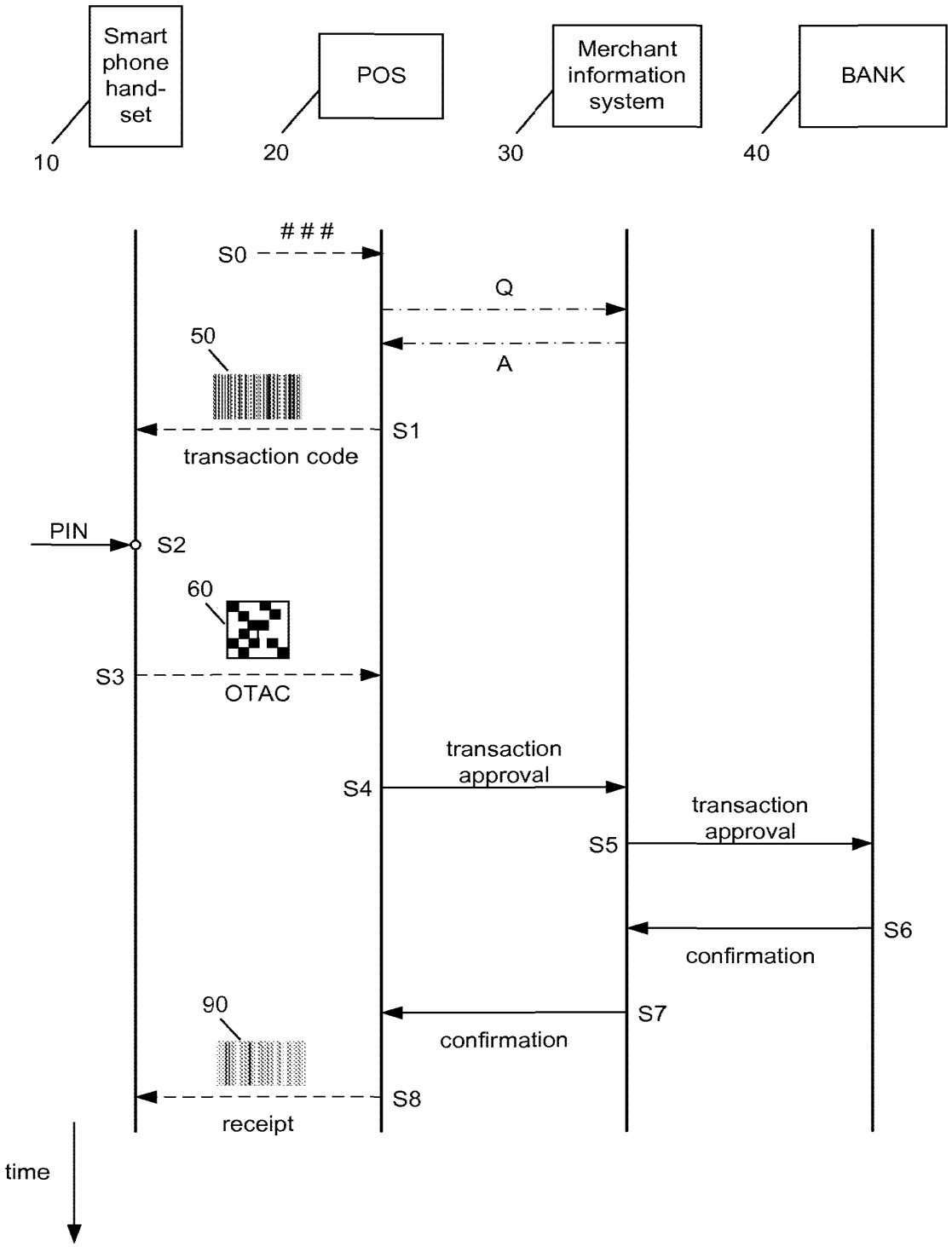
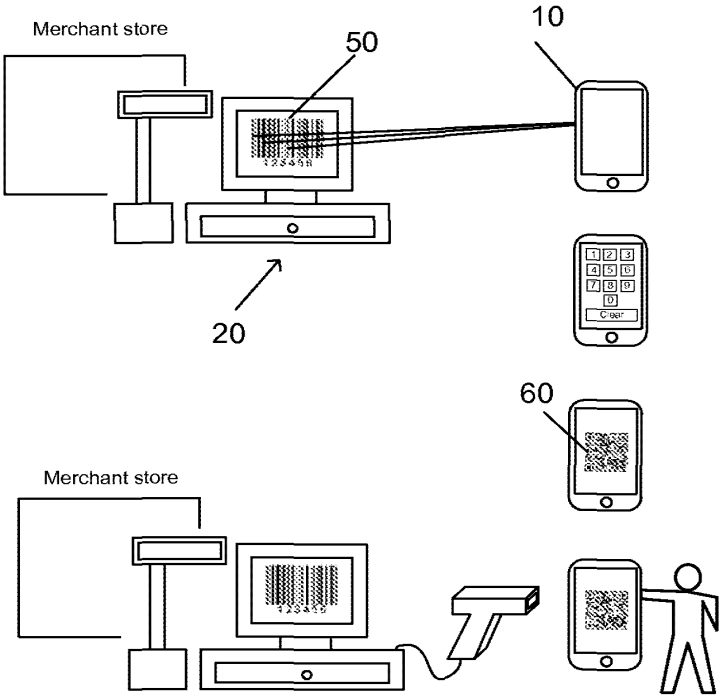

Smart phone hand-set
10
POS
20
Merchant information system
30
BANK
40
###
S0
Q
A
50
S1
transaction code
PIN
S2
60
S3
OTAC
transaction approval
S4
transaction approval
S5
S6
confirmation
90
S7
confirmation
S8
receipt
time

Fig. 4



Process for card holder present transactions

1. Merchant scans good(s) and presents via barcode the transaction ref, merchant ID and amount.

2. Customer scans barcode and depending on amount enters their PIN in to smart phone.

3. Smart phone generates a one time transaction authorisation code and card number via on screen barcode

4. Merchant scans barcode and processes payment.

14 06 11

Fig. 5

Authorisation system

The present invention relates to an authorisation system. This invention also relates to a method of authorising a transaction, and to a mobile device and a point-of-sale (POS) terminal.

Authorisation systems for enabling users to carry out transactions that make use of tokens (such as credit cards) containing RFID tags are known, for example, the MasterCard ™ PayPass ™ system. Such systems enable a user to swipe a credit card equipped with an RFID tag over a reader located at a point-of-sale (POS) terminal in order to effect a payment transaction. However, such systems may be vulnerable to eavesdropping, and the information contained on the RFID tag cannot be altered dynamically, for example, in an effort to improve security. Furthermore, since no user authentication is required, such transactions are limited in value so as to limit the financial exposure to a user and the card issuer should a card be lost or stolen.

For larger value transactions, chip and pin systems are frequently employed. However, there may be security flaws in chip and pin systems. It is known to use separate card readers, into which a credit card is inserted, to generate dynamic pass codes, such as the Visa ™ Dynamic Passcode Authentication Scheme. These systems do enhance the security of existing chip and pin systems. However, the requirement for a user to carry around a card reader, in addition to their credit card, may be inconvenient in certain circumstances.

The present invention aims to alleviate at least some of these problems.

According to one aspect of the invention, there is provided an authorisation system which comprises a transaction processing terminal for processing transactions; and a mobile user device, the user device comprising means for receiving information relating to a particular transaction from the processing terminal, and means for generating a user code to authorise a transaction in dependence upon the received information, wherein the user code is adapted to be received by the processing terminal thereby to enable the processing terminal to process the transaction.

The generation of a user code on the basis of the received transaction information may enhance the security of the system.

Preferably, the user code generating means is adapted to generate a user code which is in the form of a machine readable code.

Preferably, the user code generating means is further adapted to generate a user code which is in the form of an optical indicator. More preferably, the code is in the form of a bar code, and yet more preferably a two-dimensional bar code.

Preferably, the terminal comprises means for reading the code.

Preferably, the reading means comprises an optical scanner.

Alternatively, or in addition, the user code generating means is further adapted to generate the user code in the form of a series of audible tones, and preferably a series of dual-tone multi-frequency (DTMF) signalling tones. In this case, the terminal may be adapted to receive audible tones.

Preferably, the user code generating means is adapted to generate a unique code for each transaction. Hence, the user code is referred to herein as a one-time authorisation code (OTAC).

Preferably, the user code generating means is adapted to incorporate the information relating to a particular transaction within the user code.

Preferably, the user code generating means is adapted to incorporate at least one of the following pieces of information relating to the transaction within the user code: an identity of the terminal (a merchant identifier); the amount of the transaction; detail relating to the item(s); and a time stamp.

Preferably, the user code generating means is adapted to incorporate bank details relating to the user of the mobile device into said code.

Preferably, the bank details are stored on the mobile device, preferably in encrypted form.

Alternatively, or in addition, the bank details may be stored on a remote server, preferably a secure server connectable to the internet. Preferably, the mobile device further comprises means for accessing the server thereby to obtain the bank details from the remote server. Preferably, the mobile device comprises means for connecting the mobile device to the internet.

Alternatively, or in addition, the bank details may be provided in a physical form on an outer surface of the mobile phone. Preferably, the bank details are displayed on an outer surface of the mobile device. More preferably, the bank details are etched onto the outer surface and/or cover of the mobile device. In one example, a card number may be etched onto the rear cover of the mobile device. In an alternative example, an optical indictor, preferably in the form of a bar code, may be provided on the outer surface of the device.

Preferably, the bank details comprise at least one of the following: a credit card number; a bank account number; a Card Verification Value (CVV) code; bank and/or credit card validity dates; and a bank and/or credit card issue number.

Preferably, the user code generating means is adapted to incorporate a dynamically generated authentication code within the user code.

Preferably, the mobile device comprises means for generating a dynamic authentication code based on a clock signal of the user device and a preinstalled random seed key.

Preferably, the means for generating the dynamic authentication code is adapted to generate the code on the basis of the bank details stored on the mobile device.

In the case where the bank details are stored on a remote server, the user code generating means may be adapted to request a dynamically generated authentication

code from the server, in which case the server further comprises means for generating a dynamic authentication code.

Preferably, the mobile device further comprises means for encrypting the user code.

Preferably, the mobile device further comprised means for storing a log of all generated user codes.

Preferably, the mobile device further comprises means for authenticating a user prior to generating the user code.

Preferably, the authentication means comprises means for interrogating a user.

Preferably, the interrogating means comprises means for presenting a user with an authentication screen adapted to be displayed on a display means of the mobile device.

Preferably, the authenticating means is adapted to make use of a Personal Identification Number (PIN) code corresponding to the user's bank account and/or credit card to authenticate the user.

Preferably, the PIN code is stored in an encrypted form on the mobile device.

Preferably, the authentication means is adapted to authenticate the user using a set of images.

Preferably, the set of images includes a selection of random images and at least one image that is known to the user.

Preferably, the authentication means is adapted to authenticate a user on the basis of information relating to the user available via the user's online profile.

Preferably, the authentication means is adapted to access the online profile of a user thereby to obtain information relating to the user to form the basis of the authentication.

Preferably, the processing terminal comprises means for decoding the user code to extract information relating to the user authorisation of the transaction.

Preferably, the terminal comprises means for decrypting the user code.

Preferably, the terminal is connectable to a transaction approval system for approving transactions.

Preferably, the terminal is adapted to transmit information relating to the user authorisation of the transaction to the approval system.

Preferably, the approval system includes a banking institution.

Preferably, the processing terminal further comprises means for displaying transaction information to a user thereby to enable a user to input manually the transaction information relating to a particular transaction into the mobile device.

Preferably, the transaction information comprises at least one of the following: an identity of the terminal (a merchant identifier); the amount of the transaction; detail relating to the item(s); and a time stamp.

Preferably, the processing terminal comprises means for generating a transaction code relating to a particular transaction, said code being adapted to be read by the mobile user device thereby to enable a user to authorise the transaction via the mobile user device.

According to a further aspect of the invention, there is provided an authorisation system which comprises a processing terminal for processing transactions; and a mobile user device, wherein the processing terminal comprising means for generating a transaction code relating to a particular transaction, said code being adapted to be read by the mobile user device thereby to enable a user to authorise the transaction via the mobile user device.

Preferably, the processing terminal further comprises means for displaying the transaction code.

Preferably, the processing terminal is adapted to display the transaction code in the form of an optical indictor.

Preferably, the transaction code generating means is adapted to generate the transaction code in the form of an optical indictor, and preferably in the form of a bar code.

Alternatively, or in addition, the transaction code generating means is further adapted to generate the user code in the form of a series of audible tones, and preferably a series of dual-tone multi-frequency (DTMF) signalling tones. In this case, the mobile device may be adapted to receive audible tones.

Preferably, the truncation code incorporates at least one of the following: an identity of the terminal (a merchant identifier); the amount of the transaction; detail relating to the item(s); and a time stamp.

Preferably, the mobile device further comprises means for reading the transaction code.

Preferably, the reading means is adapted to scan the transaction code.

Preferably, the mobile device further comprises a camera adapted to photograph the transaction code. More preferably, the camera is adapted to operate as an optical scanner.

Preferably, the mobile device further comprises means for decoding the transaction code thereby to extract transaction information from the transaction code.

Preferably, the processing terminal comprises means for displaying a confirmation receipt relating to a completed transaction.

Preferably, the processing terminal comprises a user interface for enabling a user to manually enter a user code into the terminal.

Preferably, the mobile user device is in the form of a mobile telephone and/or a personal digital assistant, and preferably a smartphone.

Preferably, the processing terminal is in the form of a point-of-sale (POS) terminal.

Preferably, the processing terminal is in the form of an internet-based or online merchant.

Preferably, the system is in the form of a payment system.

According to a further aspect of the invention, there is provided a mobile device which is adapted to form part of the system as herein described.

According to another aspect of the invention, there is provided a point-of-sale (POS) device adapted to form part of the system as herein described.

According to another aspect of the invention, there is provided a method of authorising a transaction using a mobile device, the method comprising: receiving information relating to a particular transaction from a transaction processing terminal; and generating a user code on the mobile device to authorise a transaction in dependence upon the received information, wherein the user code is adapted to be received by the processing terminal thereby to enable the processing terminal to process the transaction.

According to yet another aspect of the invention, there is provided a method of processing a transaction using a point-of-sale (POS) terminal, which comprises: generating a transaction code relating to a particular transaction, said code being adapted to be read by a mobile user device thereby to enable a user to authorise the transaction via the mobile user device.

According to a further aspect of the invention, there is provided a mobile device (preferably in the form of a mobile telephone) which comprises software code adapted to carry out the various method steps as described herein.

According to a further aspect of the invention, there is provided a point-of-sale terminal which comprises software code adapted to carry out the various method steps as described herein.

According to another aspect of the invention, there is provided a mobile device, which comprises means for receiving information relating to a particular transaction from a transaction processing terminal; and means for generating a user code on the mobile device to authorise a transaction in dependence upon the received information, wherein the user code is adapted to be received by the processing terminal thereby to enable the processing terminal to process the transaction.

According to a further aspect of the invention, there is provided a point-of-sale (POS) terminal, which comprises means for generating a transaction code relating to a particular transaction, said code being adapted to be read by a mobile user device thereby to enable a user to authorise the transaction via the mobile user device.

In another aspect the invention provides a method of authorising payment transactions by exchanging dynamically generated optical indicators, preferably in the form of bar codes, between a mobile user device and a transaction processing terminal.

The invention also provides a computer program and a computer program product comprising software code adapted, when executed on a data processing apparatus, such as the processing terminal and/or mobile device to perform any of the methods described herein, including any or all of their component steps.

The invention also provides a computer program and a computer program product comprising software code which, when executed on a data processing apparatus, such as the processing terminal and/or mobile device, comprises any of the apparatus

features described herein.

The invention also provides a computer program and a computer program product having an operating system which supports a computer program for carrying out any of the methods described herein and/or for embodying any of the apparatus features described herein.

The invention also provides a computer readable medium having stored thereon the computer program as aforesaid.

The invention also provides a signal carrying the computer program as aforesaid, and a method of transmitting such a signal.

The invention extends to methods and/or apparatus substantially as herein described with reference to the accompanying drawings.

Any feature in one aspect of the invention may be applied to other aspects of the invention, in any appropriate combination. In particular, method aspects may be applied to apparatus aspects, and vice versa.

Furthermore, features implemented in hardware may be implemented in software, and vice versa. Any reference to software and hardware features herein should be construed accordingly.

Each feature disclosed in the description, and (where appropriate) the claims and drawings may be provided independently or in any appropriate combination.

The invention is now described, purely by way of example, with reference to the accompanying drawings, in which:-

Figure 1 shows an authorisation system;
Figure 2 is a block diagram of a smartphone;
Figure 3 is a block diagram of a point-of-sale (POS) terminal;

Figure 4 shows a time-sequence chart of the information exchange steps involved in making a payment for an item using the system of Figure 1; and
Figure 5 shows another embodiment of the authorisation system of Figure 1.

Figure 1 shows an authorisation system, in the form of a smartphone-based payment system 1, as may be located in a department store or shopping mall (or, in principle, in many other commercial premises). The system 1 includes a mobile user device in the form of a smartphone handset or PDA 10 which interacts with a transaction processing terminal in the form of a point-of-sale (POS) terminal 20 by means of an exchange of machine-readable codes 50, 60. The exchange of these codes 50, 60 allows the user of the smartphone 10 to authorise the purchase of an item in the department store; the authorisation is subsequently passed by the POS terminal 20 to a merchant information system (MIS) 30 and thereby used to approve the transaction and effect the appropriate transfer of funds at the bank 40 to make the payment for the item.

The exchanged codes 50, 60 comprise a transaction reference code (TRef) 50 and a one-time authorisation code (OTAC) 60.

Transaction reference code (TRef) 50 is generated dynamically by the POS terminal 20 to be read by the smartphone 10 and comprises information on the product being purchased. TRef 50 includes one or more of the following: an item description, the item price, a merchant identifier, and a time stamp. In this example, TRef 50 is in the form of an optical indicator such as a barcode, which can be readily captured by a built-in camera 100 of the smartphone 10.

The one-time authorisation code (OTAC) 60 is generated by the smartphone 10 in dependence on the received transaction reference code (TRef) 50 and also in dependence on the user's bank account and/or credit card details (which may be stored on the smartphone 10). The user of the smartphone 10 must first be authenticated thereby to authorise the transaction, for example, by entering a security PIN associated with their bank account and/or credit card, before the OTAC 60 is generated for sending on to the POS terminal 20. In this embodiment, the OTAC 60 is also an optical indicator such as a 2D barcode (1D barcodes are possible alternatives).

Also shown in Figure 1 are the transaction approval / confirmation messages 70 (exchanged by the POS terminal 20 and the merchant information system 30) and 80 (exchanged by the merchant information system 30 and the bank 40) to approve, complete, and provide feedback regarding the transaction.

Figure 2 is a block diagram of the smartphone 10, comprising a user interface 130 such as a touchscreen (for example, the Apple iPhone and various models made by Nokia, Samsung, LG and HTC amongst others) or a keypad / keyboard (for example, the Blackberry made by Research In Motion, and various models by Nokia and Sony, amongst others), a display 160 and a camera 100.

The smartphone 10 has been adapted by software to capture or scan (by means of the camera 100) and process (by means of the software modules described below) optical indicators such as barcodes used to represent transaction reference codes (TRef) 50. In operation, random-access memory (RAM) 110 of the smartphone 10 comprises a number of software modules including a reader/decoder module 120, an authentication module 140, an authorisation module 145 and a one-time authorisation code (OTAC) generator 150. Together these modules form a smartphone purchasing application. The software modules are written in a suitable programming language for the suitable software platform for the particular smartphone operating system, for example Java MIDP, C++ or Python on the S60 platform for smartphones running Symbian OS.

The reader/decoder module 120 processes optical indicator details (such as barcodes) captured by the smartphone camera 100 and representing transaction reference codes (TRef) 50. The reader/decoder module 120 decodes the captured TRef 50 into its constituent pieces of information, such as the item description, the item price, and a merchant identifier, and passes this information on to the authorisation module 145. The reader/decoder module 120 sends feedback regarding progress in capturing the TRef data and information regarding the item to the user via display 160.

The authentication module 140 assesses whether the correct security PIN has been entered by the user via the user interface 130 to authenticate the user to allow

authorisation of the purchase of the item. In this embodiment, details of the user's bank (or for example credit or debit card details) and corresponding PIN are stored (in encrypted form) within the authentication module 140. The PIN entered by the user via user interface 130 is compared to the stored PIN and if the values match, a positive authentication is sent to the authorisation module 145; if the values do not match, standard security measures are employed (for example, only a limited number of re-tries are permitted before the smartphone purchasing application is locked). The authentication module 140 sends feedback regarding PIN input and authentication to the user via the display 160.

The authorisation module 145 correlates the item information received from the reader/decoder module 120 with the result of the authentication received from the authentication module 140, recording in log 180 whether the purchase of the item has been approved by the user, providing feedback to the user via the display 160 and instructing the OTAC generator 160 to generate a OTAC to send to the POS terminal 20.

OTAC generator 150 generates a one-time authorisation code (OTAC) 60 to send to the POS terminal 20 to authorise the purchase of the item.

The One-Time Authorisation Code (OTAC) 60 is generated in dependence on data which includes information obtained from the received transaction reference code (TRef) 50 (which, as described previously, may comprise a item description, item price, and a merchant identifier) and the user's bank account details (for example, the user's account number, credit/debit card number, card valid-from/expiry date, issue number and card verification value CVV) stored on the smartphone by the authentication module 140. Additional details encoded in the OTAC may include data specific to the smartphone 10, such as the IMEI (International Mobile Equipment Identity) number, or to the user such as the IMSI (international mobile subscriber identity) stored on the SIM (subscriber identity module) card. A time-stamp is also included.

A hashing algorithm is used to combine the data (or the appropriate subset, as acceptable to authorise payment transactions by the merchant information system 30

and bank 40) and generate the OTAC 60 in the form of an optical indicator such as a 2D barcode (for example, according to an open-standard such as Data Matrix or Semacode) which is displayed on the screen 160, and is readable by the POS terminal 20.

The uniqueness of the OTAC therefore results from the particular data used in its generation. The system therefore allows for the use of a combination of "something you have" (the smartphone 10, which has encoded data specific to a user's bank account and/or credit card) with "something you know" (the PIN) as required by a two-factor authentication scheme.

The "one-time" or unique aspect of the one-time authorisation code (OTAC) 60 is further enhanced by providing the smartphone 10 with a dynamic authentication code generating means, in the form of a soft token 155, which is used to generate dynamic authentication codes which are then embedded within the OTAC 60. In one example, the system uses an authentication scheme based on RSA SecurID, which can be used to generate a series of secretly-seeded random numbers at regular time intervals. In this case, the secret seed will have been previously securely transmitted (potentially encrypted by a public-key of the user or assigned to the smartphone 10) or installed directly at the smartphone 10, and is otherwise known only to the bank 40 (or a certification authority) which therefore knows what authentication code to expect at any given time. RSA SecurID is available as a software module and executes from the smartphone 10 RAM 110.

Figure 3 is a block diagram of a point-of-sale (POS) terminal 20, comprising an optical scanner 200, a processor 215, an input / output (i/o) port 235 (to connect the POS terminal 20 to the merchant information system 30, for example by a network connection or telephone line) and a display 260.

Figure 4 shows a time-sequence chart of the information exchange steps involved in making a payment for an item using the smartphone-based payment system 1.

In a preliminary step (S0), the customer / smartphone user having taken the item to be

purchased to the POS terminal 20, the POS terminal 20 determines the item details by, for example, reading the price-tag attached to the item (this may be a barcode, a magnetic strip an RFID tag or some other form of price tag) by means of scanner 200, processing the resulting data using processor 215 (optionally, if the POS terminal 20 does not have this information stored, enquiring via the i/o port 235 of the merchant information system (MIS) 30 as to the item details, shown as exchange Q-A) and displaying on display 260 a machine-readable transaction code 50. Optionally, POS terminal 20 may also display human-readable details regarding the item on the display 260 for the convenience of (and as feedback for) the customer.

In step S1, the user scans transaction code 50 displayed by POS terminal 20 with the camera 100 of smartphone 10, that is, the camera 100 of the smartphone 10 is used as a barcode scanner.

In step S2, the user authorises the transaction by entering the PIN associated with the bank account or credit card. If the entered PIN is correct (as determined by the authentication module 140), smartphone 10 generates (by means of the OTAC generator module 150) a one-time authorisation code (OTAC) 60.

In step S3, smartphone 10 sends the OTAC code 60 authorising payment to the POS terminal 20. In practice, this means smartphone 10 displays the 2D barcode representing the OTAC code 60 on its display screen 160, and the POS terminal 20 scans the code with its scanner 200. As mentioned above, the OTAC 60 typically includes the user's bank card data (possibly including a dynamic authentication code) together with certain transaction information.

In step S4, POS terminal 20 sends the transaction approval message to merchant information system 30. Depending on the encryption scheme in use (if any), processor 215 of the POS terminal 20 may be able to decode the OTAC 60 and send pertinent transaction details to the merchant information system 30; alternatively, if processor 215 of the POS terminal 20 cannot decode the OTAC 60, POS terminal 20 acts merely as a relay and forwards the OTAC 60 to the merchant information system 30.

In step S5, merchant information system 30 (potentially having first decoded the OTAC 60) sends a transaction approval message and user bank details to bank 40. Bank 40 makes the payment, transferring money from the user's bank account to that of the merchant.

In step S6, bank 40 sends a confirmation message to merchant information system 30, confirming the payment has been made.

In step S7, merchant information system 30 sends a confirmation message to POS terminal 20, which then displays a confirmation message to the customer / smartphone user.

Optionally, in step S8, POS terminal 20 issues a receipt 90 in the form of further optical indicator, such as barcode. This is scanned by the user with the camera 100 of smartphone 10, which then stores the receipt as evidence of the purchase having been made. Alternatively, a traditional paper receipt may be issued.

Figure 5 shows another embodiment of the smartphone-based payment system 1, showing the process for card-holder present transactions, comprising the steps of:

1. Merchant scans good(s) and presents via barcode the transaction reference, merchant ID and amount;
2. Customer scans barcode with a smartphone or handset and depending on amount enters their PIN in to smartphone (low value transactions may be processed and authorised without the need to enter a pin);
3. Smartphone generates a one-time transaction authorisation code and card number via an onscreen barcode; and
4. Merchant scans barcode and then processes payment.

Further features

- Additional security

For additional security, the data may be encrypted before or during generation of the

OTAC to prevent user information being obtained surreptitiously by those obtaining the unencrypted OTAC (for example by intercepting its transmission to the POS terminal 20) and reversing the hashing algorithm. An encryption key is stored as a further software token on the smartphone handset 10. In a symmetric-key scheme, the further software token is one of identical shared secret keys; the other shared secret key is stored at the bank 40. In an asymmetric-key (or public-key) scheme, the further software token is the public key issued by the bank; the bank's private key is stored at the bank 40.

As a further alternative, the PIN needing to be entered by the user need not be the same one as used to access the user's bank account directly, but merely one to access the smartphone payment system on that particular smartphone 10.

- Remote storage of bank account details

In an example, instead of storing the user bank account details, such as a credit card number, on the smartphone 10, the bank account details are instead stored on a secure remote server that is typically connected to the banking institution's communication network infrastructure. In this case, the smartphone 10 is adapted to access the bank account details by establishing a secure connection to this server, for example via a Secure Sockets Layer (SSL) internet connection. In particular, after the user has been authenticated, for example by entering the correct security PIN, the authorisation module 145 then establishes a secure communications channel with the remote server to extract the user's bank account details from the remote server. These details are then used by the OTAC generator 150 to generate the OTAC 60.

In another example, the remote server is capable of generating a dynamic authentication code, for example, based on the user bank account details which are stored on the remote server, and when the authorisation module connects to the remote server, instead of extracting or downloading the full user bank account details or card number, the server instead generates a dynamic authentication code which is then transmitted to the smartphone for use by the OTAC generator 150 in creating the OTAC 60.

- PIN-less payments

For the convenient purchase of items of low monetary value, such as newspapers, step S2, in which the user authorises the transaction by entering the security PIN associated with the user's bank account, is optional and the payment may be termed 'PIN-less'. In this case, the user would merely click an "accept button" to authorise the transaction.

In order to limit the financial exposure were the smartphone to be stolen, PIN-less payments are restricted in that they may only be made for individual purchases not exceeding a predetermined maximum monetary value per purchase. Optionally, the total value for PIN-less payments made in total and/or during a predetermined time period may also be restricted to a predetermined maximum monetary value (reaching this value then requires the user to re-set the PIN-less payment system, which necessitates entering the requisite PIN).

- Manual entry systems

In certain examples, instead of the POS terminal 20 presenting the user with a barcode for scanning with the camera 100 of smartphone handset 10, POS terminal 20 presents transaction reference code (TRef) 50 in the form of an alphanumeric string which the user keys into the smartphone 10 manually via user interface 130. The subsequent steps S2 to S8 proceed as described above. Step S3, wherein POS terminal 20 scans the OTAC 60 displayed on the display screen 160 of smartphone 10 may also be replaced by the manual entry of an alphanumeric string by the user on the POS terminal 20. In this case the OTAC is presented in the form of an alphanumeric string which the user then enters into a keypad of the POS terminal 20.

- Telephone based transactions

The described payment system may also be adapted for the payment of goods or services over a telephone communications system. In this case, the transaction reference code (TRef) 50 and/or the OTAC 60 are generated in the form of a series of audible DTMF signalling tones. In particular, the POS terminal 20 generates the TRef code 50 in the form of a sequence of DTMF tones, which are then received by the smartphone 10, for example, via a microphone of the smartphone 10. The smartphone 10 then extracts the transaction information from the sequence of DTMF tones and then

generates the OTAC 60 in dependence on the received transaction information. In this case, the generated OTAC 60 is also in the form of a sequence of DTMF tones, which are then played to the POS terminal 20, which then receives and decodes these tones to process the transaction.

In certain examples, the payment system might use a combination of audible, visual or other OTAC 60 and TRef 50 codes. Thus, for example, the smartphone 10 might receive a TRef code 50 in the form of a sequence of DTMF tones, and then generate the OTAC 60 in the form of a 2D barcode.

- Internet based transactions

The described smartphone payment system may also be adapted for payment of goods and services over the internet. In one example, the merchant information system 30 provides a web-site which displays optical indicators such as barcodes to relate information such as item descriptions, item prices, and a merchant identifier. In an analogous way to that of the above-described POS-based embodiment, the user scans the requisite barcode with the smartphone handset 10 and enters a PIN to authorise the transaction (steps S1 and S2).

In one example, based on the manual entry systems described above, the OTAC 60 generated by smartphone 10 is in the form of an alphanumerical string which the user enters manually into a text box on the website to approve payment.

In an alternative embodiment, the user generates an OTAC 60 via smartphone 10 and merchant information system 30 uses the user's webcam to read the OTAC 60.

- Further authentication schemes

Instead of authenticating the user by having them input a PIN directly via the user interface 130 (which may require bank account or credit card information and PIN being stored on the smartphone handset 10), alternative authentication schemes may be used.

- ***Picture password authentication***

In one example, the user is shown a selection of random photographs, one of which is a 'key' photograph for the user, for example, a photograph of a person that is related to user. The user is then authenticated by selecting the correct 'key' photograph. The user might also be required to select more than one photograph displayed on the screen, or might be required to select particular photographs from successively displayed selections of photographs. 'Key' photographs are typically preselected by the user or authorising system.

- ***Online profile authentication***

In another example, items specific to the user and obtainable from the user's recent on-line activity (for example, a recent posting to a social networking website or a twitter 'tweet') are presented amongst other items of a similar form; the user authenticates by correcting identifying their own contributions.

This form of authentication might be used in combination with the above described picture password authentication, since 'key' photographs might be sourced from a user's online profile, for example, the system might make use of an image that has recently been uploaded to a user's page on a social networking site.

- ***Voice authentication***

Another possible authentication scheme is to use a speech recognition system to identify the user.

- Dynamic credit card numbers

In an example, the smartphone 10 is provided with a series of credit card numbers to be used for a successive series of transactions. In this case, each credit card number is only valid for a particular time period (for example for one day or one week) or for a particular number of transactions. After the specified time period, or after a particular number of transactions, the card number expires and the next card number in the sequence is then used for subsequent transactions. The series of credit card numbers are securely delivered to the smartphone in a similar manner to that described above

with respect to the delivery of a secret seed code. In this case, when the user carries out a payment transaction using the smartphone 10, the OTAC 60 would be generated based on the currently valid credit card number in a particular series.

- Physical card details

In one example, the user's bank account details are provided on an outer surface of the smartphone 10 itself. In particular, the user's card number, or a coded representation of the user's card number (such as a barcode), is etched onto the rear surface of the smartphone 10. In an example, the card number or barcode is etched or displayed on a removable cover of the smartphone 10. Alternatively, the card number or barcode could be provided in the form of a (removable) sticker which is stuck onto the rear surface of the smartphone 10. In this case, the OTAC generator is used to generate an OTAC which includes a dynamic authentication code, but which does not include the user's card number. The user's card number is then either manually inputted by the user into the POS terminal 20, or scanned by the POS terminal 20 from the rear surface of the smartphone 10 at the time that the user scans the transaction reference code (TRef) 50 from the POS terminal 20. In the case where the user's card number itself is provided on the surface of the smartphone, the card would be of the type that would only operate if it is used in combination with a dynamic authentication code.

While, the authorisation system has been described above mainly with reference to a payment system 1, it is also envisaged that the present authorisation system could be used in many other similar situations in which it is necessary to control access and/or authorise the provision of goods or services. For example, the system could be employed to control access to a particular controlled area, like a music concert or a public transportation system.

It will be understood that the present invention has been described above purely by way of example, and modifications of detail can be made within the scope of the invention.

Claims:

1. An authorisation system which comprises a transaction processing terminal for processing transactions; and a mobile user device, the user device comprising means for receiving information relating to a particular transaction from the processing terminal, and means for generating a user code to authorise a transaction in dependence upon the received information, wherein the user code is adapted to be received by the processing terminal thereby to enable the processing terminal to process the transaction.

2. The system of Claim 1, wherein the user code is in the form of a machine readable code.

3. The system of Claim 1 or 2, wherein the user code is in the form of an optical indicator.

4. The system of Claim 3, wherein the code is in the form of a bar code, and more preferably a two-dimensional bar code.

5. The system according to any of the preceding claims, wherein the terminal comprises means for reading the code.

6. The system according to Claim 5, wherein the reading means comprises an optical scanner.

7. The system according to any of the preceding claims, wherein the user code generating means is adapted to generate a unique code for each transaction.

8. The system according to Claim 7, wherein the user code generating means is adapted to incorporate the information relating to a particular transaction within the user code.

9. The system according to Claim 8, wherein the user code generating means is

adapted to incorporate at least one of the following pieces of information relating to the transaction within the user code: an identity of the terminal (a merchant identifier); the amount of the transaction; detail relating to the item(s); and a time stamp.

10. The system according to any of the preceding claims, wherein the user code generating means is adapted to incorporate bank details relating to the user of the mobile device into said code.

11. The system according to Claim 10, wherein the bank details are stored on the mobile device.

12. The system according to Claim 10 or 11, wherein the bank details comprise at least one of the following: a credit card number; a bank account number; a Card Verification Value (CVV) code; bank and/or credit card validity dates; and a bank and/or credit card issue number.

13. The system according to any of the preceding claims, wherein the user code generating means is adapted to incorporate a dynamically generated authentication code within the user code.

14. The system according to Claim 13, further comprising means for generating a dynamic authentication code based on a clock signal of the user device and a preinstalled random seed key.

15. The system according to any of the preceding claims, further comprising means for encrypting the user code.

16. The system according to any of the preceding claims, further comprising means for storing a log of all generated user codes.

17. The system according to any of the preceding claims, wherein the mobile device further comprises means for authenticating a user prior to generating the user code.

18. The system according to Claim 17, wherein the authentication means comprises means for interrogating a user.

19. The system according to Claim 18, wherein the interrogating means comprises means for presenting a user with an authentication screen adapted to be displayed on a display means of the mobile device.

20. The system according to any of the preceding Claims 17 to 19, wherein the authenticating means is adapted to make use of a Personal Identification Number (PIN) code corresponding to the user's bank account and/or credit card to authenticate the user.

21. The system according to Claim 20, wherein the PIN code is stored in an encrypted form on the mobile device.

22. The system according to any of the preceding Claims 17 to 19, wherein the authentication means is adapted to authenticate the user using a set of images.

23. The system according to Claim 22, wherein the set of images includes a selection of random images and at least one image that is known to the user.

24. The system according to any of the preceding Claims 17 to 19 and 22 or 23, wherein the authentication means is adapted to authenticate a user on the basis of information relating to the user available via the user's online profile.

25. The system according to Claim 24, wherein the authentication means is adapted to access the online profile of a user thereby to obtain information relating to the user to form the basis of the authentication.

26. The system according to any of the preceding claims, wherein the terminal comprises means for decoding the user code to extract information relating to the user authorisation of the transaction.

27. The system according to any of the preceding claims, wherein the terminal comprises means for decrypting the user code.

28. The system according to any of the preceding claims, wherein the terminal is connectable to a transaction approval system for approving transactions.

29. The system according to Claim 28, wherein the terminal is adapted to transmit information relating to the user authorisation of the transaction to the approval system.

30. The system according to Claim 28 or 29, wherein the approval system includes a banking institution.

31. The system according to any of the preceding claims, wherein the processing terminal further comprises means for displaying transaction information to a user thereby to enable a user to input manually the transaction information relating to a particular transaction into the mobile device.

32. The system according to Claim 31, wherein the transaction information comprises at least one of the following: an identity of the terminal (a merchant identifier); the amount of the transaction; detail relating to the item(s); and a time stamp.

33. The system according to any of the preceding claims, wherein the processing terminal comprises means for generating a transaction code relating to a particular transaction, said code being adapted to be read by the mobile user device thereby to enable a user to authorise the transaction via the mobile user device.

34. An authorisation system which comprises a processing terminal for processing transactions; and a mobile user device, wherein the processing terminal comprising means for generating a transaction code relating to a particular transaction, said code being adapted to be read by the mobile user device thereby to enable a user to authorise the transaction via the mobile user device.

35. A system according to Claim 33 or 34, wherein the processing terminal further

comprises means for displaying the transaction code.

36. A system according to Claim 35, wherein the processing terminal is adapted to display the transaction code in the form of an optical indictor.

37. A system according to Claim 35 or 36, wherein the transaction code generating means is adapted to generate the transaction code in the form of an optical indictor, and preferably in the form of a bar code.

38. A system according to any of the preceding Claims 33 to 37, wherein the truncation code incorporates at least one of the following: an identity of the terminal (a merchant identifier); the amount of the transaction; detail relating to the item(s); and a time stamp.

39. A system according to any of the preceding Claims 35 to 38, wherein the mobile device further comprises means for reading the transaction code.

40. A system according to Claim 39, wherein the reading means is adapted to scan the transaction code.

41. A system according to Claim 39 or 40, wherein the mobile device further comprises a camera adapted to photograph the transaction code.

42. A system according to any of the preceding Claims 35 to 41, wherein the mobile device further comprises means for decoding the transaction code thereby to extract transaction information from the transaction code.

43. A system according to any of the preceding claims, wherein the processing terminal comprises means for displaying a confirmation receipt relating to a completed transaction.

44. A system according to any of the preceding claims, wherein the processing terminal comprises a user interface for enabling a user to manually enter a user code

into the terminal.

45. A system according to any of the preceding claims, wherein the mobile user device is in the form of a mobile telephone and/or a personal digital assistant, and preferably a smartphone.

46. A system according to any of the preceding claims, wherein the processing terminal is in the form of a point-of-sale (POS) terminal.

47. A system according to any of the preceding Claims 1 to 45, wherein the processing terminal is in the form of an internet-based or online merchant.

48. A system according to any of the preceding claims, wherein the system is in the form of a payment system.

49. A mobile device which is adapted to form part of the system according to any of the preceding claims.

50. A point-of-sale (POS) device adapted to form part of the system according to any of the preceding Claims 1 to 49.

51. A method of authorising a transaction using a mobile device, the method comprising: receiving information relating to a particular transaction from a transaction processing terminal; and generating a user code on the mobile device to authorise a transaction in dependence upon the received information, wherein the user code is adapted to be received by the processing terminal thereby to enable the processing terminal to process the transaction.

52. A method of processing a transaction using a point-of-sale (POS) terminal, which comprises: generating a transaction code relating to a particular transaction, said code being adapted to be read by a mobile user device thereby to enable a user to authorise the transaction via the mobile user device.

53. A mobile device (preferably in the form of a mobile telephone) which comprises software code adapted to carry out the method of Claim 51.

54. A point-of-sale terminal which comprises software code adapted to carry out the method of Claim 52.

55. A mobile device, which comprises means for receiving information relating to a particular transaction from a transaction processing terminal; and means for generating a user code on the mobile device to authorise a transaction in dependence upon the received information, wherein the user code is adapted to be received by the processing terminal thereby to enable the processing terminal to process the transaction.

56. A point-of-sale (POS) terminal, which comprises means for generating a transaction code relating to a particular transaction, said code being adapted to be read by a mobile user device thereby to enable a user to authorise the transaction via the mobile user device.

57. A method of authorising payment transactions by exchanging dynamically generated optical indicators, preferably in the form of bar codes, between a mobile user device and a transaction processing terminal.

58. A system substantially as herein described and/or as illustrated with reference to the accompanying drawings.

59. A method substantially as herein described and/or as illustrated with reference to the accompanying drawings.

60. A mobile device substantially as herein described and/or as illustrated with reference to the accompanying drawings.

61. A point-of-sale (POS) terminal substantially as herein described and/or as illustrated with reference to the accompanying drawings.

Application No: GB1004246.3 **Examiner:** Mr Stuart Purdy

Claims searched: 1-33, 35-48, 51, 53, 55, 58-61 **Date of search:** 20 June 2011

Patents Act 1977: Search Report under Section 17

Documents considered to be relevant:

Category	Relevant to claims	Identity of document and passage or figure of particular relevance
X	1-9, 15, 26, 27-29, 31-33, 35-51, 53, 55	US 2005/211771 A1 (ONOZU) See whole document and note in particular paras 18-24, 26, 29, 31, 41, 44, 144, 146:
X	1-33, 35-48, 51, 53, 55	US 2008/210754 A1 US 2008210754 A1 (LOVETT) See whole document and note in particular paras 8, 36-40, 53, 102, 103, 106, 108 and 111;
A	-	US 2008/222048 A (HIGGINS) See whole document;

Categories:

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

Field of Search:

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC[X] :

Worldwide search of patent documents classified in the following areas of the IPC

G06Q; G07C; G07F

The following online and other databases have been used in the preparation of this search report

WPI & EPODOC

International Classification:

Subclass	Subgroup	Valid From
G06Q	0020/00	01/01/2006
G07C	0009/00	01/01/2006
G07F	0007/08	01/01/2006

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 December 2007 (21.12.2007)

PCT

(10) International Publication Number
WO 2007/145687 A1

(51) International Patent Classification:
G06F 21/00 (2006.01)

(21) International Application Number:
PCT/US2007/004646

(22) International Filing Date:
21 February 2007 (21.02.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/812,279	9 June 2006 (09.06.2006)	US
60/775,046	21 February 2006 (21.02.2006)	US
60/859,235	15 November 2006 (15.11.2006)	US

(71) Applicant and
(72) Inventor: **WEISS, Kenneth, P.** [US/US]; 59 Sargent Street, Newton, MA 02458 (US).

(74) Agent: **DONAHOE, Robert, V.**; Lowrie, Lando & Anastasi, Llp, One Main Street, Suite 1100, Cambridge, MA 02142 (US).

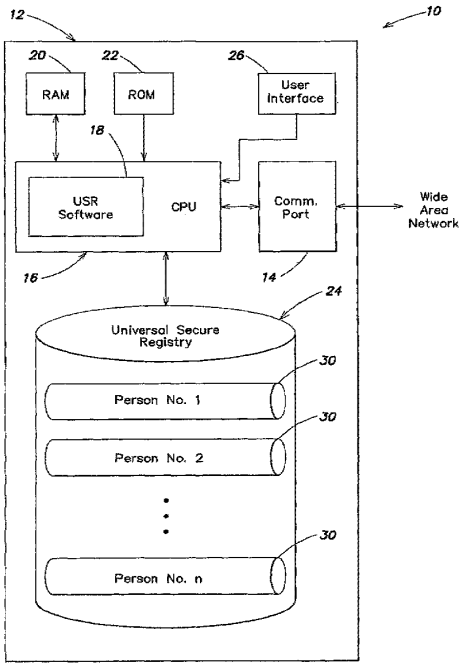
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR SECURE ACCESS PAYMENT AND IDENTIFICATION



(57) Abstract: According to one aspect, the invention provides a system for validating an identity of a user to enable or prevent an occurrence of an event. In one embodiment, the system includes a first device including a wireless transmitter which is configured to transmit validation information, a second device including a wireless receiver, where the second device is configured to receive the validation information and further transmit the validation information; and a secure system in communication with the second device. According to one embodiment, the secure system includes a database. In a further embodiment, the secure system is configured to receive the validation information transmitted from the second device, and to transmit additional information to the second device following a receipt of the validation information to assist the second device in either enabling or preventing the occurrence of the event.

WO 2007/145687 A1

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

METHOD AND APPARATUS FOR SECURE ACCESS PAYMENT AND IDENTIFICATION

BACKGROUND OF INVENTION

1. Field of Invention

Embodiments of the invention generally relate to systems, methods, and apparatus for authenticating identity or verifying the identity of individuals and other entities seeking access to certain privileges and for selectively granting privileges and providing other services in response to such identifications/verifications. In addition, embodiments of the invention relate generally to systems and methods for obtaining information from and/or transmitting information to a user device and, in particular, to systems, methods, and apparatus that provide for contactless information transmission.

2. Discussion of Related Art

Control of access to secure systems presents a problem related to the identification of a person. An individual may be provided access to the secure system after their identity is authorized. Generally, access control to secure computer networks is presently provided by an authentication scheme implemented, at least partly, in software located on a device being employed to access the secure computer network and on a server within the secure computer network. For example, if a corporation chooses to provide access control for their computer network, they may purchase authentication software that includes server-side software installed on a server in their computer system and corresponding client-side software that is installed on the devices that are used by employees to access the system. The devices may include desktop computers, laptop computers, and handheld computers (e.g., PDAs and the like).

In practice, the preceding approach has a number of disadvantages including both the difficulty and cost of maintaining the authentication system and the difficulty and cost of maintaining the security of the authentication system. More specifically, the software resides in the corporation's computers where it may be subject to tampering/unauthorized use by company employees. That is, the information technology team that manages the authentication system has access to the private keys associated with each of the authorized users. As a result, these individuals have an

opportunity to compromise the security of the system. Further, any modification and/or upgrade to the authentication system software is likely to require an update to at least the server-side software and may also require an update of the software located on each user/client device. In addition, where the company's computer systems are geographically distributed, software upgrades/updates may be required on a plurality of geographically distributed servers.

There is also a need, especially in this post September 11 environment, for secure and valid identification of an individual before allowing the individual access to highly secure areas. For example, an FBI agent or an air marshal may need to identify themselves to airport security or a gate agent, without compromising security. Typically such identification may comprise the air marshal or FBI agent showing identification indicia to appropriate personnel. However, there are inherent flaws in this process that allow for security to be compromised, including falsification of identification information and failure of the airport security or other personnel to not recognize the situation. Of course this process could be automated, for example, by equipping airport personnel or security with access to a database and requiring the FBI agent or air marshal to appropriately identify themselves to the database, for example, by again providing identification which airport personnel can then enter into the database to verify the identity of the person seeking access to a secure area. However, this process also has the inherent flaws in it as described above. In addition, there may be times when airport security or personnel may not be able to communicate with the database to check the identity of the person seeking access, for example, when they are not near a computer terminal with access to a database or are carrying a hand-held device that does not have an appropriate wireless signal to access the database. In addition, there is a need to ensure that if such a hand-held device ends up the wrong hands, that security is not compromised.

Systems capable of effectively performing all or some of these functions do not currently exist.

Further, both commercial (e.g., banking networks) and non-commercial (e.g., security systems) information systems often rely on magnetic card readers to collect information specific to a user (e.g., a security code, a credit card number, etc.) from a user device (e.g., a transaction card). Credit card purchases made in person provide an

example of the most common transaction-type that relies on a user device, the credit or debit card, which is read by a magnetic card reader. User devices that rely on magnetic-stripe based technology magnetically store information (e.g., binary information) in the magnetic stripe. The magnetic stripe reader provides an interface to a larger computerized network that receives the user's information to determine, for example, whether to authorize a transaction, to allow the user access to a secure area, etc.

Recently, such devices have seen technological advances that increase their capabilities and improve their security. For example, such devices may now include embedded processors, integral biometric sensors that sense one or more biometric feature (e.g., a fingerprint) of the user, and magnetic stripe emulators. As one result, today's user devices may provide greater security by dynamically generating the necessary information, for example, generating the credit card number at the time of a transaction. Improved security can also be provided by such devices because more sophisticated authentication schemes can be implemented with the devices.

In addition, user devices such as transaction cards may now also provide for one or more modes of information transmission other than transmission via a magnetic stripe/card reader combination. For example, user devices that may transmit information optically or via radio frequency ("RF") signal transmission to a compatible system interface are now available. Further, the architecture of a user device that includes a processor is generally compatible with both the improved security features described above and the contactless transmission modes such as optical and RF signal transmission. As a result of the improved security and greater functionality of some current user devices, there is a desire to replace magnetic-stripe based user devices with devices that include forms of information transmission other than the reading of a magnetic-stripe.

There is, however, a substantial installed base of interfaces (for example, at points of sale, at automatic teller machines ("ATM"), and the like) that include magnetic card readers which are not equipped to receive information from a user device in any other format other than from a magnetic stripe. As a result of the cost to replace or retrofit the installed base, efforts to more-widely introduce user devices that do not employ magnetic stripe devices have not been developed. Because of the potential to

substantially reduce fraud, however, the further implementation of such devices is of great interest to financial institutions among others. RF devices that transmit information wirelessly are expected to become much more prevalent and at some point, the predominant form of information transmission for user authentication based on a hand-held device, for example, credit card, debit card, drivers license, passport, social security card, personal identification, etc. Thus, new and improved methods for transitioning from a purely magnetic based form of communication to a wireless form of communication are desired.

One current approach that is intended to "transform" a smart card for use with a magnetic stripe card reader employs a "bridge" device. The bridge device requires that the smart card be inserted within it. The bridge device includes a slot for receiving the smart card, a key pad whereby the user may enter information (e.g., a PIN number), and a credit card sized extension member. Operation of the bridge device requires that the smart card be inserted within it and that an electrical contact surface of the smart card engage a similar surface within the bridge device before the bridge device (i.e., the extension member) can be used with a magnetic card reader. Thus, the contactless nature of more advanced information transmission systems is lost with the bridge device because it does not support wireless signal transmission.

SUMMARY OF INVENTION

There is thus a need for an identification system that will enable a person to be accurately identified ("identification" sometimes being used hereinafter to mean either identified or verified) and/or authenticated without compromising security, to gain access to secure systems and/or areas. Likewise, there is a need for an identification system that will enable a person to be identified universally without requiring the person to carry multiple forms of identification.

Accordingly, this invention relates, in one embodiment, to an information system that may be used as a universal identification system and/or used to selectively provide information about a person to authorized users. Transactions to and from a secure database may take place using a public key/private key security system to enable users of the system and the system itself to encrypt transaction information during the

transactions. Additionally, the private key/public key security system may be used to allow users to validate their identity. For example, in one embodiment, a smart card such as the Secure ID™ card from RSI Security, Inc. may be provided with the user's private key and the USR system's public key to enable the card to encrypt messages being sent to the USR system and to decrypt messages from the USR system 10.

The system or database of the invention may be used to identify the person in many situations, and thus may take the place of multiple conventional forms of identification. Additionally, the system may enable the user's identity to be confirmed or verified without providing any identifying information about the person to the entity requiring identification. This can be advantageous where the person suspects that providing identifying information may subject the identifying information to usurpation.

Access to the system may be by smart card, such as a Secure ID™ card, or any other secure access device. The technology enabling the user to present their identity information may be physically embodied as a separate identification device such as a smart ID card, or may be incorporated into another electronic device, such as a cell phone, pager, wrist watch, computer, personal digital assistant such as a Palm Pilot™, key fob, or other commonly available electronic device. The identity of the user possessing the identifying device may be verified at the point of use via any combination of a memorized PIN number or code, biometric identification such as a fingerprint, voice print, signature, iris or facial scan, or DNA analysis, or any other method of identifying the person possessing the device. If desired, the identifying device may also be provided with a picture of the person authorized to use the device to enhance security.

According to one embodiment of the invention, a method of controlling access to a plurality of secure computer networks using a secure registry system located remotely from the secure computer networks is disclosed. The secure registry system includes a database containing selected data of a plurality of users each authorized to access at least one of the plurality of secure computer networks. The method comprises acts of receiving authentication information from an entity at a secure computer network, communicating the authentication information to the secure registry system, and validating the authentication information at the secure registry system. The method

also includes receiving from the secure registry system an indication of whether the entity is authorized to access the secure computer network, granting the entity access to the secure computer network when the authentication information of the entity corresponds to one of the plurality of users, and denying the entity access to the secure computer network when the authentication information of the user does not correspond to one of the plurality of users.

Another embodiment of the invention comprises a method of controlling access to a secure computer network using a secure registry system. The secure registry system includes a database containing selected data of a plurality of users authorized to access the secure computer network and selected data identifying the secure computer network. The method comprises receiving an access request including authentication information and a computer network ID from an entity, determining whether the authentication information is valid for any of the plurality of users, accessing data when the authentication information of the entity is valid for one of the plurality of users to determine whether the entity is authorized to access the computer network identified by the computer network ID, and allowing the entity to access the secure computer network when the authentication information of the entity is valid for one of the plurality of users authorized to access the computer network identified by the computer network ID.

Another embodiment of the invention comprises a method of authenticating an identity of a first entity. The method comprises the acts of wirelessly transmitting from a first device, first encrypted authentication information of the first entity, receiving with a second device the wirelessly transmitted first encrypted authentication information, decrypting with the second device, the first wirelessly encrypted authentication information to provide the first authentication information of the first entity to the second device; and authenticating the identity of the first entity based upon the first authentication information; and acting based on the assessed identity of the first entity.

Another embodiment of the invention comprises a system for authenticating an identity of a first entity, comprising a first wireless device comprising a first wireless transmitter and receiver configured to transmit a first wireless signal including first encrypted authentication information, a first processor configured to compare stored

biometric data with detected biometric data of the first entity and configured to enable or disable use of the first device based on a result of the comparison, and configured to encrypt first authentication information with a first private key of the first entity into the first encrypted authentication information, a first biometric detector for detecting biometric data of the first entity, and a first memory for storing biometric data of the first entity, a private key of the first entity authorized to use the first device, and the first authentication information.

According to some embodiments, the system further comprises a second wireless device comprising a second wireless transmitter and receiver configured to receive the first wireless signal and to process the first wireless signal, a second processor configured to compare detected biometric data of a second entity with stored biometric data and configured to enable or disable use of the second device based upon a result of the comparison, and configured to decrypt the first authentication information received in the first wireless signal, a biometric detector for detecting biometric data of a second entity, and a second memory storing biometric data of the second entity and a plurality of public keys of a plurality of first entities.

Another embodiment of the invention provides a first wireless device comprising a processor configured to enable operation of the first wireless device if it receives an enablement signal validating first biometric information of a first entity and configured to generate a non-predictable signal from the biometric information, a first wireless transmitter and receiver configured to transmit a first wireless signal including first encrypted biometric information of the first entity and to receive the enablement signal, and a first biometric detector for detecting the first biometric information of the first entity.

In one aspect of the invention, a device converts a wireless transaction device to a magnetic-stripe emulator device. In one embodiment, the device includes a wireless signal receiver that is configured to receive a wireless signal and provide information from the wireless signal. In addition, the device may include a magnetic-stripe emulator which is communicatively coupled to the wireless signal receiver and adapted to provide a time-varying signal which emulates data provided by a magnetic-stripe card to a magnetic card reader in response to receiving the information from the wireless signal. In one embodiment, the device includes a processor communicatively

coupled to the wireless signal receiver and to the magnetic-stripe emulator. The device may also include an LED. In a version of this embodiment, the processor is configured to control the LED to indicate that the device is properly aligned with the magnetic card reader. In another embodiment, the device includes an output device that can provide information to a network or to a network device. In a version of this embodiment, the output device is a wireless transmitter device.

Further embodiments of the invention may include additional features, for example, in one embodiment the output device is a data port to which the device can provide data to a network or to a network device. In a version of this embodiment, the data port is also configured to receive data from the network or the network's device. In a further embodiment, the device is configured to communicate with the magnetic card reader via the data port.

In a further embodiment, the wireless receiver and/or processors configure, decrypt and encrypt the wireless signal. In a further embodiment, the processor is configured to determine whether a user is authorized to provide the information contained within the wireless signal from data within the wireless signal. In a version of this embodiment, the data contained within the wireless signal includes user ID information. In yet another embodiment, the data contained within the wireless signal includes biometric information of the user.

According to another aspect, the invention provides a system for validating an identity of a user to enable or prevent an occurrence of an event. In one embodiment, the system includes a first device including a wireless transmitter which is configured to transmit validation information, a second device including a wireless receiver, where the second device is configured to receive the validation information and further transmit the validation information; and a secure system in communication with the second device. According to one embodiment, the secure system includes a database. In a further embodiment, the secure system is configured to receive the validation information transmitted from the second device, and to transmit additional information to the second device following a receipt of the validation information to assist the second device in either enabling or preventing the occurrence of the event. In various embodiments, the event that is enabled or prevented may be a transaction (e.g., a

financial transaction), access control (e.g., physical or electronic access) or other action that is either enabled or prevented.

According to a further aspect, the invention provides a method employing a system to validate an identity of a user to enable or prevent an occurrence of an event. In one embodiment, the system includes a first device, a second device and a secure system including a database. According to one embodiment, the method includes acts of receiving at the second device validation information wirelessly transmitted from the first device, communicating the validation information from the second device to the secure system, and receiving at the second device additional information from the secure system. In a further embodiment, the additional information assists the second device in either enabling or preventing the occurrence of the event. In various embodiments, the event that is enabled or prevented may be a transaction (e.g., a financial transaction), access control (e.g., physical or electronic access) or other action that is either enabled or prevented.

BRIEF DESCRIPTION OF DRAWINGS

This invention is pointed out with particularity in the appended claims. The above and further advantages of this invention may be better understood by referring to the following description when taken in conjunction with the accompanying drawings. The accompanying drawings are not intended to be drawn to scale. In the drawings, each identical or nearly identical component that is illustrated in various figures is represented by a like numeral. For purposes of clarity, not every component may be labeled in every thawing. In the drawings:

FIG. 1 is a functional block diagram of a computer system configured to implement the universal secure registry ("USR"), including a USR database, according to one embodiment of the invention;

FIG. 2 is a functional block diagram of a first embodiment of a networked environment including the computer system of FIG. 1;

FIG. 3 is a functional block diagram of an entry of a database forming the USR database of FIG. 1;

FIG. 4 is a functional block diagram of a second embodiment of a networked environment including the computer system of FIG. 1;

FIG. 5 is a flow chart illustrating steps in a process of inputting data into the USR database;

FIG. 6 is a flow chart illustrating steps in a process of retrieving data from the USR database;

FIG. 7 is a flow chart illustrating a first protocol for purchasing goods from a merchant via the USR database without transmitting credit card information to the merchant;

FIG. 8 is a flow chart illustrating a second protocol for purchasing goods from a merchant via the USR database without transmitting credit card information to the merchant;

FIG. 9 is a flow chart illustrating a protocol for purchasing goods from a merchant via the USR database by validating the user's check;

FIG. 10 is a flow chart illustrating a protocol for purchasing goods from an on-line merchant via the USR database without transmitting credit card information to the on-line merchant, and enabling the on-line merchant to ship the goods to a virtual address;

FIG. 11 is a flow chart illustrating a protocol for shipping goods to a virtual address via the USR database;

FIG. 12 is a flow chart illustrating a protocol for telephoning a virtual phone number via the USR database;

FIG. 13 is a flow chart illustrating a protocol for identifying a person via the USR database;

FIG. 14 is a flow chart illustrating a protocol for identifying a person to a policeman via the USR database;

FIG. 15 is a flow chart illustrating a protocol for providing information to an authorized recipient of the information via the USR database;

FIG. 16 is a flow chart illustrating a protocol for providing application information to an authorized recipient of the information via the USR database;

FIG. 17 is a functional block diagram of an embodiment configured to use information in the USR system to activate or keep active property secured through the USR system; and

FIG. 18A is a functional block diagram of an embodiment configured to use the USR system to control access to a secure computer network;

FIG. 18B is a functional block diagram of another embodiment configured to use the USR system to control access to a secure computer network;

FIG. 19 is a flow diagram of a process for controlling access to a secure computer network with the USR system in accordance with an embodiment of the invention;

FIG. 20 is a flow diagram of a process for controlling access to a secure computer network with the USR system in accordance with another embodiment of the invention;

FIG. 21 illustrates an embodiment of a system for validating the identity of an individual;

FIGS. 22A and 22B illustrate one embodiment of a process for validating the identity of an individual;

FIG. 23 illustrates one embodiment of various fields included within a first wireless signal and a second wireless signal as transmitted by the system of FIG. 21;

FIG. 24 illustrates one embodiment of a process for verifying or authenticating the identity of a first user of a first wireless transmission device;

FIG. 25 illustrates another embodiment of a process for authenticating the identity of a first user of a wireless transmission device;

FIG. 26 illustrates still another embodiment of a process for authenticating the identity of a first user of a wireless transmission device; and

FIG. 27 illustrates one embodiment of a data structure that can be used by any wireless device of the system of FIG. 21;

FIG. 28 illustrates a system in accordance with one embodiment of the invention;

FIG. 29 illustrates a process in accordance with an embodiment of the invention; and

FIGS. 30A-30D illustrate a converter device in accordance with one embodiment of the invention.

DETAILED DESCRIPTION

This invention is not limited in its application to the details of construction and the arrangement of components set forth in the following description or illustrated in the drawings. The invention is capable of other embodiments and of being practiced or of being carried out in various ways. Also, the phraseology and terminology used herein is for the purpose of description and should not be regarded as limiting. The use of "including," "comprising," or "having," "containing", "involving", and variations thereof herein, is meant to encompass the items listed thereafter and equivalents thereof as well as additional items.

In one embodiment, an information system is formed as a computer program running on a computer or group of computers configured to provide a universal secure registry (USR) system. The computer, in this instance, may be configured to run autonomously (without the intervention of a human operator), or may require intervention or approval for all, a selected subset, or particular classes of transactions. The invention is not limited to the disclosed embodiments, and may take on many different forms depending on the particular requirements of the information system, the type of information being exchanged, and the type of computer equipment employed. An information system according to this invention, may optionally, but need not necessarily, perform functions additional to those described herein, and the invention is not limited to a computer system performing solely the described functions.

In the embodiment shown in FIG. 1, a computer system 10 for implementing a USR system according to the invention includes at least one main unit 12 connected to a wide area network, such as the Internet, via a communications port 14. The main unit 12 may include one or more processors (CPU 16) running USR software 18 configured to implement the USR system functionality discussed in greater detail below. The CPU 16 may be connected to a memory system including one or more memory devices, such as a random access memory system RAM 20, a read only memory system ROM 22, and one or more databases 24. In the illustrated embodiment, the database 24 contains a universal secure registry database. The invention is not limited to this particular manner of storing the USR database. Rather, the USR database may be included in any aspect of the memory system, such as in RAM 20, ROM 22 or disc, and may also be separately stored on one or more dedicated data servers.

The computer system may be a general purpose computer system which is programmable using a computer programming language, such as C, C++, Java, or other language, such as a scripting language or even assembly language. The computer system may also be specially programmed, special purpose hardware, an application specific integrated circuit (ASIC) or a hybrid system including both special purpose components and programmed general purpose components.

In a general purpose computer system, the processor is typically a commercially available microprocessor, such as Pentium series processor available from Intel, or other similar commercially available device. Such a microprocessor executes a program called an operating system, such as UNIX, Linux, Windows NT, Windows 95, 98, or 2000, or any other commercially available operating system, which controls the execution of other computer programs and provides scheduling, debugging, input/output control, accounting, compilation, storage assignment, data management, memory management, communication control and related services, and many other functions. The processor and operating system defines a computer platform for which application programs in high-level programming languages are written.

The database 24 may be any kind of database, including a relational database, object-oriented database, unstructured database, or other database. Example relational databases include Oracle 81 from Oracle Corporation of Redwood City, California; Informix Dynamic Server from Informix Software, Inc. of Menlo Park, California; DB2 from International Business Machines of Armonk, New York; and Access from Microsoft Corporation of Redmond, Washington. An example object-oriented database is ObjectStore from Object Design of Burlington, Massachusetts. An example of an unstructured database is Notes from the Lotus Corporation, of Cambridge, Massachusetts. A database also may be constructed using a flat file system, for example by using files with character-delimited fields, such as in early versions of dBASE, now known as Visual dBASE from Inprise Corp. of Scotts Valley, California, formerly Borland International Corp.

The main unit 12 may optionally include or be connected to an user interface 26 containing, for example, one or more input and output devices to enable an operator to interface with the USR system 10. Illustrative input devices include a keyboard, keypad, track ball, mouse, pen and tablet, communication device, and data input

devices such as voice and other audio and video capture devices. Illustrative output devices include cathode ray tube (CRT) displays, liquid crystal displays (LCD) and other video output devices, printers, communication devices such as modems, storage devices such as a disk or tape, and audio or video output devices. Optionally, the user interface 26 may be omitted, in which case the operator may communicate with the USR system 10 in a networked fashion via the communication port 14. It should be understood that the invention is not limited to any particular manner of interfacing an operator with the USR system.

It also should be understood that the invention is not limited to a particular computer platform, particular processor, or particular high-level programming language. Additionally, the computer system may be a multiprocessor computer system or may include multiple computers connected over a computer network. It further should be understood that each module or step shown in the accompanying figures and the substeps or subparts shown in the remaining figures may correspond to separate modules of a computer program, or may be separate computer programs. Such modules may be operable on separate computers. The data produced by these components may be stored in a memory system or transmitted between computer systems.

Such a system may be implemented in software, hardware, or firmware, or any combination thereof. The various elements of the information system disclosed herein, either individually or in combination, may be implemented as a computer program product, such as USR software 18, tangibly embodied in a machine-readable storage device for execution by the computer processor 16. Various steps of the process may be performed by the computer processor 16 executing the program 18 tangibly embodied on a computer-readable medium to perform functions by operating on input and generating output. Computer programming languages suitable for implementing such a system include procedural programming languages, object-oriented programming languages, and combinations of the two.

As shown in FIG. 2, the computer system 10 may be connected to a plurality of interface centers 27 over a wide area network 28. The wide area network 28 may be formed from a plurality of dedicated connections between the interface centers 27 and the computer system 10, or may take place, in whole or in part, over a public network

such as the Internet. Communication between the interface centers 27 and the computer system 10 may take place according to any protocol, such as TCP/IP, ftp, OFX, or XML, and may include any desired level of interaction between the interface centers 27 and the computer system 10. To enhance security, especially where communication takes place over a publicly accessible network such as the Internet, communications facilitating or relating to transmission of data from/to the USR database 24 or the computer system 10 may be encrypted using an encryption algorithm, such as PGP, DES, or other conventional symmetric or asymmetric encryption algorithm.

In one embodiment, the USR system 10 or USR database 24 may be able to authenticate its identity to a user or other entity accessing the system by providing an appropriate code which may be displayed on the user's smart card, for example a SecurID™ card or its equivalent, or other code generator, for example a single use code generator, being employed by the user. A comparison by the user or the code generator between the provided number and an expected number can validate, to the user (or other entity) or the code generator, that communication is with the database and not an imposter. In another embodiment, a challenge-response protocol is employed to authenticate the identity of the USR system and/or the user to the other.

The database 24 shown in FIG. 1 has a USR database containing entries related to persons 1-n. The data in the USR database may also be segregated, as shown in FIG. 4, according to data type to enable individual computer modules to handle discrete applications on discrete data types. Segregating the data, as illustrated in FIG. 4, may make access to the database more robust by enabling portions of the data in the USR database 24 to be accessible even when it is necessary to perform maintenance on a portion of the database. However, storing the data in the USR database 24 according to the scheme illustrated in FIG. 1 may make it easier for a user of the database to make changes to multiple types of data simultaneously or in a single session. There are advantages and disadvantages to each data structure, and the invention is not limited to a particular manner of organizing the data within the database 24, data structures other than the two shown also being possible.

As shown in FIG. 3, each entry 30 in the database 24 may contain multiple types of information. For example, in the embodiment shown in FIG. 3, the entry

contains validation information 32, access information 34, publicly available information 36, address information 38, credit card and other financial information 40, medical information 42, job application information 44, and tax information 46. The invention is not limited to a USR containing entries with all of this information or only this particular information, as any information on a person or other entity such as a company, institution, etc. may be stored in USR database 24.

If the database information is split between multiple databases, each database will typically include at least the validation and access information to enable the USR software to correlate a validation attempt with a verified validation, and to enable the USR software to determine access privileges to the requested data. Alternatively, databases may be linked to permit information not in a main USR database to be retrieved, with validation/identification for all databases accessed being done at the USR system.

In FIG. 3, the validation information is information about the user of the database to whom the data pertains and is to be used by the USR software 18 to validate that the person attempting to access the information is the person to whom the data pertains or is otherwise authorized to receive it. The validation information may be any type of information that will reliably authenticate the identity of the individual. For example, in some embodiments, the information may include any of a secret known by the user (e.g., a pin, a phrase, a password, etc.), a token possessed by the user that is difficult to counterfeit (e.g., a secure discrete microchip), and/or a measurement such as a biometric (e.g., a voiceprint, a fingerprint, DNA, a retinal image, a photograph, etc.).

The user's identifying information may be manually entered or scanned at the interface center. However, a variety of types of communication may be employed to communicate the user's identifying information from the identification card or token to the computer system. For example, near field signal may be employed to communicate information between the identification card or token and the computer system 10. According to one embodiment, the user's identifying information is included in (or entered via) the user's cell phone where it is then communicated to the computer system 10. In one embodiment, the cell phone is also configured to receive information from the computer system 10 at the interface center 27.

In one embodiment, the user of the database will carry a SecurID™ card available from RSA Security, formerly Security Dynamics Technologies, Inc., of Cambridge, MA. Use of this card enables secure access to the USR database without requiring the user to transmit any personal information. Specifically, to access the USR database, the card retrieves a secret user code and/or time varying value from memory and obtains from the user a secret personal identification code. The card mathematically combines these three numbers using a predetermined algorithm to generate a one-time nonpredictable code which is transmitted to the computer system 10. The computer system, specifically USR software 18, utilizes the received one-time nonpredictable code to determine if the user is authorized access to the USR database and grants access to the USR database if the user is determined to be authorized. The verification information 32 in the database entry in the embodiment of the invention illustrated in FIG. 3 contains information to enable the USR software 18 to validate the user using such a card in this manner.

Alternative types of identification cards or tokens may likewise be used. For example, other smart cards may be used which generate non-predictable single use codes, which may or may not be time varying, or other access code generators may be used. An algorithm generating such non-predictable codes may also be programmed onto a processor on a smart card or other computing device, such as a cell phone, pager, ID badge, wrist watch, computer, personal digital assistant, key fob, or other commonly available electronic device. For convenience, the term "electronic ID device" will be used generically to refer to any type of electronic device that may be used to obtain access to the USR database.

Likewise, various types of biometric information may be stored in the verification area of the database entry to enable the identity of the user possessing the identifying device to be verified at the point of use. Examples of the type of biometric information that may be used in this situation includes a personal identification number (PIN), fingerprint, voice print, signature, iris or facial scan, or DNA analysis. If desired, the verifying section of the database may contain a picture to be transmitted back to the person seeking to validate the device to ensure the person using the device is the correct person. Optionally, the identifying device itself may also be provided

with a picture of the person authorized to use the card to provide a facial confirmation of the person's right to use the card.

Further, a challenge-response protocol may be employed in combination with or as an alternative to the preceding to validate the person attempting to access the information. Various embodiments may employ a challenge-response protocol with or without an identification card.

In FIG. 3, the Access information 34 is provided to enable different levels of security to attach to different types of information stored in the entry 30 in the USR database 14. For example, the person may desire that their address information be made available only to certain classes of people, for example colleagues, friends, family, Federal Express, U.P.S., and the U.S. mail service. The names or universal identifiers for those selected individuals, companies, organizations and/or agencies may be entered into appropriate fields in the Access information to specify to the USR software 18 those individuals to whom the address information may be released. Likewise, access fields may be specified for the other types of information. For example, the individual may specify that only particular individuals and/or companies have access to the credit card and other financial information 40, medical information 42, job application information 44 and tax information 46. Additionally, the individual may specify that no one have access to that information unless the individual participates in the transaction (see FIG. 6).

As shown in FIG. 1, the USR software 18 contains algorithms for execution by the CPU 16 that enables the CPU 16 to perform the methods and functions of the USR software described below in connection with Figs. 5-16. The USR software 18, in this embodiment, performs all functions associated with validating an electronic ID card. If desired, a separate validation software module may be provided to validate electronic ID devices outside of a firewall segregating the validation information from other user information.

This algorithm comprising the USR software 18 may be used to implement, in one exemplary embodiment, a USR system configured to enable selected information to be disseminated to selected individuals in a secure and dynamic fashion. This information may be used for numerous purposes, several of which are set forth below and discussed in greater detail in connection with Figs. 5-16.

For example, the USR system may be used to identify the person, enable the person to be contacted by telephone or mail anonymously, enable the person to be contacted by telephone or by mail without revealing the person's telephone number or present location, enable the person to purchase items over the Internet or in a store without revealing to the merchant any personal identification information or credit card information, enable the person to complete a job application without completing a job application form, enable the police to discern the person's identity and any outstanding warrants on the individual, and numerous other uses. The invention is not limited to these several enumerated uses, but rather extends to any use of the USR database. The methods of using the USR database 24 will now be discussed in connection with Figs. 5-16.

FIG. 5 illustrates a method of training the USR database 24. As shown in FIG. 5, the USR software 18 first validates the person's identification (500). The initial validation of the person's identification (500) may take place at the point of sale of an electronic ID device (for example, a smart card). This may be done in any conventional manner, such as by requiring the person to show a government issued identification card, passport, birth certificate, etc. Once the person's electronic ID device has been issued and initially validated, the validation process proceeds as discussed above.

After the validation process (500), the USR software 18 determines if the person has rights to enter data into the system (502). This step enables the system to charge persons for maintaining information in the USR database 24. For example, the USR software 18 may poll a database of current accounts or a database of accounts that are currently in default to determine if the person has paid the access fee to enter data into the database. A similar account status inquiry process may be performed by the USR software 18 in connection with each of the other methods set forth in Figs. 6-16. If the person is not authorized to enter data into the USR database 24, the person is notified of the status of their account and the process returns (512) to wait for further input from another person. Alternatively, a person may be permitted to enter some classes of data into the system and update such classes of data at no charge, with a fee possibly being required for other classes of data, for example medical records. This would facilitate a more robust database.

If the person is authorized, the USR software 18 then enables the person to enter basic personal data into the USR database 24 (504). Optionally, personal data may be one class of data the USR software 18 allows the person to enter into the USR database 18 regardless of account status, i.e., for free.

The USR software 18 will then check to see if the person has additional rights to enter additional data (506), such as data to be entered into one of the other categories of data in FIG. 3. Optionally, this step of checking the person's rights to enter data (506) may be combined with the initial check (502). If the person does not have rights to enter any further data, the USR software 18 notifies the user and returns (512).

If the USR software 18 determines that the person has the right to enter additional data into the USR database 24, the person is prompted through the use of appropriate prompts, provided with forms, and otherwise enabled to enter advanced personal data into the USR database 24 (508). For each type of data entered, the person is asked to specify the type of access restrictions and/or whom should be allowed to access the advanced personal data (510). When the person has completed entering data into the database, the process returns (512) and commits the data to the database.

In the situation where only one person has access to enter and/or modify data for a given person in the database, there should be no conflict with committing data to the database. If, however, multiple people have access to a given account to modify data, the database may perform an integrity check to ensure the absence of conflict in the data before committing the new data to the database.

Enabling access to the information in the database will be explained in greater detail in connection with FIG. 6. As shown in FIG. 6, the database will generally allow anyone to access basic personal data on anyone without performing any authorization check (600).

If information beyond that specified in the basic personal information area is requested, the USR software 18 queries whether the requestor has the right to access the type of requested data (602). The process of determining the requestor's rights (602) typically involves validating the requestor's identity and correlating the identity, the requested information and the access information 34 provided by the person to the USR database during the training process described above with respect to FIG. 5.

If the USR software 18 determines that the requestor has rights to access the type of requested data (604), the USR software 18 instructs the USR database 24 to enable access to the type of requested data (606). The actual step of enabling access to the type of requested data may involve multiple steps of formulating a database query, querying the USR database 24, retrieving the results, assembling the results into a user friendly or user readable format, and transmitting the information to the user.

If the USR software 18 determines that the requestor does not have the appropriate rights to access the type of requested data (604), the USR software 18 checks to see if the person is participating in the transaction (608). Checking to see if the person is participating in the transaction enables the user to authorize access to the requested data in real time. For example, a person may wish to participate in a transaction to give a potential employer one-time access to job application information 44 (see FIG. 3). If the person is not participating in the transaction, the USR software 18 determines that the requestor is not authorized to have access to the requested data, notifies the requestor of this determination, and ends (610).

If the person is participating in the transaction (608), however, the USR software 18 validates the person's identity (612) and enables the person to change access rights to the data (614). If the USR software 18 is not able to validate the person's identity, the USR software 18 refuses to allow the person to update the database, notifies the person and/or requestor of this determination, and returns (610).

It is also possible that a person may be required to grant access to certain data, for example financial data such as account numbers, under duress. The system may provide the person with the ability to safely signal this when accessing the system by using a selected access code or by making a known modification to the access code provided by the electronic ID device. On receiving such code, the system would take appropriate steps to protect the person, including for example alerting the police, tracking the person's location to the extent possible, providing traceable data, and the like.

Once the person has had the opportunity to change access rights to the data (614), the USR software 18 again checks to see if the requestor has rights to access the type of requested data (616). Although step 616 may seem redundant, given the fact that the person is participating in the transaction and has just previously changed access

rights to the database to enable the requestor to have access to the data, step 616 is actually useful at preventing a different type of fraud. Specifically, the requestor may not be forthright with the person regarding the type of information they are requesting. If step 616 were omitted, the USR software 18 may inadvertently allow access to an unauthorized type of information in the situation where the requestor has surreptitiously requested multiple types of data.

If the USR software 18 determines that the requestor has rights to the type of data requested (616), it causes the USR database to enable access to the type of requested data (606). Otherwise, it notifies the requestor of the decision to deny access to the requested data and returns (610).

Various applications of the USR database 24 and USR software 18 will now be discussed in connection with Figs. 7-16. These applications are merely exemplary of the types of applications enabled by the USR software 18 and USR database 24, and the invention is not limited to these particular applications.

Figure 7 illustrates one embodiment of a method of using the USR software 18 and USR database 24 to purchase goods or services from a merchant without revealing to the merchant account information relating to the person's bank or credit card.

As shown in FIG. 7, when a user initiates a purchase (700), the user enters a secret code in the user's electronic ID device (702) to cause the ID device to generate a onetime code or other appropriate code, and presents the electronic ID device with the code to the merchant or otherwise presents the code to the merchant. The merchant transmits to the credit card company (1) the code from the electronic ID device, (2) the store number, (3) the amount of the purchase (704), and the time of receipt of the code. The credit card company takes this information and passes the code from the electronic ID device to the USR software 18 (706). The USR software 18 determines if the code is valid, or was valid at the time offered, and if valid accesses the user's credit card information and transmits the appropriate credit card number to the credit card company (708). While the link between the USR system and the credit card system is a secure link, there is always a danger that the link may be penetrated and credit card numbers obtained. This may be avoided by instead transmitting, on approval, a multidigit public ID code for the credit card holder which the credit card company can map to the correct credit card number. Even if the link is violated, the public ID code is

of no value and the secure link prevents this code from being improperly sent to the credit card company. The credit card company checks the credit worthiness of the user and declines the card or debits the user's account in accordance with its standard transaction processing system (710). The credit card company then notifies the merchant of the result of the transaction (712). In this embodiment, the user has been able to purchase goods or services from a merchant without ever providing to the merchant the credit card number. Since the electronic ID device generates a time variant code or otherwise generates a code that can for example only be used for a single transaction, the merchant retains no information from the transaction that may be fraudulently used in subsequent transactions.

Another embodiment of a system for facilitating purchase of goods or services without providing financial information to the merchant is set forth in FIG. 8. In FIG. 8, like FIG. 7, the user initiates a purchase (800), enters a secret code in the electronic ID device (802) and presents the resultant code to the merchant. The merchant, in this embodiment, transmits to the USR software 18, (1) the code from the electronic ID, (2) the store number, and (3) the amount of the purchase (804). The USR software 18 determines if the code is valid (806) and, if valid, accesses from the USR database 24 the user's credit card information (808). The USR software then transmits to the credit card company (1) the credit card number, (2) the store number, and (3) the amount of purchase (808). The information in this embodiment transmitted to the credit card company is intended to be in a format recognizable to the credit card company. Accordingly, the invention is not limited to transferring from the USR system 10 to the credit card company the enumerated information, but rather encompasses any transfer of information that will enable the use of the USR system 10 to appear transparent to the credit card company.

The credit card company then processes the transaction in a standard fashion, such as by checking the credit worthiness of the person, declining the card or debiting the user's account and transferring money to the merchant's account (810). The credit card company then notifies the USR system 10 the result of the transaction (812) and the USR software 18 in turn notifies the merchant of the result of the transaction (814).

In this embodiment, like the embodiment of FIG. 7, the user can use the USR system 10 to purchase goods or services from a merchant without providing the

merchant with the user's credit card number. In the embodiment of FIG. 8, the interposition of the USR system 10 between the merchant and the credit card company is transparent to the credit card company and thus requires no or minimal cooperation from the credit card company to implement.

FIG. 9 illustrates one embodiment of a method of using the USR system 10 to verify funds when using a check to purchase goods or services from a merchant. In the embodiment of FIG. 9, the user initiates a purchase and writes a check to the merchant (900). The check may be a conventional check containing identifying information, or may be a check bearing a unique serial number and no identifying information to enable the check to be used anonymously.

In either situation, the user enters a secret code into the electronic ID card and presents the resulting code to the merchant along with the check (902). The merchant transmits to the USR software 18 (1) the code from the electronic ID card, (2) the store number, and (3) the amount of the purchase (904). Where the check is an anonymous check, the merchant also transmits to the USR software 18 the check number.

The USR software 18 then determines if the code from the electronic ID is valid (906), and if valid accesses the user's bank information and transmits to the bank: (1) the user's bank account number, (2) the store number, and (3) the amount of the purchase (908). Optionally, the USR software 18 may additionally inform the bank of the check number.

The bank polls its own database to determine if there are sufficient funds in the user's account (910) and notifies the USR software 18 of the result (912). The USR software 18 then, in turn, notifies the merchant of the result of the verification (914).

This check verification system may take place over an unsecured connection between the merchant and the USR system 10 since the user's bank account information is not sent over the connection between the merchant and the USR system 10. Moreover, where an anonymous check is used, the merchant is not even provided with the person's name or account information in written form. This provides additional security against unauthorized persons writing subsequent checks.

The check verification system may be conducted over a telephone network, such as by having the merchant call a toll free number or over a network connection such as over the Internet.

FIG. 10 illustrates a method of conducting a transaction with a merchant without requiring the user to provide to the merchant the user's name, address, or other identifying information, while enabling the merchant to ship the goods to the user. This may be beneficially employed, for example, in connection with transactions that take place between remote parties in a networked environment, such as the Internet.

As shown in FIG. 10, the user initiates an anonymous purchase by entering a secret code into the electronic ID device and transmitting the result to the on-line merchant (1000). The merchant transmits this information to the USR software 18, along with the store number and the amount of the purchase (1002). Optionally, the merchant may provide the store number and purchase price to the user and the user may send this information directly to the USR software 18 along with the code from the electronic ID. Where the number from the electronic ID device is a time varying number, the merchant may also need to input the time the number was received. Alternatively, the electronic ID device may encode or encrypt the time with the number, the USR software being able to extract time when receiving the number from the merchant. This may not be required where the time varying number varies slowly, for example changing every hour rather then every minute as for some existing such devices.

In either event, the USR software 18 determines if the code is valid (1004) and, if valid, accesses the user's credit card information from the USR database 24 (1006). The USR software 18 then contacts the user's credit card company, as described above in connection with FIG. 8 (1008) and notifies the USR software 18 of the result (1010).

If the user's credit is declined, the USR software 18 notifies the on-line merchant and the transaction is terminated (1012). If the user's credit is honored, the USR software 18 polls the USR database 24 for the user's address and/or address code (1014). Address codes are discussed below in greater detail with reference to FIG. 11. The merchant then packages the goods into a parcel, labels the parcel with the appropriate address and/or address code and ships the parcel to the user (1016). Having the USR system 10 provide the address and/or address code to the on-line merchant enables the user to purchase items in a networked environment without requiring the user to input address information in connection with every sale.

RECTIFIED SHEET (RULE 91)
ISA/EP

FIG. 11 illustrates a use of the USR database 24 to deliver mail to a user without requiring the user to provide address information to the sender. This may be useful in many contexts. For example, the user may wish that the address information be known only by the post office. In this instance, using the USR database 24 according to the method of the invention described below, will enable the user to receive parcels without requiring the user to provide the merchant with the address information. Additionally, the user's address may change, temporarily, permanently, or frequently. Enabling the sender to send mail by entering a code instead of an address enables the post office to effectively deliver the coded mail to the corresponding address regardless of the frequency with which the address changes or the duration in which the address will remain valid.

In FIG. 11, the user provides an address code on a public area of the USR database 24 that is available to all persons to see (1100). This code may for example be six alpha characters, which should be adequate for currently anticipated system populations. Optionally, the user may provide this code directly to a merchant or other person desirous of sending the person one or more parcels.

The user also provides address information to the address information area 38 of the user's entry in the USR database 24 (1102). Access to the address information 38 is restricted by a rule or other appropriate entry in the access information 34 of the user's entry to only permit mail, parcel or other material delivery services, such as the US mail, UPS and Fed Ex to access the address information.

When someone wishes to have a parcel or other items delivered to the user, the sender retrieves the user's address code from the USR database 24 or otherwise receives the address code from the user, and prints the address code on the parcel (1104).

The delivery service accesses the USR software 18, validates its identity, and queries the USR database 24 for address information corresponding to the address code (1106). The USR database 24 retrieves the appropriate address data and provides the address information to the delivery service. The delivery service then either prints out an address label, prints a machine readable bar code to be attached to the package, or correlates an entry in a delivery database between the address code and the user address (1110). The delivery service then uses this retrieved information to deliver the package

to the user while never supplying the merchant with the user's permanent or temporary address. A user may also assure that mail, parcels, etc. are delivered to a current location by providing only a single notice to the USR system, regardless of how frequently the person moves. The person can also automatically provide for address changes where the person moves according to a known schedule. Thus, deliveries to be made on a weekday could be directed to one address and deliveries on a weekend to another address; or deliveries during winter months to one address and during summer months to a different address.

FIG. 12 illustrates a method of enabling a person to telephone a user of the USR system 10 without providing the user's telephone number to the person. In the embodiment illustrated in FIG. 12, the user provides a telephone code on the publicly available area of his entry on the USR database 24 (1200). This code may be assigned by the USR software 18 or made up by the user. The user also provides the USR database 24 with actual telephone information to enable the USR system 10 to connect callers with the user (1202).

The person wishing to telephone the user of the USR system 10 calls a telephone number and enters the telephone code of the user (1204). The USR software 18, optionally, may require the person to identify themselves to see if they are authorized to call the user. Assuming that the person is authorized to call the person, or if no authorization check is performed, the USR connects the person to the telephone number in the USR database 24 without providing the person with the telephone number.

Enabling the user to specify the telephone number may be advantageous for many reasons. First, the user may frequently be switching between telephone coverage areas and may wish to be reachable at all times. Simply by instructing the USR database 24 to connect incoming telephone calls to one of a myriad of numbers will facilitate connecting the incoming calls to, for example, the user's cell phone, work phone, pager, car phone or home phone, without necessitating the user to provide all these numbers to the caller. A similar system may be implemented for facsimile transmissions, e-mails or other communications.

The user also may have predefined rules to enable telephone calls to follow a set pattern. For example, the user may desire to receive telephone calls only from family

members during the night time at home, may wish to have all incoming calls routed to a car phone during commuting hours, and may wish to have all incoming calls routed to a cell phone during lunch. These time dependent rules may and/or caller specific rules may be entered into the USR database to specify accessibility and connectivity of incoming telephone calls.

The publicly available address code and telephone code and any other codes may be the same, or may be different, there being some advantages to having a single code usable for all such applications for each person on the system. The codes could be accessible through a variety of media including telephone and the Internet. Where two or more people on the system have the same name, which will frequently be the case, additional publicly available biographical data may be provided with the name to assure that the right code is selected. The system may similarly be used to provide public keys for use in a public key/private key encryption system, to provide other public codes for an individual or to provide other public information. Access to such information would typically be unrestricted.

Where the system is used to provide public keys, the public code used to obtain the key, or possibly the public key itself, may be used as above to obtain the e-mail address, telephone number or the like for the person to whom the message is being sent, and the USR system may also be used to perform the encryption. When the recipient receives the message, he deencrypts it using the recipient's private key in standard fashion, including deencrypting the name of the sender. However, this does not necessarily verify the sender and such verification may be desirable for important messages, particularly ones involving large financial transactions. The USR system may accomplish such verification by also storing private keys for people in the system. The sender first authenticates himself to the system, and the system then adds a second signature to the message which is encrypted with the sender's private key. The receiving party deencrypts this signature with the sender's public key. Since the system only sends such signatures for authenticated users, the message is thus verified.

FIG. 13 illustrates a general method of using the USR database 24 to authenticate a user's identification. This may be used in connection with any of the other methods disclosed herein to ensure that the electronic ID device has not been stolen and/or hacked by an unauthorized holder.

Specifically, in the embodiment illustrated in FIG. 13, the user attempts to prove identification to a validator, such as to prove that the possessor of the electronic ID device is of sufficient age to purchase alcohol (1300). In connection with this attempt, the user enters a secret code into the electronic ID (1302). The validator transmits to the USR software 18 the code from the electronic ID (1304). If the USR software 18 determines that the code is valid (1306), it accesses the user's photograph, age information, or any other desired information, and transmits that information to the validator (1308). By transmitting back to the validator a picture of the person to whom the electronic ID card was issued, the validator can ensure that the person using the electronic ID card is the proper person. Likewise, the validator can ensure, based on the information provided by the USR system 10, that the person is as old as the person claims to be.

A specific embodiment of this identification validation procedure is illustrated in FIG. 14. In FIG. 14, a policeman takes the place of the validator. In this scenario, however, instead of simply transmitting to the policeman a validation of the user's identity, such as their picture, the policeman may also receive additional information, such as the user's police records, records of any arrests, outstanding warrants, and other similar information that may be of use to the policeman when determining how to handle a particular individual.

FIG. 15 illustrates a process for enabling the user to provide specific information to a party, such as medical staff in an emergency room. As shown in FIG. 15, if the user desires to provide information to a party (1500), the user enters a secret code in the electronic ID device and provides the electronic ID code to the party (1502). The party transmits to the USR software 18 the ID code and the party code (1504). The party code may be a code from for example an electronic device which identifies the party, may be a status code which identifies the class of users to which the party belongs, for example policeman, emergency room personnel, doctor, etc. or may be a combination of both, the status code for example being encrypted into the ID code. The USR software 18 determines if the code is valid (1506), accesses the user's information in the USR database 24 and transmits available information to the party (1508). In this scenario, the user may be provided with a plurality of different codes to enter into the electronic ID device depending on the type of information to be released

to the party. For example, the user's basic code may be 1234. The fifth digit of the electronic code may specify the type of information to be provided, i.e., 1 = address information, 2 = medical information; 3 = telephone information, 4 = job application information, etc. Using multiple codes eliminates any ambiguity about the authority provided by the user to the party, but requires the user to remember additional information.

The above assumes the user is able to provide an ID code when the information is required. However, in for example an emergency room situation, the user may not be in a position to provide the ID code, but would still want medical records provided. The release authorization for certain portions of the user's database could therefore specify that the information be released to certain class or classes of individuals and the USR system would release such information to individuals or organizations based only on status code. Thus, the status code of an emergency room could alone trigger release of medical data.

FIG. 16 illustrates one embodiment of a method of using the USR database 24 to complete a standard application, such as a job application or an application to rent an apartment. This embodiment is a specific example of the more generic method of enabling a party to retrieve information discussed above with respect to FIG. 15. In FIG. 16, however, the party may be provided with the opportunity to provide a form to the USR software 18, the fields of which may be automatically completed with information from the job application information section of the USR database 24.

As can be seen from the above, many of the users of the USR system are organizations or agencies such as carriers (post office, UPS, FedEx), communication companies, law enforcement organizations, hospitals and other medical facilities and the like. Each of these organizations can be provided with specialized software either on a disc or other suitable media or electronically, for example over the Internet, which performs a number of functions, for example automatically generating status codes for data access requests, controlling information received, and formatting data received in response to a request in a desired way. This can result in an access request from such organization for a given user causing all data on the user required to complete the form being retrieved and presented to the organization in the format of their form. A user may also authorize an organization for which a form has been completed using the USR

system to receive updates, either in response to a request from the organization or at selected intervals, for example once a year, so as to maintain information in the forms current. Since the user will be providing information to the system on a regular basis, this is a relatively easy and painless way for the user to maintain current information with many organizations the user deals with.

Another potential use of the system is to permit a person to be located where only limited biographical information on the person is known. Users of the USR system wishing to participate in this feature could be cued to provide non-confidential biographical data when they come on the system or at any time thereafter when they decide to participate. They can also indicate whether they wish their name given out in response to such an inquiry or to merely be alerted to an inquiry which might involve them and information on the requester. A person seeking to find another person or group of people can input appropriate biographical data, for example members of 1975 Harvard University hockey team, or information of a person's last known address plus school information, etc. The system will then provide a list of persons who meet the listed criteria from which the person making the inquiry can hopefully find the person they are looking for.

In the above application and others, when a person is located, the person may request that only the person's address code or general access code (i.e. a single code which is used to get current address, telephone, e-mail, etc. information) be provided when the person is located. This can further protect the individual from undesired contacts.

Further, although each of FIGS. 13-16 refer to the entry of a secret code for validation by the USR system, the processes illustrated for each of FIGS. 13-16 may include a challenge-response protocol by which the user's identity is authenticated.

FIG. 17 illustrates another embodiment of the invention. As shown in FIG. 17, the USR system 10 may be used to secure expensive personal equipment, such as stereos, televisions, laptop computers, cellular telephones, cars, boats, and other items of value to a person. In this embodiment, each item to be secured using the USR system is provided with a USR timer chip imbedded in the electronics. If the USR timer chip is not provided with a code within a predefined period of time, for example every 30 days, the equipment is deactivated. Thus, for example, a television, mobile

phone, laptop computer, automobile, heavy equipment, weapon or facility may be provided with a security chip having an internal timer that must be reset before expiration by provision of a particular code. When reset does not occur, the timer will disable the electronic device or other device using any one of a number of known disablement methods. Exemplary codes may be transmitted in the same manner as beeper signals are conventionally transmitted or may be transmitted to wired devices over the Internet or other public network.

The USR system 10 may be advantageously employed to automatically provide the secured property with the necessary codes at appropriate intervals, unless instructed by the user of the USR system 10 to cease doing so. Alternatively, the USR system 10 may require participation by the user prior to sending out the activation codes.

In this embodiment, the user may provide to the USR system 10, information indicative of the codes to be transmitted, timing information, and automation information -- i.e., whether the codes should be sent automatically or should require user intervention. Optionally, where the user opts to require user intervention, the USR system 10 may notify the user of the upcoming deadline via e-mail or another method.

This system may be useful to secure sensitive equipment other than personal equipment as well, such as military equipment, public equipment, school equipment and any other equipment that is subject to theft.

FIG. 18A illustrates another embodiment of the invention that can provide a centralized system to control access to a plurality of secure networks. As shown in FIG. 18A, for example, a system 1800 may employ the USR 10 to control access to a plurality of secure systems 1804 (e.g., a plurality of secure computer networks). The system 1800 may include one or more access devices 1802 that can be employed by a user to access a secure computer network included in the plurality of secure systems. In addition, the system 1800 may be employed to protect other secure systems such as secure communication networks and/or other resources that are accessed electronically. According to one embodiment, the system 1800 includes a first communication link 1801 that provides a communication path between the access device 1802 and the USR 10, and a second communication link 1803 that provides a communication path between the USR 10 and the plurality of secure system 1804. In one embodiment, each

of the first communication link 1801 and the second communication link 1803 are wide area networks, for example, the Internet.

Each of the secure systems 1804 can be associated with an organization. An organization is any entity that employs a secure (e.g., restricted access) host system to provide resources to a plurality of users. For example, an organization may be a corporation (including a non-profit corporation), partnership, other business entity, an affiliation or individual that employs a secure host system to provide resources to a plurality of authorized users. As should be apparent to those of ordinary skill in the art, an organization is not restricted to any particular size, for example, as measured by the number of members or employees.

More specifically, each of the secure systems No. 1, No. 2, No. 3, etc. may be associated with a different organization and the USR 10 may control access to each of the secure systems. That is, the USR 10 can provide access control for a plurality of secure computer networks each associated with a different and unrelated organization. Further, each of the secure computer networks may have a different plurality of users who are authorized to access the network.

The access device may include any of a desktop computer, a laptop computer, and a handheld computer (e.g., a PDA, call phone and the like). Further, as shown in phantom, a plurality of access devices may communicate with the USR 10. Where a web-based system is employed, for example, each of a plurality of computers connected to the Internet may be individually employed as a separate access device to communicate (e.g., independently communicate) with the USR 10 to gain access to one or more of the secure systems 1804.

For example, the access device 1802 may be a computer employed with a client-server network. In this example, to access resources provided by one of the secure system 1804, the user initiates an access request for a secure system 1804 selected by the user. That is, the user may supply authentication information and a computer network ID to the USR. As is described in further detail below, the authentication information and the computer network ID are processed by the USR to authenticate the user and determine whether the user is authorized to access the secure system 1804 that is identified by the computer network ID. The USR then routes

communications between the user and the secure system provided that the user authentication is successfully completed.

According to one embodiment, the USR 10 connects the access device 1802 to one of the secure systems 1804 via a communication path that does not include the USR 10. In an alternate embodiment, the USR 10 connects the access device 1802 to one of the secure system 1804 via a communication path that does include the USR.

Referring now to FIG. 18B, a system 1810 employs a USR 10 to control access to a secure system (e.g., a secure computer network) according to another embodiment. In one embodiment, the system 1810 includes the USR 10, an access device 1802, and a plurality of secure system 1804. According to this embodiment, the user selects from the plurality of secure systems 1804 a secure system that the user would like to access. With the access device 1802, the user communicates authentication information directly to the selected secure system 1804, e.g., without gaining access to the system. The secure system then communicates the authentication information and/or information corresponding to the authentication information to the USR 10. The USR 10 processes the information received from the secure system and then communicates an indication of whether the authentication information corresponds to one of the plurality of users authorized to access the secure system. The secure system grants or denies access to the secure system (and the associated resources) based on the indication received from the USR 10.

As illustrated in Figs. 18A and 18B, the USR 10 can provide a centralized access control system (e.g., an authentication system) for a plurality of secure systems 1804 that are associated with independent organizations that may have no affiliation with one another. Referring to Figs. 18A and 18B, a first organization may be associated with (have resources located on and/or accessed by) the secure system no. 1, a second organization may be associated with the secure system no. 2, and so on. In addition, a single organization may also be associated with a plurality of the secure systems 1804. Thus, in one embodiment, the USR 10 provides access control to a plurality of secure systems for a single organization.

The systems 1800 and 1810 allow an organization to operate a secure system without hosting the authentication system software or at least without the need to host a substantial part of authentication system software. Thus, in one embodiment, software

upgrades/maintenance can be implemented at the USR 10 (e.g., centrally) for the plurality of secure systems 1804 and specialized authentication software is not required at the access device. In a further embodiment, specialized authentication software is also not required at the secure system. In versions of these embodiments, the USR 10 provides a web-based system in which the user employs a web-browser when communicating with the USR 10 and the secure system.

The USR 10 can also provide centralized administration and management for the plurality of secure systems 1804. The centralized administration can include routine tasks such as adding or removing authorized users for each of the plurality of secure systems 1804, for example, based on the hiring or resignation, respectively, of an employee. Additional administrative functions such as maintaining a secure database of private keys associated with each user, generating time varying codes, maintaining encryption software, maintaining audit trails and other functions may also be accomplished in a centralized fashion with the USR 10 for a plurality of organizations.

In one embodiment, following the connection of the access device 1802 to the secure system 1804, the USR 10 develops an audit trail by monitoring the communication path to capture information concerning the use of the secure system. For example, the USR 10 may collect and store information concerning the length of time during which the access device remains connected to the secure system, the type of resources accessed by the user, the type of data transmitted (including the identification of specific documents) during a login period and the volume of data transmitted.

According to one embodiment, the USR continuously monitors the communication between a plurality of access devices 1802 and a secure computer network and collects information to generate an audit trail for each device. According to another embodiment, the USR does not continuously monitor communications. Instead, the secure computer network intermittently (e.g., periodically) transmits audit information to the USR 10 where the audit information may concern one or a plurality of users connected to the network during a specific time period.

In each of the embodiments, described with reference to FIGS. 18A and 18B, the USR 10 may be located in an ultra-secure facility that employs heightened security

relative to the security provided by the organizations that it serves. The physical facility where the USR is located may meet requirements generally associated with critical military installations. For example, the USR 10 may be housed in a facility that is hardened against radiation, shielded against electromagnetic interference, and/or protected against earthquakes, hurricanes, etc. to allow operation of the USR during times of general emergency. Further, the personnel and hiring policies of the facility operating the USR 10 may also be more secure relative to the security measures taken by the organizations associated with the secure systems 1804. That is, the individuals operating the USR 10 may undergo more rigorous background checks that include a detailed investigation of their personal and employment histories.

The centralized approach described above can provide increased security because the administration of the access control system (e.g., authentication software) is in the hands of a highly trusted third party who has taken heightened security measures regarding the hiring of the administrative personnel, in particular, the personnel who have access to authentication data (e.g., private encryption keys, etc.).

In any of the preceding embodiments, the USR 10 may be geographically remote from the secure systems.

Further, in any of the preceding embodiments, there may be situations where a user employs the access device 1802 to connect to more than one of the plurality of secure systems 1804. In one embodiment, the user is independently authorized to access separate secure systems 1804 associated with independent organizations. In another embodiment, the user is authorized to access separate secure systems 1804 each associated with the same organization. In either situation, the user may employ one or more of the authentication procedures described herein before being allowed access to any one of the secure systems 1804.

Referring now to FIG. 19, a process 1900 that employs a USR to control access to a secure computer network is illustrated. In one embodiment, the process 1900 is employed with the system 1800 illustrated in FIG. 18A. At step 1902 an entity initiates an access request. In general, the access request will be initiated when the user or entity inputs information into an access device such as a computer. At stage 1904, the entity supplies authentication information and a computer network ID to the USR (e.g., the information is electronically transmitted from the access device to the USR).

According to one embodiment, the information is transmitted via the Internet from the access device to the USR. At stage 1906, the USR receives the access request which includes the authentication information and the computer network ID. At stage 1908, the USR determines whether the authentication information is valid for a user. According to one embodiment, the USR includes a database containing selected data of a plurality of users authorized to access a secure computer network, and may compare the authentication information supplied by the entity with authentication information included in the database to determine whether the authentication information corresponds or is valid for a user. If the authentication information is valid, the process 1900 moves to stage 1910 where the USR determines whether the entity is authorized to access the computer network identified by the computer network ID. If the entity is authorized to access the computer network then the USR may allow communication between the entity and the secure computer network at stage 1912. As previously indicated, the USR may route communications between the entity and the secure computer network and remain in the communication path employed by the access device to communicate with the secure computer network. Alternatively, the USR may simply provide a connection between the access device and the secure computer network where the communication path provided by the connection does not involve the USR.

Returning to stage 1908 if the authentication information supplied by the entity is not valid for any of the plurality of users then the process 1900 moves to stage 1914 where an indication is provided to the entity that access is denied. Similarly, if at stage 1910 the entity is not authorized to access the computer network identified by the computer network ID, an indication is provided that the entity is denied access at stage 1914. In various embodiments, the entity may be allowed additional opportunities to successfully access the system.

Referring now to FIG. 20, a process 2000 for controlling access to a secure computer network is illustrated in accordance with one embodiment. In one embodiment, the process 2000 is employed with the system 1810 illustrated in FIG. 18B.

In one embodiment the entity initiates an access request at stage 2002. As described above, the access request can be initiated using an access device and each

secure computer network may communicate with a plurality of access devices. At stage 2004, the entity supplies authentication information to the secure computer network, for example, by entering the information in a web browser and transmitting the authentication information over the Internet to the secure computer network. At stage 2006, the secure computer network receives the authentication information. At stage 2008, the secure computer network communicates authentication information to the USR (or information corresponding to the authentication information) to allow the USR to authenticate the access request. At stage 2010, the USR validates the authentication information to determine whether the entity is authorized to access the secure system, and at stage 2014, the secure system receives an indication from the USR concerning whether the entity is authorized to access the system. In one embodiment, the indication is transmitted from the USR to the secure system via the Internet. At stage 2016, the secure system grants or denies the entity access to the secure system based on the indication received from the USR.

As should be recognized by those of ordinary skill, the processes 1900 and 2000 can be accomplished in a variety of stages that may include any of the stages described above in various combinations and sequences including one or more of the stages described above in combination with one or more additional stages.

Various embodiments can be employed to control access to a physical facility. That is, an electronic device (e.g., a keypad, a card reader, a biometric scanner, etc.) or combination of electronic devices can be located at an access point to a secure area (e.g., a door, a gate, etc.). The entity initiates the request using the electronic device. In one embodiment, the physical facility includes all or a portion of the secure computer network. Thus, in one embodiment, the secure system receives an indication of whether an entity is authorized to access a physical facility. The secure system communicates authentication information to the USR. The USR validates the authentication information and communicates an indication of whether the entity is authorized to access the physical facility. The secure system receives the indication and grants or denies the entity access to the physical facility.

Each of the embodiments described with reference to any FIGS. 18-20, may include a challenge-response protocol, for example, to authenticate the identity of the entity and/or the USR system to the other.

FIG. 21 illustrates an embodiment of a system 2100 for validating the identity of an individual or an entity. The system includes a first wireless device 2110 and a second wireless device 2112. The first wireless device 2110 comprises a first wireless transmitter and receiver 2114, a first processor 2116 and a first memory 2118. Similarly, the second wireless device 2112 comprises a second wireless transmitter and receiver 2120, a second processor 2122 and a second memory 2124. According to aspects of the invention, the first wireless device and the second wireless device are configured to wirelessly communicate with each other so that the entity associated with the first wireless device can communicate his identity to the entity associated with the second wireless device. It is to be appreciated that the first wireless transmitter and the second wireless transmitter can be configured to communicate by any form of a wireless signal such as low power Bluetooth signal, infrared signals, RF signals and electromagnetic signals in general. In accordance with one embodiment, the first wireless device and the second wireless device communicate via near field signal.

The first wireless device can also comprise user interface 2126 that allows the first entity to interact with the first wireless device and can also comprise a display, such as a LCD display, 2128 that allows the first entity to further interact with the first wireless device. In accordance with some embodiments the invention, the first wireless device can be configured so that the first entity must enter a PIN identification number, for example, via the user interface to gain access to the wireless device. Alternatively, or in addition, the first wireless device may comprise a biometric sensor or detector 2130 that enable the first entity to present biometric data to the first wireless device to gain access to the first wireless device. For example, the biometric sensor can be configured to detect a fingerprint of the first entity. For such embodiment, the memory 2118 also comprises stored biometric data of the first entity, which is compared, for example, by the processor 2116 with the detected biometric data to determine whether the first entity is enabled or should be disabled from using the first wireless device. It is also to be appreciated that the biometric data need not be fingerprint data and can be any biometric data known to those of skill in the art, and that the biometric sensor need not be a fingerprint sensor and can be any biometric sensor known to those of skill in the art.

RECTIFIED SHEET (RULE 91)
ISA/EP

Similarly, the second wireless device 2112 can also be configured as discussed above with respect to the first wireless device, namely with any or all of a user interface 2132, a display 2134 and a biometric sensor 2136 and can be configured to require any and/or all of a second entity to provide a PIN number, or the second wireless device to match biometric information of the second entity with stored biometric information to enable or disable the second entity to gain access to the second wireless device. Each of the first wireless device 2110 and the second wireless device 2112 comprise a power source or a power source interface 2138, 2140 that can be coupled to a power source that provides power to respective devices. It is to be appreciated that the power source can be any power source, such as, alkaline batteries, rechargeable batteries, proprietary power sources, and interfaces to power sources such as standard 120 VAC, or an AC to DC conversion device, as well as any other type of power source known to those of skilled in the art. In addition, it is to be appreciated that each of the first wireless device 2110 and the second wireless device 2112 can also comprise an additional wireless transmitter and receiver device 2142, 2144, respectively, which enable each of these devices to communicate wirelessly via other wireless communication systems such as, via any cell phone standard, via satellite communications, over wireless area networks, local area networks, wide area networks, as well as any other wireless communication standard know to those of skill in the art.

According to some embodiments of the system 2100 of FIG. 21, either or both of the first wireless device 2110 and the second wireless device 2112 can be configured to communicate with a secure database 2146, as will be discussed in further detail herein. According to some embodiments, either of the first or second wireless devices may communicate with the secure database on a periodic basis to update it's corresponding data, or to stay alive as will be discussed herein, or to retrieve information in the secure database that is used in the communication protocol between the first and second wireless devices to verify the identity of at least the first entity. Accordingly, it is to be appreciated that communication with a secure database can be, for example, via the additional respective wireless transmitters and receivers 2142, 2144 of the first and second wireless devices, or can be via a network interface 2152, 2154 of the respective devices, that communicate with a network 2148 and to the secure database 2146.

Referring now to FIG. 22, there is illustrated one embodiment of an overall communication process that occurs with the system 2100 of FIG. 21. In particular, the process is effected by the system of FIG. 1 so as to identify and authenticate the identity of the first user associated with the first wireless device 2110 to the second user associated with the second wireless device 2112. For example, consider the situation where an air marshal or an FBI agent is carrying the first wireless device 2110 and airport security or security personnel generally want to ensure the identity of the user of the device 2110. The communication protocol 200 illustrated in FIG. 22 is one embodiment of a protocol that enables secure authentication of the first user of the wireless device 2110.

According to one embodiment of the process, the first user of the first wireless device 2110 first authenticates his or herself to the wireless device 2110, for example as has been discussed above, by either entering a PIN via the user interface 2126 of the first wireless device or by interacting with the biometric sensor of the first wireless device at step 202. In various embodiments, a challenge-response protocol is employed in which the first user supplies information (a biometric, a PIN or other information) to authenticate his or herself to the wireless device 2110. If the user of the device does not enter the correct PIN number or does not match the biometric data stored in memory 2118 of the first authorized user of the device, then the device at a minimum shuts down at step 204. However, according to some embodiments, the device 2110 can also be configured to automatically delete any portion of or all of the data stored in memory 2118 at step 206. In addition, as will be discussed in further detail herein, according to some aspects of the invention, the first wireless device can be configured to periodically communicate with the secure database 2146 to remain alive, for example, after the first user of the first device authenticates itself to the first device. If the first device does not communicate with the secure database at such periodic intervals at step 208, then the first device can be configured to delete any or a portion of the data stored in memory at step 206.

The communication protocol also comprises a second user of the second device to authenticate his or herself to the second device at step 210. It is to be appreciated that the authentication by the second device of the second user by any of the mechanisms discussed herein and above with respect to the first wireless device,

including entering a PIN number to the user interface 2132 of the second wireless device or by interacting with the biometric sensor 2136 of the second wireless device. In addition, it is to be appreciated that as discussed above with respect to the first wireless device, if such identification is not successful, the second wireless device will at a minimum shut itself down at step 212. However, it is also to be appreciated that the second wireless device can be configured to automatically delete a portion of or all of the data stored in the memory 2124 of the second wireless device, should such authentication not be successful at step 214. In addition, it is to be appreciated that the second wireless device can also be configured at step 216 to communicate with the secure database 2146 within defined periods of time, or even a periodic interval once the second user authenticates himself to the second wireless device, and to delete a portion of or all of the data in memory 2124 should such periodic communication not occur.

If both the first user and the second user are successful in authenticating themselves to the first and second wireless devices respectively, then a communication protocol is initiated between the first wireless device 2110 and the second wireless device 2112 at step 218. If the communication protocol is not a valid communication protocol between the devices, the devices wait until there is a valid communication protocol. If the communication protocol is a valid protocol (218 yes), then the first wireless device transmits a first wireless signal containing encrypted authentication information of the first user to the second wireless device 2112 at step 220. The details of the communication protocol and the encrypted authentication information will be discussed further herein.

The second wireless device 2112 receives the first wireless signal and processes the wireless signal to determine the identity of the first user. In particular, as will be discussed herein, according to some aspects of the invention, the authentication of the first user includes displaying a picture of the first user to the second user on the display 2134 of the second wireless device as a result of the communication from the first wireless device to the second wireless device. The user of the second wireless device can view the picture on the display and ascertain whether the first user of the first wireless device is who he or she purports to be. However, as will also be discussed herein, it is to be appreciated that the second wireless device need not be a device that

requires a user to interact with it and can be, for example, an unmanned detection system that receives the first encrypted authentication information and determines from the first authenticated encrypted information whether the first user is authorized to gain access to a secured place, a secure network, or a secure computer, to do whatever the first person is seeking to do. If the first user is not who they purport to be, the communication process goes back to looking for a valid communication protocol. In addition, the process allows the second user or the system associated with the second wireless device to take an appropriate action such as denying access to the secure site at step 224.

If the user of the first wireless device is authenticated (at step 222 yes), then according to some aspects of the invention, the communication process allows for the second wireless device to transmit a second wireless signal comprising encrypted authentication information of the second user to the first wireless device at step 226. In addition, according to such aspects, the communication protocol and the first wireless device are configured to authenticate the identity of the second user to the first user at step 228. It is to be appreciated that the authentication of the second user to the first user can be in any of the manners discussed above with respect to the authentication of the first user of the first device, such as by viewing a picture of the second user as provided on the display 2128 of the first wireless device, by matching one-time information contained in the encrypted authentication information or via a challenge-response protocol.

In addition, according to some embodiments of the protocol, either or both of the first wireless device 2110 and the second wireless device 2112 may communicate with the secure database 2146 to retrieve additional information at step 230. Such information, as will be discussed herein, can include for example, a portion of the biographic data of the first user of the first wireless device or of the second user of the second wireless device, or full biometric information of the first user or the second user, which can be communicated back to the respective device and used by the respective device to authenticate the user. In addition, the information can be periodic updates as provided the secure database to the respective device, such as will be described herein, including periodic updates of public keys of a plurality of first users as stored in memory on the second wireless device, or updates to public keys of a

plurality of second users as stored in memory on the first wireless device. In addition, such information may include periodic updates of the biometric information of a plurality of first users as stored on the second wireless device or a plurality of second users as stored on the first wireless device, which can comprise for example a portion of the biometric information or all of the biometric information.

Referring now to FIG. 23, there is illustrated one embodiment of various fields included within the first wireless signal and the second wireless signal as transmitted between the first wireless device and the second wireless device. According to some embodiments, the signal comprises a header field 302. The header field can be any header field known to those of skill in the art. In addition, the signal comprises a public ID field 304, which can comprise, for example, any of name information, a badge number, an employee number, an e-mail address, a social security number, and the like, of the first user. In addition, the first wireless signal may also include a digital signature field 306 containing a digital signature of the first user. For example, the digital signature may be generated with the user's private PKI key. Further, the first wireless signal may comprise a one-time time varying code field 308 that includes a random code as generated by the first wireless device. According to some embodiments, the digital signature field and the one-time code field can be used, for example by the second wireless device, to allow access to a secure place without the need for a user of the second wireless device to interact with the second wireless device to authenticate the first user. As an example, referring to FIG. 24, the digital signature and one time code can be encrypted with the private key of the first user and transmitted to the second wireless device. The second wireless device can decrypt the digital signature and one time code with the public key of the first user at steps 402-404 to authenticate or not the first user at step 406.

In addition, referring back to FIG. 23, the first wireless signal also comprises a PKI encrypted one-time DES key field 310 comprising a PKI encrypted one-time DES key. Further, the first wireless signal comprises a DES key encrypted biometric data field 312, which includes at least a portion of biometric data of the first user encrypted with the DES key. As will be discussed in further detail herein, according to some aspects of the invention, the public key of a first user, for example, stored in memory 24 of the second wireless device can be used to decrypt the DES key, and the DES key

can be used to decrypt at least a portion of the biometric data of the first user to use in the authentication of the identity of the first user. According to some embodiments, the first wireless signal can also comprise another ID data field 314, which can contain other information such as name, height, weight, eye color or anything else.

It is to be appreciated that although the embodiment of the wireless signal discussed in FIG. 23 has been discussed with reference to the first wireless signal transmitted from the first wireless device 2110 of FIG. 21 to the second wireless 2112, that the same protocol can be used when transmitting a second wireless signal from the second wireless device 2112 to the first wireless device 2110 to authenticate the identity of the user of the second wireless device to the user of the first wireless device. It is to be further appreciated that various fields of the signal can be used and not all of the fields of the wireless signal are needed to authenticate identity of the user.

Referring now to FIG. 24, there is illustrated one embodiment of a process 400 as identified by act 222 in FIG. 22 for verifying or authenticating the identity of the first user of the first device. According to this embodiment, which has been briefly discussed herein with respect to FIG. 23, the second wireless device can verify the identity of the respondent without necessarily interacting with a second user by decrypting the first user's digital signature from the digital signature field 306 at step 402 and verifying that it is the digital signature of the first user, decrypting the one-time code from the one-time code field 308 at step 404, and using this information at step 406 to authenticate the first user. If the first user is authenticated at 406, an appropriate action such as allowing access to the secure site, or computer, or network can be granted.

Referring now to FIG. 25 there is illustrated another embodiment of a process 520 for authenticating the identity of the first user at step 222 of the communication process of FIG. 22. According to aspects of the invention, the second wireless device at step 522 receives the first wireless signal and extracts the PKI encrypted DES key from field 310. The wireless device looks up the public key of the first user from memory 2124 [See FIG. 21] or from a secure server based on the information provided in the public ID field 304 at step 524. The second wireless device uses the first public key to decrypt the PKI encrypted DES key at step 526. The second wireless device acts on the DES key encrypted biometric information from the field 312 and uses the

decrypted DES key to decrypt the at least a portion of the biometric information of the first user as included in the first wireless signal at step 528.

According to some embodiments, the biometric information included in the first wireless signal is a portion of the biometric information of the first user and the second wireless device is configured to store a remainder of the biometric information of the first user in memory. According to such embodiments, the process 520 also comprises looking up the remainder of the biometric information stored in the memory at step 530 and combining the remainder of the biometric information with the decrypted and extracted biometric information to provide complete biometric information of the first user at step 532. According to some aspects of the invention, the biometric information can comprise a digital image of the first user and for such aspects, the digital image can be displayed on display 2134 of the second wireless device so that the second user can ascertain whether the first user associated with the first device is who he or she purports to be. However, it is to also be appreciated that the biometric information can be fingerprint information, a voiceprint, DNA codes of the first user, or any other biometric information known and used by those of skill in the art. Accordingly, the processor 2122 of device 2112 can also be configured to process the combined biometric information to authenticate the first user at step 536.

Referring now to FIG. 26, there is illustrated another embodiment of a process 620 that can be used to authenticate the identity of the first user at step 222 of the process 200 of FIG. 22. According to this embodiment, some of the steps are similar to the steps of the process 520 illustrated in FIG. 25 and accordingly a full description of these steps will not be herein duplicated. It is to be appreciated that this embodiment can be used for example, where the biometric information of the plurality of first users is not stored on the second wireless device 2112 but is instead stored at the secure database 2146 as illustrated in FIG. 21. In particular, for highly secure applications, where there is a worry that the second wireless device can be compromised (even with the necessity to authenticate the second user to the second wireless device), the second wireless device can be configured to interact with the secure database to obtain at least a portion of the biometric information of the first user, rather than storing at least a portion of the biometric information of the first user in memory on the second wireless device.

According to such embodiments, the second wireless device can receive the first wireless signal including the fields discussed above in respect to FIG. 23, in particular, the public ID field 304 and optionally the PKI encrypted DES key. According to some embodiments, the PKI encrypted DES key may be used by this process. At step 624, the second wireless device accesses public key information of the first user from the public keys stored in memory on the second wireless device. However, it is to be appreciated that in some embodiments, the public keys may not be stored on the second wireless device and for such embodiments, the second wireless device will communicate with the secure database to obtain the public key of the first user also at step 624. According to some embodiments, at step 626 the second wireless device transmits a signal to the secure database comprising public identification number to identify the second device to the secure database, presumably after the second user of the second device has authenticated his or herself to the second device. For such embodiments, at step 628, the secure database determines whether the second device is authorized to access the secure database at step 628. It is to be appreciated that according to some embodiments, this communication between the second wireless device and the secure database can be accomplished with encrypted signals and in some embodiments the encrypted signals can include using time varying one time codes to further secure the communication. If the second device is authorized to interact with the secure database, the process also comprises transmitting the first public ID from the second wireless device 2112 to the secure database at step 630, and with this information, the secure database accesses the biometric or identification information of the first user at step 632. The biometric or the at least a portion of the biometric information can then be transmitted by the secure database to the second wireless device at step 634. Again, this transmission can be encrypted and further include time varying or one time codes to further secure the communication. The second wireless device can use the received portion of the first biometric information and combine it with portion of the first biometric information provided in the first wireless signal, or can receive all of the first biometric information as provided by the secure database and, for example, display it on the display 2134 of the second wireless device 2112 at step 636, or can process the biometric or identification information at step 638 to determine whether the first user is authenticated.

RECTIFIED SHEET (RULE 91)
ISA/EP

Referring now to FIG. 27 there is illustrated one embodiment of a data structure 720 that can comprise memory 2124 of the second wireless device 2112. It is to be appreciated that any or all of the various portions of this data structure can be present in the memory 2124. According to some aspects of the invention, the memory will include the private key of the second user at field 722. The private key can be used, for example, when communicating by the second wireless device to the first wireless device to provide a digital signature of the second entity encrypted with the second user's private PKI key to the first user. In addition, the memory can also comprise a plurality of public keys of a plurality of first users at area 724. Such public keys of a plurality of first users can be used as has been discussed herein in combination with the private key of the first user to decrypt information of the first user. For example, the public and private key can be used to decrypt the DES key of the first user. In addition, the memory can also comprise at least a portion of biometric data of a plurality of first users, at area 726. As been discussed herein, the at least a portion of the biometric data of the plurality of first users can be combined with the portion of the biometric data provided in the first wireless signal or from the secure database, to create the complete biometric data of the first user for ascertaining or authenticating the identity of the first user as has been described herein. In addition, the memory can also comprise biometric data of the second user at field 728. The biometric information of the second user can be used, for example, as has been discussed herein to compare the biometric data detected by the biometric sensor 2136 of the second wireless device to determine whether the second user is authorized to have access to the second wireless device. It is to be appreciated that the data structure 720 of FIG. 27 can also comprise the memory 2118 of the first wireless device 2110, and that any or all of the fields of the data structure 720 can exist in the memory 2118 in the first wireless device. It is also to be appreciated that the first wireless device can access the data structure 720 and the various fields for the same purposes as discussed above with respect to the second wireless device, namely, to provide the first digital signature of the first entity encrypted with the first private key in the first wireless signal, to access the public keys of a plurality of second users for the purpose of decrypting information provided in the second wireless signal, to access at least a portion of biometric information of the second user stored in the field 726, as well as to compare biometric information of the

RECTIFIED SHEET (RULE 91)
ISA/EP

first user with sensed biometric data provided by the biometric sensor 2130 of the first wireless device.

In one embodiment, the method comprises acts of receiving first authentication information about the first entity with the first device, transmitting the authentication information about the first entity to a secure database, determining whether or not the first entity is allowed to access the first device based on the first authentication information, and transmitting an enablement signal to the first device indicating to enable nor not enable the first entity to access the first device. According to a further embodiment, the method also includes an act of allowing or not allowing operation of the first device based on the enablement signal. In another embodiment, the act of receiving the first authentication information of the first entity comprises receiving biometric information of the first entity by detecting the biometric information with the first device.

In yet another embodiment, the act of transmitting the first authentication information about the first entity to a secure database comprises generating a non-predictable signal from the biometric information. In a further embodiment, the act of generating the non-predictable signal from the biometric information comprises generating a time varying non-predictable signal from the biometric information. In a still further embodiment, the act of receiving biometric information of the first entity comprises receiving a voice signature of the first entity with the first device and the act of generating the non-predictable signal from the biometric information comprises mixing the voice signature of the first entity with a random code to generate the non-predictable signal. In yet a further embodiment, the act of transmitting the enablement signal to the first device comprises sending the random code to the first device. In a still further embodiment, the act of receiving biometric information of the first entity comprises receiving fingerprint data of the first entity with the first device and the act of generating the non-predictable signal from the biometric information comprises mixing the fingerprint data of the first entity with a random code to generate the non-predictable signal. In another embodiment, the act of transmitting the enablement signal to the first device comprises sending the random code to the first device.

In a further embodiment, the act of authenticating the biometric of the first entity comprises authenticating a voice signature of the first entity. In another

embodiment, the act of authenticating the biometric information of the first entity comprises authenticating a finger print of the first entity.

In one embodiment, a first wireless device includes a biometric detector comprising a fingerprint detector that detects a fingerprint of the first entity. In an alternate embodiment, the biometric detector comprises a voice signature that detects a voice signature of the first entity.

According to one embodiment, the system comprises a first wireless device including a processor configured to enable operation of the first wireless device if it receives an enablement signal validating first biometric information of a first entity and configured to generate a non-predictable signal from the biometric information, a first wireless transmitter and receiver configured to transmit a first wireless signal including first encrypted biometric information of the first entity and to receive the enablement signal, a first biometric detector for detecting the first biometric information of the first entity and a secure database configured receive the first wireless signal, to authenticate or not authenticate the first biometric information of the first entity, and to provide the enablement signal validating or not validating the first biometric data of the first entity.

In a further embodiment, the secure database further comprises biometric data of a plurality of first entities. In another embodiment, the processor is configured to generate the non-predictable signal from the biometric information by generating a time varying non-predictable signal from the biometric information. In a still further embodiment, the processor is configured to generate the non-predictable signal from the biometric information by mixing the biometric information of the first entity with a random code to generate the non-predictable signal. In yet another embodiment, the secure database is configured to transmit the enablement signal to the first device including the random code so as to authenticate the secure database to the first device. In still another embodiment, the system includes a memory for storing a private key of the first entity authorized to use the first device.

It should be understood that various changes and modifications of the embodiments shown in the drawings and described in the specification may be made within the spirit and scope of the present invention. Accordingly, it is intended that all matter contained in the above description and shown in the accompanying drawings be

interpreted in an illustrative and not in a limiting sense. The invention is limited only as defined in the following claims and the equivalents thereto.

FIG. 28 illustrates an embodiment of a system 100 that employs a converter device 102 to provide an interface between a user device 104 (e.g., a transaction card, a cell phone, etc.) and a system interface 106 where, for example, the system interface 106 employs a magnetic card reader and the user device 104 is not equipped with a magnetic stripe. That is, in one embodiment, the converter device 102 provides a mode of information transmission between the user device 102 and the system interface 106 which would otherwise be unavailable to the user device 102. The converter device 102 provides a modified system 100 that provides compatibility with a greater variety of user devices, for example, user devices such as transaction cards, cell phones or PDAs that are not equipped with a magnetic stripe. For example, in one embodiment, the converter device 102 includes a magnetic stripe emulator 137 communicatively coupled to a wireless signal receiver 140 and adapted to provide a time-varying signal emulating data provided by a magnetic stripe card to a magnetic card reader 152.

The user device need not be a "card" and may, for example, take the form of a fob used as a key ring, a cell phone, a watch, a personal digital assistant or any device that can include a wireless transmitter, or a magnetic stripe emulator.

In various embodiments, the user device 104 employs near field signal to communicate with the converter device 102. In one embodiment, the near field communication is bi-directional such that the user device 104 may both send and receive wireless communication. That is, the user device includes a transceiver.

In general, the system interface 106 provides an interface to a larger information system (e.g., a financial system, an access control system, a medical records system, and the like) that in one embodiment includes a system processor or controller 110, a database 112, a network 114, other systems 116, such as a universal secure registry 118 as will be described further herein. Each of the preceding system elements may be placed in communication with any one or any combination of the system elements, for example, over communication links 120A, 120B, 120C, 120D. It should be recognized that the communication links 120 need not provide the communication paths shown in FIG. 28 and that other communication paths may be employed. For example, the database 112 may be connected to the network 114 via the communication link 120A

and to the system processor 110 via the communication link 120B instead of being connected as shown in FIG. 28.

The communication link may be a wireless communication link, a hardwired communication link, a fiber optic communication link, any communication link used in the art, as well as a combination of any of the preceding or any other any communication link capable of transmitting signals between the elements of the system 100. The system processor 110 allows information transfer of both data and instructions, for example, between the interface 106 and one or more databases which may be connected to the system or other network elements.

In general, the operation of the converter device 102 allows a user in possession of the user device 104 to wirelessly communicate information to the device so that the device can be employed to interface with a network system. For example, in one embodiment, the network system may provide a magnetic card reader interface and the converter device 102 provides a magnetic stripe emulator that can interface with the system. In general, the overall operation of the system 100 includes the communication of information between the user device 104 and the converter device 102, for example, RF communication. In one embodiment, the communication is bi-directional such that information can be communicated both to and from the user device 104. The converter device 102 provides an interface by which information derived from the information being transmitted to or from the user device 104 is transmitted between the converter device and the system interface 106. The system interface 106 provides the communication interface between it and the remainder of the system 100 (e.g., processor 110, database 112, network 114, etc.).

According to one embodiment, the user device 104 includes a processor 122, a user interface 124, a wireless transmitter 126 and device indicia 128. In another embodiment, the user device 104 includes a biometric sensor 130. In various embodiments, the processor 122 is communicatively coupled to each of the wireless transmitter 126, the user interface 124 and the biometric sensor 130.

The processor 122 may include a chip such as a general purpose processor, an application specific integrated circuit ("ASIC"), or a field programmable gate array ("FPGA") and the like that may execute various programs and/or provide logic inputs and outputs. For example, the processor 122 may process biometric information

received from the biometric sensor 130 to verify the identity of the user before the user can employ the user device 104. Exemplary details of a processor and biometric sensor which are configured to authenticate a fingerprint of a user are disclosed in U.S. published application 2004/0133787, published on July 8, 2004, which is herein incorporated by reference in its entirety. The processor 122 may also include or be coupled to driver circuitry to drive a display included in the user interface 124 and can be configured to process user input data entered via the user interface 124. In one embodiment, the user interface 124 includes one or more control inputs (for example, control buttons).

The wireless transmitter 126 can process information provided by the processor and convert the information to an RF signal and can also include an RF antenna that transmits the RF information wirelessly. In another embodiment, the user device may also include an RF receiver that receives a wireless RF signal from the RF antenna and converts the RF signal to an information signal provided to the processor. It is to be appreciated that the wireless transmitter and/or receiver need not be an RF device, it can also be any of a IR device, an optical device, a Bluetooth signal or any other wireless signal transmitter or receiver used in the art.

The user device may also include a power source such as a battery that fits within the device. In one alternative embodiment, the user device remains in a sleep mode until it is placed in the vicinity of an RF transmitter at which time the user device 104 converts received RF energy into electrical energy used to provide power to the processor 122 and the other components included in the user device 104.

According to one embodiment, the user device 104 can be a smart card configured for wireless signal transmission using RF signals. For example, the wireless transmitter 126 may be an RF transmitter device or any other wireless transmitter device configured to transmit the smart card information of the card. Alternatively, it is to be appreciated that the card can be many cards such as a debit card, a plurality of credit cards such as VISA, MasterCard, American Express, or any other card with the card indicia and relevant information being stored in card memory 129 and read out by processor 122 and provided to the wireless transmitter 126. However, the user device 104 need not be in the form of a card and may instead include a cell phone or PDA.

In the embodiment illustrated in FIG. 28, the converter device 102 includes a substrate 132 which may include a stripe 134 and a magnetic field generator 136 which together comprise the magnetic stripe emulator 137, a processor 138, a wireless receiver 140, a user interface 142, a memory 144, and a power source 146. In a further embodiment, the converter device 102 includes an indicating light 148 (e.g., an LED) and an output device 150.

According to one embodiment, the system interface 106 with which the converter device 132 is employed includes any of or all of a magnetic card reader 152, a wireless transceiver 154 and a data port 156.

In general, according to one embodiment, the converter device 102 receives a wireless signal from the user device 104, processes the information that is received and provides an output in the form of a time-varying signal provided to the stripe 134 (e.g., a magnetic stripe). The signal provided to the stripe 134 can then be provided to the system processor 110 by inserting the stripe and the associated substrate 132 or portion thereof in the magnetic card reader of the system interface 106. That is, in one embodiment, the stripe 134 and at least a portion of the substrate 132 can be either slid by the magnetic card reader 152 or inserted to sit statically in front of the read head of the card reader.

The processor 138 may be a general purpose processor, an application specific integrated circuit ("ASIC"), or a field programmable gate array ("FPGA") and may be implemented in hardware, software, firmware or any combination of the preceding. The processor 138 may be communicatively coupled with any of the magnetic field generator 136 the wireless receiver 140, the memory 144, the user interface 142, the light source 148, the power source 146 and the output device 150. In general, the processor can be configured to receive inputs from one or more of the preceding elements and may provide outputs to each of the elements included in converter device 138.

For example, according to one embodiment, the magnetic stripe 134 is a programmable magnetic stripe and the magnetic field generator 136 generates a magnetic signal that controls the information provided by the magnetic stripe 134. The U.S. Patent Application No. 10/680,050, filed October 7, 2003, entitled "System Method and Apparatus for Enabling Transactions Using a Biometrically Enabled

Programmable Magnetic Stripe which was published on July 8, 2004 as US2004/0133787 (the '050 application), provides further details concerning embodiments of the user device that emulates a magnetic stripe and may also include, for example, a biometric sensor. The '050 application is incorporated herein by reference in its entirety. In this embodiment, the processor 138 may control the operation of the magnetic field generator 136 to provide the desired information to the stripe 134. For example, the processor 138 may provide an output to the stripe 134 in response to receiving information from the wireless receiver 140, where the information from the wireless receiver is information transmitted from the user device 104.

Further, the processor 138 may be configured to provide signals to drive a display included in the user interface 142 and process user input data entered with the user interface 142. In one embodiment, the user interface 142 includes a display screen that can be used to display an image of the user to whom the user device 104 belongs, for security purposes. The image to be displayed by the UI can either be part of the information transmitted by the user device 104, for example, where the user device 104 also requires some authentication by the user before transmitting the device information and image, or can be provided, for example, by the USR system 118 through the system interface 106 as part of the user authentication process, as will be described in more detail herein. In further embodiments, the user interface 142 may include a plurality of control elements that allow the user and/or the transaction processor (e.g., store clerk, security guard, medical service provider, etc.) to enter information into the converter device 102. According to one embodiment, the user interface 142 includes an LCD display.

The processor 138 may also be configured to provide signals to operate the indicating light 148. The indicating light 148 may provide an indication of the operational status of the converter device 102, for example, the indicating light 148 may indicate any of the following: that the converter device 102 is receiving a transmission from a user device 104; that the converter device 102 has generated output data to the stripe 134; the status of the power source 146 is normal or conversely that the power source has a low power level; that the converter device 102 is transmitting information via the output device 150; that the converter device 102 is properly aligned

with the magnetic card reader 152; that the converter device 102 has received authorization for a transaction; and the like. It should be apparent to one of skill in the art that the indicating light may be a single lamp or a plurality of lamps and that the lamp or lamps may be a single color including white or may included a plurality of colors. Further, it should also be apparent that the lights may provide a plurality of status indications based on their color, intensity, rate of change of the preceding characteristics or any combination of these and other features.

The power source 146 may include a battery power source or other energy sources suitable for the form factor of the converter device 102. For example, in a form factor where the converter device 102 is a hand-held device the power source 146 may be any one of a standard size battery (e.g., a AA battery). In a further embodiment, the power source is a lithium battery. Alternatively, the power source can be any of an AC power source, an AC to DC converter device, or any other DC power source known to those skilled in the art.

According to one embodiment, the converter device 102 includes a power bus 158 that provides a path for the transmission of power to the various components included in the converter device 102.

In accordance with one embodiment, the converter device 102 includes the output device 150. It is to be appreciated that the output device can be any standard interface device to be coupled to a data bus such as a USB device, or the output device can be configured for contactless communication with the system interface 106. For example, in one embodiment, the output device is an optical transmitter device. In general, the communication between the converter device 102 and the system interface 106 is bi-directional such that information (e.g., information associated with the user's identity) may be transmitted to the system interface 106, the system processor 110 may generate a response (e.g., a transaction approval), and the response may transmitted to the converter device 102 via the system interface 106.

In one embodiment, the processor 138 is configured in combination with the output device 150 to provide an encrypted output signal. In a further embodiment, the processor 138 is configured in combination with the output device 150 to provide a time-varying encrypted output signal. In yet another embodiment, the processor 138 is configured in combination with the output device 150 to provide a time-varying

encrypted (or not) public and private key output signal. In addition, the processor can also be configured in combination with the wireless receiver to receive and decrypt any and all of an encrypted signal, a time-varying encrypted signal and a signal encrypted with a private key as provided by the user device 104. A challenge-response protocol may also be employed alternatively or in addition to any of the preceding.

For example, embodiments of the invention may employ a protocol that does not require synchronized clocks in each of the user device 104 and the converter device and/or elsewhere in the system 100 to complete a validation and/or authentication process. That is, according to one embodiment, an information exchange between the user device 104 and the converter device 102 includes a first piece of information transmitted from the user device 104 to the converter device 102 and a subsequent challenge (e.g., an encrypted challenge) generated by the converter device and transmitted from the converter device to the user device 104. According to one embodiment, the user employs the user device to respond to the challenge. In one embodiment, the user's response is at least in part based on information included in the challenge. An identity of a user who responds accurately to the challenge can be successfully validated. In various embodiments, a challenge-response protocol includes an information exchange whereby the identity of the converter 102 is also authenticated by the user with the user device 104.

In various embodiments, the above-described challenge-response protocol may not require any further action by the user than is required under current approaches that require synchronized clocks in disparate devices.

In some embodiments, the output device 150 need not transmit any personal information associated with the user. For example, commonly owned U.S. Patent Application No. 09/810,703, filed March 16, 2001, entitled "Universal Secure Registry" ("the '703 application") describes an approach that can improve security and reduce the need for multiple forms of identification. The '703 application is incorporated herein by reference in its entirety. The universal secure registry 118 included in the system 100 provides one example of the integration of such a registry into a system that employs a converter device 102. With the USR system, for example, the user device 104 can provide some information, e.g., such as a public code of the user, which can be authenticated by the user, for example by providing an ID through

the user interface 124 or through biometric sensor 130. The public code can be provided to the USR via the converter 102, system interface 104, and network 114. The USR can then provide back to any of the system interface and the converter device any or all of device information (e.g., transaction card information), authorization for a transaction, e.g., where the network or the USR also communicates with the relevant authority, and indicia about the holder of the user device.

The system 100 may include a variety of system interfaces 106 of different types such as the wireless transceiver 154 and the data port 156 in addition to the magnetic card reader 152. Although not illustrated, other system interfaces such as an optical interface, a smart card reader interface or any other system interface known to those of skill in the art can also be included. Further, the system interfaces may be either commonly located or may be geographically distributed such that some locations include a wireless transceiver 154, some locations include a data port 156, some locations include a magnetic card reader 152, and some locations include a plurality of types of system interfaces.

Thus, in some embodiments the output device 150 of the converter device 102 may include a data port via which the converter device 102 can provide data to a network or a networked device. In one embodiment, the data port is also configured to receive data from the network or a networked device.

Embodiments of the converter device 102 can be configured to provide communication to the system interface 106 via any of the preceding approaches including wireless signal transmission. In a version of this embodiment, the converter device 102 may receive wireless signals from the user device and transmit wireless signals to the system interface 106. Further, the converter device may include a transmitter that allows it to transmit information back to the user device.

Referring now to FIG. 29, a process 260 employing the converter device 102 is illustrated in accordance with one embodiment. The process begins at Stage 262 – START. Here, the converter device 102 is in a steady state in which it awaits receipt of a signal from a user device 104. At Stage 264, the converter device 102 receives data, for example, a wireless signal transmitted from the user device 104. At Stage 266, the converter device 266 extracts information from the wireless signal for processing. As one example, the converter device 102 may extract information corresponding to the

user's identity and/or the identity of the individual to whom the user device was issued. The extracted information is then provided to the system interface, for example, it is simulated as magnetic striped data to the magnetic card reader. At Stage 268, the system 100 authenticates the user. In one embodiment, if the authentication is successful, the process continues at Stage 270. In this embodiment, if the authentication is unsuccessful, the process returns to Stage 262 where, for example, the user may be prompted to attempt to authenticate again.

Various user authentication approaches may be implemented using the converter device 102. For example, the authentication may be performed locally, that is, without the need for communication between the converter device 102 and the system interface 106 and system processor 110. In one embodiment, the authentication process employs the universal secure registry 118. In further embodiments, the authentication process employs one or more authentication protocols such as public-key cryptography, key exchange protocols, protocols employing one-way functions, and the like that are well known by those of ordinary skill in the art. In other embodiments, however, the authentication may require an exchange of information between the converter device 102 and any of the system interface 106, the network 114, the USR 118 and another database 112. A challenge-response protocol may also be employed alternatively or in combination with any of the preceding authentication approaches.

At Stage 270, the completion of the transaction may be involve any of a wide variety of acts including: authorizing a withdrawal of money from a user's account, permitting the user access to a secure area, permitting a user to view medical information concerning themselves or a third party, or permitting the user to access other confidential information.

In addition, in some embodiments, the process 260 includes Stage 274 where following authentication the converter device 102 receives information associated with the user. The information may, for example, be necessary for the completion of the transaction. For example, where the system 100 is employed in conjunction with a check-authorization process, the converter device 102 may receive an indication that the user has sufficient funds to cover the amount of the check that is presented at a point of sale. Alternatively, or in addition, the information may include indicia related

to the authorized holder of the user device 104, such as a picture ID. The process 260 is completed at Stage 272 – END.

An embodiment, of the converter device 302 is illustrated in FIGS. 30A through 30D. As illustrated in the front view of FIG. 30A, in one embodiment, the converter device 302 includes a housing 380, a substrate 332, and a magnetic stripe 334. In one embodiment, the housing 380 is manufactured from a rigid material, for example, metal or plastic and the converter device 302 is designed to be a hand-held device. FIG. 30B illustrates a side view perspective of an embodiment of the converter device 302, showing an indicating light 348 (e.g., an LED). As described in greater detail above, the indicating light 348 can include a single indicating light or a plurality of indicating lights.

FIGS. 30A-30D illustrate an embodiment where the substrate extends substantially perpendicular from a side of the housing 380, however, the specific angle at which the substrate extends from the housing may vary so long as the housing does not interfere with the insertion of the substrate into, for example, the magnetic card reader 152.

FIG. 30D illustrates a top view of an embodiment of the converter device 302 which includes a display screen (e.g., an LCD display screen) that may provide the user interface 342 or a portion of the user interface of the converter device 302. In one embodiment, the user interface 342 includes a display screen that displays either a black and white or a color image of the individual to whom the user device 104 was issued. It should be recognized that the display screen may provide a wide range of functionality, for example, the display screen may display a variety of data received by the converter device 302 including data represented in alpha numeric format.

The magnetic stripe 334 may be a programmable magnetic stripe such that the converter device 302 provides a magnetic stripe emulator. In one embodiment, as has been described herein, the converter device 302 receives a wireless signal from a user device 104 and provides a time varying signal which emulates data provided by a magnetic-stripe card to a magnetic card reader in response to receiving the information from the wireless signal. In a further embodiment, the information is provided to the magnetic card reader by inserting the magnetic stripe 334 into the magnetic card reader.

RECTIFIED SHEET (RULE 91)
ISA/EP

The various embodiments of a system and method for converting a wireless transaction device to a magnetic stripe emulator device may include any of the following or any combination of the following: a converter device with a processor communicatively coupled to a wireless signal receiver and to a magnetic stripe emulator. The converter device may optionally include an LED. Further the processor may be configured for any combination of the following: control of the LED to indicate that the device is properly aligned with the magnetic card reader, control of the LED to indicate that the device has received authorization for a transaction, and where the converter device includes a power supply, a processor configured to control the LED to indicate that the device has power.

In one embodiment, the information received from the wireless signal by the converter device may include any of a name, a card number, user identification, a device code, amount of credit available, and an expiration date of the card for a transaction.

Further, in various embodiments, the converter device may include an output device that can provide information to a network or to a networked device. In various embodiments, the output device can be configured as a wireless transmitter device, such as an optical transmitter device.

In various embodiments the wireless transmitter device where the wireless transmitter may generally be configured as an RF transmitter device, and in particular, as a Bluetooth transmitter device.

In addition, in various embodiments, the processor can be configured in combination with the output device to provide any of an encrypted output signal, a time-varying encrypted output signal, and in particular, a time-varying public and private key output signal.

In further embodiments, the converter device may include an output device configured as a data port via which the converter device can provide data to a network or a networked device and to receive data from the network or a networked device.

In one embodiment, the converter device may also include an LCD screen for displaying at least some of the data received by the converter device, and a processor configured in combination with the LCD device to display indicia corresponding to the

authorization of a transaction, and in particular, indicia that includes picture information of the cardholder.

In addition to the above described features, the various embodiments of a system and method for converting a wireless transaction device to a magnetic stripe emulator device may include any combination of the following or any combination of the following and the above listed features: the converter device can be configured to communicate with the magnetic card reader via the data port; the wireless receiver and/or processor is configured to decrypt an encrypted wireless signal; the converter device is configured to decrypt a time-varying encrypted wireless signal; the converter device configured to decrypt time-varying public and private key information contained within the wireless signal; the converter device includes a user interface communicatively coupled to the processor; the converter device processor is configured to determine whether the user is authorized to provide the information contained within the wireless signal from data provided through the user interface.

In addition, the following further additional features may be combined alone or in combination with the preceding: the data contained within the wireless signal received by the converter device may include any combination of the following: user I.D. information, biometric information of the user, secret information, (for example, a PIN, a password, or a passcode of the user), or information about an uncounterfeitable token of the user.

In various embodiments, the converter device may include a substrate housing the magnetic stripe emulator, and the substrate may include a programmable magnetic stripe.

In various embodiments, the system employed with the converter device may also include a system interface coupled to a network where the system interface includes a magnetic stripe reading device configured to read a time-varying signal. In a further embodiments, the system interface may be configured to transmit data received from the wireless transaction device to a networked credit card authentication entity also coupled to the network. The system may also include any of a keyboard, a printer, an (LCD) display, and an audio signal transducer.

Although the preceding description is primarily directed to an embodiment of the user device 104 that does not include a magnetic stripe, it should be recognized that

some embodiments of the user device 104 may include a magnetic stripe. In these various embodiments, the converter device 102 may be employed to convert information coded on the magnetic stripe for transmission via another mode of information transmission.

What is claimed is:

CLAIMS

1. A system for validating an identity of a user to enable or prevent an occurrence of an event, the system comprising:

a first device including a wireless transmitter configured to transmit validation information;

a second device including a wireless receiver, the second device configured to receive the validation information and further transmit the validation information; and

a secure system in communication with the second device, the secure system including a database,

wherein the secure system is configured to receive the validation information transmitted from the second device, and

wherein the secure system is further configured to transmit additional information to the second device following a receipt of the validation information to assist the second device in either enabling or preventing the occurrence of the event.

2. The system of claim 1 wherein the second device includes a magnetic stripe emulator communicatively coupled to the wireless receiver and adapted to provide a time-varying signal emulating data provided by a magnetic stripe card to a magnetic card reader, in response to receiving the validation information from the first device.

3. The system of claim 2, wherein the second device includes a processor communicatively coupled to the wireless receiver and to the magnetic stripe emulator.

4. The system of claim 3, wherein the information includes any of a name, a card number, user identification, a device code, an amount of credit available, and an expiration date of the card for a transaction.

5. The system of claim 3, wherein the second device includes a LCD screen for displaying at least some of the information received by the second device.

6. The system of claim 5, wherein the processor is configured in combination with the LCD device to display indicia corresponding to the authorization of a transaction.

7. The system of claim 6, wherein the indicia includes picture information of a user of the first device.

8. The system of claim 2, wherein the second device includes an output device configured to transmit the validation information.

9. The system of claim 8, wherein the second device is configured to communicate with the magnetic card reader via the output device.

10. The system of claim 1, wherein the second device is configured to decrypt an encrypted wireless signal transmitted from the first device.

11. The system of claim 10, wherein the second device is configured to decrypt a time-varying encrypted wireless signal transmitted from the first device.

12. The system of claim 11, wherein the second device is configured to decrypt time-varying public and private key information contained within the wireless signal.

13. The system of claim 3, wherein the second device includes a user interface communicatively coupled to the processor.

14. The system of claim 13, wherein the processor is configured to determine whether the user is authorized to provide the information transmitted from the first device from data provided through the user interface.

15. The system of claim 1, wherein the second device is configured to determine whether the user is authorized to provide the validation information from the validation information transmitted from the first device.

16. The system of claim 15, wherein the validation information transmitted from the first device comprises user I.D. information.

17. The system of claim 15, wherein the validation information transmitted from the first device comprises biometric information of the user.

18. The system of claim 15, wherein the validation information transmitted from the first device comprises any of secret information, a PIN, a password, or a passcode of the user.

19. The system of claim 15, wherein the data transmitted from the first device comprises information about an uncounterfeitable token of the user.

20. The system of claim 2, wherein the second device includes a substrate housing the magnetic stripe emulator.

21. The system of claim 20, wherein the substrate comprises a programmable magnetic stripe.

22. The system of claim 3, wherein the processor is configured to provide binary data to the magnetic stripe emulator.

23. The system of claim 1, further wherein the secure system is configured to transmit data received from the second device to a networked credit card validation entity coupled to the secure system.

24, The system of claim 1, wherein the first device is configured to receive authentication information of the user.

25. The system of claim 24, wherein the authentication information includes biometric information of the user.

26. The system of claim 25, wherein the first device is configured to generate a non-predictable signal from the biometric information.

27. The system of claim 26, wherein the first device is further configured to generate a time varying non-predictable signal from the biometric information.

28. The system of claim 24, wherein the first device is configured to authenticate the authentication information of the user and to allow or not allow operation of the first device based on the authentication information.

29. The system of claim 28, wherein the authentication information includes biometric information of the user.

30. The system of claim 29, wherein the biometric information of the user comprises a voice signature of the user.

31. The system of claim 30, wherein the biometric information of the user comprises a fingerprint of the user.

32. The system of claim 31, wherein the authentication information of the user comprises a PIN.

33. The system of claim 1, wherein the secure system is configured to access authenticating indicia of the user; and to transmit the authenticating indicia from the secure database to the second device.

34. The system of claim 33, further comprising an act of generating a non-predictable code at the second device from the first authentication information.

35. The system of claim 34, wherein the non-predictable code is a time-varying code.

36. The system of claim 35, wherein the second device is configured to transmit the time-varying code to the secure system; and wherein the secure system is configured to determine from the time-varying code the authentication information.

37. The system of claim 36, wherein communication between the second device and the secure system is over any of a wide area network, the Internet, and a wireless network.

38. The system of claim 1, wherein the second device includes a processor, wherein the second device includes a memory configured to store public keys of a plurality of users, and wherein the wireless receiver and/or processor is configured to decrypt an encrypted wireless signal transmitted from the first device.

39. The system of claim 38, wherein the second device is configured to look up a public key of the user and to decrypt the authentication information with the public key of the user.

40. The system of claim 39, wherein the authentication information includes any of a name, an identification number, an e-mail address, and at least a portion of a picture of the user.

41. The system of claim 38, wherein the second device is configured to periodically update the public keys of the plurality of users.

42. The system of claim 1, wherein the second device includes a processor, wherein the second device includes a memory configured to store picture data, wherein the wireless receiver and/or processor is configured to decrypt an encrypted wireless signal transmitted from the first device, and wherein the second device is configured to access the picture data based on the decrypted authentication information.

43. The system of claim 42, wherein picture information of the user may be viewed with the second device.

44. The system of claim 42, wherein the encrypted wireless signal transmitted from the first device includes a first portion of the picture information of the user. .

45. The system of claim 44, wherein the second device is configured to access a second portion of the picture information of the user and to combine the first portion of the picture and the second portion of the picture.

46. The system of claim 1, wherein the second device includes a processor, wherein the wireless receiver and/or processor is configured to decrypt an encrypted wireless signal transmitted from the first device, and wherein the encrypted wireless signal includes encrypted authentication information which has been encrypted with a first private key of the user.

47. The system of claim 1, wherein the second device includes a processor, wherein the wireless receiver and/or processor is configured to decrypt an encrypted wireless signal transmitted from the first device, and wherein the second device is configured to request the encrypted wireless signal from the first device.

48. The system of claim 1, wherein the first device is configured to transmit a first wireless signal including first encrypted authentication information.

49. The system of claim 48, wherein the first device includes a first processor, a first biometric detector and a first memory,

wherein the first processor is configured to compare stored biometric data with detected biometric data of the user and configured to enable or disable use of the first device based on a result of the comparison and configured to encrypt first authentication information with a first private key into first encrypted authentication information,

wherein the first biometric detector is configured for detecting biometric data of the user, and

wherein the first memory is configured to store biometric data of the user, a private key of the user authorized to use the first device, and the first authentication information.

50. The system of claim 49, wherein the second device includes a second processor, a second biometric detector and a second memory,

wherein the second biometric detector configured to detect biometric data of a user of the second device, and

wherein, the second memory configured to store biometric data of the user of the second device and a plurality of public keys of a plurality of users associated with a plurality of devices configured to transmit authentication information to the second device.

51. The system of claim 50, wherein the biometric data is fingerprint data and each biometric detector is a fingerprint sensor.

52. The system of claim 50, wherein the second processor is configured to use the public key of the user to decrypt the encrypted first authentication information.

53. The system of claim 49, wherein the first encrypted authentication information includes an encrypted DES key of the user.

54. The system of claim 53, wherein the first encrypted authentication information also includes a DES key encrypted portion of biometric data of the user.

55. The system of claim 54, wherein the portion of biometric data is a portion of a digital image of the user.

56. The system of claim 49, wherein the first encrypted authentication information comprises a digital signature of the user.

57. The system of claim 49, wherein the first encrypted authentication information comprises a one-time random code of the user.

58. The system of claim 50, wherein the second memory also comprises a portion of authentication data of a plurality of first users.

59. The system of claim 58, wherein the biometric data of the plurality of first users comprises at least a portion of a digital image of the plurality of first users.

60. The system of claim 50, wherein the first device can be any of a handheld device, a cell phone, a PDA, a PC, a credit card sized device, an ID badge, a key FOB, a passport, and a wrist watch.

61. The system of claim 50, wherein the database comprises biometric information of a plurality of users.

62. The system of claim 61, wherein the biometric information of the plurality of users includes at least a portion of digital image data of the plurality of users.

63. A method employing a system to validate an identity of a user to enable or prevent an occurrence of an event, the system including a first device, a second device and a secure system including a database, the method comprising acts of:

receiving at the second device validation information wirelessly transmitted from the first device;

communicating the validation information from the second device to the secure system; and

receiving at the second device additional information from the secure system, wherein the additional information assists the second device in either enabling or preventing the occurrence of the event.

64. The method of claim 63 wherein the second device includes a magnetic stripe emulator communicatively coupled to the wireless receiver, and wherein the method

further comprises an act of providing a time-varying signal emulating data provided by a magnetic stripe card to a magnetic card reader, in response to receiving the validation information from the first device.

65. The method of claim 64, wherein the second device includes a processor communicatively coupled to the wireless receiver and to the magnetic stripe emulator.

66. The method of claim 65, wherein the information includes any of a name, a card number, user identification, a device code, an amount of credit available, and an expiration date of the card for a transaction.

67. The method of claim 65, wherein the second device includes a LCD screen, and wherein the method further comprises an act of displaying at least some of the information received by the second device on the LCD screen.

68. The method of claim 67, wherein the processor is configured in combination with the LCD device to display indicia corresponding to the authorization of a transaction.

69. The method of claim 68, further comprising an act of including picture information of a user of the first device in the indicia.

70. The method of claim 64, wherein the second device includes an output device, and wherein the method further comprises an act of transmitting the validation information from the second device with the output device.

71. The method of claim 70, further comprising an act of communicating with the magnetic card reader via the output device.

72. The method of claim 65, further comprising an act of decrypting an encrypted wireless signal transmitted from the first device with the second device.

73. The method of claim 72 further comprising an act of decrypting, with the second device, a time-varying encrypted wireless signal transmitted from the first device.

74. The method of claim 73, further comprising an act of decrypting, with the second device, information encrypted with a private key contained within the wireless signal.

75. The method of claim 65, wherein the second device includes a user interface communicatively coupled to the processor.

76. The method of claim 75, further comprising an act of determining with the processor whether the user is authorized to provide the validation information transmitted from the first device from data provided through the user interface.

77. The method of claim 65, further comprising an act of determining with the processor whether the user is authorized to provide the validation information from the validation information transmitted from the first device.

78. The method of claim 77, further comprising an act of including user I.D. information in the validation information transmitted from the first device.

79. The method of claim 77, further comprising an act of including biometric information of the user in the validation information transmitted from the first device.

80. The method of claim 77, further comprising an act of including any of secret information, a PIN, a password, or a passcode of the user in the validation information transmitted from the first device.

81. The method of claim 77, further comprising an act of including information about an uncounterfeitable token of the user in the data transmitted from the first device.

82. The method of claim 64, wherein the second device includes a substrate housing the magnetic stripe emulator.

83. The method of claim 82, wherein the substrate comprises a programmable magnetic stripe.

84. The method of claim 65, further comprising an act of providing binary data to the magnetic stripe emulator with the processor.

85. The method of claim 63, further comprising an act of, with the secure system, transmitting data received from the second device to a networked credit card validation-information entity coupled to the secure system.

86. The method of claim 63, further comprising an act of receiving, with the first device, authentication information of the user.

87. The method of claim 86, further comprising an act of including the biometric information of the user in the authentication information.

88. The method of claim 87, further comprising an act of generating, with the first device, a non-predictable signal from the biometric information.

89. The method of claim 88, further comprising an act of generating, with the first device, a time varying non-predictable signal from the biometric information.

90. The method of claim 86, further comprising acts of:

authenticating, with the first device, the authentication information of the user; and

allowing or not allowing operation of the first device based on the authentication information.

91. The method of claim 90, further comprising an act of including biometric information of the user in the authentication information.

92. The method of claim 91, wherein the biometric information of the user comprises a voice signature of the user.

93. The method of claim 92, wherein the biometric information of the user comprises a fingerprint of the user.

94. The method of claim 93, wherein the authentication information of the user comprises a PIN.

95. The method of claim 63, wherein the secure system is configured to accessing, with the secure system, authenticating indicia of the user; and to transmit the authenticating indicia from the secure database to the second device.

96. The method of claim 95, further comprising an act of generating a non-predictable code at the second device from the first authentication information.

97. The method of claim 96, wherein the non-predictable code is a time-varying code.

98. The method of claim 97, further comprising an act of transmitting the time-varying code to the secure system with the second device; and determining from the time-varying code the authentication information with the secure system.

99. The method of claim 98, further comprising an act of communicating between the second device and the secure system over any of a wide area network, the Internet, and a wireless network.

100. The method of claim 63, wherein the second device includes a processor and a memory, and wherein the method further comprises acts of:

storing public keys of a plurality of users in the memory; and

decrypting an encrypted wireless signal transmitted from the first device using the wireless receiver and/or processor.

101. The method of claim 100, further comprising acts of:

looking up a public key of the user with the second device; and

decrypting, with the second device, the authentication information with the public key of the user.

102. The method of claim 101, wherein the authentication information includes any of a name, an identification number, an e-mail address, and at least a portion of a picture of the user.

103. The method of claim 100, further comprising an act of periodically updating the public keys of the plurality of users with the second device.

104. The method of claim 63, wherein the second device includes a processor, and a memory configured to store picture data, and wherein the method further comprises acts of:

decrypting, with the wireless receiver and/or processor, an encrypted wireless signal transmitted from the first device, and

accessing, with the second device, the picture data based on the decrypted authentication information.

105. The method of claim 104, further comprising an act of viewing the picture information of the user with the second device.

106. The method of claim 104, further comprising an act of including a first portion of the picture information of the user in the encrypted wireless signal transmitted from the first device.

107. The method of claim 106, further comprising acts of:

accessing a second portion of the picture information of the user with the second device; and

combining the first portion of the picture and the second portion of the picture with the second device.

108. The method of claim 63, wherein the second device includes a processor, and wherein the method includes acts of:

decrypting an encrypted wireless signal transmitted from the first device with the wireless receiver and/or processor;

encrypting the authentication information with a first private key of the user; and

including the encrypted authentication information in the encrypted wireless signal.

109. The method of claim 63, wherein the second device includes a processor, and wherein the method further comprises acts of:

decrypting an encrypted wireless signal transmitted from the first device with the wireless receiver and/or processor, and

requesting the encrypted wireless signal from the first device with the second device.

110. The method of claim 63, further comprising an act of transmitting a first wireless signal including first encrypted authentication information with the first device.

111. The method of claim 110, wherein the first device includes a first processor, a first biometric detector and a first memory, and wherein the method further comprises acts of:

comparing stored biometric data with detected biometric data of the user with the first processor;

enabling or disabling use of the first device based on a result of the act of comparing with the first processor;

encrypting first authentication information with a first private key into first encrypted authentication information with the first processor;

detecting biometric data of the user with the first biometric detector; and

storing biometric data of the user, a private key of the user authorized to use the first device, and the first authentication information in the memory.

112. The method of claim 111, wherein the second device includes a second processor, a second biometric detector and a second memory, and wherein the method further comprises acts of:

detecting biometric data of a user of the second device with the second biometric detector,

storing, in the second memory, biometric data of the user of the second device and a plurality of public keys of a plurality of users associated with a plurality of devices configured to transmit authentication information to the second device.

113. The method of claim 112, wherein the biometric data is fingerprint data and each biometric detector is a fingerprint sensor.

114. The method of claim 112, further comprising an act of decrypting the encrypted first authentication information with the public key of the user.

115. The method of claim 111, wherein the first encrypted authentication information includes an encrypted DES key of the user.

116. The method of claim 115, wherein the first encrypted authentication information also includes a DES key encrypted portion of biometric data of the user.

117. The method of claim 116, wherein the portion of biometric data is a portion of a digital image of the user.

118. The method of claim 111, wherein the first encrypted authentication information comprises a digital signature of the user.

119. The method of claim 111, wherein the first encrypted authentication information comprises a one-time random code of the user.

120. The method of claim 112, further comprising an act of including a portion of authentication data of a plurality of first users in the second memory.

121. The method of claim 120, wherein the biometric data of the plurality of first users comprises at least a portion of a digital image of the plurality of first users.

122. The method of claim 112, wherein the first device can be any of a handheld device, a cell phone, a PDA, a PC, a credit card sized device, an ID badge, a key FOB, a passport, and a wrist watch.

123. The method of claim 112, further comprising an act of including biometric information of a plurality of users in the database.

124. The method of claim 123, further comprising an act of including at least a portion of digital image data of the plurality of users in the biometric information of the plurality of users.

125. The system of claim 1, wherein the second device communicates an amount of purchase by a user of the first device with the secure system and receives any of an approval or denial for the purchase without the credit card number, a credit card number of a user and an approval or denial of the purchase, and an available balance of the user.

126. The system of claim 1, wherein the second device validates the information transmitted from the first device and transmits the validated information to the secure system, and wherein the secure system provides the additional information to enable or prevents the occurrence of the event based on the validated information as communicated by the second device.

127. The system of claim 1, wherein the secure system validates the information transmitted from the second device and wherein the secure system provides the additional information to enable or prevents the occurrence of the event based on the validated information.

128. The system of claim 1, wherein the second device validates the information transmitted from the first device based on the validation information transmitted from the first device and the additional information provided by the secure system, and wherein the second device enables or prevents the occurrence of the event based on the validation information and the additional information.

129. The method of claim 63, further comprising acts of communicating with the second device an amount of purchase by a user of the first device to the secure system and receiving from the secure system any of an approval or denial for the purchase without the credit card number, a credit card number of a user and an approval or denial of the purchase, and an available balance of the user.

130. The method of claim 63, further comprising acts of validating with the second device the information transmitted from the first device and transmitting the validated information to the secure system, and receiving from the secure system the additional information to enable or prevent the occurrence of the event based on the validated information.

131. The method of claim 63, further comprising the act of validating with the secure system information transmitted from the second device and providing with the secure system the additional information to enable or prevents the occurrence of the event based on the validated information.

132. The method of claim 63, further comprising validating with the second device the information transmitted from the first device based on the validation information transmitted from the first device and the additional information provided by the secure

system, and enabling or preventing with the second device the occurrence of the event based on the validation information and the additional information.

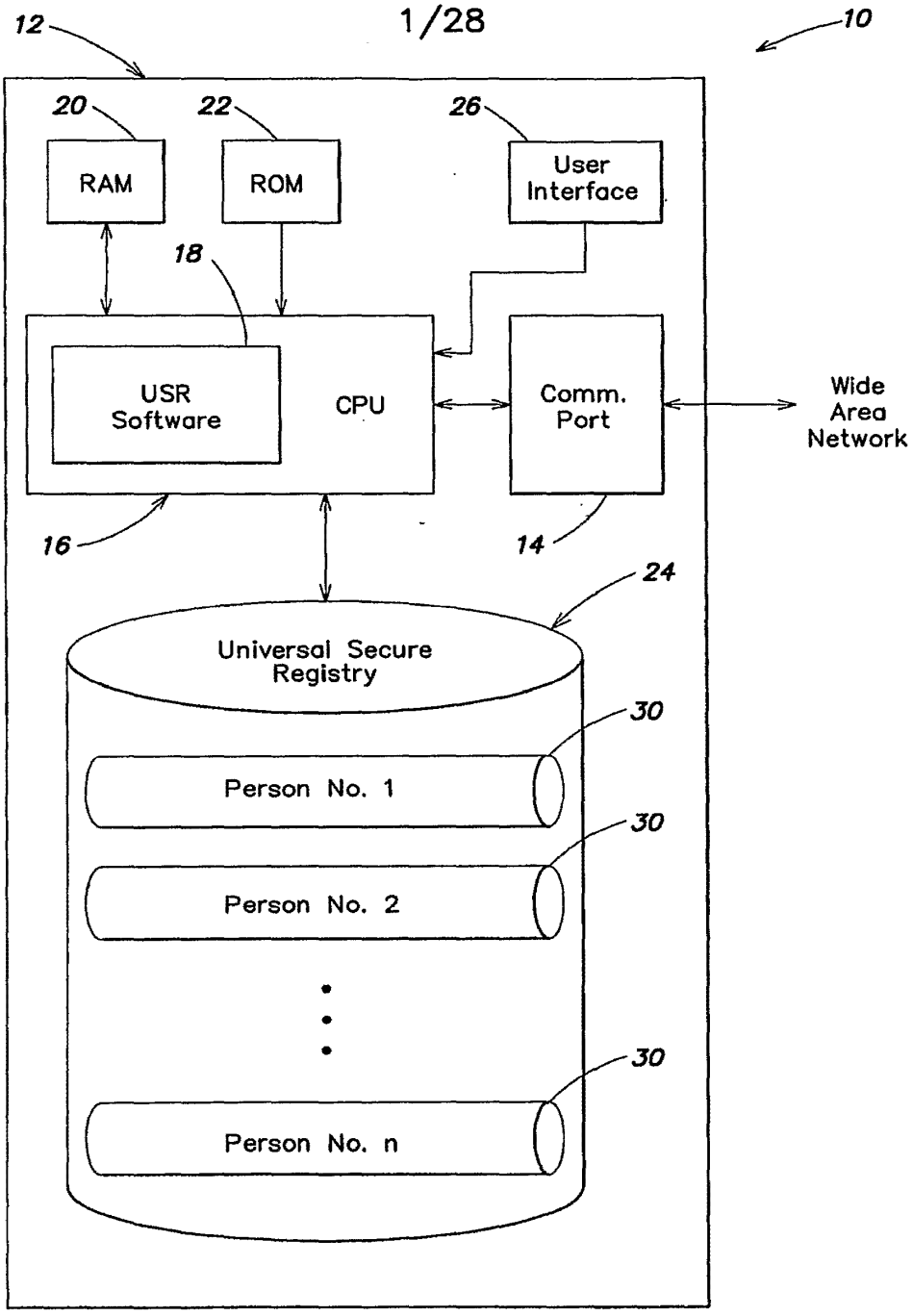

12
10
20
22
26
RAM
ROM
User Interface
18
USR Software
CPU
Comm. Port
Wide Area Network
16
14
24
Universal Secure Registry
30
Person No. 1
30
Person No. 2
30
Person No. n

FIG. 1

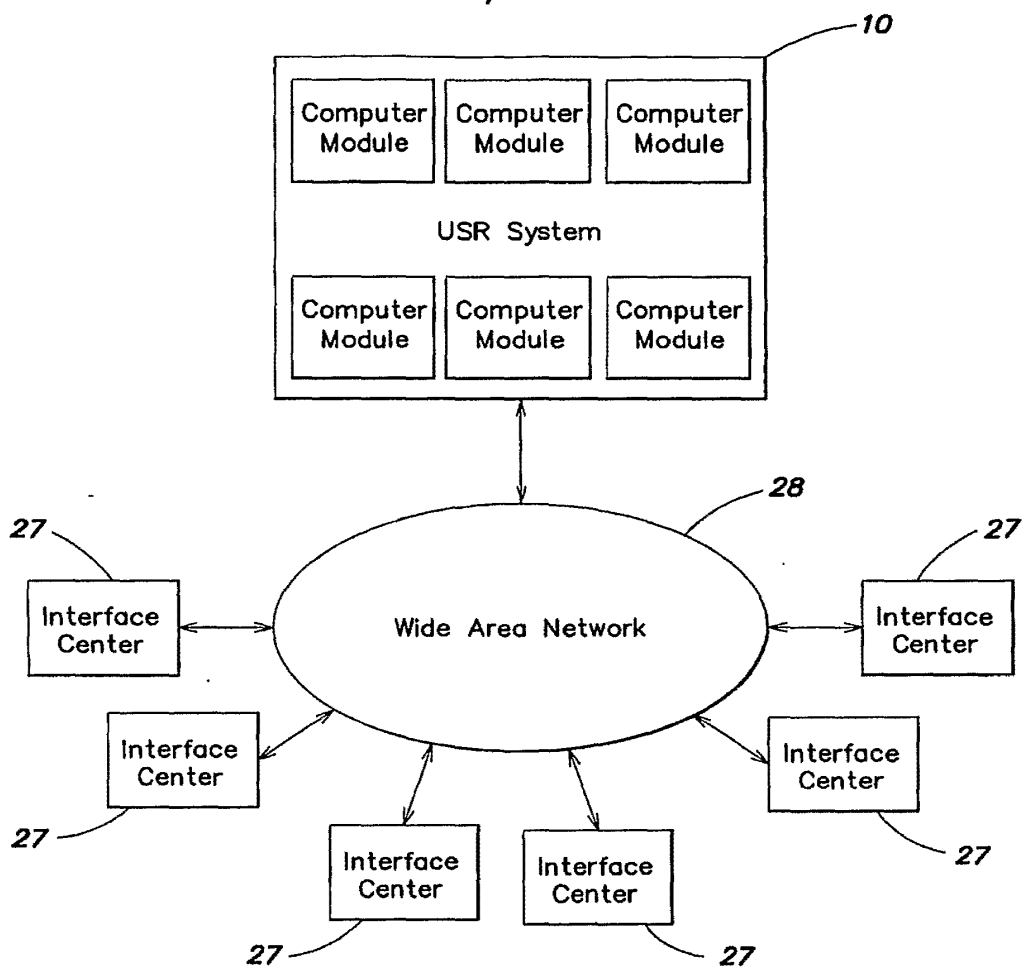

10
Computer Module
Computer Module
Computer Module
USR System
Computer Module
Computer Module
Computer Module
28
27
Interface Center
Wide Area Network
27
Interface Center
Interface Center
Interface Center
27
27
Interface Center
Interface Center
27
27

FIG. 2

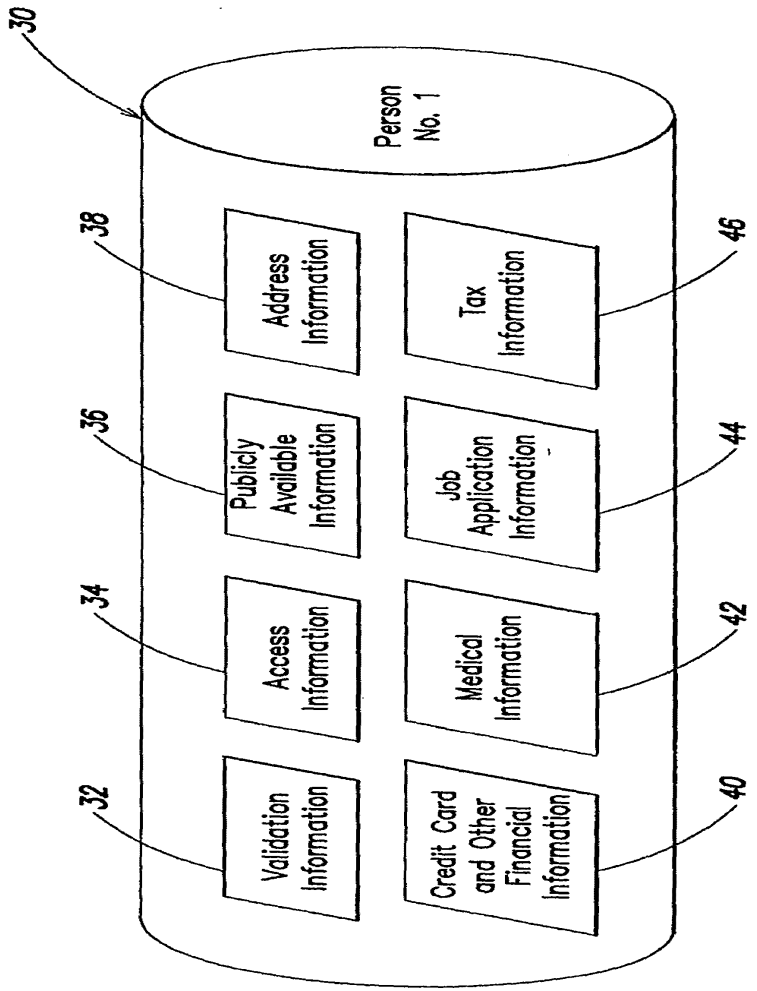

30
Person No. 1
38
Address Information
36
Publicly Available Information
34
Access Information
32
Validation Information
46
Tax Information
44
Job Application Information
42
Medical Information
40
Credit Card and Other Financial Information

FIG. 3

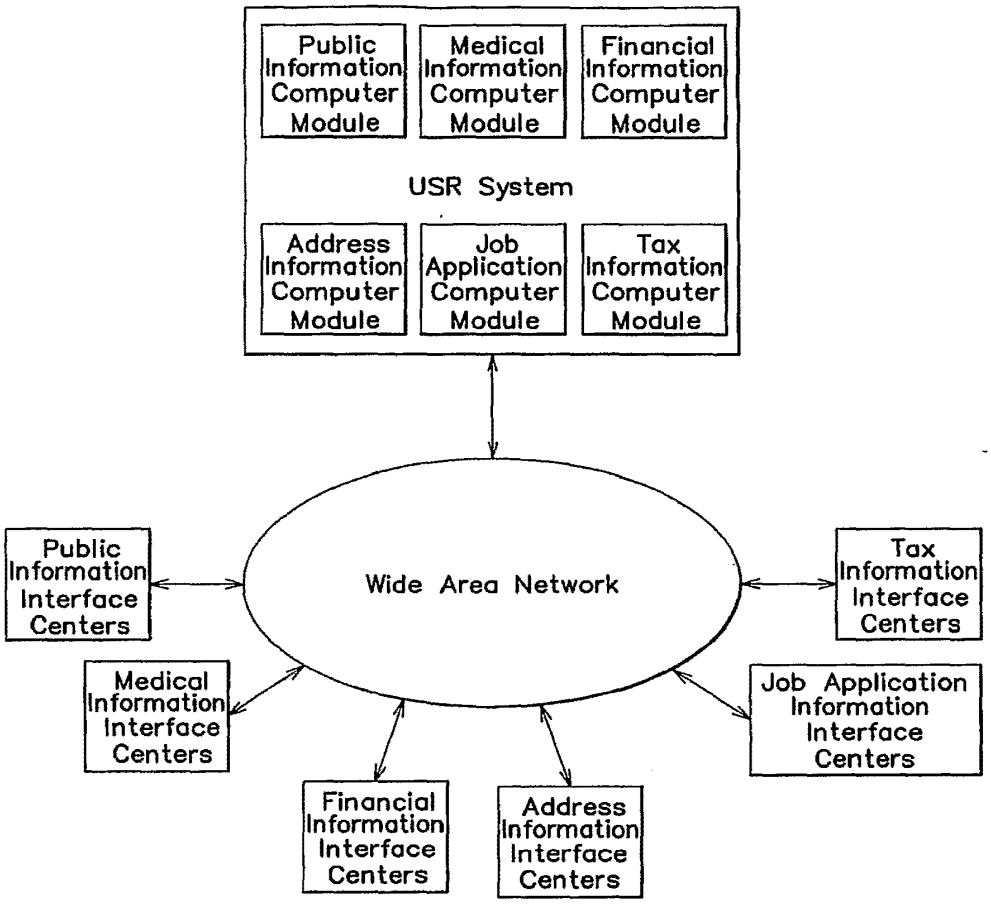

Public Information Computer Module
Medical Information Computer Module
Financial Information Computer Module
USR System
Address Information Computer Module
Job Application Computer Module
Tax Information Computer Module
Wide Area Network
Public Information Interface Centers
Tax Information Interface Centers
Medical Information Interface Centers
Job Application Information Interface Centers
Financial Information Interface Centers
Address Information Interface Centers

FIG. 4

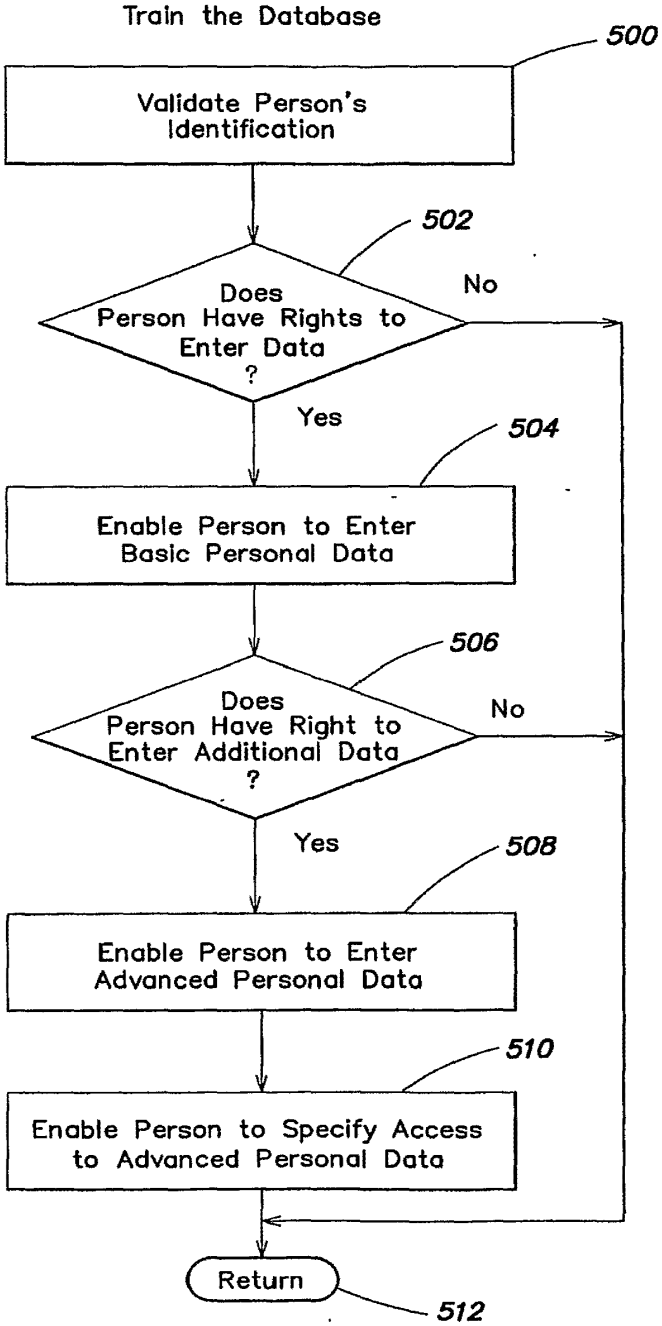

Train the Database
500
Validate Person's Identification
502
Does Person Have Rights to Enter Data ?
No
Yes
504
Enable Person to Enter Basic Personal Data
506
Does Person Have Right to Enter Additional Data ?
No
Yes
508
Enable Person to Enter Advanced Personal Data
510
Enable Person to Specify Access to Advanced Personal Data
Return
512

FIG. 5

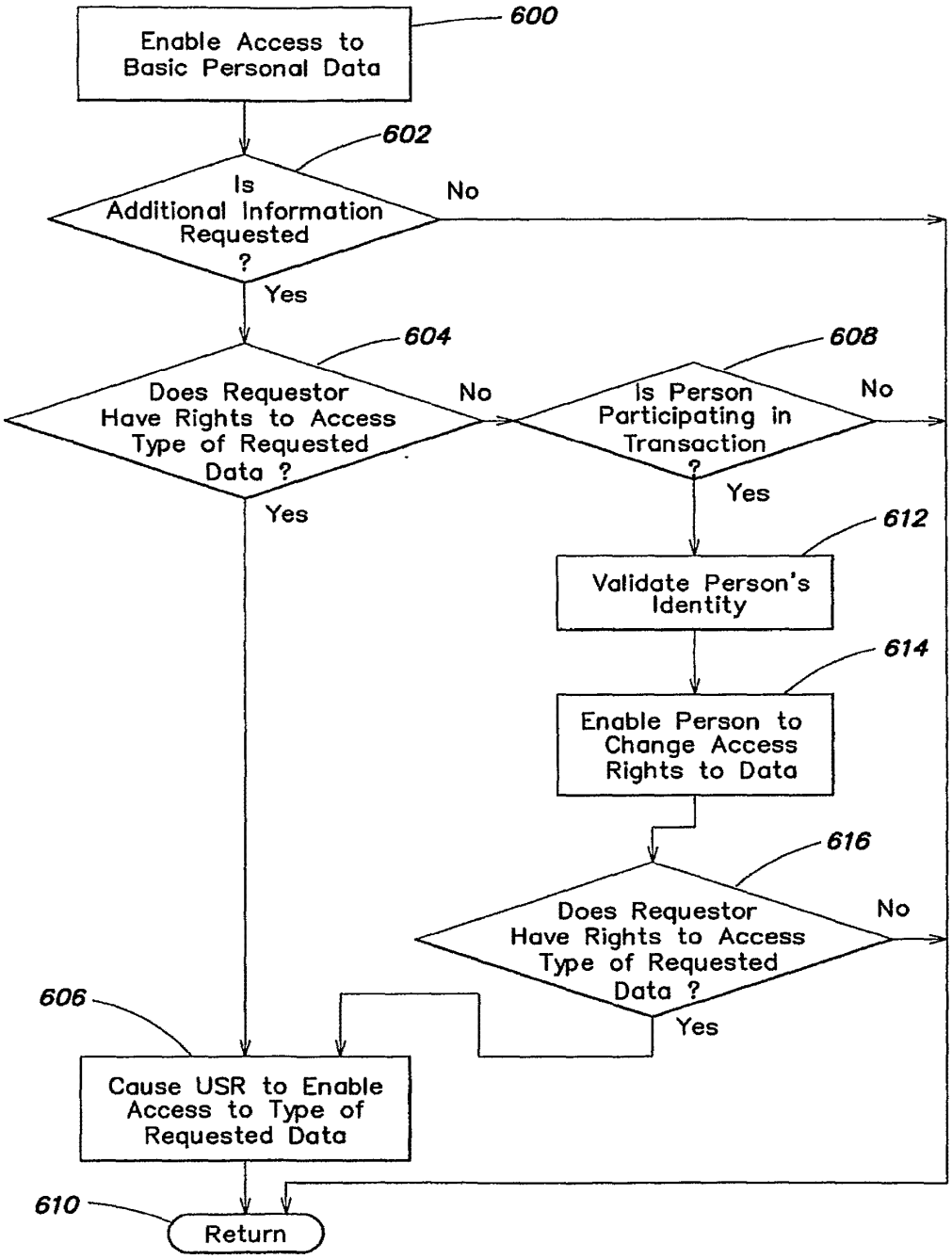

600
Enable Access to Basic Personal Data
602
Is Additional Information Requested ?
No
Yes
604
Does Requestor Have Rights to Access Type of Requested Data ?
No
Yes
608
Is Person Participating in Transaction ?
No
Yes
612
Validate Person's Identity
614
Enable Person to Change Access Rights to Data
616
Does Requestor Have Rights to Access Type of Requested Data ?
No
Yes
606
Cause USR to Enable Access to Type of Requested Data
610
Return

FIG. 6

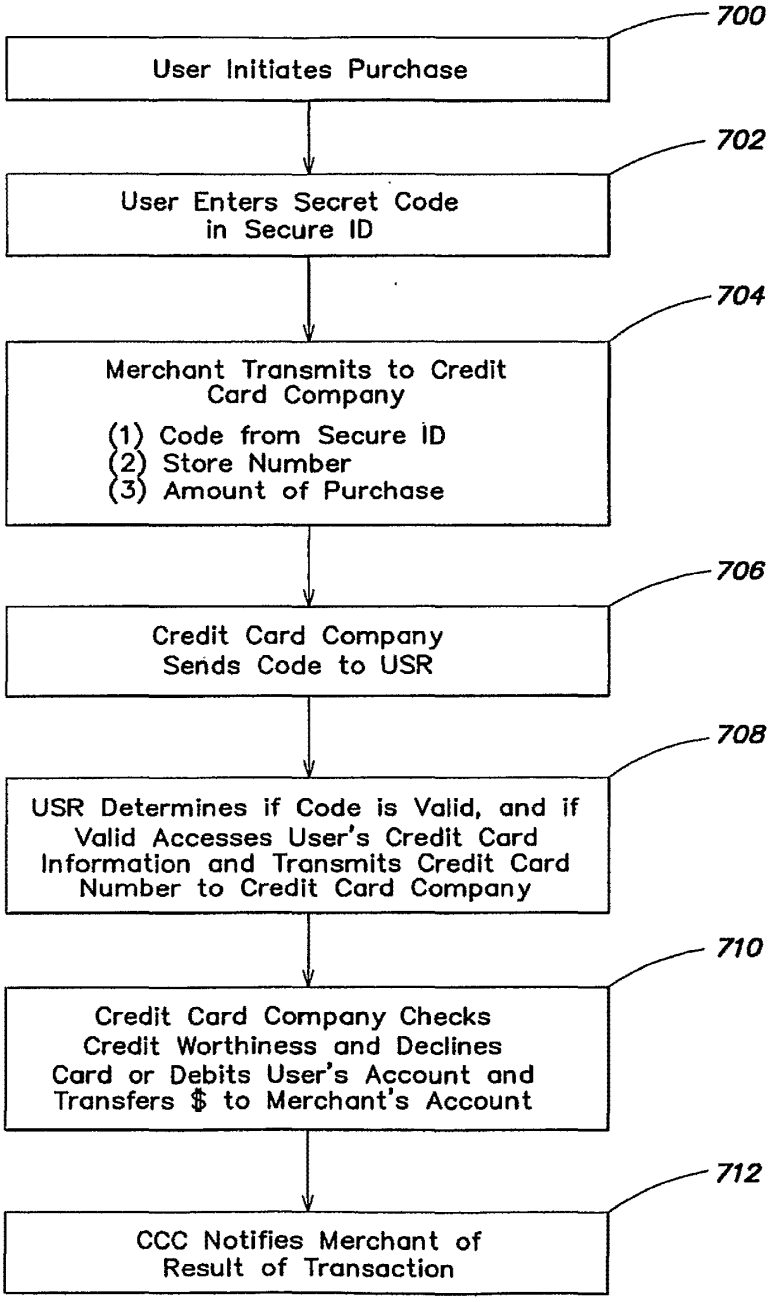

700
User Initiates Purchase
702
User Enters Secret Code in Secure ID
704
Merchant Transmits to Credit Card Company
(1) Code from Secure ID
(2) Store Number
(3) Amount of Purchase
706
Credit Card Company Sends Code to USR
708
USR Determines if Code is Valid, and if Valid Accesses User's Credit Card Information and Transmits Credit Card Number to Credit Card Company
710
Credit Card Company Checks Credit Worthiness and Declines Card or Debits User's Account and Transfers $ to Merchant's Account
712
CCC Notifies Merchant of Result of Transaction

FIG. 7

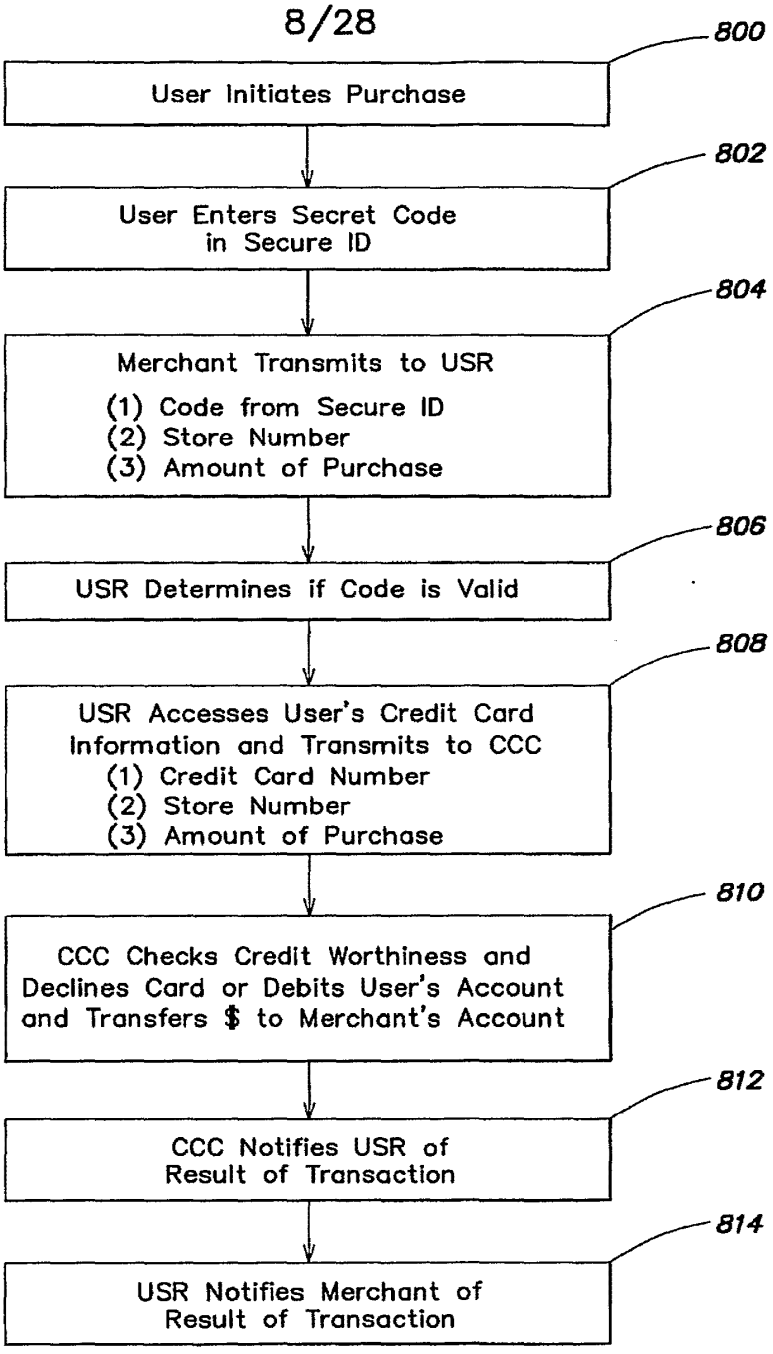

800
User Initiates Purchase
802
User Enters Secret Code in Secure ID
804
Merchant Transmits to USR
(1) Code from Secure ID
(2) Store Number
(3) Amount of Purchase
806
USR Determines if Code is Valid
808
USR Accesses User's Credit Card Information and Transmits to CCC
(1) Credit Card Number
(2) Store Number
(3) Amount of Purchase
810
CCC Checks Credit Worthiness and Declines Card or Debits User's Account and Transfers $ to Merchant's Account
812
CCC Notifies USR of Result of Transaction
814
USR Notifies Merchant of Result of Transaction

FIG. 8

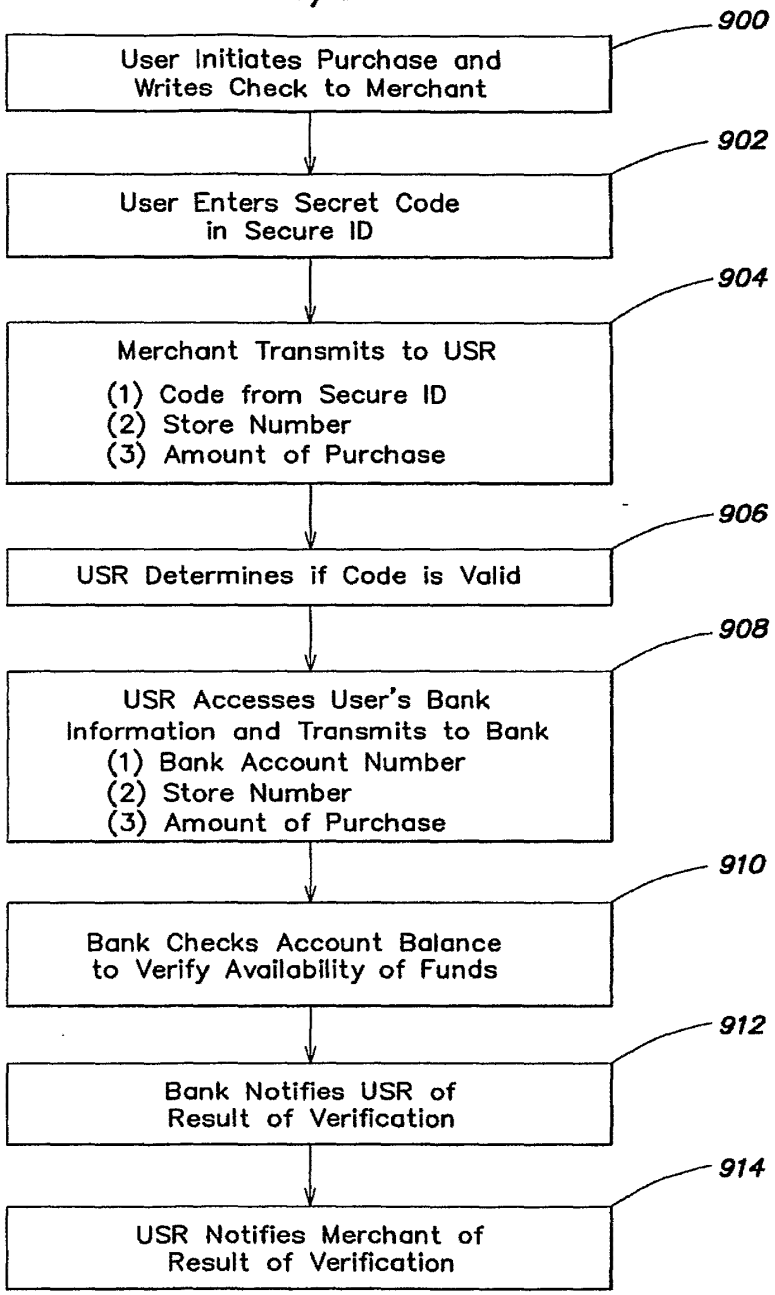

900
User Initiates Purchase and Writes Check to Merchant
902
User Enters Secret Code in Secure ID
904
Merchant Transmits to USR
(1) Code from Secure ID
(2) Store Number
(3) Amount of Purchase
906
USR Determines if Code is Valid
908
USR Accesses User's Bank Information and Transmits to Bank
(1) Bank Account Number
(2) Store Number
(3) Amount of Purchase
910
Bank Checks Account Balance to Verify Availability of Funds
912
Bank Notifies USR of Result of Verification
914
USR Notifies Merchant of Result of Verification

FIG. 9

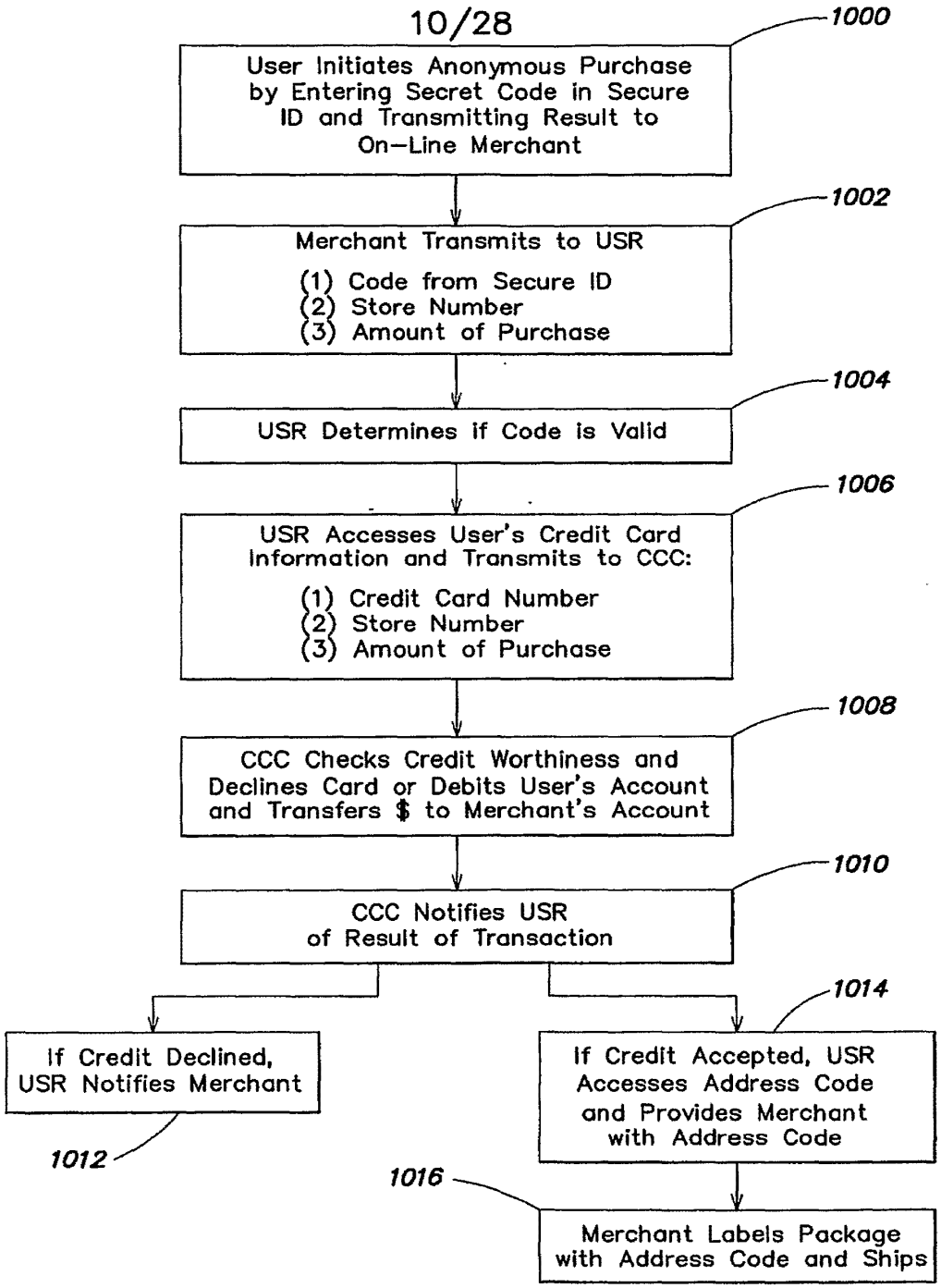

1000
User Initiates Anonymous Purchase by Entering Secret Code in Secure ID and Transmitting Result to On-Line Merchant
1002
Merchant Transmits to USR
(1) Code from Secure ID
(2) Store Number
(3) Amount of Purchase
1004
USR Determines if Code is Valid
1006
USR Accesses User's Credit Card Information and Transmits to CCC:
(1) Credit Card Number
(2) Store Number
(3) Amount of Purchase
1008
CCC Checks Credit Worthiness and Declines Card or Debits User's Account and Transfers $ to Merchant's Account
1010
CCC Notifies USR of Result of Transaction
1014
If Credit Declined, USR Notifies Merchant
1012
If Credit Accepted, USR Accesses Address Code and Provides Merchant with Address Code
1016
Merchant Labels Package with Address Code and Ships

FIG. 10

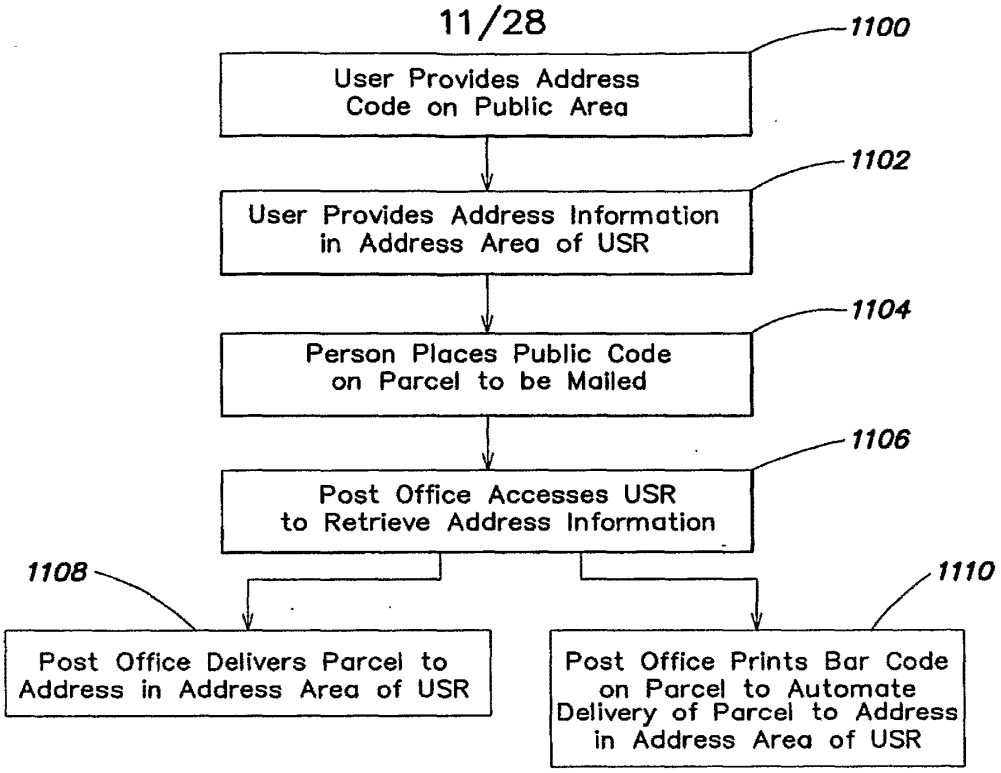

1100
User Provides Address Code on Public Area
1102
User Provides Address Information in Address Area of USR
1104
Person Places Public Code on Parcel to be Mailed
1106
Post Office Accesses USR to Retrieve Address Information
1108
Post Office Delivers Parcel to Address in Address Area of USR
1110
Post Office Prints Bar Code on Parcel to Automate Delivery of Parcel to Address in Address Area of USR

FIG. 11

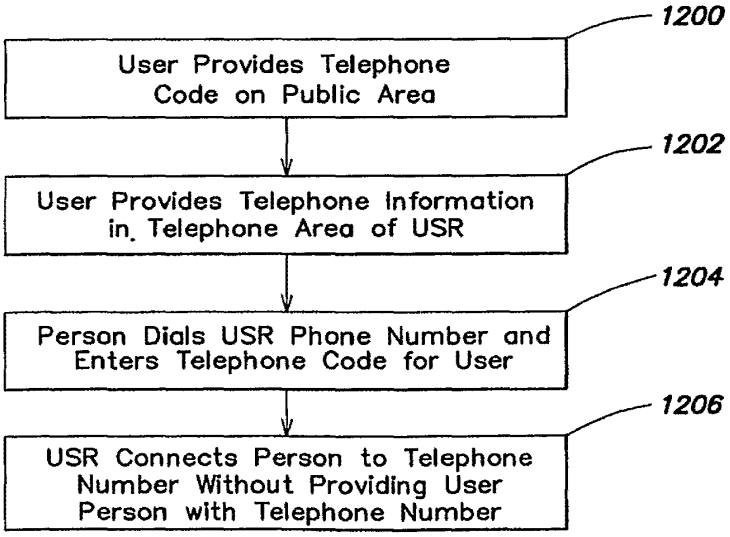

1200
User Provides Telephone Code on Public Area
1202
User Provides Telephone Information in Telephone Area of USR
1204
Person Dials USR Phone Number and Enters Telephone Code for User
1206
USR Connects Person to Telephone Number Without Providing User Person with Telephone Number

FIG. 12

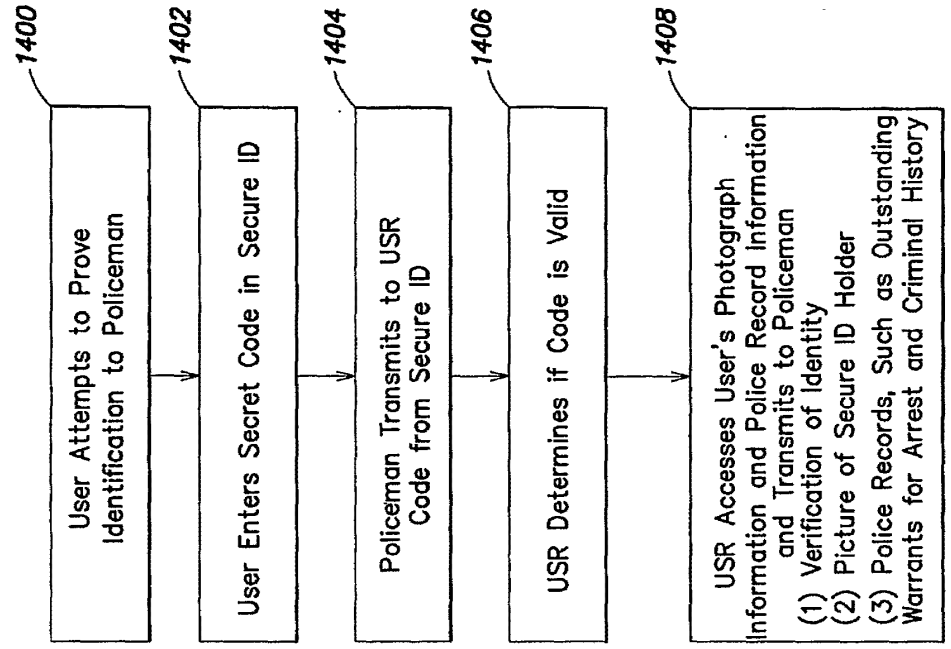

1400
User Attempts to Prove Identification to Policeman
1402
User Enters Secret Code in Secure ID
1404
Policeman Transmits to USR Code from Secure ID
1406
USR Determines if Code is Valid
1408
USR Accesses User's Photograph Information and Police Record Information and Transmits to Policeman
(1) Verification of Identity
(2) Picture of Secure ID Holder
(3) Police Records, Such as Outstanding Warrants for Arrest and Criminal History

FIG. 14

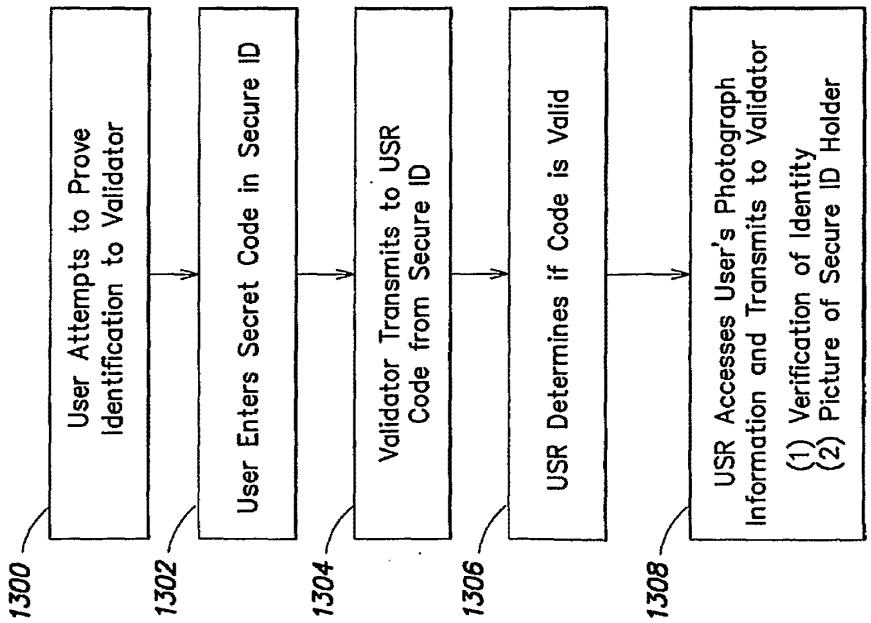

1300
User Attempts to Prove Identification to Validator
1302
User Enters Secret Code in Secure ID
1304
Validator Transmits to USR Code from Secure ID
1306
USR Determines if Code is Valid
1308
USR Accesses User's Photograph Information and Transmits to Validator
(1) Verification of Identity
(2) Picture of Secure ID Holder

FIG. 13

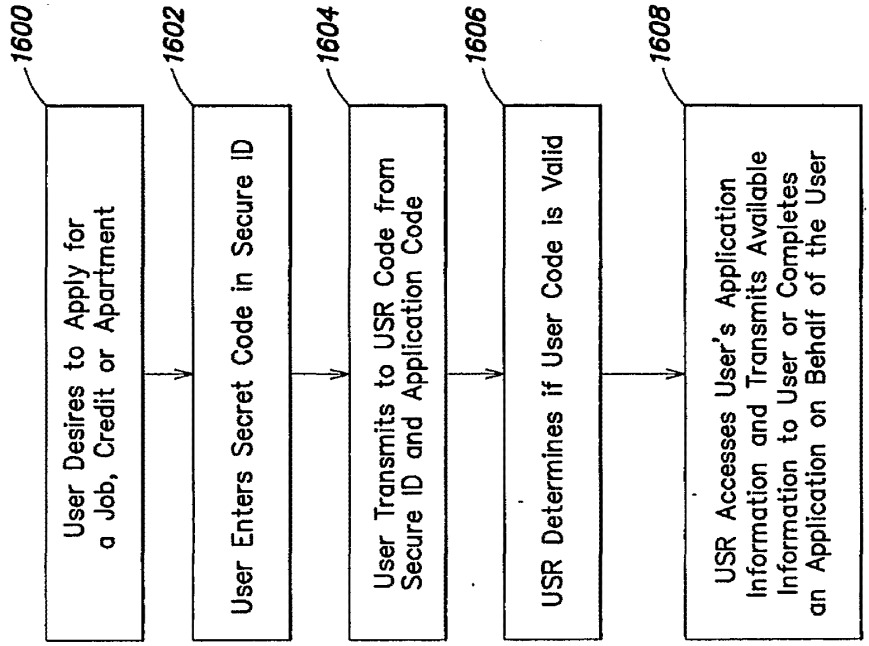

1600
User Desires to Apply for a Job, Credit or Apartment
1602
User Enters Secret Code in Secure ID
1604
User Transmits to USR Code from Secure ID and Application Code
1606
USR Determines if User Code is Valid
1608
USR Accesses User's Application Information and Transmits Available Information to User or Completes an Application on Behalf of the User

FIG. 16

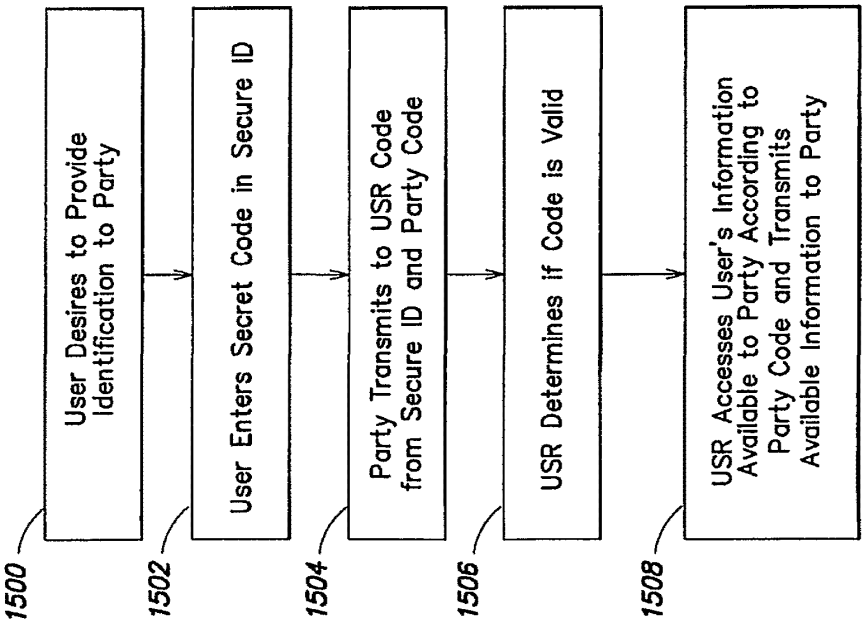

1500
User Desires to Provide Identification to Party
1502
User Enters Secret Code in Secure ID
1504
Party Transmits to USR Code from Secure ID and Party Code
1506
USR Determines if Code is Valid
1508
USR Accesses User's Information Available to Party According to Party Code and Transmits Available Information to Party

FIG. 15

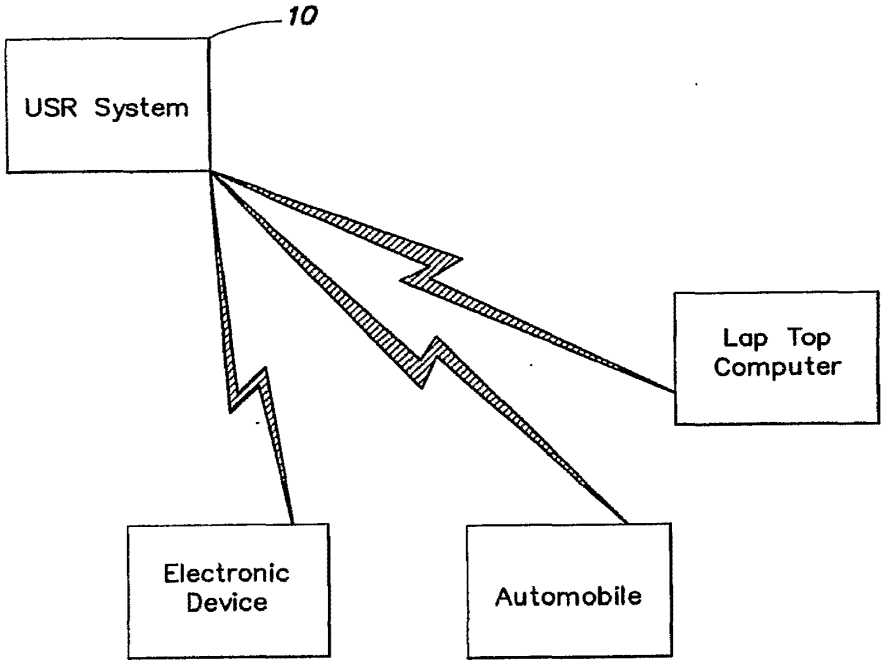

10
USR System
Lap Top Computer
Electronic Device
Automobile

FIG. 17

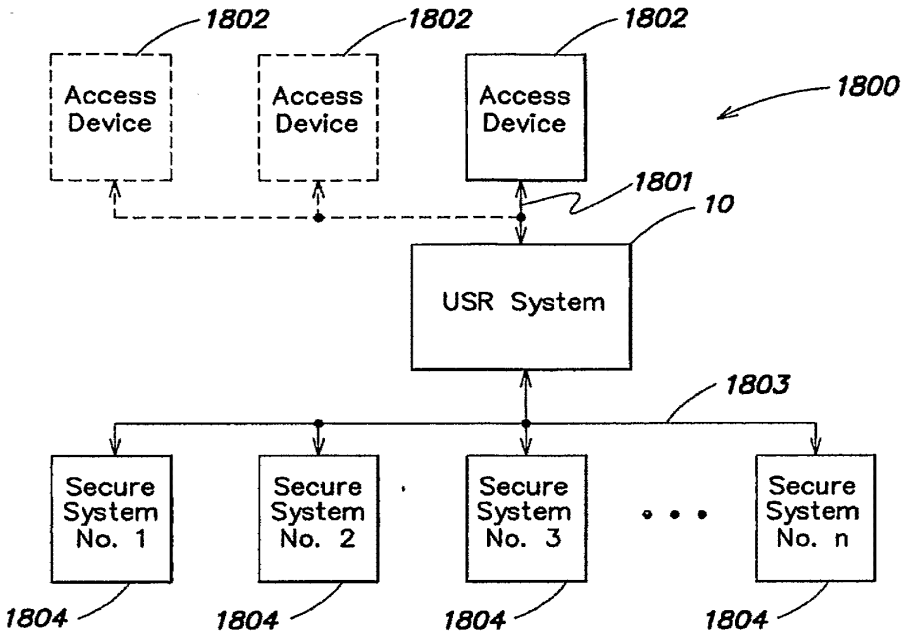


FIG. 18A

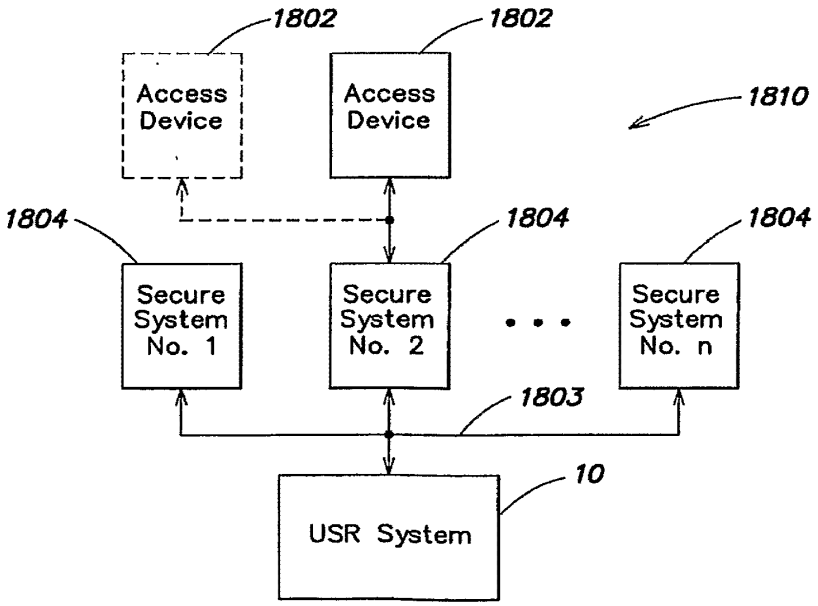


FIG. 18B

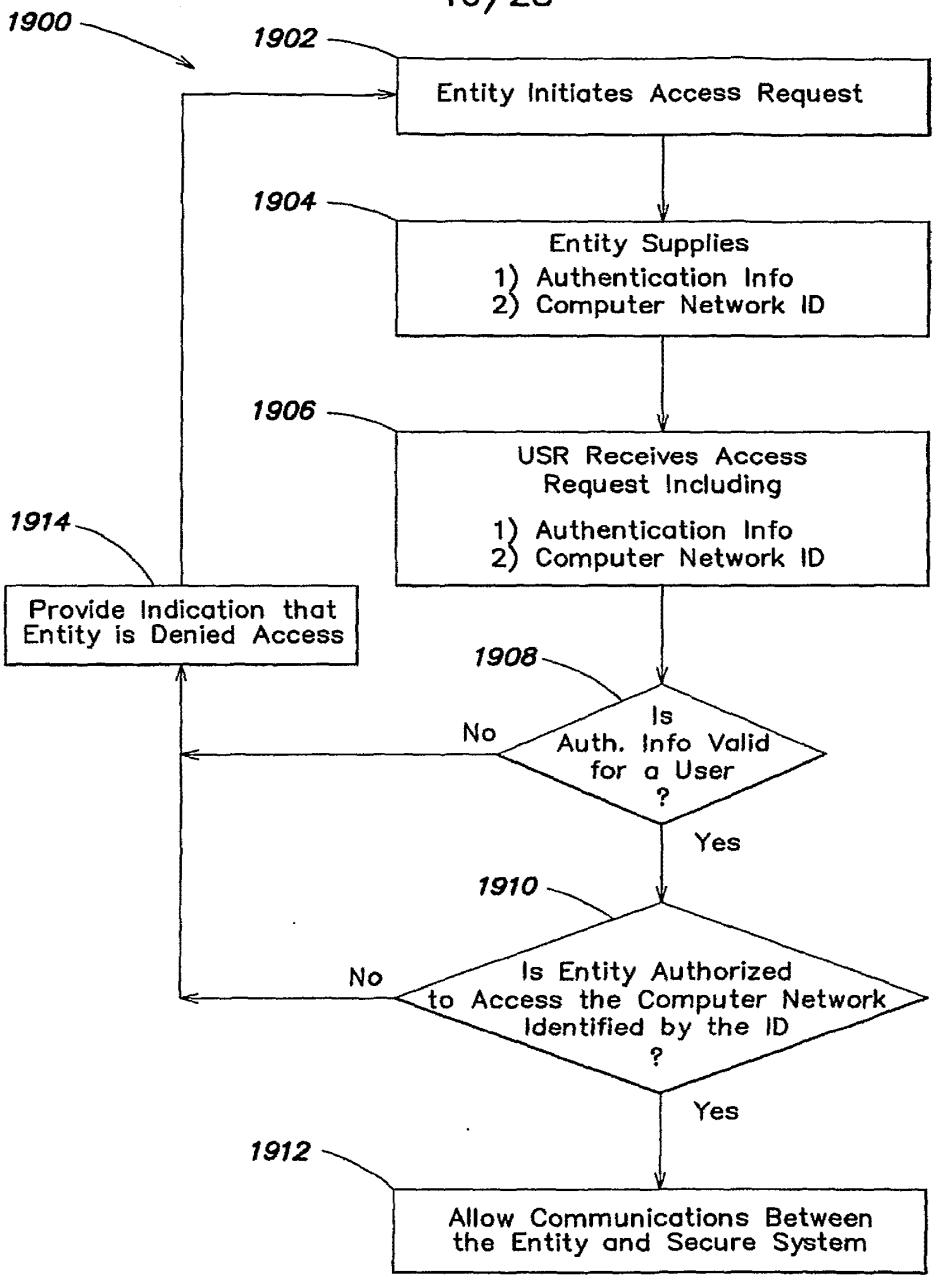

1900
1902
Entity Initiates Access Request
1904
Entity Supplies
1) Authentication Info
2) Computer Network ID
1906
USR Receives Access Request Including
1) Authentication Info
2) Computer Network ID
1914
Provide Indication that Entity is Denied Access
1908
Is Auth. Info Valid for a User ?
No
Yes
1910
Is Entity Authorized to Access the Computer Network Identified by the ID ?
No
Yes
1912
Allow Communications Between the Entity and Secure System

FIG. 19

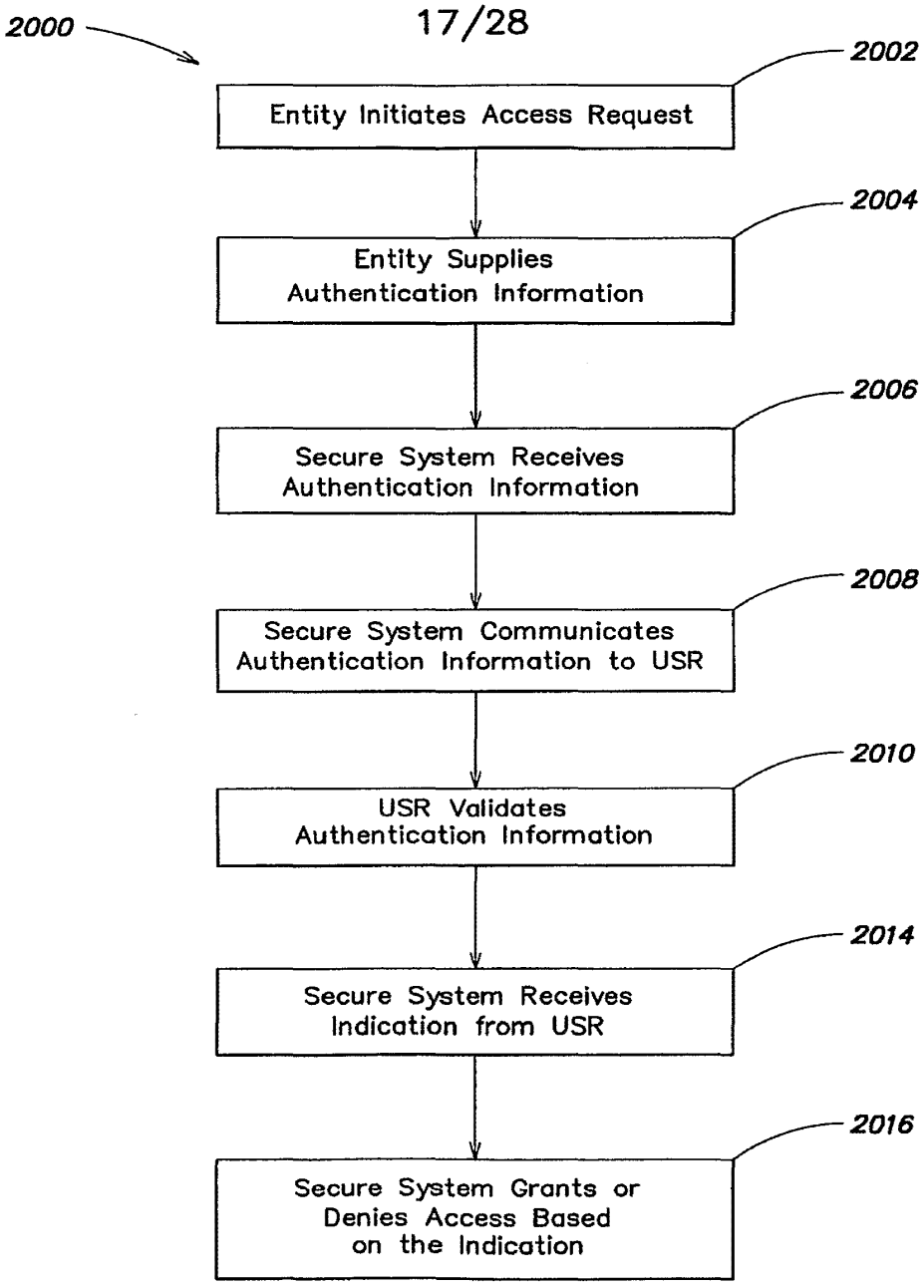

2000
2002
Entity Initiates Access Request
2004
Entity Supplies Authentication Information
2006
Secure System Receives Authentication Information
2008
Secure System Communicates Authentication Information to USR
2010
USR Validates Authentication Information
2014
Secure System Receives Indication from USR
2016
Secure System Grants or Denies Access Based on the Indication

FIG. 20

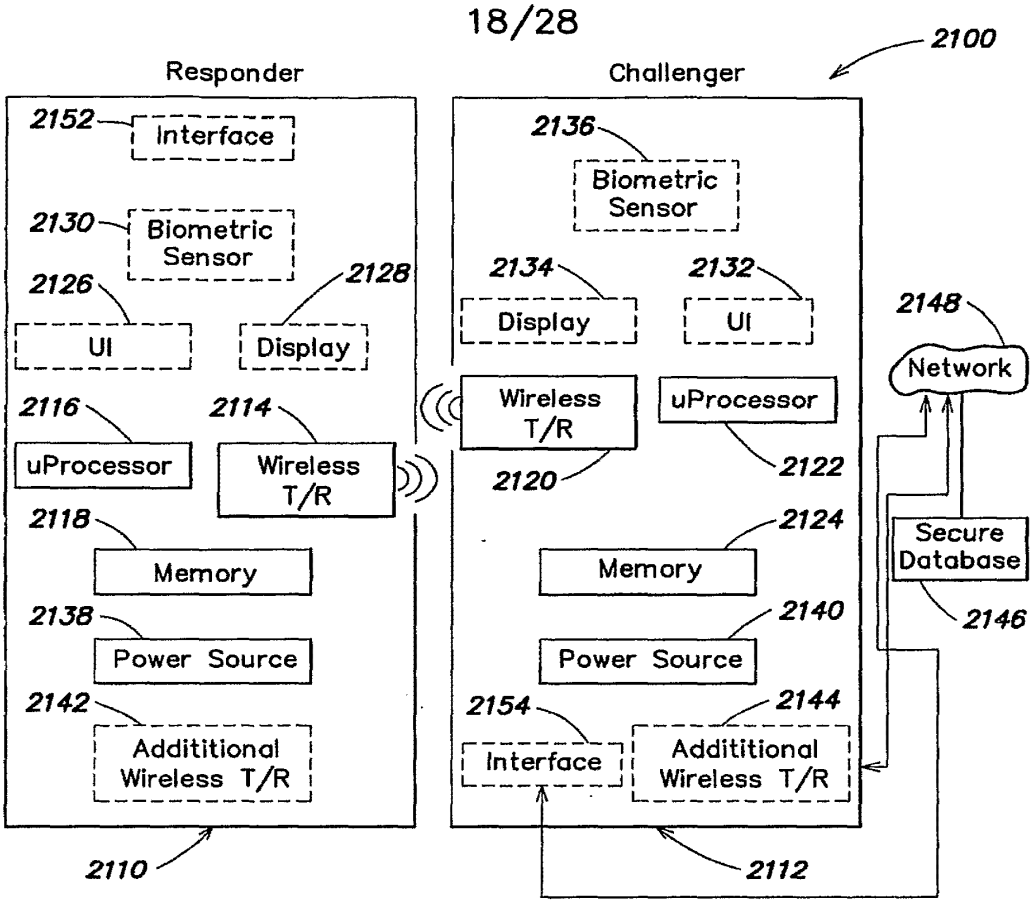

2100
Responder
Challenger
2152
Interface
2130
Biometric Sensor
2126
UI
2128
Display
2116
uProcessor
2114
Wireless T/R
2118
Memory
2138
Power Source
2142
Additional Wireless T/R
2110
2136
Biometric Sensor
2134
Display
2132
UI
Wireless T/R
uProcessor
2120
2122
2124
Memory
2140
Power Source
2154
Interface
2144
Additional Wireless T/R
2112
2148
Network
Secure Database
2146

FIG. 21

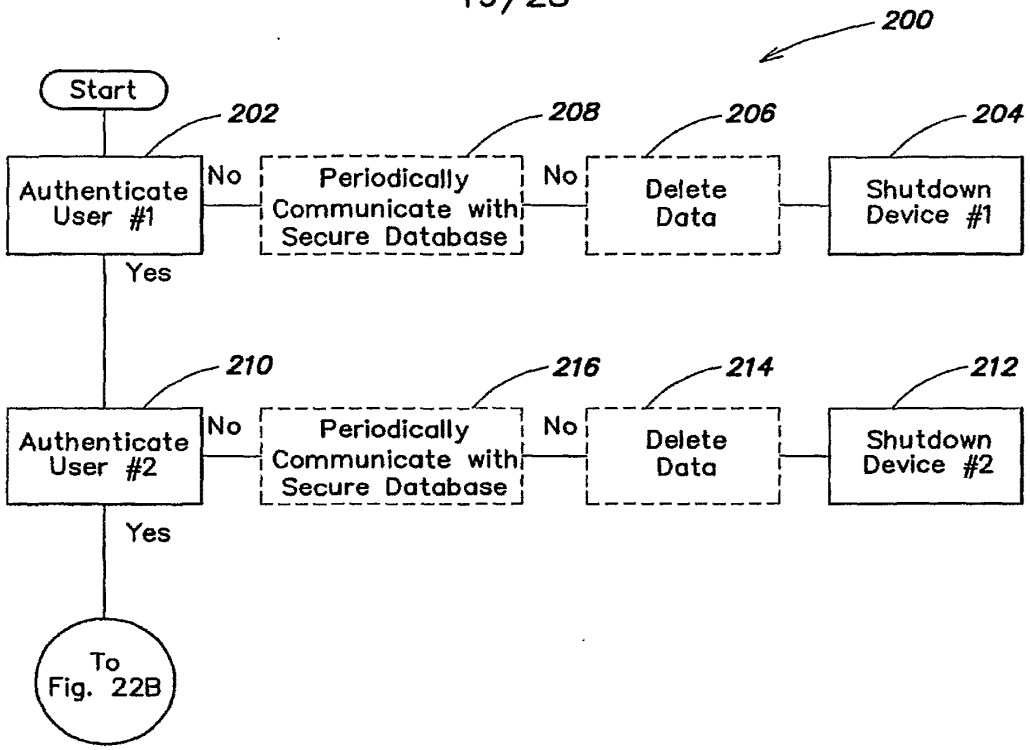

200
Start
202
208
206
204
Authenticate User #1
No
Periodically Communicate with Secure Database
No
Delete Data
Shutdown Device #1
Yes
210
216
214
212
Authenticate User #2
No
Periodically Communicate with Secure Database
No
Delete Data
Shutdown Device #2
Yes
To Fig. 22B

FIG. 22A

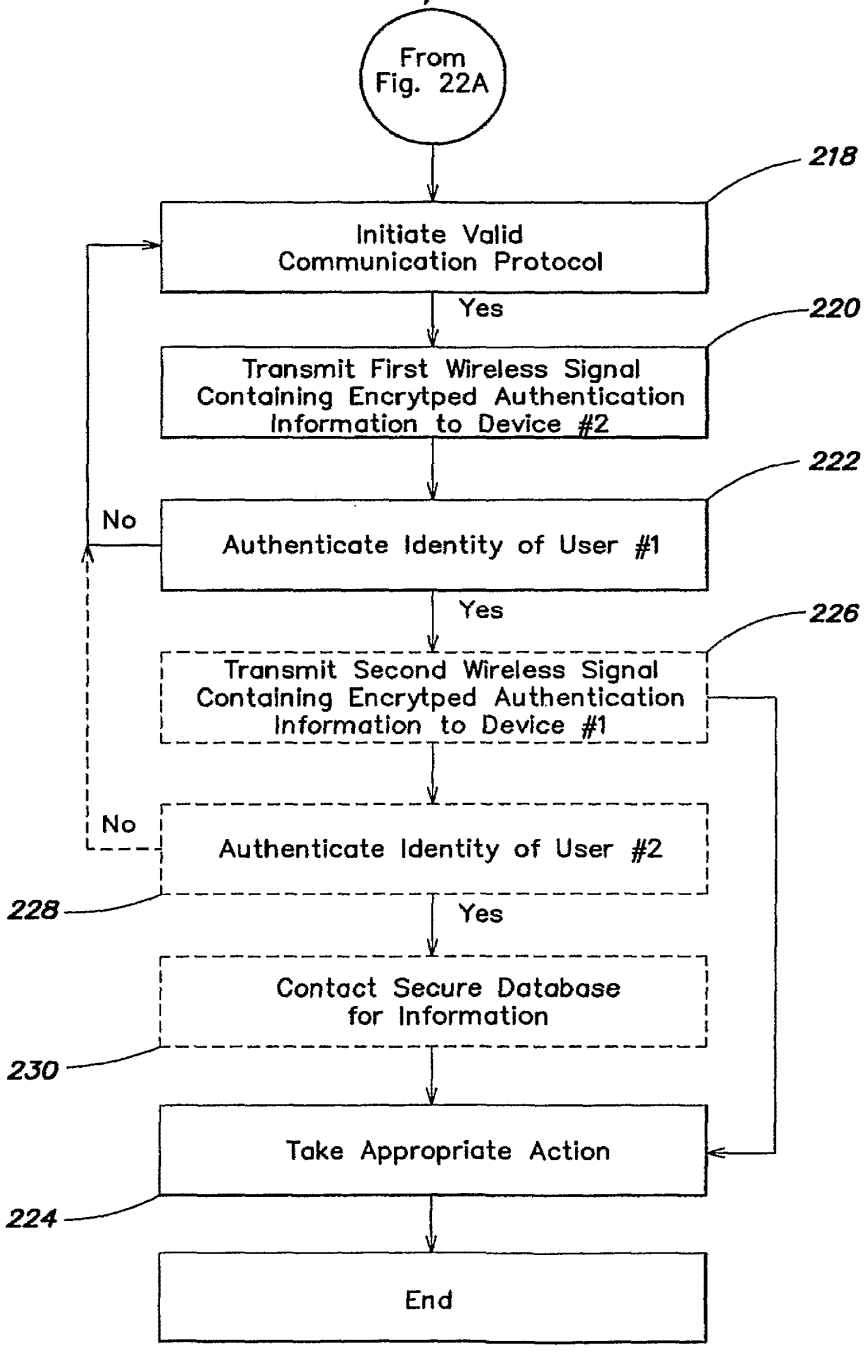

From Fig. 22A
218
Initiate Valid Communication Protocol
Yes
220
Transmit First Wireless Signal Containing Encrytped Authentication Information to Device #2
222
No
Authenticate Identity of User #1
Yes
226
Transmit Second Wireless Signal Containing Encrytped Authentication Information to Device #1
No
Authenticate Identity of User #2
228
Yes
Contact Secure Database for Information
230
Take Appropriate Action
224
End

FIG. 22B

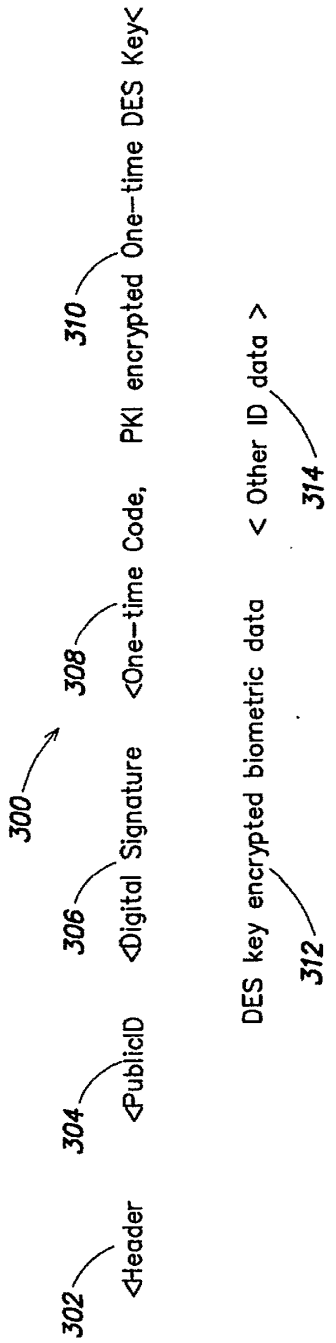

300
302
<Header
304
<PublicID
306
<Digital Signature
308
<One-time Code,
310
PKI encrypted One-time DES Key<
312
DES key encrypted biometric data
314
< Other ID data >

FIG. 23

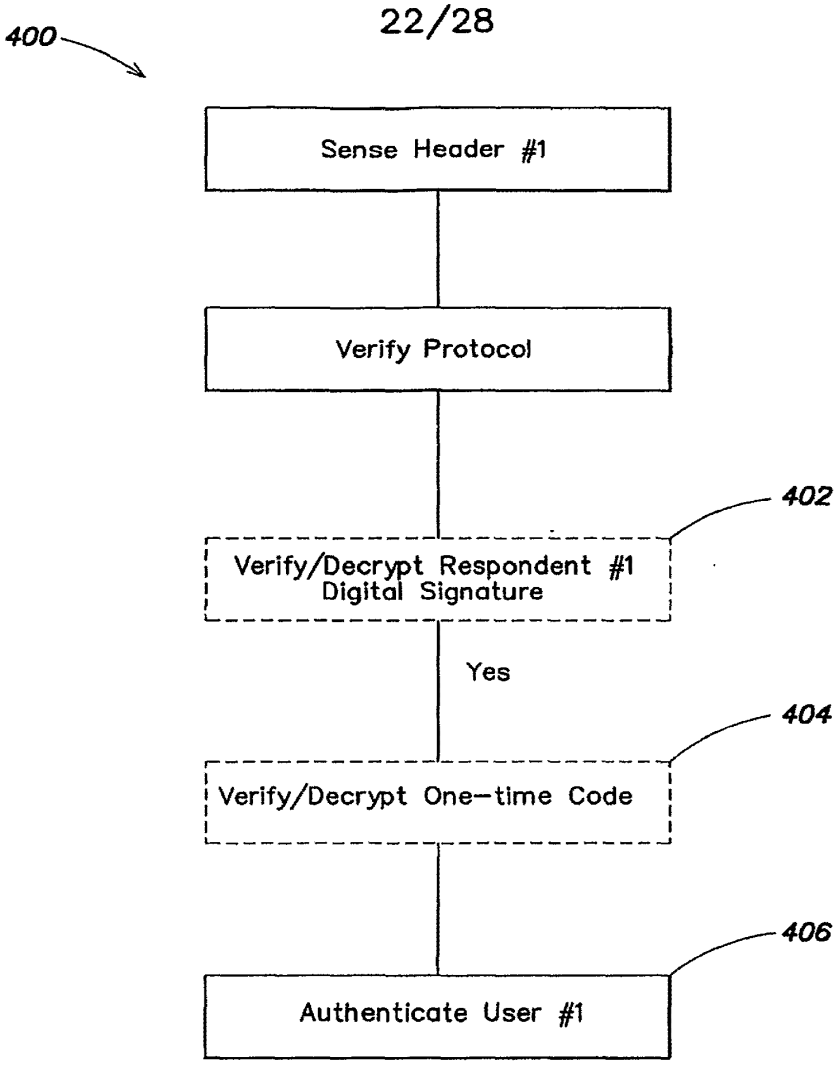

400
Sense Header #1
Verify Protocol
402
Verify/Decrypt Respondent #1 Digital Signature
Yes
404
Verify/Decrypt One-time Code
406
Authenticate User #1

FIG. 24

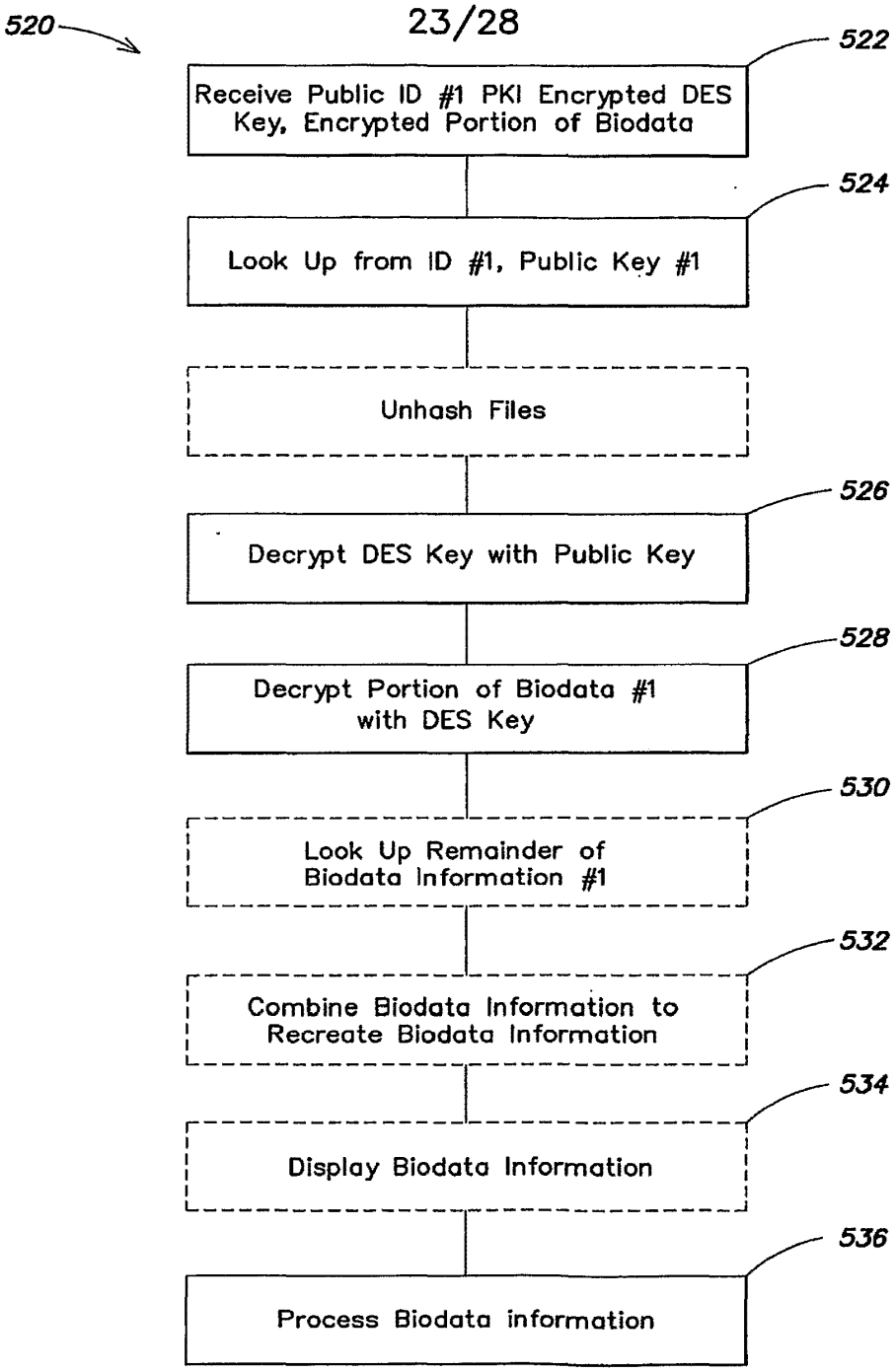

520
522
Receive Public ID #1 PKI Encrypted DES Key, Encrypted Portion of Biodata
524
Look Up from ID #1, Public Key #1
Unhash Files
526
Decrypt DES Key with Public Key
528
Decrypt Portion of Biodata #1 with DES Key
530
Look Up Remainder of Biodata Information #1
532
Combine Biodata Information to Recreate Biodata Information
534
Display Biodata Information
536
Process Biodata information

FIG. 25

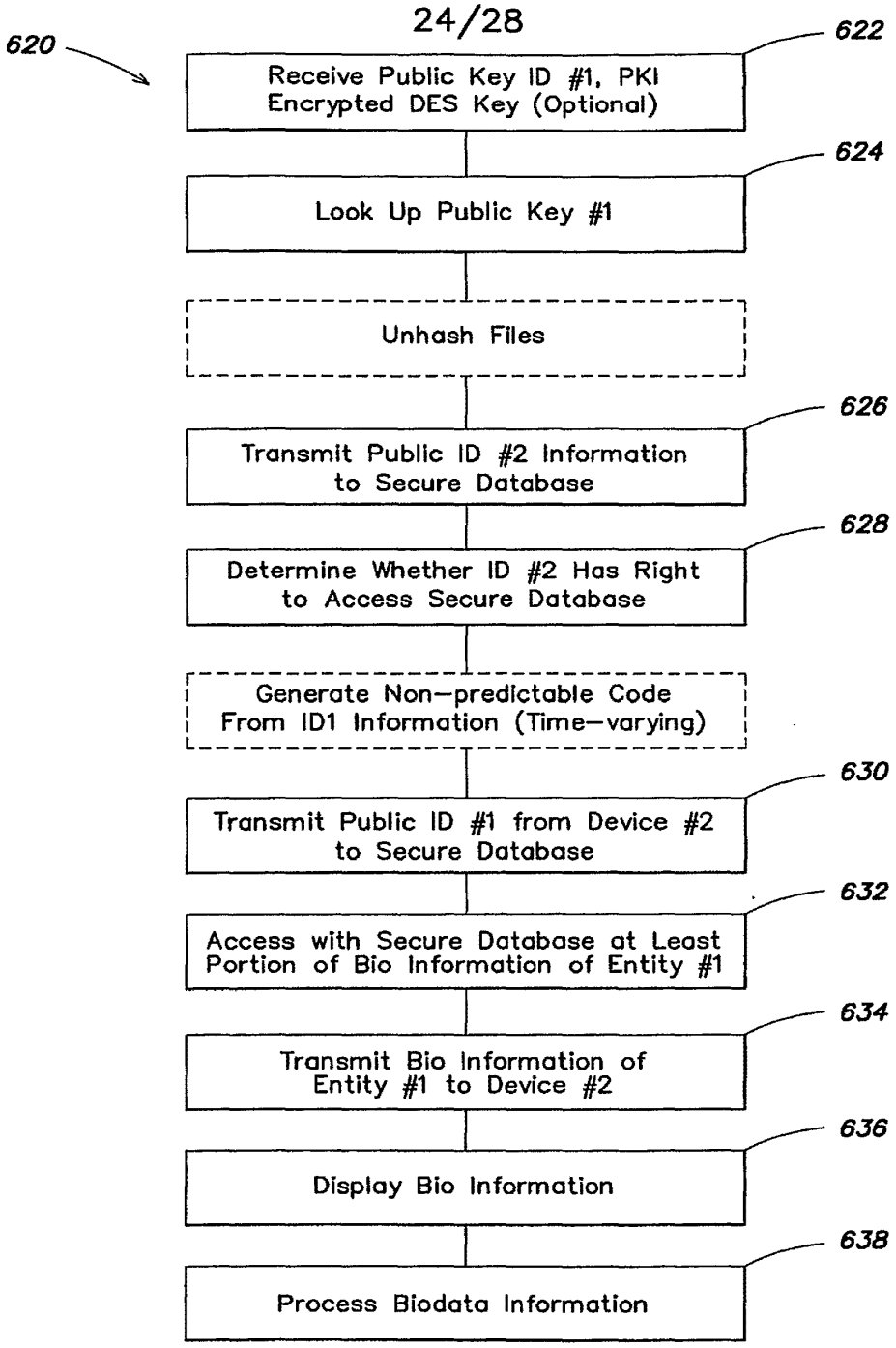

620
622
Receive Public Key ID #1, PKI Encrypted DES Key (Optional)
624
Look Up Public Key #1
Unhash Files
626
Transmit Public ID #2 Information to Secure Database
628
Determine Whether ID #2 Has Right to Access Secure Database
Generate Non-predictable Code From ID1 Information (Time-varying)
630
Transmit Public ID #1 from Device #2 to Secure Database
632
Access with Secure Database at Least Portion of Bio Information of Entity #1
634
Transmit Bio Information of Entity #1 to Device #2
636
Display Bio Information
638
Process Biodata Information

FIG. 26

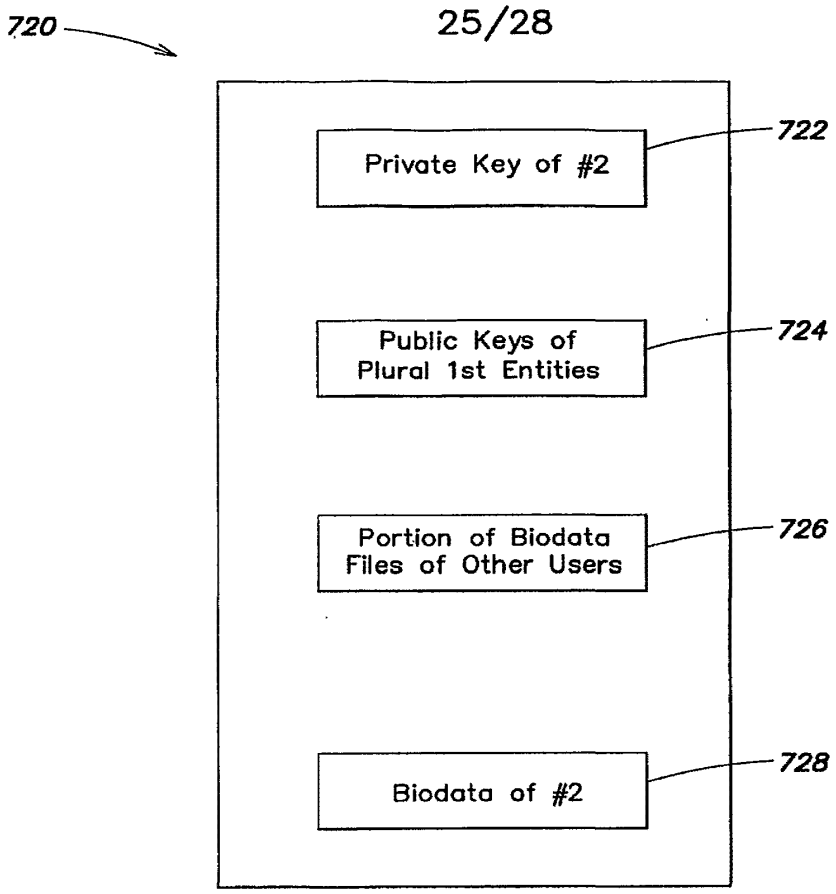

720
Private Key of #2
722
Public Keys of Plural 1st Entities
724
Portion of Biodata Files of Other Users
726
Biodata of #2
728

FIG. 27

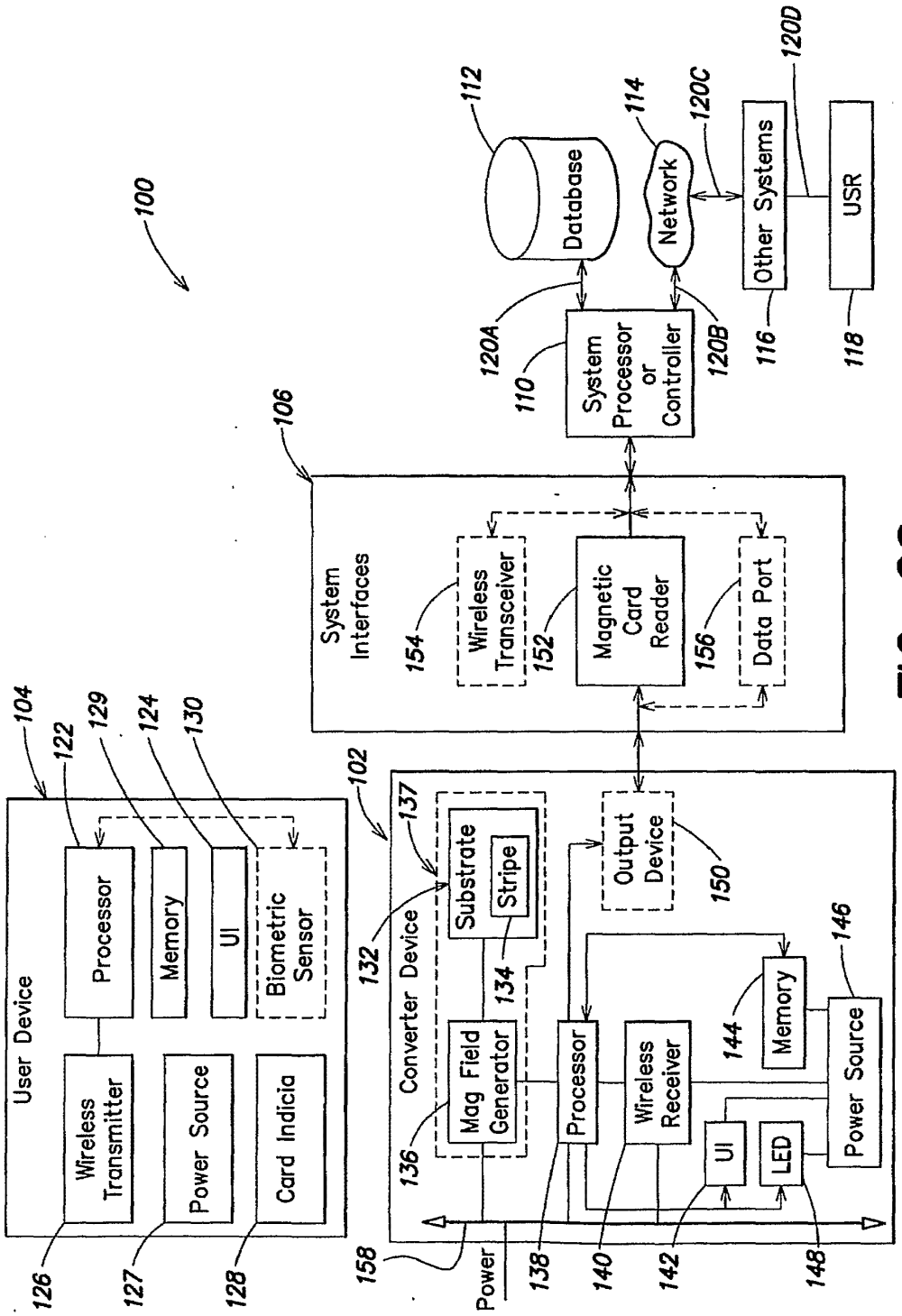

100
112
Database
114
Network
120C
Other Systems
120D
USR
120A
110
System Processor or Controller
120B
116
118
106
System Interfaces
154
Wireless Transceiver
152
Magnetic Card Reader
156
Data Port
104
122
129
124
130
User Device
Processor
Memory
UI
Biometric Sensor
102
137
Converter Device
Substrate
Stripe
132
134
Output Device
150
146
144
Memory
Power Source
Wireless Transmitter
Power Source
Card Indicia
Mag Field Generator
Processor
Wireless Receiver
UI
LED
136
126
127
128
158
Power
138
140
142
148

FIG. 28

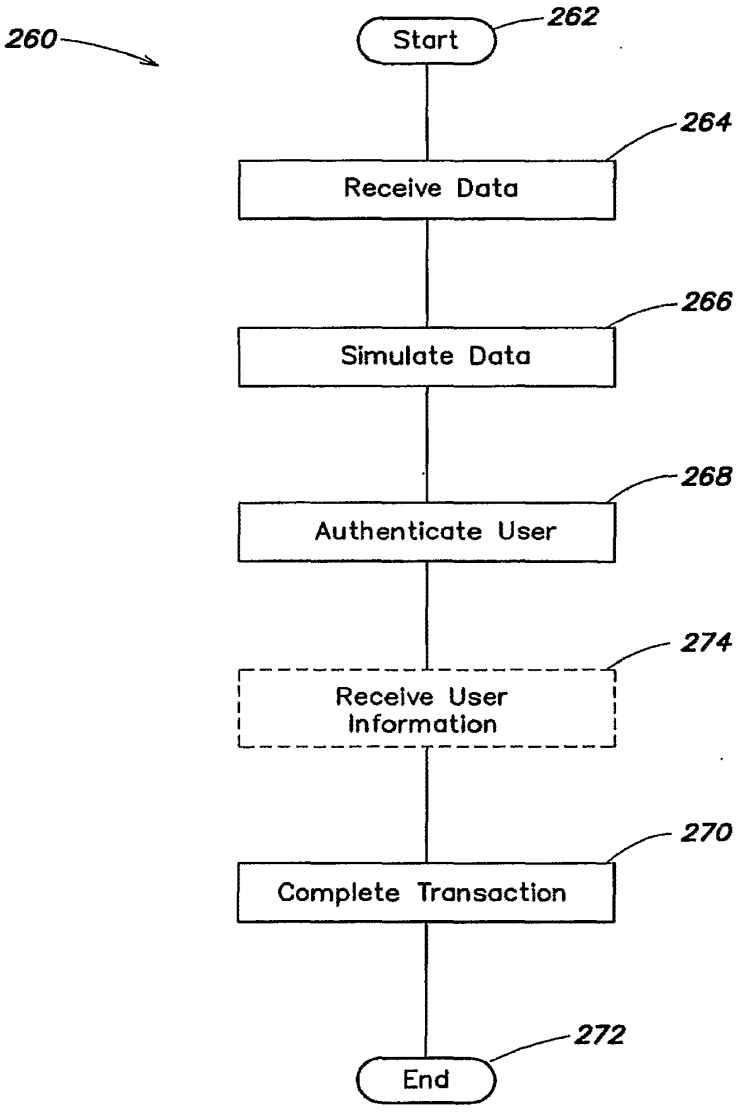

260
Start
262
Receive Data
264
Simulate Data
266
Authenticate User
268
Receive User Information
274
Complete Transaction
270
End
272

FIG. 29

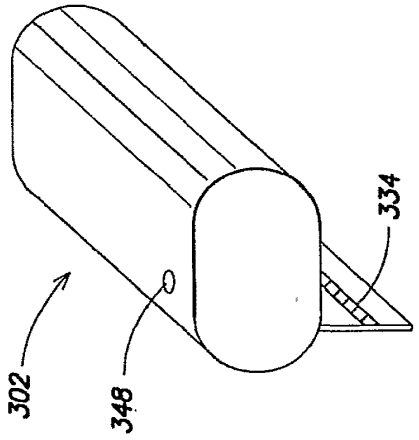


FIG. 30B

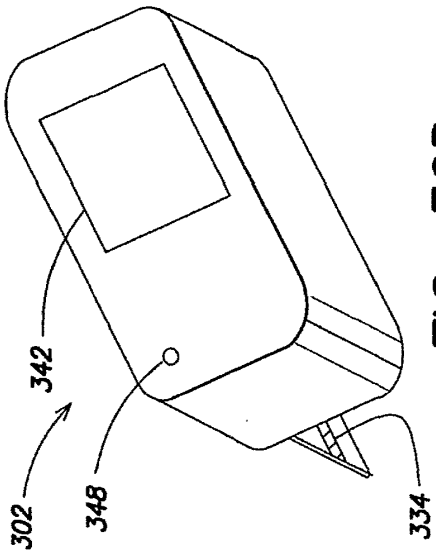


FIG. 30D

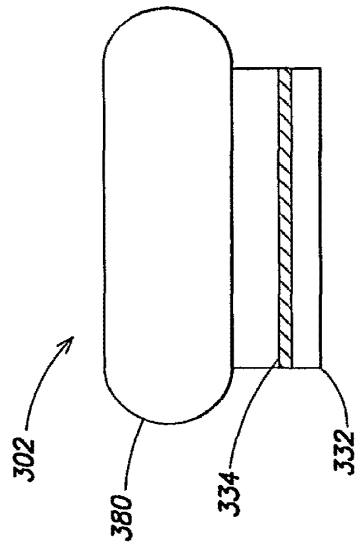


FIG. 30A

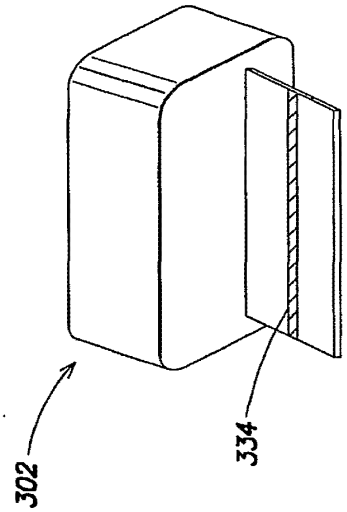


FIG. 30C

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2007/004646

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F G07C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	GB 2 382 006 A (IBM [US]) 14 May 2003 (2003-05-14) figure 3 page 4, line 29 - line 34 page 17, line 10 - line 27 page 18, line 5 - line 24	1,63
Y		2-9,13, 20-22, 64-84
Y	US 2005/001711 A1 (DOUGHTY RALPH O [US] ET AL) 6 January 2005 (2005-01-06) paragraph [0012] paragraph [0061]	2-9,13, 20-22, 64-84

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 November 2007	27/11/2007

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Chabot, Pedro

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2007/004646

Box II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☒ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

1-9,13-14,20-22,63-84

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☒ No protest accompanied the payment of additional search fees.

Form PCT/ISA/210 (continuation of first sheet (2)) (January 2004)

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1,63

   Giving authorization for an operation to a second device by a third device depending on information given by a first device.

   ---

2. claims: 2-9, 20-22, 13-14,64-84

   Emulating a credit card and providing the services associated to the credit card.

   ---

3. claims: 10-12, 38-41,46,47, 100-103, 108-109

   Secure communications between the first and the second devices using cryptography.

   ---

4. claims: 15-19, 24-32, 86-94

   Different methods of authenticating the user at a second the device, using user information sent from the first device.

   ---

5. claims: 33-37, 95-99

   Accessing user information from a data base by the secure system. The secure system access user authentication information and send it to the second device.

   ---

6. claims: 42-45, 48-62, 104-107, 110-124

   Authentication of a user at a first device, a second user at a second device, sending authentication information from the first device to the second to authenticate the first user at the second device. Permit two users to manipulate their respective devices and authenticate the one first user by the second via information sent from the first device to the second.

   ---

7. claims: 23,85 125, 129

   Send to credit card information for validation at a credit card service.

   ---

8. claims: 126-128, 130-132

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

Information validation based on information sent from a first and third devices to a second device.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2007/004646

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
GB 2382006 A	14-05-2003	NONE	
US 2005001711 A1	06-01-2005	NONE	

Form PCT/ISA/210 (patent family annex) (April 2005)

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : G06F 17/60, H04K 1/00, H04L 9/00 | A1

(11) International Publication Number: **WO 00/62214**

(43) International Publication Date: 19 October 2000 (19.10.00)

(21) International Application Number: PCT/IL00/00211

(22) International Filing Date: 6 April 2000 (06.04.00)

(30) Priority Data:

129361	8 April 1999 (08.04.99)	IL
60/174,476	3 January 2000 (03.01.00)	US

(71) Applicant *(for all designated States except US)*: CLEARTOGO.COM [IL/IL]; Amnon Ve–Tamar Street 12, 46417 Herzliya (IL).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: SOLBERG, Yoram [IL/IL]; Amnon Ve–Tamar Street 12, 46417 Herzliya (IL). BERLIN, Arie [IL/IL]; Yoram Solberg, Amnon Ve–Tamar Street 12, 46417 Herzliya (IL).

(74) Agents: SANFORD T. COLB & CO. et al.; P.O. Box 2273, 76122 Rehovot (IL).

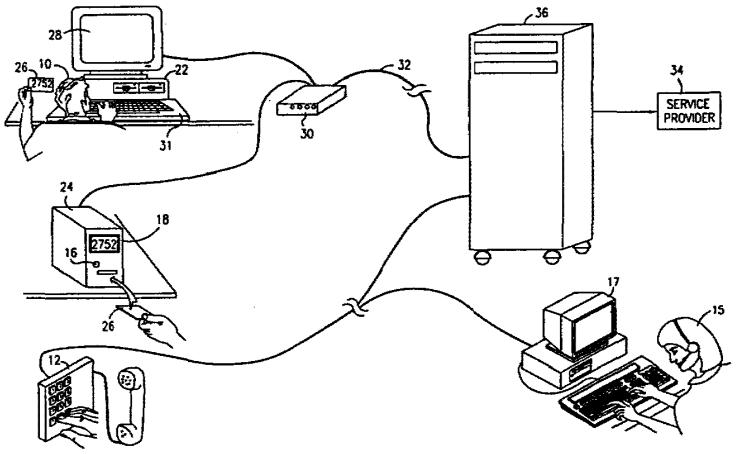
(81) Designated States: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published

With international search report.

Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: CREDIT CARD SECURITY TECHNIQUE



(57) Abstract

A technique for secure electronic commerce is disclosed wherein a transaction initiator (26) has a primary identifier and a list of secondary identifiers stored therein, each of which is valid for a single transaction. An identification center (36) receives the primary and secondary verification numbers and verifies that the primary number is valid and that the secondary number is appropriate for a current transaction using the primary number. The transaction initiator comprises an enhanced monetary card, such as a credit card or a stored value card, which includes an embedded processor, and which provides the secondary number for each transaction. The secondary numbers are stored in a lookup table, which is also available to the identification center. The values in the lookup table are indexed according to a transaction counter and are preferably communicated to the identification center without encryption or challenge. In some embodiments the transaction initiator comprises other types of hardware such as a personal computer in conjunction with secondary memory such as a CDr for storing secondary numbers and software.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

Credit Card Security Technique

BACKGROUND OF THE INVENTION

1. Field of the Invention.

The present invention relates generally to the execution of remote transactions, and to the secure transmission of identification data over insecure channels. More particularly the invention relates to authentication in monetary transactions and electronic commerce, and in other fields such as cellular telecommunication, electronic document transmission, application service providers, and home banking transactions over public communication networks.

2. Description of the Related Art.

Commerce over open public networks, such as the Internet and telephone lines, especially cellular telephones, is rapidly increasing. Generally, it is desired to use public networks to pass a credit card number from a user who constitutes a first party of a transaction to a service provider who constitutes a second party of the transaction. However, unauthorized users may easily listen to data passed over the open network, and thus gain access to credit card numbers and use them for unauthorized transactions. Furthermore, regular telephone calls and transactions over point to point networks, such as specially established computer connections, are not immune from unauthorized use, especially due to the wide number of service providers who receive credit card numbers from users. It is also known that at the present time merchant credit card databases are notoriously insecure, and prone to hacking attacks.

A most serious problem is the possibility of hackers obtaining access to credit card numbers and personal information stored in merchant databases, and appropriating them for unauthorized transactions or illegal resale. Consequently, the consumer is reluctant to expose his credit number to the Internet. This problem is solved by the present invention, which provides the consumer with a degree of security heretofore unknown, yet preserves the convenience and advantages of electronic commerce. Various encryption methods have been proposed to overcome unauthorized determination and use of the credit card number. In such methods only the user (or a computer of the user) and the credit card provider have access to the rules of encryption and decryption. However, technologies to break encryption schemes are being developed as rapidly as the encryption schemes themselves.

Digital signature schemes are also well known in the art. In a conventional signature scheme, a user has a public code and a secret code. The user sends a digital "signature" which can be easily verified using only the public code, but may be generated efficiently only with knowledge of both the public and secret codes. However, such schemes have been successfully attacked by forgers, using methods such as an adaptively chosen plaintext attack which is described, for example, in U.S. Patent No. 5,016,274 to Micali *et al.*, which is incorporated herein by reference. U.S. Patent No. 5,016,274 suggests a more complex method, which can be performed partially off-line before the message is chosen. However, it is commonly believed that as computer hardware and software develops any code may be successfully attacked. Also, the coding and decoding require large computation resources

PCT publication WO96/34471, which is incorporated herein by reference, suggests using, for identification of credit card users, a unique calling party identification code which is passed from the telephone of a user to a network switch. Such a unique code, referred to as a calling party identifier number (CPIDN), limits the credit card user to performing transactions only from specific telephone numbers.

In U.S. Patent No. 5,991,412 to Wissenburgh *et al.*, a method is proposed for protecting transactions involving a smart card and a terminal, such as a cash register. Security is provided by having the terminal (e.g. a cash register) provide a random number to the smart card. The smart card then responds by generating a first authentication value, which could be an incrementing counter, and a first authentication code, which may be an encrypted form of the random number combined with the first authentication value, and also combined with the balance sought to be transferred. The terminal supplies a different random number for each subsequent transaction, and the smart card responds with a different authentication value. In a further step, a second authentication code is provided by the terminal to the smart card which is an encrypted version of the smart card's new balance and a second random number, again generated by the terminal.

U.S. Patent No. 5,559,887 to Davis *et al.* discloses a financial transaction system, adapted to smart cards, in which encrypted certification signals are employed to establish a secure session using any of a plurality of transaction devices, or transaction processors. Among the various devices or processors disclosed in the system are vending machines, collection devices, off-line terminals, and various processors used for internetwork financial settlements. En-

cryption is accomplished using the conventional data encryption standard DES. The smart card, which is typically a stored value card (SVC), stores a unique card identification number, a transaction count, a derived password, and the identification number of the issuing entity or financial institution. Each smart card is provided with a unique set of keys derived from a master set maintained in a separate secure location. These keys are derived by an encryption technique from a set of master keys maintained by a card issuing entity.

Blind signatures are used in smart cards to form a monetary transaction system. Each blind signature represents a specified amount of money and may be used only once. A verification system may verify that a user is entitled to use a specific blind signature and that the blind signature was not used already. However, use of blind signatures is very limiting when it is desired to perform transactions which involve arbitrary sums, as is common with credit cards.

Similar verification systems are used in cellular and wireless phones to prevent unauthorized use of a phone line. For example, the Panasonic KX-TC256BX-W model wireless phone, selects a different one of 65,000 security codes each time the handset of the phone is placed on the base. In order to initiate a call, this code must be transferred from the handset to the base. However, in some cases the users of wireless phones do not place the handset on the base for a few days, providing sufficient time for an unauthorized user to determine the security code and use the phone line.

In cellular communications based on the GSM standard, in order to make a cellular call, a user must insert a dedicated "smart card" into the telephone handset. The card includes a private key number. When a call is initiated, a cellular switching center sends the handset an authentication message, indicating a proprietary algorithm which is used by a processor in the handset together with the private key to return an authentication response to the switching center. Only if the response is correct will the handset be allowed to initiate the call. This method is computationally intensive and is not suitable for all purposes.

SUMMARY OF THE INVENTION

It is an object of some aspects of the present invention to provide methods and apparatus for securely performing transactions over public networks.

It is another object of some aspects of the present invention to provide simple methods and apparatus for securely performing remote transactions which do not require complex coding or decoding.

It is another object of some aspects of the present invention to provide methods and apparatus for securely performing remote transactions which are immune to systematic access attacks.

It is another object of some aspects of the present invention to provide methods and apparatus for preventing unauthorized users from deriving identification information of a transaction and using the information to perform unauthorized transactions.

It is still another object of some aspects of the present invention to provide methods and apparatus for securely performing monetary and non-monetary transactions, in which an unauthorized person who derives identification information passed from a credit card to a verification station does not have sufficient information to perform unauthorized transactions.

In aspects of the present invention, a first party to a transaction uses a device, referred to herein as a transaction initiator, which is identified by a fixed primary identification number and a varying secondary identification number. An identification center (or centers) receives the primary and secondary verification numbers and verifies that the primary number is valid and that the secondary number is appropriate for a current transaction using the primary number. Optionally the secondary numbers can be stored on other devices such as a CD, or in software that may be loaded into a computer.

In some aspects of the present invention, the transaction initiator comprises a transaction card, such as a credit card or a stored value card, which includes an embedded processor which provides the secondary number for each transaction. The stored value card may use the secondary number in performing purchase transactions and/or to perform reloading transactions.

In other aspects of the present invention, the transaction initiator comprises a cellular or wireless phone, and the secondary number is provided separately for each phone call or number of phone calls. The identification center is accordingly within the base of the wireless phone or within a cellular switching center which provides services to the cellular phone.

In still other aspects of the present invention, the transaction initiator may be used to monitor access to sensitive information, such as, bank accounts, health information, etc.

Preferably, the secondary number is passed from the transaction initiator to the identification center over the telephone, either by dialing appropriate numbers or by voice, over the Internet or other computer connections, facsimile, or any other suitable communication mechanism. In some embodiments the secondary number is passed in an unencrypted format.

In some aspects of the present invention, the secondary number is selected from a look up table (LUT) of values of the secondary number. Preferably, the LUT includes a series of random or pseudo-random numbers which do not allow determination of a next number in the series based on some or even all of the previous numbers in the series. Identical copies of the LUT are kept both in the transaction initiator and in the identification center.

Preferably, the secondary identification number is selected according to a rule based on external data known both to the transaction initiator and the identification center. The external data includes at least some information unrelated to the transaction. Preferably, the rule is entirely unrelated to the details of the transaction, such that the secondary number may be provided before the details of the transaction are known. Alternatively, the rule is partially based on external data related to the transaction, such as the date, time and/or sum of the transaction. In a preferred embodiment of the present invention, the rule is based on the number of transactions performed using the transaction initiator. Preferably, the secondary identification numbers are retrieved sequentially from the LUT.

In some aspects of the present invention, each of the secondary numbers in the LUT may be used only once. When all of the entries in the LUT are exhausted, the transaction initiator is replaced or is refilled with new secondary numbers. Preferably, a display on the transaction initiator notifies the user of the card when the number of secondary numbers remaining therein is below a predetermined value. Alternatively, when all of the entries in the LUT are exhausted, the secondary numbers in the LUT are reused using the same or a different access rule. The LUT in an authentication server may store some keys and algorithms from which a secondary number can be generated. This avoids the storage of actual secondary numbers which could be detected by an unauthorized person, and provides an additional line of defense against hacking of the authentication server.

In some aspects of the present invention, both the transaction initiator and the identification center keep track of an entrance key to the LUT. Each time a transaction is performed, the entrance keys are updated according to the rule. Alternatively or additionally, when the identification center is not connected on-line to the parties performing the transaction, the entrance key is updated by the transaction initiator only a few minutes after the transaction is performed in order to allow sufficient time for the identification center to receive notification of the transac-

tion. Preferably, transactions performed during these few minutes use the same secondary number. Alternatively, during these few minutes another transaction may not be initiated.

Alternatively or additionally, the secondary number is determined or changed according to a predetermined function without the use of a LUT. The predetermined function may comprise a pseudo-random function or any other function which does not allow easy determination of the next secondary number based on a series of previous secondary numbers. Additionally or alternatively, the function is partially dependent on details of the transaction, such as, the date and/or time of the transaction, and/or the monetary sum of the transaction.

An unauthorized user who intercepts the primary and secondary identification numbers cannot use the intercepted data to perform any transactions since the unauthorized user knows only one possible secondary identification number and furthermore does not know the rule which governs the changes of the secondary number.

In some aspects of the present invention, the LUT is implemented by a memory or logic chip, such as a programmable logic array (PLA), which cannot be read by an external reader. Thus, even one who holds the transaction initiator cannot make a copy of the LUT.

In some aspects of the present invention, the transaction initiator includes a display which presents the secondary number, and a switch or button for indicating the completion of a transaction. When a transaction is to be performed the holder of the initiator reads the secondary number from the display and passes it to the other party in the transaction or directly to the identification center. Thereafter, the user presses the button to receive a new secondary number. Alternatively, the user presses the button before the transaction is performed, and only then the secondary number is displayed. Further alternatively, a secret code is necessary to display the secondary number, so that the transaction initiator cannot be used even if an unauthorized user has possession of the transaction initiator.

In some aspects of the present invention, a monetary card-reader reads both the primary and secondary numbers and instructs the processor to change the secondary number once the number was read. Preferably, the card-reader is connected to the center to verify the primary and secondary numbers.

In some aspects of the present invention, the card-reader may be coupled to a personal computer in order that a user of the personal computer may easily perform transactions over the Internet. Alternatively or additionally, the monetary card includes a display window which

shows the secondary number. When a user desires to perform a transaction over the Internet and the identification number of his card is requested, the user types in the primary number of the card and the secondary number from the display window. If the transaction was successful, the user is instructed to notify the card to update the secondary number, for example, by pressing a button on the card. Alternatively or additionally, the user may be required to sign his signature or give his finger print in order to update the secondary number.

In some aspects of the present invention, each card may have three identification numbers: a card identification number which is generally imprinted on the card, a secret code which is known only to the user and prevents unauthorized use of the card in case it is lost, and the secondary number which changes with each transaction. It is noted that the term "identification number" is used herein in a general way to refer to any type of code.

It is noted that the present invention may be used together with other coding schemes which may be used to code the primary and/or secondary identification numbers.

In some aspects of the present invention, when the identification center encounters an attempt to perform a transaction with an incorrect secondary number, the use of the transaction initiator is suspended in order to prevent continuous attacks directed to determine the secondary number. Preferably, the secondary number on which a possible attack was performed may not be used to perform a transaction, and the next secondary number must be used. Preferably, when a suspended transaction initiator requests to perform a transaction, the identification center requests that it provide the correct secondary number to remove the suspension. Only then may a new transaction be performed using the next secondary number.

According to some aspects of the invention, a virtual credit card number is provided for a first credit card company, suitable for co-branding with a second credit card company. A fixed identifier, such as a specific prefix (4-5 digits) indicates that a credit card is associated with the first credit card company, while the rest of the identifier may contain identifying information and a current secondary number. In this case the virtual credit card is suitable for a one-time transaction.

In some aspects of the invention, credit card transactions can be conducted in a manner that protects merchant databases and consumers by omitting the storage of primary credit card numbers in the merchant databases, instead utilizing one-time secondary identification numbers.

The invention provides a method of performing a remote transaction, which is performed by initiating a first communication link between a first party and a second party. The first party has a fixed primary identification. At the first party, a variable secondary identification is selected from a list carried by the first party, responsive to a predetermined rule. The secondary identification is transferred from the first party to the second party via the first communication link. A second communications link is established between the second party and an authentication center, the secondary identification is communicated from the second party to the authentication center via the second communications link. The authentication center is aware of the fixed primary identification of the first party. The method further includes verifying at the authentication center that the secondary identification is a permissible identification for performing the transaction, establishing a third communications link between the authentication center and a payment processing agent, and communicating the fixed primary identification from the authentication center to the payment processing agent via the third communications link.

According to another aspect of the invention the method further includes establishing a fourth communication link between the first party and the authentication center, and communicating the secondary identification from the first party to the authentication center via the fourth communication link.

According to yet another aspect of the invention the first party effects communication on the first communication link using a communication device that has memorized data and program instructions. The data and program instructions may be stored on a CD, or on software which has been transferred to the communication device.

Preferably confidential information is transferred from the first party to the authentication center prior to initiating a first communication link.

According to an aspect of the invention the authentication center associates the secondary identification with the confidential information of the first party, and transfers the confidential information and the fixed primary identification to the payment processing agent.

BRIEF DESCRIPTION OF THE DRAWING

For a better understanding of these and other objects of the present invention, reference is made to the detailed description of the invention, by way of example, which is to be read in conjunction with the following drawings, wherein:

Fig. 1 is a schematic view of a system for performing monetary-card transactions, in accordance with a preferred embodiment of the present invention;

Fig. 2 is a schematic view of a monetary card, in accordance with a preferred embodiment of the present invention;

Fig. 3 is a schematic view of a LUT in the monetary card of Fig. 2 and in a compatible identification center, in accordance with another preferred embodiment of the present invention;

Fig. 4 is a flow chart illustrating the actions of an identification center in processing a transaction, in accordance with a preferred embodiment of the present invention;

Fig. 5 is a schematic illustration of a cellular communication system, in accordance with a preferred embodiment of the present invention;

Fig. 6 is a block diagram illustrating an arrangement of electronic commerce suitable for use with preferred embodiments of the invention;

Fig. 7 is a plan view of a transaction card in accordance with a preferred embodiment of the invention;

Fig. 8 is a diagram of a ROM which is a component of the transaction card shown in Fig. 7;

Fig. 9 is a perspective view of a transaction card in accordance with an alternate embodiment of the invention;

Fig. 10 is a block diagram of the electronic circuitry of the transaction card illustrated in Fig. 9;

Fig. 11 illustrates a check out form of a merchant site to be completed by a consumer;

Fig. 12 illustrates a merchant's version of a check-out form similar to the form shown in Fig. 11;

Fig. 13 illustrates information which is stored in a central authentication server in the arrangement of Fig. 6;

Fig. 14 illustrates an arrangement of electronic commerce in accordance with an alternate embodiment of the invention;

Fig. 15 is a block diagram of an arrangement of an authentication server in a system of electronic commerce in an alternate embodiment of the invention;

Fig. 16 illustrates an arrangement of electronic commerce in accordance with another alternate embodiment of the invention; and

Fig. 17 is a block diagram illustrating an arrangement of electronic commerce in accordance with another alternate embodiment of the invention.

DESCRIPTION OF THE PREFERRED EMBODIMENT

In the following description, numerous specific details are set forth in order to provide a through understanding of the present invention. It will be apparent however, to one skilled in the art that the present invention may be practiced without these specific details. In other instances well known circuits, control logic, and the details of computer program instructions for conventional algorithms and processes have not been shown in detail in order not to unnecessarily obscure the present invention.

Fig. 1 is a schematic view of a system for performing remote monetary-card transactions, in accordance with a preferred embodiment of the present invention. A user 10 performs a remote transaction with a service provider 34 using details of a transaction card 26. Card 26 preferably comprises either a credit card or a stored value card, and is also referred to in the context of the present patent application and in the claims as a type of "transaction initiator." Some of the details of card 26 vary for each remote transaction, as described hereinbelow. An identification center 36 receives the details of card 26 and verifies that the card is valid and that the details are compatible with the current transaction. Identification center 36 receives the details of card 26 either directly from user 10 as described hereinbelow, or from service provider 34, which in turn receives the details from user 10. If the details of card 26 allow performance of the transaction, identification center 36 notifies service provider 34, and the transaction is carried out. Preferably, identification center 36 also notifies user 10 of the successful completion of the transaction, whereupon the user updates the details of card 26 as described hereinbelow.

Preferably, user 10 relays the details of card 26 via a telephone 12, either by reading the details to an operator 15 or by inputting the details directly to service provider 34 or identification center 36, using the telephone keypad, for example, as is known in the art. Alternatively or additionally, user 10 may send the details to operator 15 using e-mail, fax, etc. The details of card 26 can optionally be automatically transmitted via an e-wallet platform, in which case the consumer does not have to type in the details.

Alternatively or additionally, the details of card 26 are read by a card reader 24, which passes the details, preferably via a modem 30 and a communication line 32, to server 36. Preferably, reader 24 includes a display 18 which shows the details of card 26, and a button 16

which is actuated by user 10 to update the details of card 26 when and as required. Preferably, reader 24 operates with any compatible card 26. Alternatively, each card 26 operates only with specific readers 24, so that an unauthorized user who finds card 26 cannot perform remote transactions using the card without having the proper reader 24.

In some aspects of the present invention, reader 24 updates the details of card 26 automatically upon acknowledgment of the transaction by identification center 36, before card 26 is ejected from the reader. Alternatively, the details are updated when a transaction is initiated or when a significant number of steps of the transaction have been performed, without acknowledgment from identification center 36. Preferably, reader 24 comprises an additional button (not shown) which may be used to cancel an update which was performed erroneously.

Further alternatively or additionally, user 10 establishes a computer connection with service provider 34, using a computer 22. The computer connection is established either through a direct computer link or through a public network such as the Internet. When user 10 desires to perform a monetary transaction, computer 22 prompts the user (for example, by displaying an appropriate message on a display 28) to enter the details of card 26. Preferably, the details are entered through a keyboard 31. Alternatively or additionally, reader 24 may be coupled to computer 22 so that the details are automatically passed to computer 22. Thereafter computer 22 passes the details of card 26 to identification center 36 via modem 30

An individual who eavesdrops on the traffic on link 32 cannot determine sufficient information to perform remote transactions using card 26, because the details of the card change between transactions. Preferably, by the time the eavesdropper determines the current details passed on link 32, a transaction has been completed, and an additional transaction cannot be performed using these details.

Fig. 2 is a schematic view of card 26, in accordance with a preferred embodiment of the present invention. Card 26 has a primary identification number which identifies the card. Preferably, the primary number appears in an embossment 66 on card 26, as is known in the art. Preferably, card 26 includes an embedded memory 52 which stores a look-up table (LUT) of secondary identification numbers. Card 26 preferably also includes an embedded processor 50, which generates and/or updates a key for access to the LUT. Preferably, processor 50 comprises a simple counter, and the key is an indexing integer number whose maximum value is of the size of the LUT.

Alternatively or additionally, the key is chosen according to a more complex rule, for example one which is partially dependent on the time, date and or sum of the transaction. It is noted however, that the rule is at least partially dependent on external data not related to the details of the specific transaction. Further alternatively or additionally, processor 50 calculates the secondary number directly without access to a LUT. In such a case, processor 50 generates and applies a pseudo-random number, so that it is substantially impossible to determine the next secondary number based on a short sequence of secondary numbers. Preferably, memory 52 comprises or is coupled to a programmable logic array (PLA) which cannot be read by an external device. Other memory devices may also be used, including memories internal to processor 50.

Card 26 preferably comprises a display 54, such as an LED or LCD display, which shows the secondary number. Preferably, card 26 comprises an additional display 56, which shows the index of the secondary number in the LUT. Card 26 preferably further comprises a button 58 which is actuated by user 10 to change the secondary number. Alternatively, card 26 comprises a privileged input device which may only be actuated by a user who knows a proper code. For example, card 26 may comprise a signature receiving pad, and the card provides a new secondary number only if the signature resembles the signature of the true owner of the card. Thus, even if an unauthorized person has access to card 26, the person cannot use the card more than once without properly signing the signature of the card's owner.

In a preferred embodiment of the present invention, card 26 comprises an additional button 59 which undoes the operation of button 58 in case it was erroneously pressed. Alternatively or additionally, card 26 comprises a keypad (not shown) for entering data and commands to the card.

In a preferred embodiment of the present invention, processor 50 includes an internal clock, which keeps track of the current date and/or time.

Fig. 3 is a schematic illustration of a LUT 70 in memory 52 and a compatible LUT 72 in identification center 36, in accordance with a preferred embodiment of the present invention. LUT 70 comprises a plurality of entries of secondary numbers, in a predetermined order, such that there is substantially no correlation between the entries in the LUT. Specifically, the secondary numbers are preferably chosen randomly so that from the knowledge of a sequence of a few secondary numbers, it is not possible to deduce the next secondary number. Preferably,

LUT 70 comprises a large number of entries, for example between 1,000 and 10,000 entries, although the LUT may comprise substantially any number of entries. Preferably, each entry to LUT 70 is used for only a single transaction. Alternatively, once all the entries of the LUT are used, the entries of the LUT are reused.

LUT 72 in identification center 36 is an identical copy of LUT 70 in memory 52. For each card 26, identification center 36 comprises, in addition to LUT 72, an index 74 to the current entry in the LUT, and a status variable 76. Index 74 points to the same entry as is pointed to by processor 50, and is updated in the same manner and preferably at the same time as the index in processor 50. Status variable 76 states whether card 26 is ready for use or is suspended due to a possible unauthorized use, as described hereinbelow.

Fig. 4 is a flow chart illustrating the actions of identification center 36 in processing a transaction, in accordance with a preferred embodiment of the present invention. When a user of card 26 desires to perform a remote transaction, identification center 36 receives the primary number of card 26. Identification center 36 checks that the primary number is of a valid card, and preferably also checks for a password, if a password is associated with card 26. Thereafter, identification center 36 checks whether card 26 was suspended due to a possible attempt to illegally use the card. If the card is not suspended, index 74 (having a value N) is updated according to a rule known both to center 36 and processor 50. In a preferred embodiment of the present invention, the rule is a simple incrementation. Thereafter, user 10 is requested to enter the secondary number having index N in LUT 70. Alternatively, user 10 is requested to enter the current secondary number without stating the current index. Preferably, user 10 keeps track of the current index by pressing button 58 each time a transaction is successfully concluded, as described hereinbelow.

If the secondary number is correct, approval of the transaction is passed to service provider 34. Preferably, user 10 is prompted to press button 58 so as to update the index to LUT 70 of card 26. However, if the secondary number from user 10 is incorrect, the card is preferably set to a suspended status, as indicated by status variable 76. Thus, it is not possible to determine the secondary number by continually guessing. The user is preferably immediately allowed to attempt to get card 26 out of the suspended status by entering the requested secondary number. Alternatively, the user must re-enter the primary identification and password in order to attempt to get card 26 out of the suspended status. If the secondary number is correct, status

variable 76 is set to ready, index 74 is incremented, and user 10 is preferably prompted to press button 58 so as to update the index to LUT 70. In order to perform the transaction, user 10 is requested to enter the next secondary number. Thus, an unauthorized user who succeeds in determining a secondary number in a systematic attempt to get card 26 out of its suspended status, still cannot perform a transaction without guessing the succeeding secondary number in a single try. On the other hand, if the card was suspended due to a mistake, all that is needed in order to cancel the suspension and perform a transaction is to enter two numbers.

Preferably, user 10 is instructed to press button 58 upon conclusion of the transaction. Alternatively, user 10 presses button 58 immediately before performing a transaction.

Alternatively or additionally, each time a transaction is performed, identification center 36 sends card 26 a key to be used in the next transaction of the card to point to a selected value in LUT 70. It is noted that an unauthorized listener cannot use the key without knowing the contents of the LUT. Further alternatively or additionally, center 36 may send to processor 50 a function or set of commands to be performed in providing the secondary number for the next transaction.

Alternatively or additionally, each time a transaction is performed, identification center 36 sends user 10 a random index for which the user must return the corresponding secondary number. In such a case, card 26 preferably comprises a suitable number pad or another user interface for entering the received index. Alternatively or additionally, reader 24 (Fig. 1) comprises a keyboard (not shown) for entering the received index. Thus, card 26 remains relatively simple while allowing relatively large amounts of data to be entered to the card.

Optionally, transactions involving small purchases made in person, which are generally performed by physically passing card 26 through a reader, as is known in the art, do not require use of the secondary number. Alternatively, the secondary number is automatically updated by a reader used in such a transaction.

Fig. 5 is a schematic illustration of a cellular phone 90, in accordance with a preferred embodiment of the present invention. Phone 90 comprises a memory chip 92 which stores a LUT of secondary identification numbers. When a call is initiated from phone 90, identification information is passed from the phone to a base station 94. The identification information includes a secondary number which changes for each call. Thus, an unauthorized user who determines the identification information of phone 90 by eavesdropping on the call between the phone and sta-

tion 94 cannot use the information to perform calls. Preferably, base station 94 passes the identification information to an identification center 96 which has an identical copy of the LUT in memory 92, in a manner similar to that described above regarding card 26. Preferably, the process of checking whether the secondary number is correct is performed automatically, without need of any human intervention.

It is noted that although the term secondary number is used to refer to the secondary identification of card 26, any type of identification may be used including letters, symbols, voltage levels, tones, etc.

Application to Electronic Commerce

The invention disclosed herein solves two major problems of electronic commerce ("e-commerce") transactions as well as in offline ones: (a) extensive fraud, causing consumer hesitance in using credit cards, and (b) non-secure merchant credit card databases. The basis for this technology is a specific transaction personal identification number (STP), a code which can be used for one transaction only and then becomes meaningless and cannot be used for future transactions. STPs are generated and ordered randomly and uniquely, or are created using an STP generation algorithm and thus STPs applying to subsequent transactions cannot be determined by detecting a currently transmitted STP, even after decryption. The STP generation algorithm can be dependent on several parameters such as time, personal details, transaction information or personal password. At the time that the STPs are created they are mirrored in a database file which exists in the authentication server.

According to some aspects, the technology of the invention provides consumers with several different options to receive STPs which can be entered at an e-commerce site instead of a credit card number. The user of the device has an optional personal password that makes it impossible for a thief or otherwise unauthorized person to use the device without knowledge of this personal password. A consumer in e-commerce can further prevent unauthorized use by configuring the device, or his account such that only transactions utilizing STPs can be made at e-commerce sites. The stored STPs can also function in e-commerce that is conducted via cellular telephone.

Elements of the system which are disclosed hereinbelow are the consumer's STP device, optional software on the e-commerce site, which can be integrated into the merchant's shopping engine, payment server or a third party e-commerce payment gateway, and the authentication

server, which can be central or distributed. It is further contemplated that the STP device may be provided with loadable software for initial programming and updating.

Fig. 6 illustrates an arrangement for the execution of e-commerce suitable for use with the invention. According to this embodiment the consumer transmits an STP to the merchant. The merchant relays the STP to a secure identification center, which in turn converts the STP to the actual credit card number. The actual credit card number is transmitted by the secure identification center to the next processing entities in the payment chain as disclosed hereinbelow.

An STP device 100 communicates with a merchant e-commerce site 102 over a communications network 104, which is typically the Internet. The merchant e-commerce site 102 is in communication with an authentication server 106 over a network 108, which could also be the Internet, or a private network. The authentication server 106 authenticates the STP device 100 seeking to execute a transaction. Following authentication, the authentication server 106, which is aware of the actual credit card number of the consumer, submits information to a payment processing facility 110, which may be a backend server integral to the merchant e-commerce site 102, or an independent facility such as a third party payment gateway. The payment processing facility 110 communicates via a secure channel 112 with an appropriate credit card transaction processor 114. Thus the merchant stores only the STP in his database, but not the actual credit card number of the consumer. The information retained by the merchant is meaningless to a person wishing to perform future unauthorized transactions. This is an important advantage of the present invention. To the inventors' knowledge, All other existing methods known to the inventors, including smartcards, encryption techniques, and digital signatures, do not prevent the merchant from receiving and storing the consumer's credit card number in his database. The STP device 100 in accordance with one preferred embodiment of the invention is now disclosed in further detail with reference to Fig. 7, wherein the consumer's STP device 116 is a modified transaction card, such as a credit card, which has a screen 118, and a keypad comprising one or more buttons 120 which are used to advance an STP once it has been used, and for other functions. The STP device 100 can also be a cellular phone; personal digital assistant ("PDA"); pager; compact disk; diskette; hard disk (installed via the Internet or via a physical medium); a plurality of conventional credit cards; a sheet of paper with a list of STPs; or any other device which can create, store and or process STPs. If a credit card-like device is used then one or more of the following enhancements may be added in order to conveniently transfer the STP

and other encoded information: a magnetic strip, reader interface, calculator, photosensor, key-pad, microphone, speaker, radiofrequency or infrared interface, and image sensor. As shown schematically in Fig. 8, the STP device 116 holds any number of randomly generated STPs which are either embedded on a read-only memory ("ROM") or erasable programmable read-only memory ("EPROM") chip 122 in the device or created on the fly. Once the number of STPs runs low the device will alert the consumer so that he can simply call the issuing company and receive a new STP device. The STP device 116 may also be constructed as a reusable card which can be recharged with new STPs once they run out, using a reader, the Internet, special software, or other techniques as are known to the art. Once consumers receive their STPs they can add information about other credit cards they may want to use to the information stored in the STP device 116, as well as change the password that they have been given. It should be noted that since the STPs are prestored, no computational resources or time need be dedicated to their generation during execution of the transaction.

In some aspects of the invention the STP is constructed so that part of the number can be constant, signifying personal details about the card holder, such as issuing bank, country, etc., while the rest of the number changes for each transaction. The STP can also be produced through a mathematical integration of these details with the STP. The card also has a serial number 124, which is used only when the consumer deals directly with the company for customer service and reloading of the STP device 116.

Another embodiment of the STP device 116 (Fig. 6)is disclosed with reference to Fig. 9, in which the STP device 116 is realized as an enhanced transaction card 126. The transaction card 126 is provided with a display 128, which is preferably a liquid crystal type, and most preferably has graphic capabilities. In some versions the display 128 could be limited to a 7 segment type for reasons of economy, but it provides at least a single line of 16 characters. A printed coil, magnetic emulator 130, emulates a sequence of magnetic indications that occur when the transaction card 126 is swept through a credit card reader (not shown). It is intended that the user place the transaction card 126 into a card reader, rather than sweeping it, during which period the magnetic emulator 130 will operate to identify the transaction card 126 to the card reader. The magnetic emulator 130 is important mainly when conducting off-line transactions.

The transaction card 126 has lockout capability, which will protect the user against losing the card. In order to activate the card the user will have to enter his code.

The transaction card 126 has a keypad comprising five top pushbuttons 132, which allow the user to create a 5-digit personal code. The card locks itself permanently after three trials. The probability of an unauthorized user breaking this personal code in three attempts is negligible.

A standard smart card interface 134 is provided. The user is thereby afforded the ability to use and program the transaction card 126 as a smart card. The transaction card 126 is able to interface directly with a computer for verification and other purposes, using an infrared receiver 136 and an infrared transmitter 138. It is possible to incorporate other communications features, for example ultrasonic communication or radiofrequency communication using protocols such as HomeRF™ or Bluetooth™.In operation the user places the transaction card 126 in front of a suitably programmed computer, and the transaction will be verified automatically.

The processor 140 of the transaction card 126 is disclosed in further detail with reference to Fig. 10. A single ASIC 142 generally controls the transaction card 126, handles the I/O, and controls the power supply. A battery 144 provides power, and is preferably a poly-lithium flat battery, zinc oxide button battery or a light-powered battery. The battery 144 should provide power for at least 3 years and should allow the transaction card 126 to exceed 5000 operations. Provision is made for self-deactivation of the transaction card 126 after 15 seconds of powered operation.

The memory, preferably a 64 kb PROM 146, is capable of storing up to 10,000 STP numbers, each containing 16 characters (6 bits each). A controller 148 and an ancillary display controller 150 are provided for controlling the display 152, the PROM 146, and a RAM 154, which is used for various computational functions. The controller 148 controls the magnetic strip emulator 156 and the IR interface 158. Programming of the transaction card 126 is accomplished through a standard smart card interface 160. The interaction of the STP device 116 with software on the e-commerce site in accordance with some preferred embodiments of the invention is now disclosed with reference to Figs. 6, 11 and 12.

The consumer fills in the standard check-out form 162 of the merchant e-commerce site 102, and selects a payment method. The consumer is then directed to the appropriate page. The consumer manually fills in the STP number shown on the screen 118 of the STP device 116 (Fig. 7) on the line 164 instead of entering the credit card number. This entry could also be accomplished automatically or via a reader. Additional information which might be entered on

lines 166, 168, and 170, if relevant, are a personal password, the type of credit card being used, and its expiry. Appropriate software to process the consumer's order is integrated into the merchant's shopping engine, payment server or a third party e-commerce payment. Such software is known to the art, and is not further described herein, as it is outside the scope of the invention. An electronic "shopping cart" is filled by iteration of a portion of the check-out form 162 for different products. The product in some cases necessitates minimal changes to the electronic shopping cart, such as adding the card to the credit card list, which can be accomplished through an applications program interface ("API") available to conventional major shopping cart engines and internally developed ones. As shown in Fig. 12, the form 172 can be configured so that it is completely transparent to the merchant. The merchant's transaction directing software is integrated into a payment processing facility 110. This software may direct the transaction to the appropriate payment processing site or server according to the conditions specified by the STP device 100. The STPs can be entered through an e-wallet platform, or can be entered into a special coding area (not shown) within the check-out form 162.

The authentication server 106 stores data on all the STPs that have been issued to consumers, together with the comparable existing credit card numbers or bank account numbers and the consumer's personal details, as shown in Fig. 13. The data that the consumer has entered into the shopping cart is transferred through the payment processing facility 110 to the authentication server 106, together with the merchant identification, and the transaction amount. The authentication server 106 validates that the STP has not been used before, and crosschecks it against at least some of the consumer's name, address, and password. If valid, the transaction is authorized and directed to an appropriate transaction processor 114 which processes it in the same manner as a conventional credit card transaction. The merchant e-commerce site 102 may have commercial relationships with any number of transaction processors 114. The charge is then transferred from the authentication server 106 over the secure channel 112, which is typically a secure leased line, to the designated transaction processor 114, which authorizes the purchase through the card issuing bank specified by the consumer. An authorization number is returned to the merchant e-commerce site 102 via the authentication server 106, and the transaction is approved. The authentication server 106 can optionally send an email to a consumer address 119 via the Internet immediately following every transaction that occurs with an STP under his name with full transaction details. The actual transaction can be carried out using a per-

sonal computer or a telephone circuit such as a cellular phone. In this way the consumer can track the purchases and verify that all are legitimate. Alternatively, the consecutive STP or the STP counter number is sent to the consumer in a transaction authorization notice. This is used as a verification signal to the consumer that the STP has indeed reached the authentication server 106.

According to preferred embodiments of the invention, the authentication server can be implemented in either a central or distributed configuration. With the central configuration, which was explained above with reference to Fig. 6, there is a single location for the authentication server 106, which can be realized at one of several dispositions: between the STP device 100 and the merchant e-commerce site 102; between the merchant e-commerce site 102 and the transaction processor 114; between the transaction processor 114 and an issuing bank (not shown); or between an issuing bank and a the server of a credit card company (not shown).

In accordance with an alternate embodiment of the invention, in a distributed configuration, illustrated schematically in Fig. 14, there are a plurality of authentication servers 176, located at a transaction processor 178, at an issuing bank 180, an Internet portal 182, an Internet e-commerce site 184, or at a credit card company 186.

In another alternate embodiment of the invention, which is disclosed with reference to Fig. 15, the authentication server can be realized as a central database server 188 which synchronizes information with a plurality of distributed database servers 190. The distributed database servers 190 are only allowed to hold the next available STP.

The authentication server has several fraud protection mechanisms such as fraud protection algorithms, address verification system ("AVS") checks, illegal user detection, hacking interference and blocks on random number tests, in which users are only allowed to try to enter an STP a small number of times, after which the transaction will be blocked.

In yet another alternate embodiment of the invention, the STP device 100 (Fig. 6) may be realized as a wireless communication device, as shown in Fig. 16. This is similar to the previous embodiments, except now an authentication server 192 accesses the consumer's wireless device 194, preferably over a wireless channel 196. The authentication server 192 includes an STP generator 198, which produces a randomly generated STP which then is displayed on the screen of the wireless device 194. The consumer then enters this STP into the electronic shopping cart in the same manner as disclosed with respect to the previous embodiment. The STP is then

passed back to the authentication server 192, which verifies the data. The authentication server can be either centrally located or distributed. The transaction continues as explained with respect to the previous embodiment. The wireless device 194 communicates information such as the PIN, password and STP to a wireless internet provider 200 over a wireless channel 202, and receives back a transaction acknowledgement on the same wireless channel 202 or another wireless channel 204. It is still possible for the wireless device 194 to communicate directly with a merchant e-commerce site 206 over a conventional telephone line 208. At the conclusion of the transaction the authentication server 192 may communicate a transaction acknowledgment to the wireless device 194 over the wireless channel 196.

In an alternate embodiment of the invention, the consumer dials in to the authentication server through the wireless device 194 and receives an STP, which is displayed on the screen.

In still another alternative embodiment of the invention, the STPs are pre-stored on a ROM or EPROM chip of the wireless device 194. This embodiment has the advantage of increased reliability, as the transmission of the STP on the wireless channel 196 is eliminated.

Referring now to Fig. 17, an alternate embodiment of the invention is now disclosed which is suitable for use by an association of organizations which participate in e-commerce. A consumer 210 is a client of a an e-commerce service provider 212, which is a collaborator in a credit card organization. The consumer 210 has been issued appropriate credentials 214 by the e-commerce service provider 212, which allow the use of its facilities for conducting e-commerce transactions. The credentials 214 preferably include an STP device as disclosed in the previous embodiments. The e-commerce service provider 212 can be a credit card company, or an organization which facilitates e-commerce by providing secure electronic facilities for authentication for the benefit of the transaction participants, and for the transmission of other transaction-related information as will be disclosed in further detail hereinbelow. The consumer 210 is provided with an electronic communications device 216, such as a personal computer, for interfacing with they e-commerce service provider 212 and other participants in the transaction. The communications device 216 may communicate over the public telephone network, a wireless channel, or an Internet. The Internet communication may occur via the World-Wide-Web. Software in the communications device 216 can be periodically updated by downloading from the computing facilities of the e-commerce service provider 212.

When the consumer 210 accesses the Internet, using the communications device 216, he is connected immediately to a specialized authentication server 218 which checks from time to time to determine whether the connection has been terminated or is still active. When the consumer 210 desires to make a transaction he completes a check-out form 162 (Fig. 11) and submits it to a merchant web server 222. The transaction information is routed via a payment application server 224, and a gateway processing server 226, ultimately reaching a card issuing bank 228, which is a co-participant in the association. The bank 228 recognizes the relationship between the consumer 210 and the e-commerce service provider 212. The bank 228 then communicates with the authentication server 218 via the gateway processing server 226.

Upon receiving the communication from the bank 228 the authentication server 218 presents the consumer 210 with a pop-up window on the display (not shown) of the communications device 216, and requests the consumer's STP. The consumer 210 inputs the STP, which is returned to the authentication server 218 and authenticated as disclosed above. The result of the authentication is returned to the bank 228 via the gateway processing server 226, and if successful, the transaction process continues in the manner disclosed with respect to the previous embodiments.

In yet another alternate embodiment of the invention, even greater efficiency can be achieved. This is similar to the previous embodiment, except now the consumer 210 includes his STP in the check-out form 162 (Fig. 11) which is submitted to the merchant web server 222, and concurrently to the authentication server 218. Now, when the bank 228 communicates with the authentication server 218, the response is immediate because the authentication server 218 has been expecting a communication in respect of the particular STP. Communication between the consumer 210 and the authentication server 218 can be direct, or via a trusted third party, and by any communications technique, as described above. It may be encrypted or unencrypted. The technology is also applicable to offline shopping methods such as point-of-sale ("POS") shopping or card-not-present methods, such as telephone or mail transactions. This can be accomplished in several ways, for example using a magnetic strip on the card and card reader for telephone transmission. New STPs are loaded into the magnetic strip and from there they are transferred under a conventional offline transaction process into an authentication server. The STPs can be installed in a multi-application smart card or into a stand-alone credit card. The technology can also be used for non-monetary transactions such as building security, medical

file transmission, and fields such as cellular telecommunication, electronic document transmission, application service providers, and home banking transactions over public communication networks.

While this invention has been explained with reference to the structure disclosed herein, it is not confined to the details set forth and this application is intended to cover any modifications and changes as may come within the scope of the following claims:

Claims

1. A method for verifying by an identification center permissibility of a remote transaction, comprising:

selecting a variable secondary identification from a list carried by a remote party, said party being remote from said identification center, responsive to a predetermined rule;

transferring said secondary identification together with a primary identification of a transaction initiator to said identification center; wherein said secondary identification is transferred to said identification center in an unencrypted format; and

verifying at said identification center that said secondary identification is a permissible identification for performing said transaction.

2. The method according to claim 1, wherein selecting said secondary identification comprises selecting said secondary identification from a look up table.

3. The method according to claim 1, wherein selecting said secondary identification comprises determining a key to said look up table.

4. The method according to claim 3, wherein determining said key comprises incrementing an index of said key.

5. The method according to claim 3, wherein determining said key comprises receiving said key from said identification center together with acknowledgment of a previous transaction.

6. The method according to claim 1, wherein determining said secondary identification comprises changing said secondary identification responsive to performing a previous transaction.

7. The method according to claim 6, wherein changing said secondary identification comprises changing said secondary identification upon reception of confirmation of said previous transaction from said identification center.

8. The method according to claim 1, wherein said list in said remote party is carried in a memory of a transaction card; and

wherein determining said secondary identification comprises changing said secondary identification responsive to a command of a user of said card.

9. The method according to claim 8, wherein communication between said transaction card and said identification center is effected via a wireless channel.

10. The method according to claim 8, wherein changing said secondary identification responsive to said command comprises changing said secondary identification responsive to an action which uniquely identifies an owner of said card.

11. The method according to claim 1 wherein determining said secondary identification comprises determining said secondary identification responsive to one or more details of said transaction.

12. The method according to claim 1, wherein determining said secondary identification comprises determining said secondary identification irrespective of any details of said transaction.

13. The method according to claim 12, wherein determining said secondary identification comprises determining said secondary identification substantially immediately after a previous transaction.

14. The method according to claim 1, wherein verifying that said secondary identification is a permissible identification for performing said transaction comprises verifying that said secondary identification has not been used before with said primary identification.

15. The method according to claim 1, wherein said secondary identification may be used more than once with said primary identification provided said secondary identification fulfills said predetermined rule.

16. A method for verifying by an identification center permissibility of a remote transaction, comprising:

causing a remote party to initiate a communication link with an identification center, wherein said remote party is remote from said identification center;

at said remote party, selecting a variable secondary identification from a list carried by said remote party, responsive to a predetermined rule;

transferring said secondary identification together with a constant primary identification of a transaction initiator to said identification center; and

verifying at said identification center that said secondary identification is a permissible identification for performing said transaction.

17. The method according to claim 16, wherein said secondary identification is transferred to said identification center in an unencrypted format.

18. The method according to claim 16, wherein selecting said secondary identification comprises selecting said secondary identification from a look up table.

19. The method according to claim 16, wherein selecting said secondary identification comprises determining a key to said look up table.

20. The method according to claim 19, wherein determining said key comprises incrementing an index of said key.

21. The method according to claim 19, wherein determining said key comprises receiving said key from said identification center together with acknowledgment of a previous transaction.

22. The method according to claim 16, wherein determining said secondary identification comprises changing said secondary identification responsive to performing a previous transaction.

23. The method according to claim 16, wherein said list in said remote party is carried in a memory of a transaction card; and

wherein determining said secondary identification comprises changing said secondary identification responsive to a command of a user of said card.

24. The method according to claim 23, wherein communication between said transaction card and said identification center is effected via a wireless channel.

25. The method according to claim 23, wherein changing said secondary identification responsive to said command comprises changing said secondary identification responsive to an action which uniquely identifies an owner of said card.

26. The method according to claim 16 wherein determining said secondary identification comprises determining said secondary identification responsive to one or more details of said transaction.

27. The method according to claim 16, wherein determining said secondary identification comprises determining said secondary identification irrespective of any details of said transaction.

28. The method according to claim 27, wherein determining said secondary identification comprises determining said secondary identification substantially immediately after a previous transaction.

29. The method according to claim 16, wherein verifying that said secondary identification is a permissible identification for performing said transaction comprises verifying that said secondary identification has not been used before with said primary identification.

30. The method according to claim 16, wherein said secondary identification may be used more than once with said primary identification provided said secondary identification fulfills said predetermined rule.

31. A method for verifying by an identification center permissibility of a remote transaction, comprising:

selecting a variable identification from a list carried by a remote party, said remote party being remote from said identification center, responsive to a predetermined rule;

transferring said variable identification to said identification center; wherein said variable identification is transferred to said identification center in an unencrypted format; and

verifying at said identification center that said variable identification is a permissible identification for performing said transaction.

32. The method according to claim 31 wherein selecting said variable identification comprises selecting said variable identification from a look up table.

33. The method according to claim 31, wherein selecting said variable identification comprises determining a key to said look up table.

34. The method according to claim 31, wherein determining said key comprises incrementing an index of said key.

35. The method according to claim 31, wherein determining said key comprises receiving said key from said identification center together with acknowledgment of a previous transaction.

36. The method according to claim 31, wherein selecting said variable identification comprises changing said variable identification responsive to performing a previous transaction.

37. The method according to claim 36, wherein changing said variable identification comprises changing said variable identification upon reception of confirmation of said previous transaction from said identification center.

38. The method according to claim 31, wherein said list in said remote party is carried in a memory of a transaction card; and

wherein selecting said variable identification comprises changing said variable identification responsive to a command of a user of said card.

39. The method according to claim 38, wherein communication between said transaction card and said identification center is effected via a wireless channel.

40. The method according to claim 38, wherein changing said variable identification responsive to said command comprises changing said identification responsive to an action which uniquely identifies an owner of said card.

41. The method according to claim 31, wherein selecting said variable identification comprises selecting said variable identification responsive to one or more details of said transaction.

42. The method according to claim 31, wherein selecting said identification comprises selecting said identification irrespective of any details of said transaction.

43. The method according to claim 42, wherein selecting said identification comprises selecting said identification substantially immediately after a previous transaction.

44. The method according to claim 31, wherein verifying that said variable identification is a permissible identification for performing said transaction comprises verifying that said variable identification has not been used before.

45. The method according to claim 31, wherein said variable identification may be used more than once provided said variable identification fulfills said predetermined rule.

46. A transaction card for performing transactions with a verifying center, comprising:

a primary memory which stores a primary permanent identification; and

an embedded unit having a secondary memory disposed in said transaction card which provides according to a predetermined rule a secondary varying identification which is at least partially based on information non-related to any details of said transaction;

wherein said secondary varying identification is selected from a plurality of memorized identifiers in said secondary memory.

47. The transaction card according to claim 46, wherein said embedded unit comprises a processor which determines an index to said memorized identifiers.

48. The transaction card according to claim 47, wherein said processor comprises a counter of completed transactions, and a value of said index to said memorized identifiers is responsive to a value of said counter.

49. The transaction card according to claim 46, further comprising:

a display screen for displaying a currently selected secondary identification; and

a keypad for data entry by a user; and

a communications interface.

50. A method of performing a remote transaction, comprising the steps of:

initiating a first communication link between a first party and a second party, said first party having a fixed primary identification;

at said first party, selecting a variable secondary identification from a list carried by said first party, responsive to a predetermined rule;

transferring said secondary identification from said first party to said second party via said first communication link;

establishing a second communications link between said second party and an authentication center, and communicating said secondary identification from said second party to said authentication center via said second communications link, wherein said authentication center is aware of said fixed primary identification of said first party;

verifying at said authentication center that said secondary identification is a permissible identification for performing said transaction;

establishing a third communications link between said authentication center and a payment processing agent; and

communicating said fixed primary identification from said authentication center to said payment processing agent via said third communications link.

51. The method according to claim 50, wherein said secondary identification is transferred to said authentication center in an unencrypted format.

52. The method according to claim 50, wherein selecting said secondary identification comprises determining a key to a look up table.

53. The method according to claim 52, wherein determining said key comprises incrementing an index of said key.

54. The method according to claim 50, wherein selecting said secondary identification comprises changing said secondary identification responsive to a previous transaction.

55. The method according to claim 50,wherein selecting said secondary identification comprises selecting said secondary identification responsive to a detail of said transaction.

56. The method according to claim 50, wherein determining said secondary identification comprises determining said secondary identification irrespective of any details of said transaction.

57. The method according to claim 50, wherein verifying that said secondary identification is said permissible identification for performing said transaction comprises verifying that said secondary identification has not been used before with said primary identification.

58. The method according to claim 50, further comprising the steps of:

establishing a fourth communication link between said first party and said authentication center; and

communicating said secondary identification from said first party to said authentication center via said fourth communication link.

59. The method according to claim 50, wherein said first party effects communication on said first communication link using a communication device having memorized data and program instructions.

60. The method according to claim 59, wherein said communication device comprises a CD.

61. The method according to claim 59, further comprising the steps of:

storing a plurality of identification data as software on a media;

transferring said software to said communication device; and

selecting a datum from said identification data for use as said secondary identification.

62. The method according to claim 60, further comprising the step of transferring confidential information from said first party to said authentication center prior to initiating a first communication link.

63. The method according to claim 62, further comprising the step of

at said authentication center associating said secondary identification with said confidential information of said first party; and

transferring said confidential information with said fixed primary identification to said payment processing agent.

FIG. 1

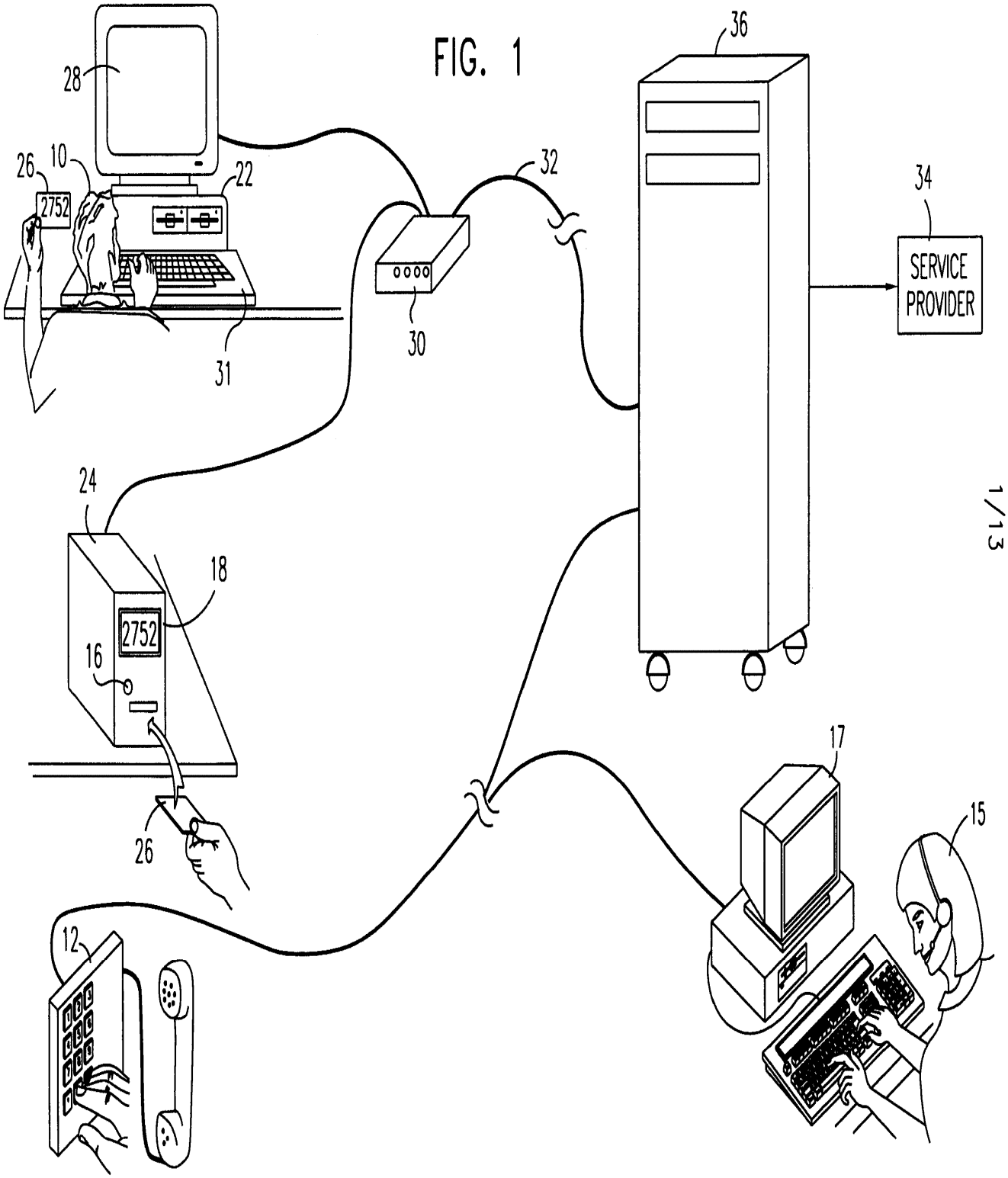

28
36
26
10
22
32
34
2752
SERVICE PROVIDER
30
31
24
18
2752
16
17
15
26
12

FIG. 2

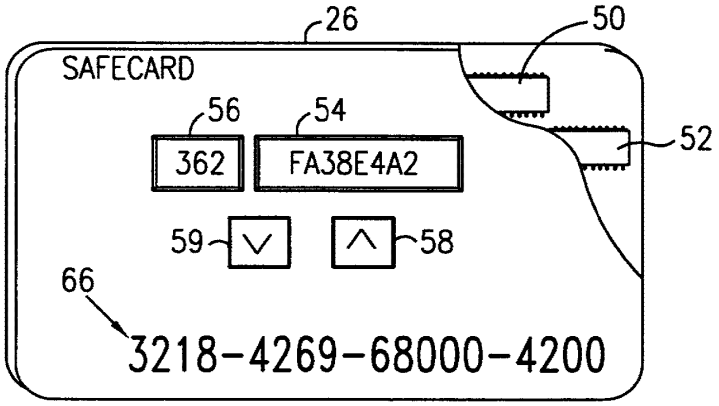

26
50
SAFECARD
56
54
362
FA38E4A2
52
59
58
66
3218-4269-68000-4200

FIG. 3

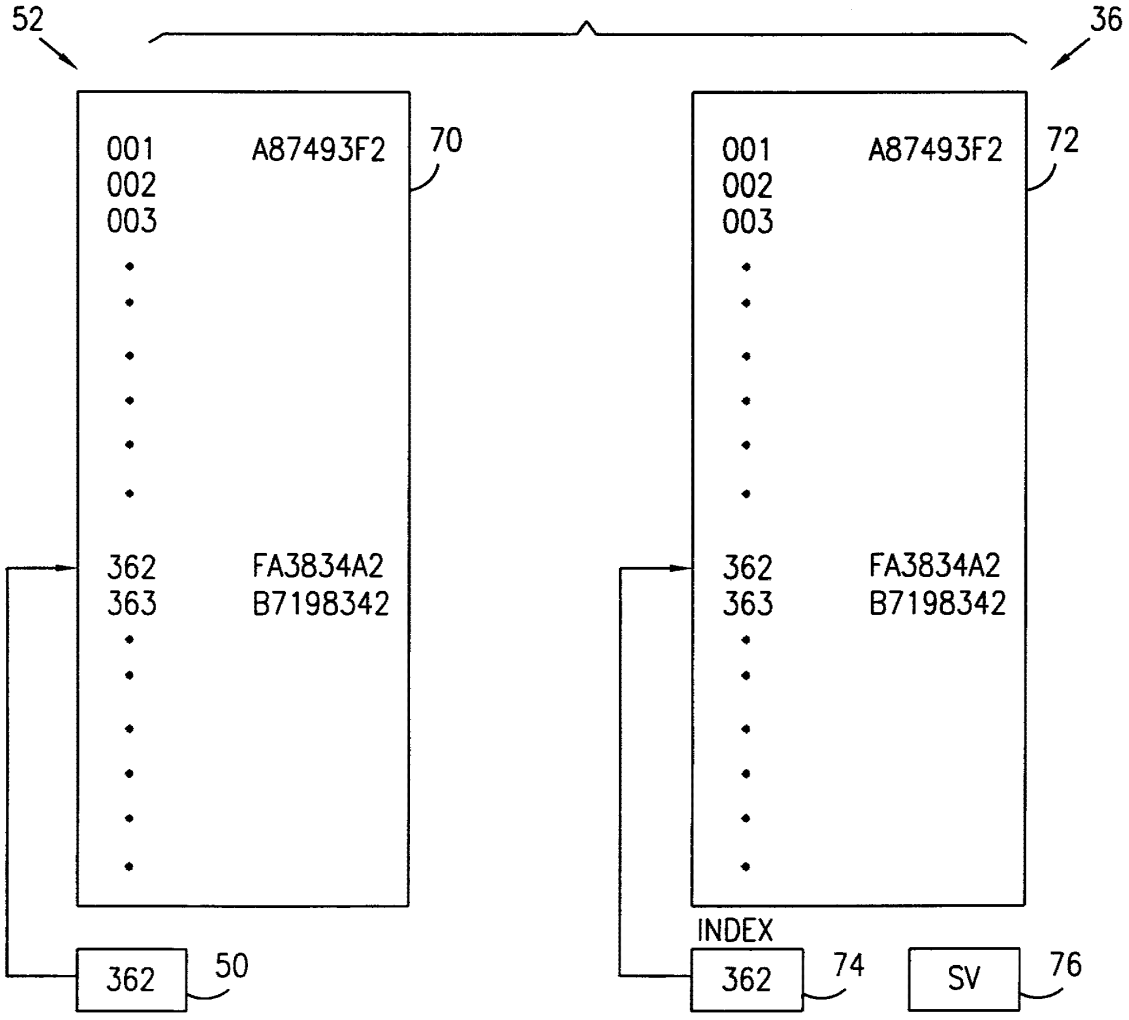

52
36
001 A87493F2
002
003
70
362 FA3834A2
363 B7198342
362
50
001 A87493F2
002
003
72
362 FA3834A2
363 B7198342
INDEX
362
74
SV
76

FIG. 4

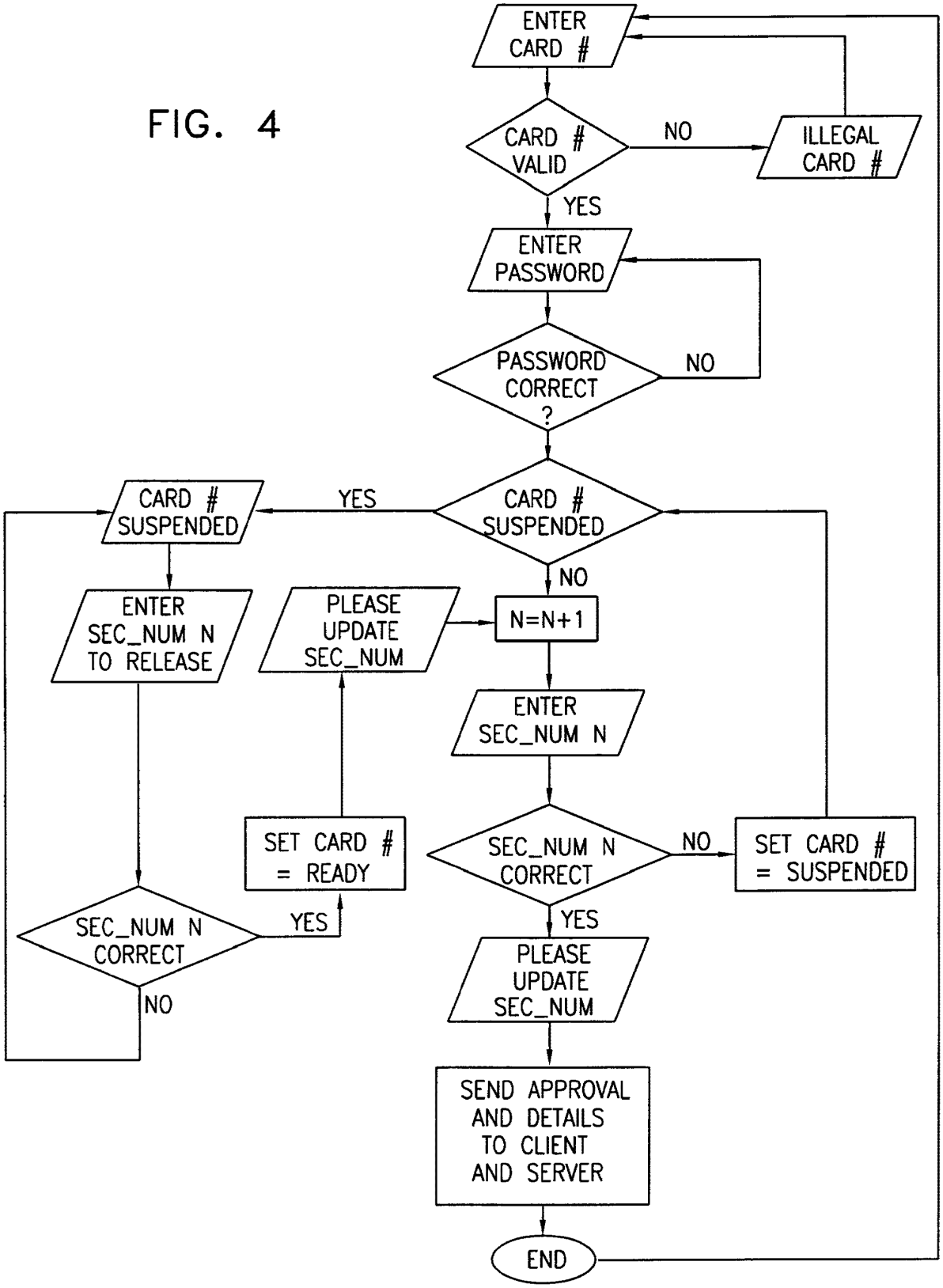

ENTER CARD #
CARD # VALID
NO
ILLEGAL CARD #
YES
ENTER PASSWORD
PASSWORD CORRECT ?
NO
CARD # SUSPENDED
YES
CARD # SUSPENDED
NO
ENTER SEC_NUM N TO RELEASE
PLEASE UPDATE SEC_NUM
N=N+1
ENTER SEC_NUM N
SET CARD # = READY
SEC_NUM N CORRECT
NO
SET CARD # = SUSPENDED
SEC_NUM N CORRECT
YES
NO
YES
PLEASE UPDATE SEC_NUM
SEND APPROVAL AND DETAILS TO CLIENT AND SERVER
END

FIG. 5

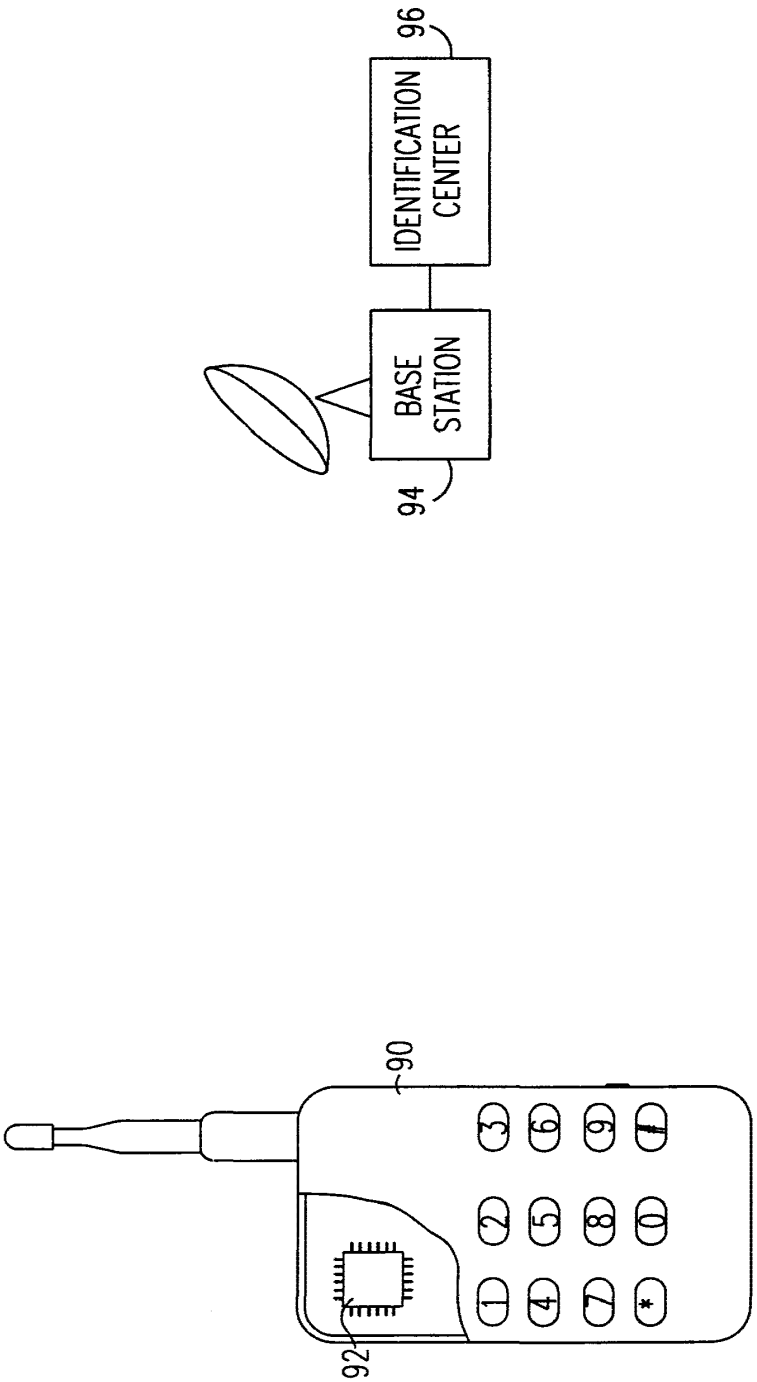


FIG. 6

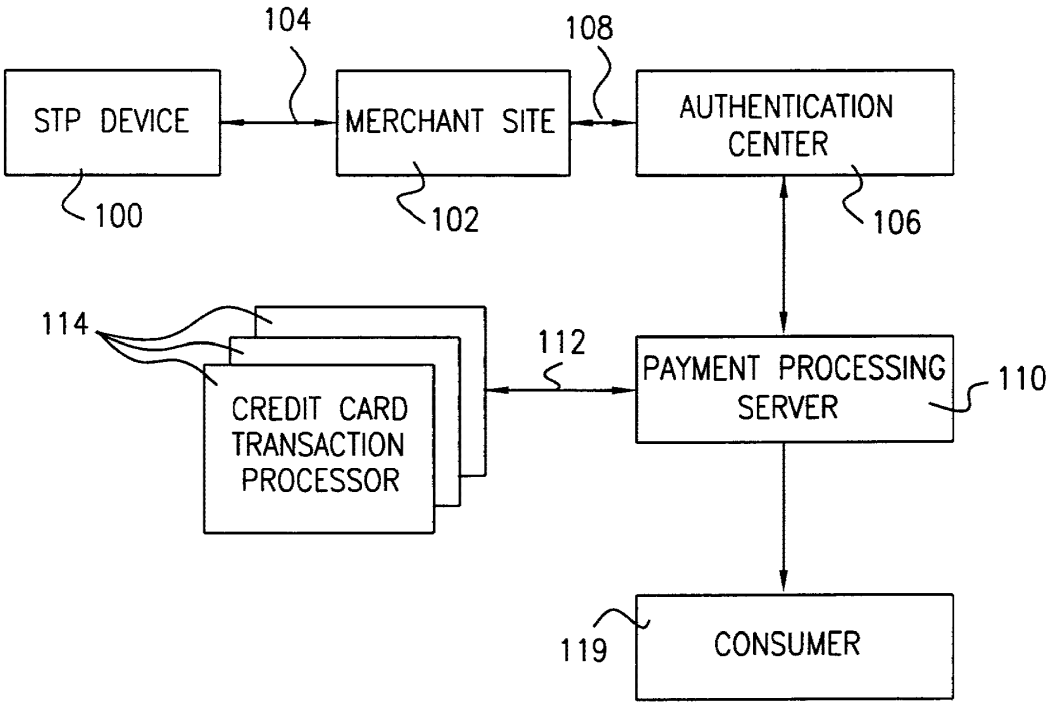

104
108
STP DEVICE
MERCHANT SITE
AUTHENTICATION CENTER
100
102
106
114
112
PAYMENT PROCESSING SERVER
110
CREDIT CARD TRANSACTION PROCESSOR
119
CONSUMER

FIG. 7

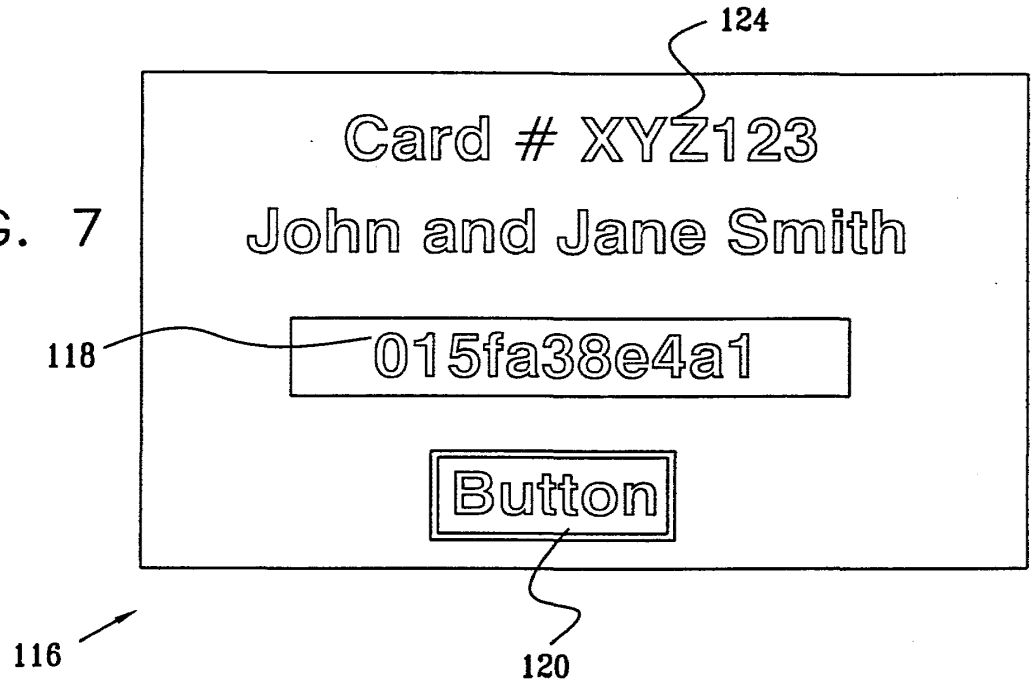


FIG. 8

ROM	001 rt237yu5 ... 015 fa38e4a1 016 xy568AD9 017 k6a7F18

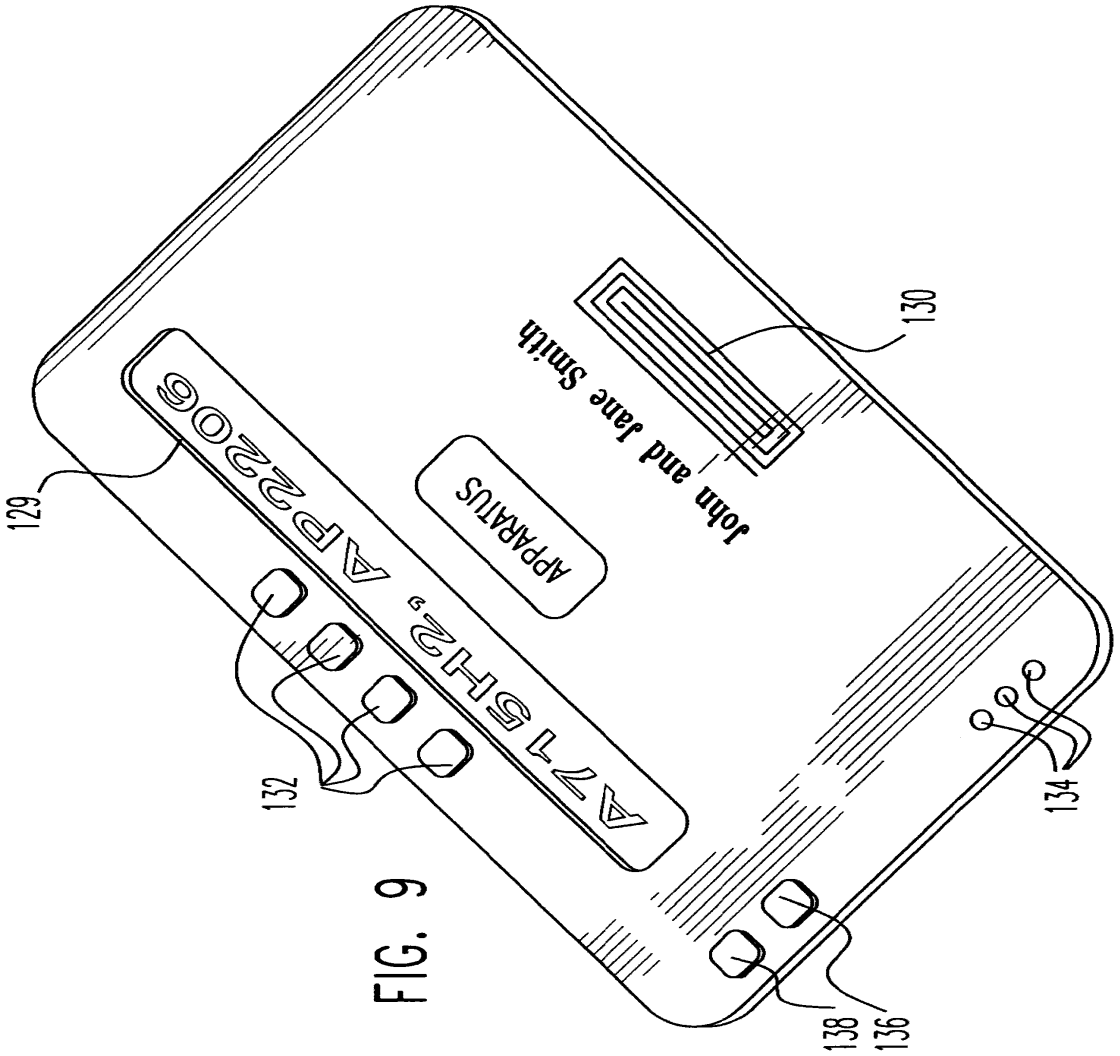


FIG. 9

FIG. 10

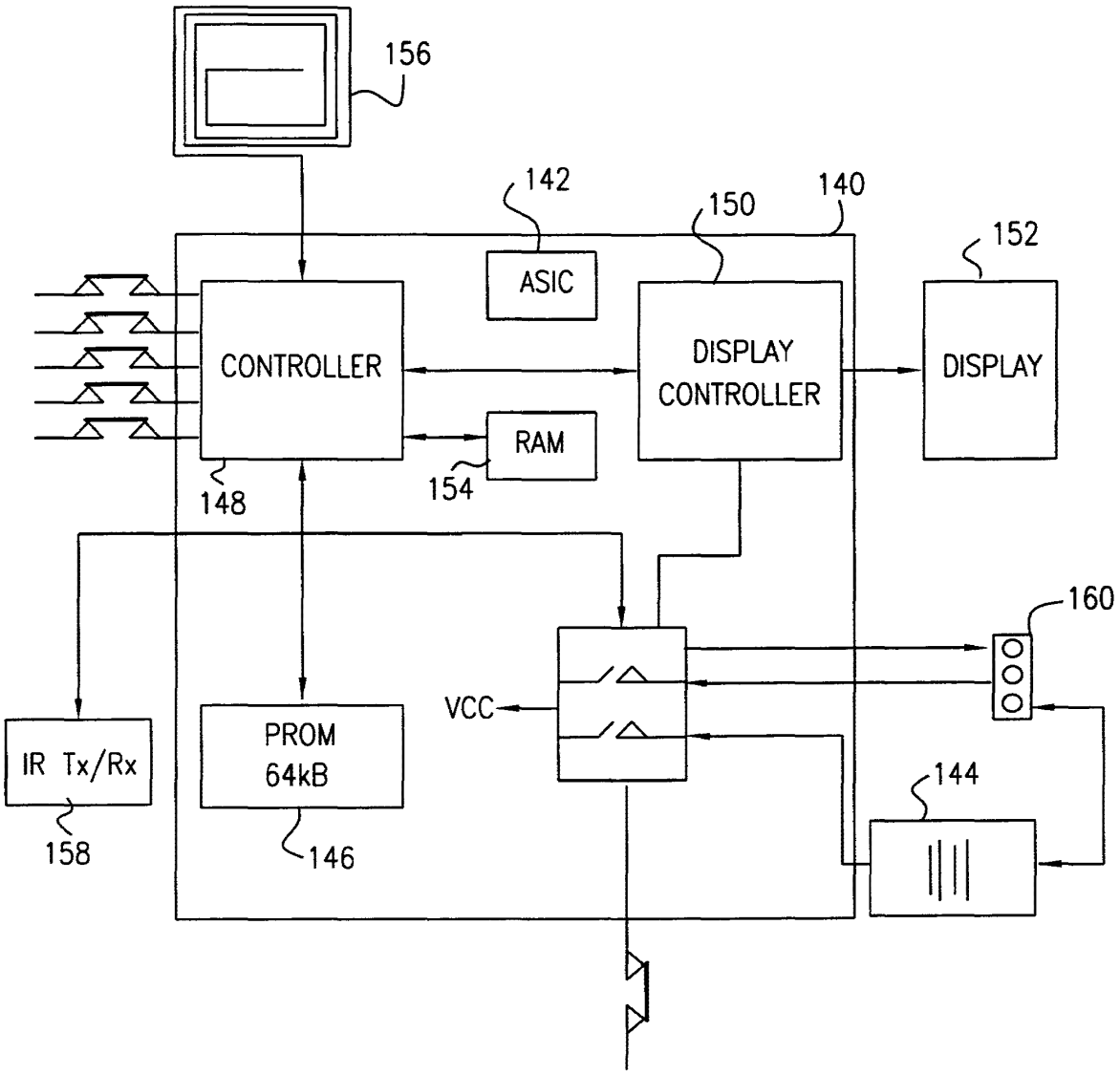

156
142
150
140
152
ASIC
CONTROLLER
DISPLAY CONTROLLER
DISPLAY
RAM
148
154
160
VCC
IR Tx/Rx
PROM 64kB
144
158
146

FIG. 11

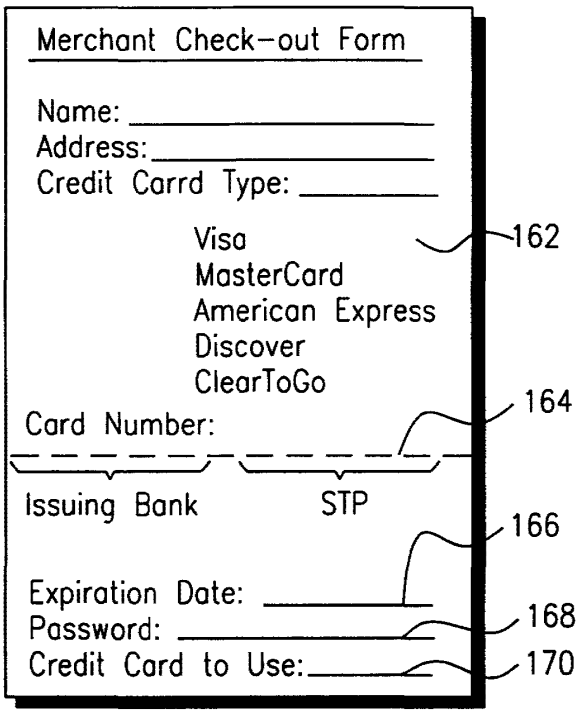


FIG. 12

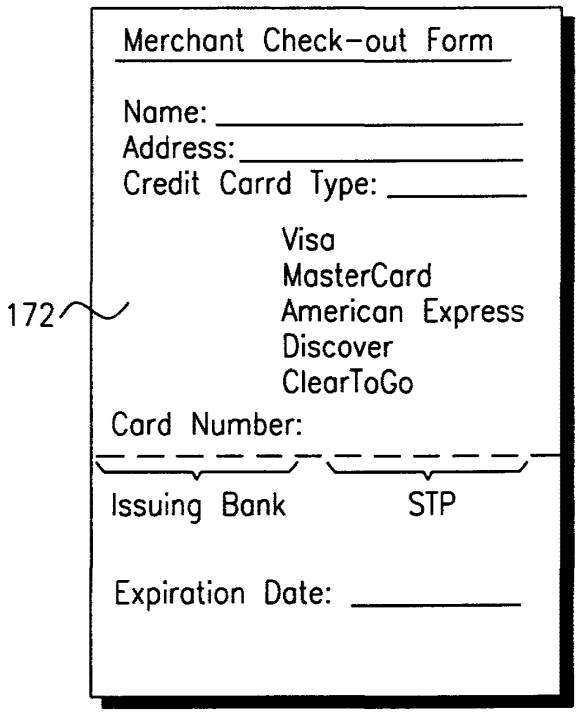


FIG. 13

Information stored in the Central Authentication Server			
Card # XYZ123, John and Jane Smith, Address, password: A2F8			
STPs:	001..... .... 015fa38e4a1 016.....	Credit Cards:	Visa# MasterCard # AmEx # Discover # ....

FIG. 14

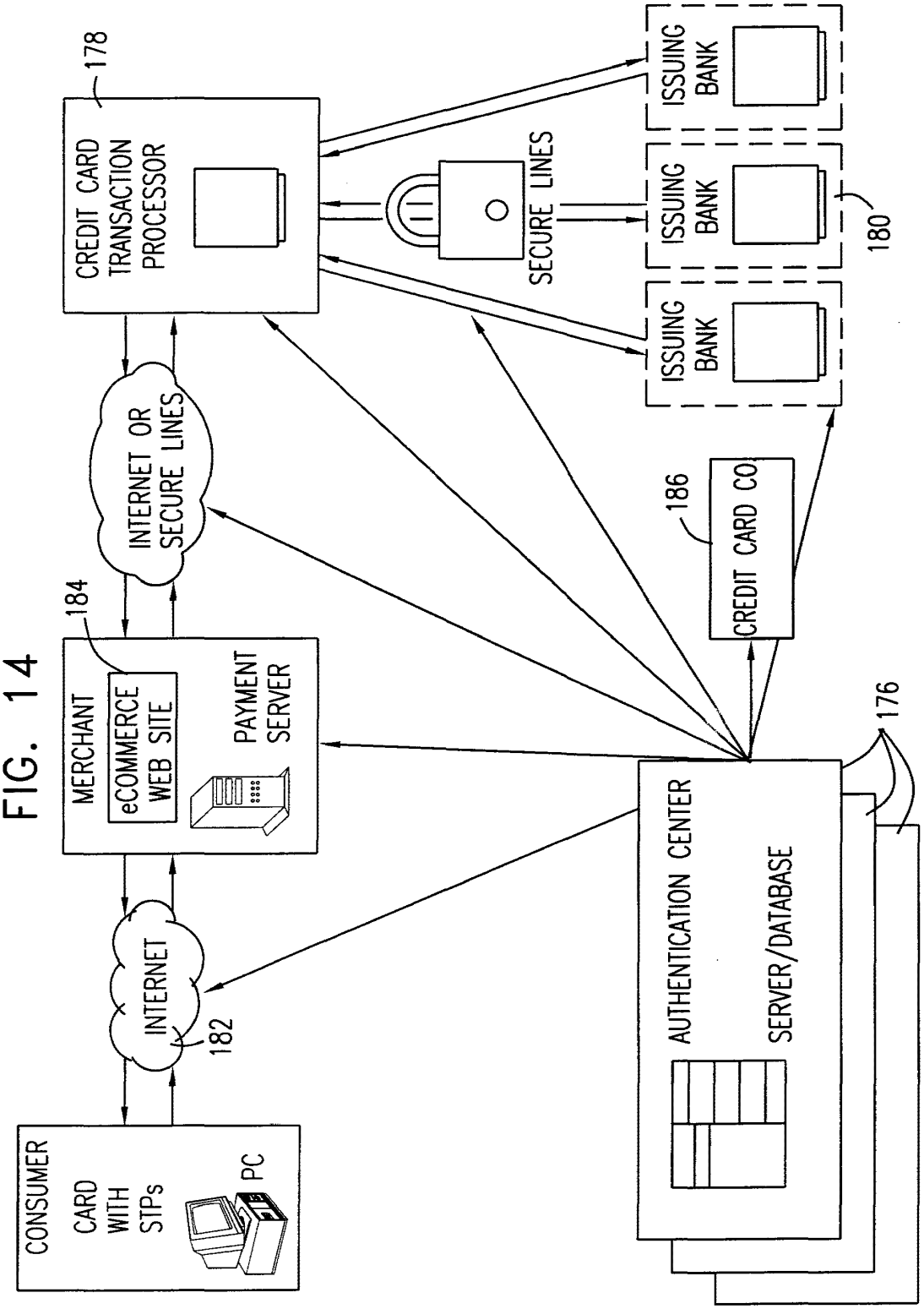

178
CREDIT CARD TRANSACTION PROCESSOR
SECURE LINES
ISSUING BANK
ISSUING BANK
ISSUING BANK
180
INTERNET OR SECURE LINES
186
CREDIT CARD CO
184
MERCHANT
eCOMMERCE WEB SITE
PAYMENT SERVER
176
AUTHENTICATION CENTER
SERVER/DATABASE
INTERNET
182
CONSUMER
CARD WITH STPs
PC

FIG. 15

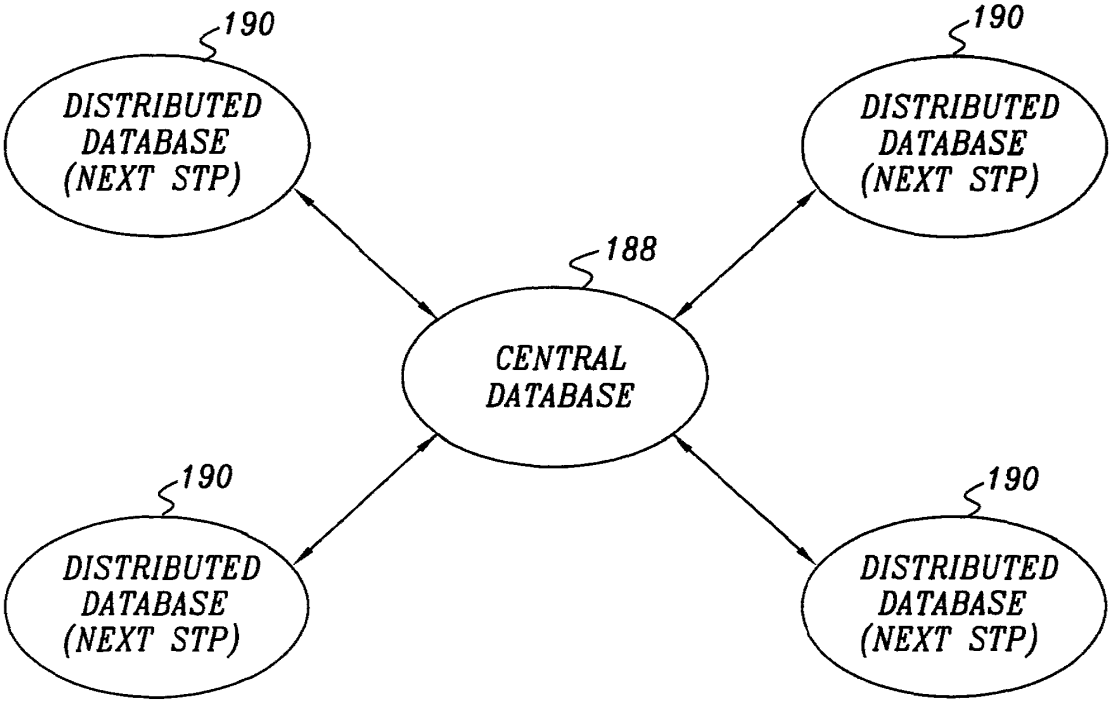
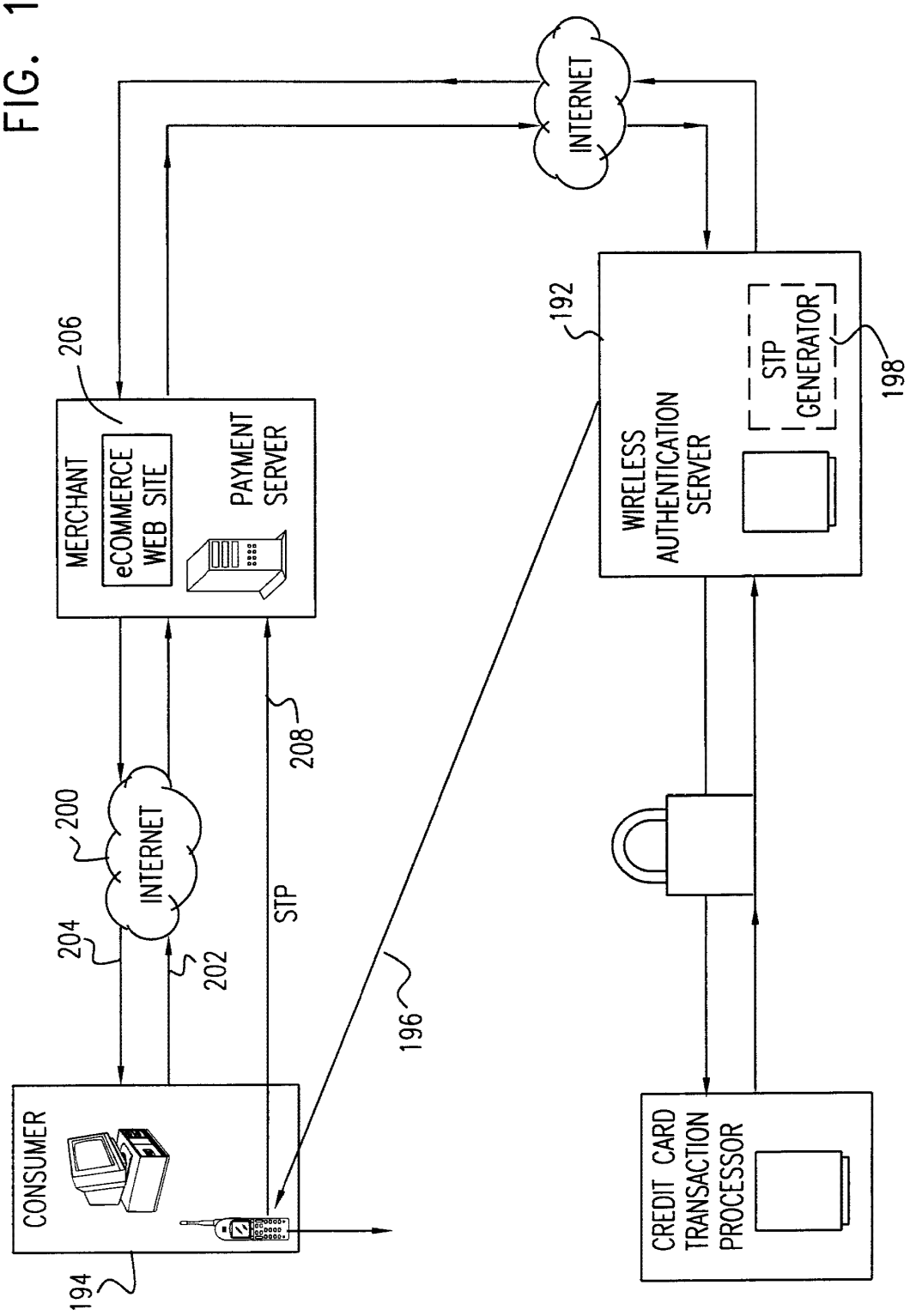

190
DISTRIBUTED DATABASE (NEXT STP)
190
DISTRIBUTED DATABASE (NEXT STP)
188
CENTRAL DATABASE
190
DISTRIBUTED DATABASE (NEXT STP)
190
DISTRIBUTED DATABASE (NEXT STP)

FIG. 16


INTERNET
206
MERCHANT
eCOMMERCE WEB SITE
PAYMENT SERVER
192
WIRELESS AUTHENTICATION SERVER
STP GENERATOR
198
208
200
INTERNET
204
202
STP
196
CONSUMER
194
CREDIT CARD TRANSACTION PROCESSOR

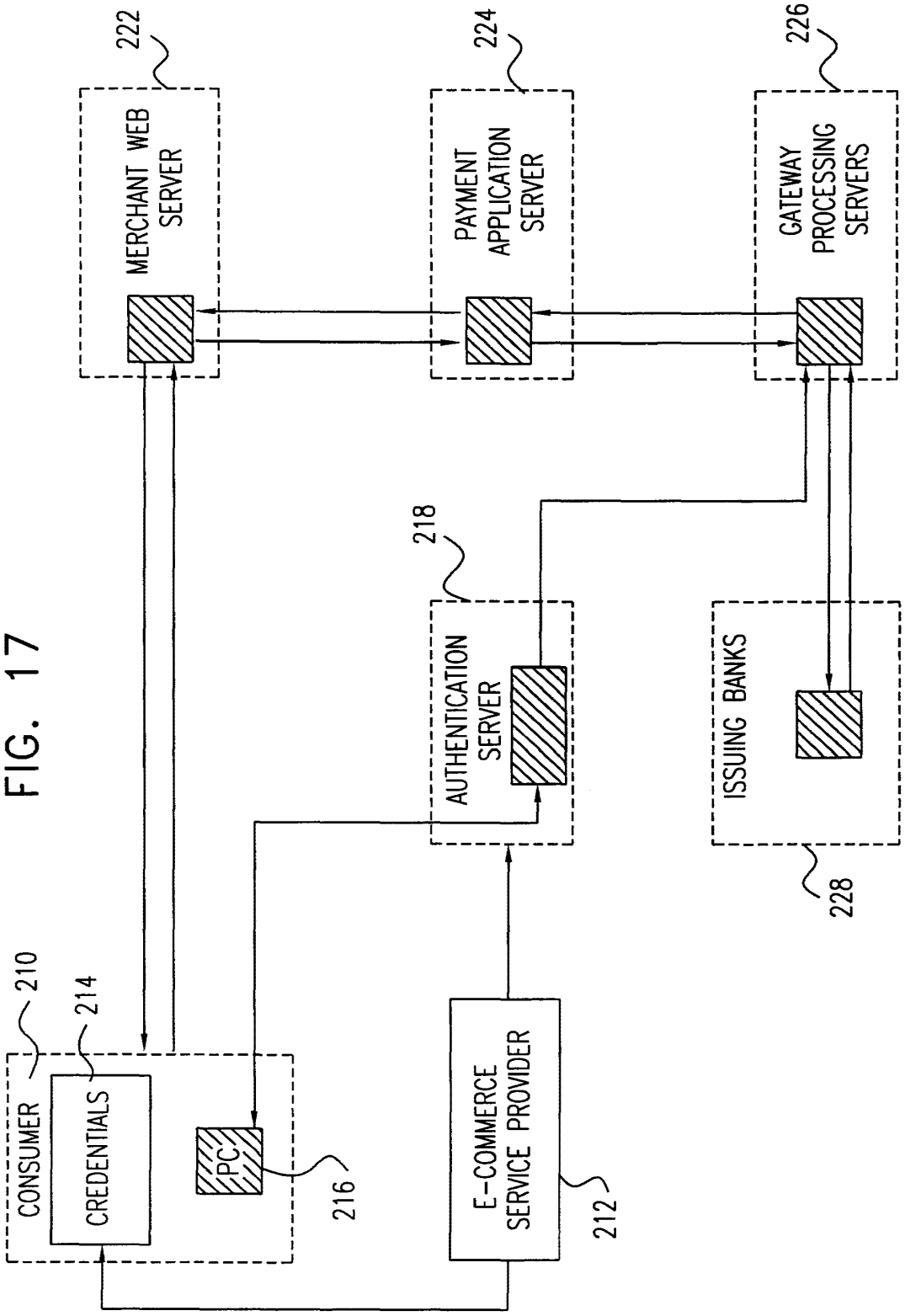

222
MERCHANT WEB SERVER
224
PAYMENT APPLICATION SERVER
226
GATEWAY PROCESSING SERVERS
218
AUTHENTICATION SERVER
ISSUING BANKS
228
210
CONSUMER
214
CREDENTIALS
PC
216
E-COMMERCE SERVICE PROVIDER
212

FIG. 17

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL00/00211

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :GO6F 17/60; H06K 1/00; H04L 9/00
US CL :705/67

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 705/67

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Please See Extra Sheet.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,502,765 A (ISHIGURO et al.) 26 March 1996, Abstract; col. 2, lines 24-67; col. 3 lines 1-17; col. 5, lines 65-67; col. 6, lines 1-67; col. 7, lines 1-28; col. 8, lines 8-48; col. 10, lines 7-48; col. 11, lines 3-39; col. 12, lines 21-32; col. 14, lines 26-44; col. 16, lines 11-57	1-63
Y	US 5,717,756 A (COLEMAN) 10 February 1998, Abstract; col. 3, lines 31-63; col. 4, lines 47-55; col. 7, lines 46-67; col. 8, lines 1-60; col. 9, lines 24-44; col. 10, lines 48-67; col. 11, lines 1-67; col. 12, lines 1-6; fig. 3A [100, 202, 206, 208, 210, 212, 213, 214, 218]	1-63

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 16 JUNE 2000	Date of mailing of the international search report 20 SEP 2000
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer ALLEN MACDONALD Telephone No. (703) 305-3900

Form PCT/ISA/210 (second sheet) (July 1998)★

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL00/00211

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,721,781 A (DEO et al.) 24 February 1998, Abstract; fig. 1 [2b, 3, 4]; fig. 4A [2,4]; fig. 7 [4, 5, 6]; fig. 9 [2b, 4, 6]	1-63
A	US 5,396,558 A (ISHIGURO et al.) 07 March 1995, Abstract	1-63
A	US 5,436,970 A (RAY et al.) 25 July 1995, Abstract	1-63
A	US 5,526,428 A (ARNOLD) 11 June 1996, Abstract.	1-63
A	US 5,581,615 A (STERN) 03 December 1996, Abstract.	1-63
A	US 5,887,065 A (AUDEBERT) 23 March 1999, Abstract.	1-63
A,P	US 5,999,624 A (HOPKINS) 07 December 1999, Abstract.	1-63
A,P	US 6,005,939 A (FORTENBERRY et al.) 21 December 1999, Abstract.	1-63

Form PCT/ISA/210 (continuation of second sheet) (July 1998)★

B. FIELDS SEARCHED
Electronic data bases consulted (Name of data base and where practicable terms used):

DIALOG, STN
SEARCH TERMS: remote transaction, network, link, code, credit/purchase/debit/smart card, encrypt$4, identif$7, stor$4, database, table, list, verif$7

PTO/SB/30EFS (01-22)
Approved for use through 05/31/2024. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL
(Submitted Only via EFS-Web)

Application Number	17528073	Filing Date	2021-11-16	Docket Number (if applicable)	WYAT-0002-13C12US	Art Unit	2876
First Named Inventor	David WYATT			Examiner Name	LEE, SEUNG H.		

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV

SUBMISSION REQUIRED UNDER 37 CFR 1.114

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

- ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____
- ☐ Other _____

☒ Enclosed

- ☐ Amendment/Reply
- ☒ Information Disclosure Statement (IDS)
- ☐ Affidavit(s)/ Declaration(s)
- ☐ Other _____

MISCELLANEOUS

☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months _____
(Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

☐ Other _____

FEES

The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.
☒ The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to Deposit Account No 504160

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

☒ Patent Practitioner Signature

Applicant Signature

PTO/SB/30EFS (01-22)
Approved for use through 05/31/2024. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Signature of Registered U.S. Patent Practitioner			
Signature	/Jose S. Garcia/	Date (YYYY-MM-DD)	2023-01-12
Name	Jose S. Garcia	Registration Number	43,628

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

(12) UK Patent Application (19) GB (11) 2485442 (13) A

(43) Date of A Publication 16.05.2012

(21) Application No: 1118513.9

(22) Date of Filing: 26.10.2011

(30) Priority Data:
(31) 61406821 (32) 26.10.2010 (33) US
(31) 13281272 (32) 25.10.2011 (33) US

(71) Applicant(s):
Cubic Corporation
(Incorporated in USA – California)
9333 Balboa Avenue, San Diego, California 92123,
United States of America

(72) Inventor(s):
Philip B Dixon
David Lapczynski

(74) Agent and/or Address for Service:
J A Kemp
14 South Square, Gray's Inn, London, WC1R 5JJ,
United Kingdom

(51) INT CL:
G06Q 50/30 (2012.01) ***G06Q 20/22*** (2012.01)

(56) Documents Cited:
None

(58) Field of Search:
Other: **No search performed: Section 17(5)(b)**

(54) Title of the Invention: **Determining companion and joint cards in transit**
Abstract Title: **Analysis of transport identifier data to recognize potential patterns, relationships or sequences that could represent misuse of an account**

(57) Detecting potential misuse of a primary account number (PAN) associated with a first handheld media in a transit system having one or more access points, including creating a user account, enrolling a first handheld media for use as a fare media for a transit product, where the PAN is stored in the user account, receiving a plurality of fare transaction records, each fare transaction record includes the PAN associated with the first handheld media and a transaction identifier, determining a potential misuse of a handheld media associated with the PAN based on at least the relationship, pattern or sequence between a plurality of the transaction identifiers and in response an action is taken related to using the first handheld media as a fare media for the transit product.

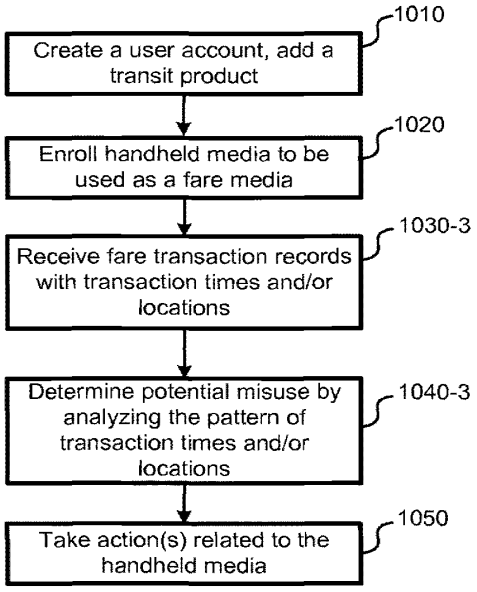


FIG. 10C

GB 2485442 A

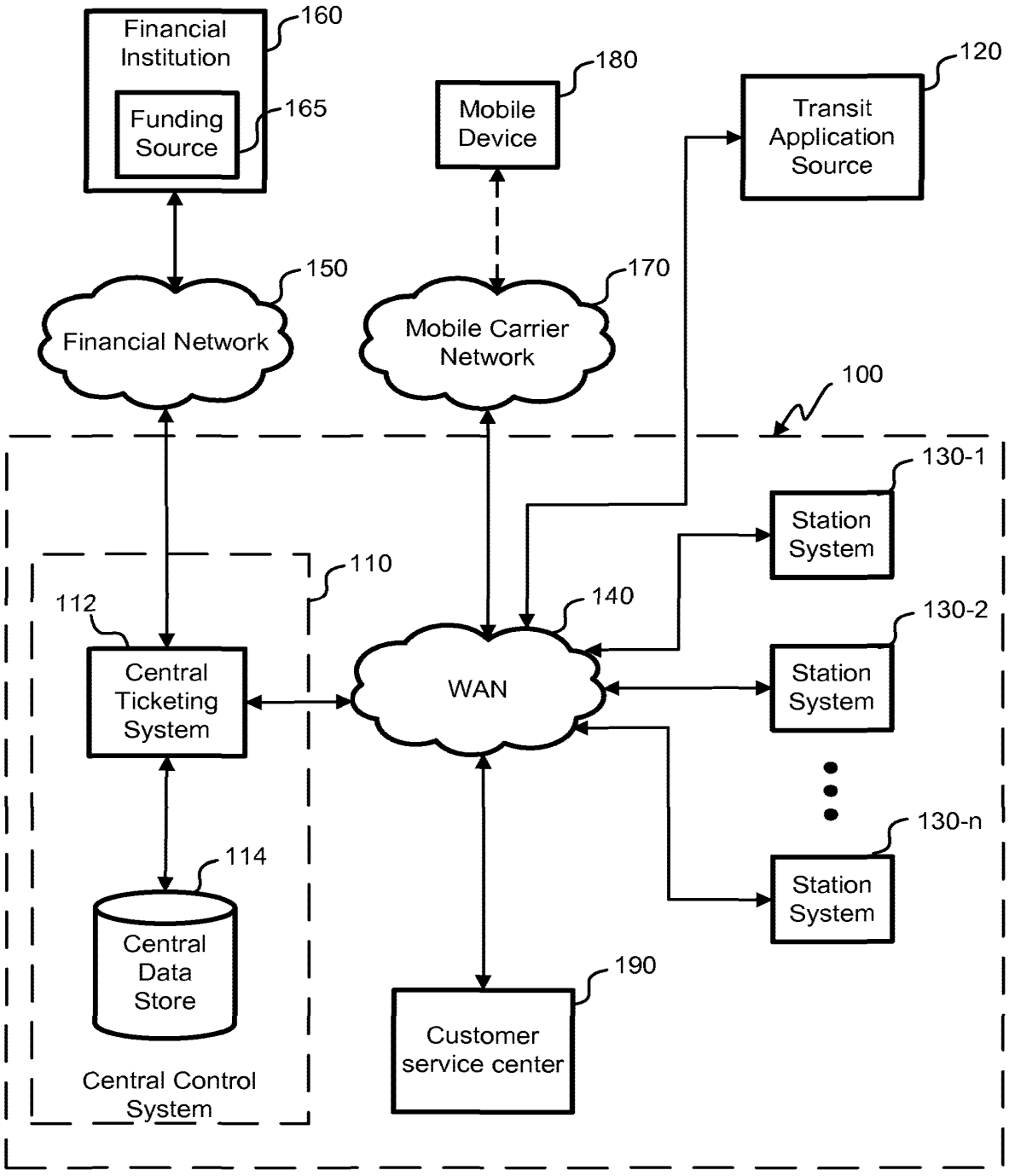

Financial Institution
160
Funding Source
165
Mobile Device
180
Transit Application Source
120
Financial Network
150
Mobile Carrier Network
170
100
130-1
Station System
110
112
140
130-2
Central Ticketing System
WAN
Station System
130-n
114
Station System
Central Data Store
190
Customer service center
Central Control System

FIG. 1

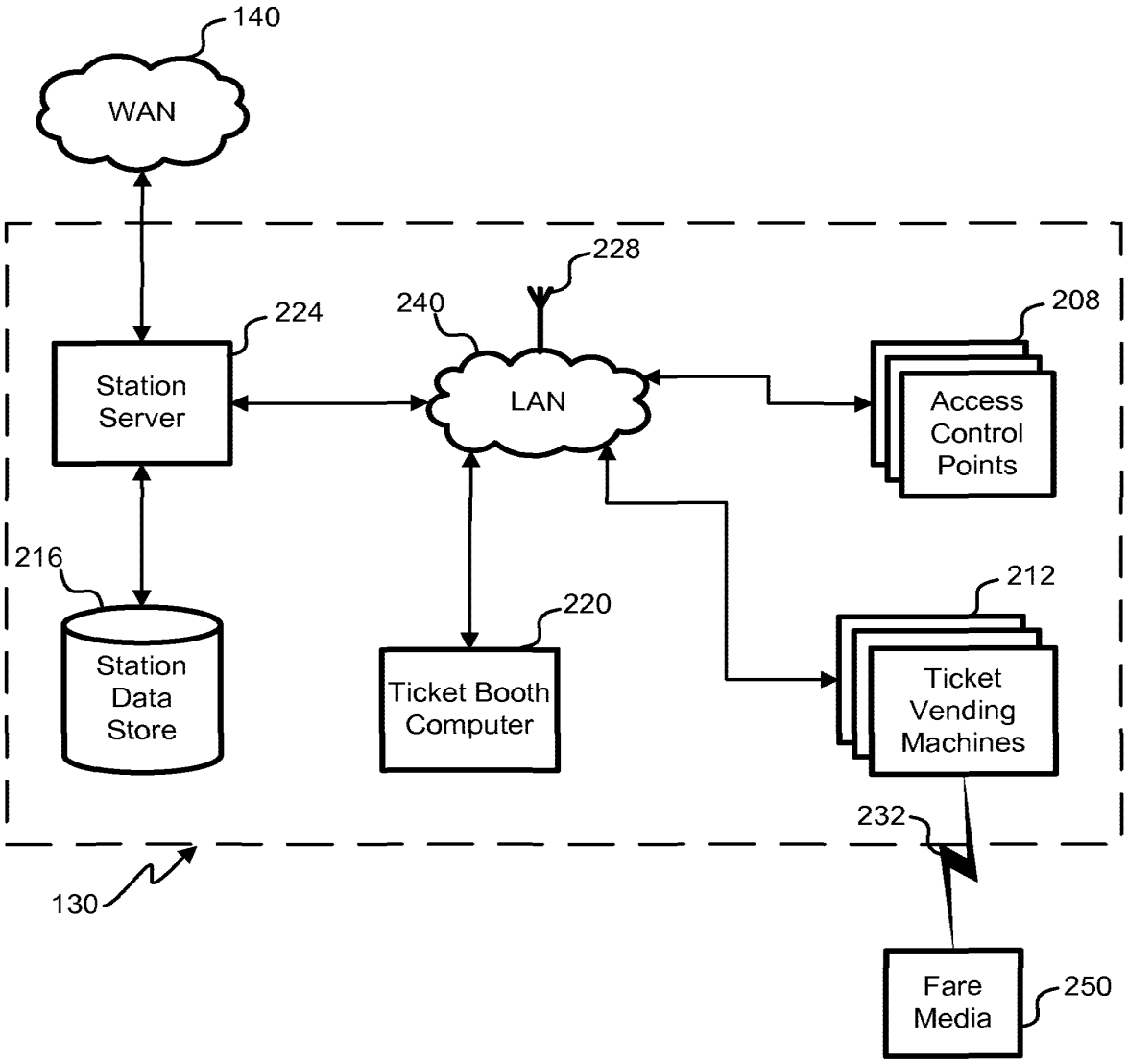

140
WAN
228
240
224
208
Station Server
LAN
Access Control Points
216
212
220
Station Data Store
Ticket Booth Computer
Ticket Vending Machines
232
130
Fare Media
250

FIG. 2

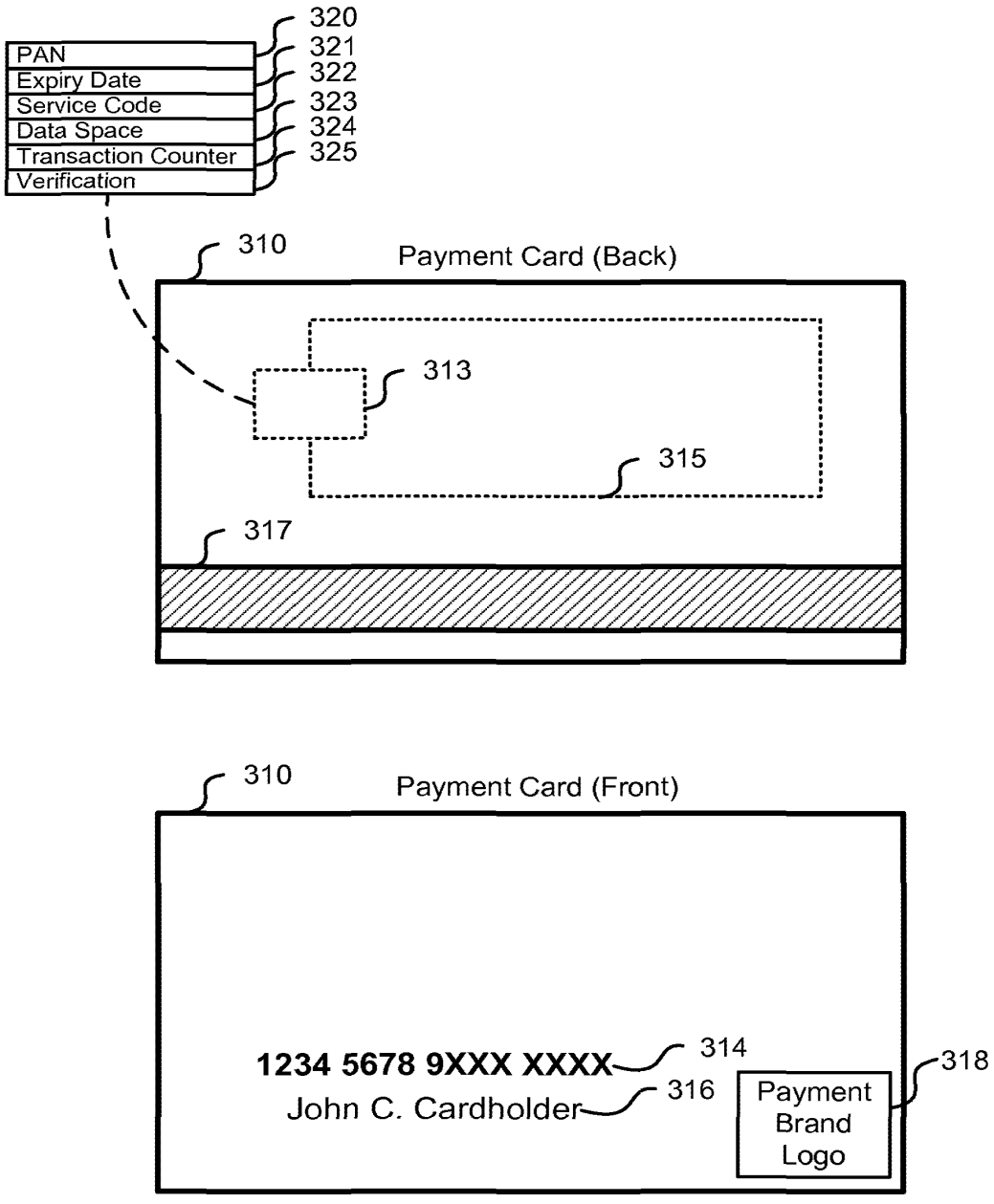

PAN
Expiry Date
Service Code
Data Space
Transaction Counter
Verification
320
321
322
323
324
325
310
Payment Card (Back)
313
315
317
310
Payment Card (Front)
1234 5678 9XXX XXXX
314
John C. Cardholder
316
Payment Brand Logo
318

FIG. 3

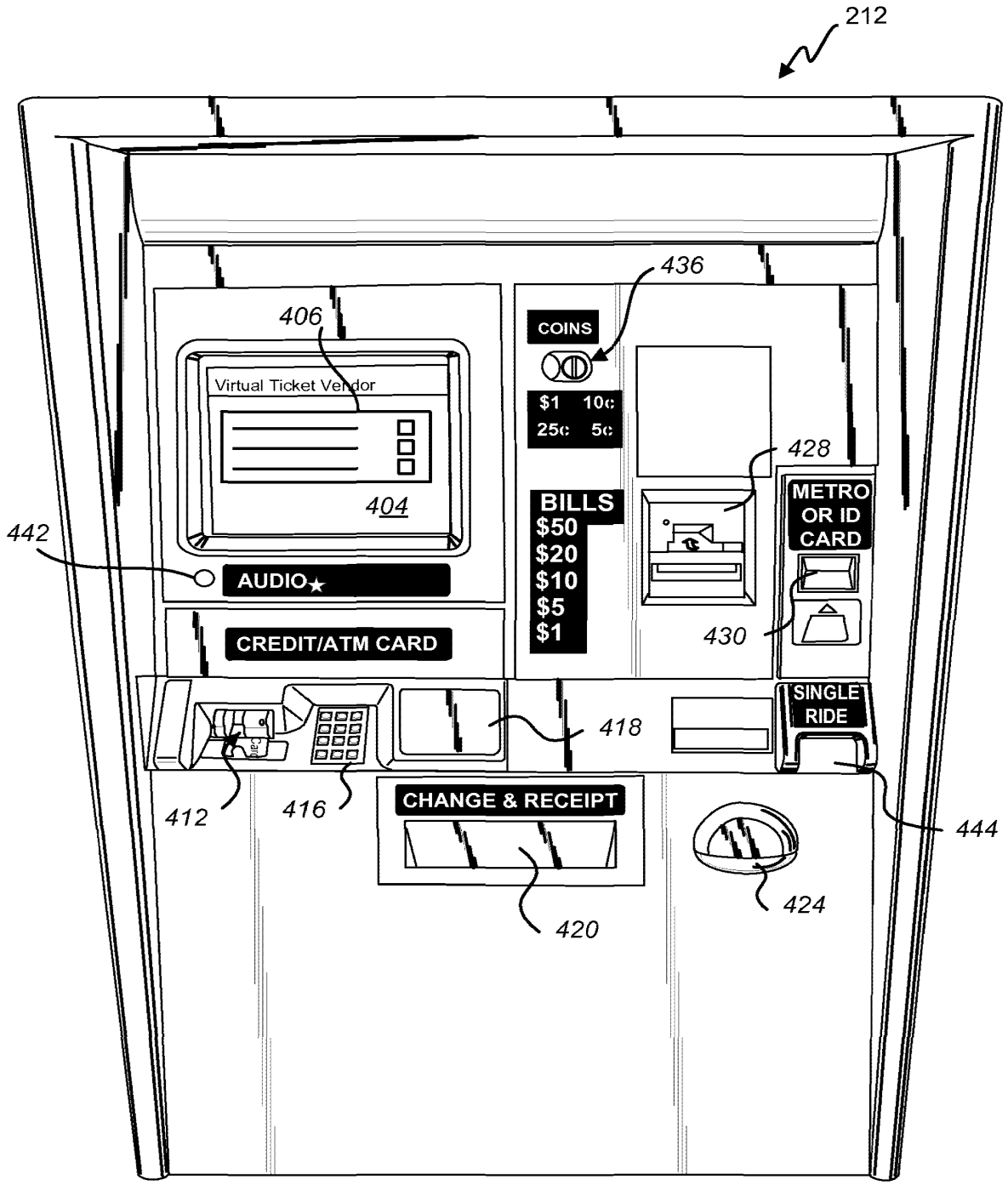

212
436
406
COINS
Virtual Ticket Vendor
$1 10¢
25¢ 5¢
428
404
BILLS
$50
$20
$10
$5
$1
METRO OR ID CARD
442
AUDIO★
CREDIT/ATM CARD
430
SINGLE RIDE
418
412
416
CHANGE & RECEIPT
444
424
420

FIG. 4

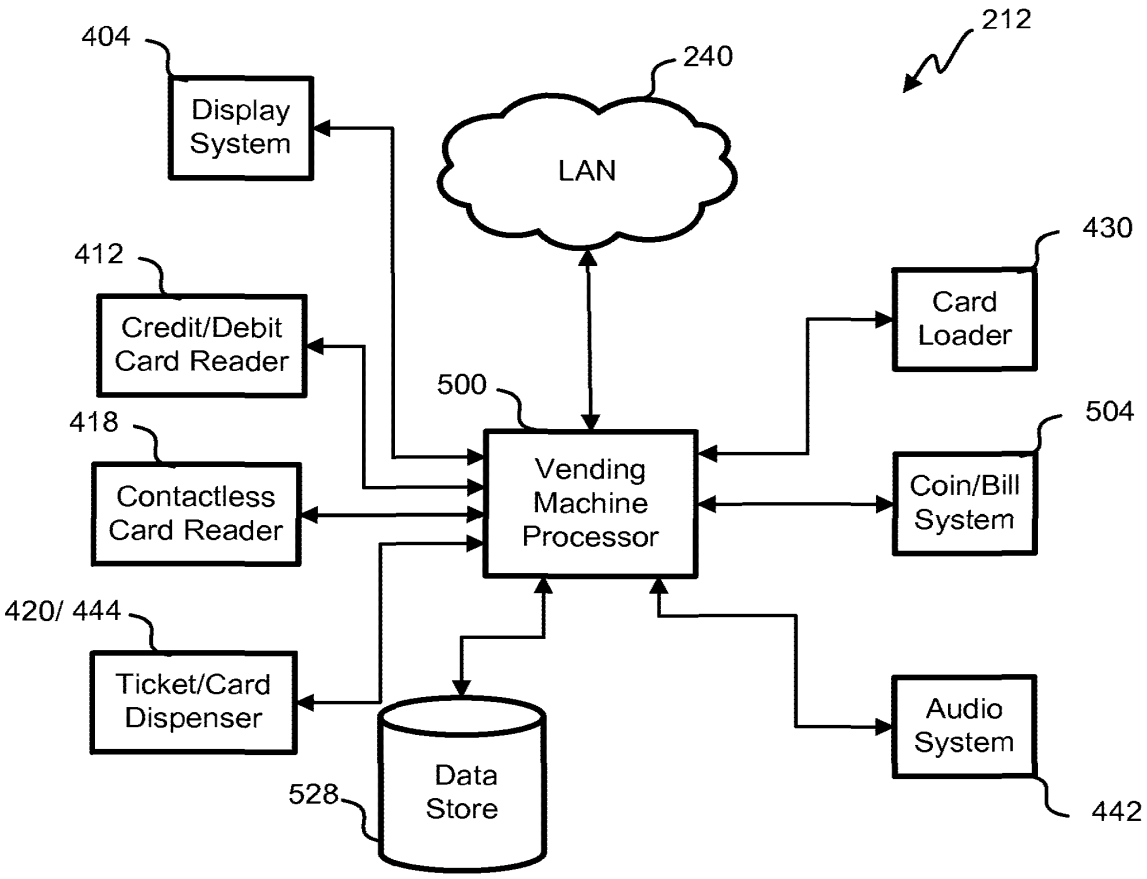

212
404
Display System
240
LAN
412
Credit/Debit Card Reader
430
Card Loader
500
418
Contactless Card Reader
Vending Machine Processor
504
Coin/Bill System
420/ 444
Ticket/Card Dispenser
Audio System
528
Data Store
442

FIG. 5

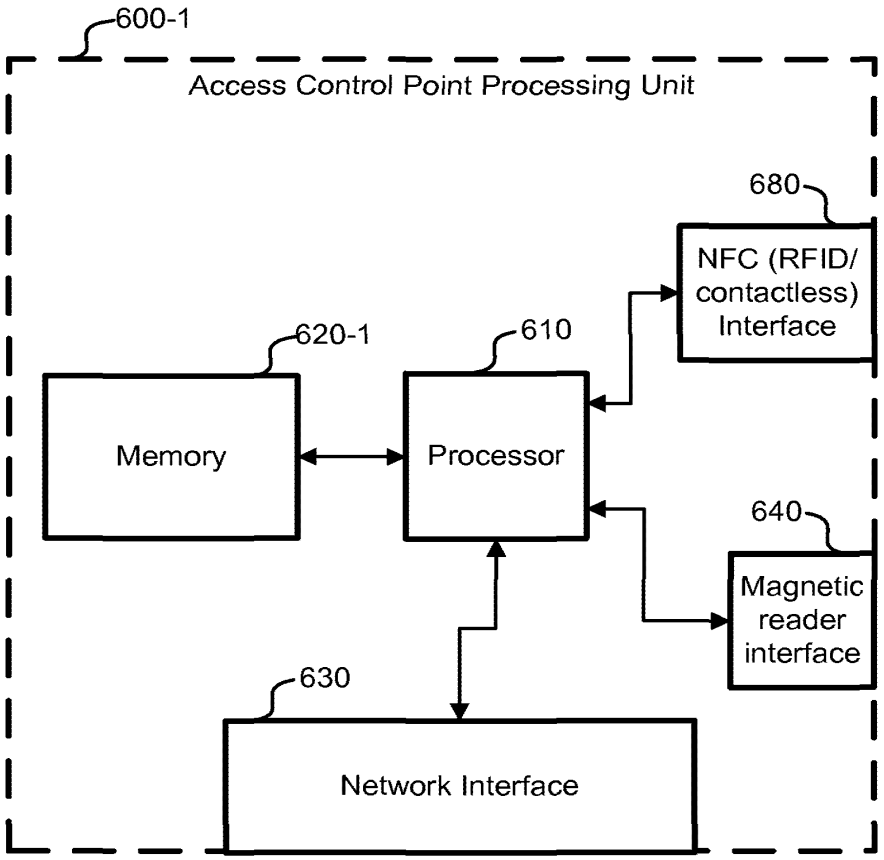

600-1
Access Control Point Processing Unit
680
NFC (RFID/ contactless) Interface
620-1
610
Memory
Processor
640
Magnetic reader interface
630
Network Interface

FIG. 6A

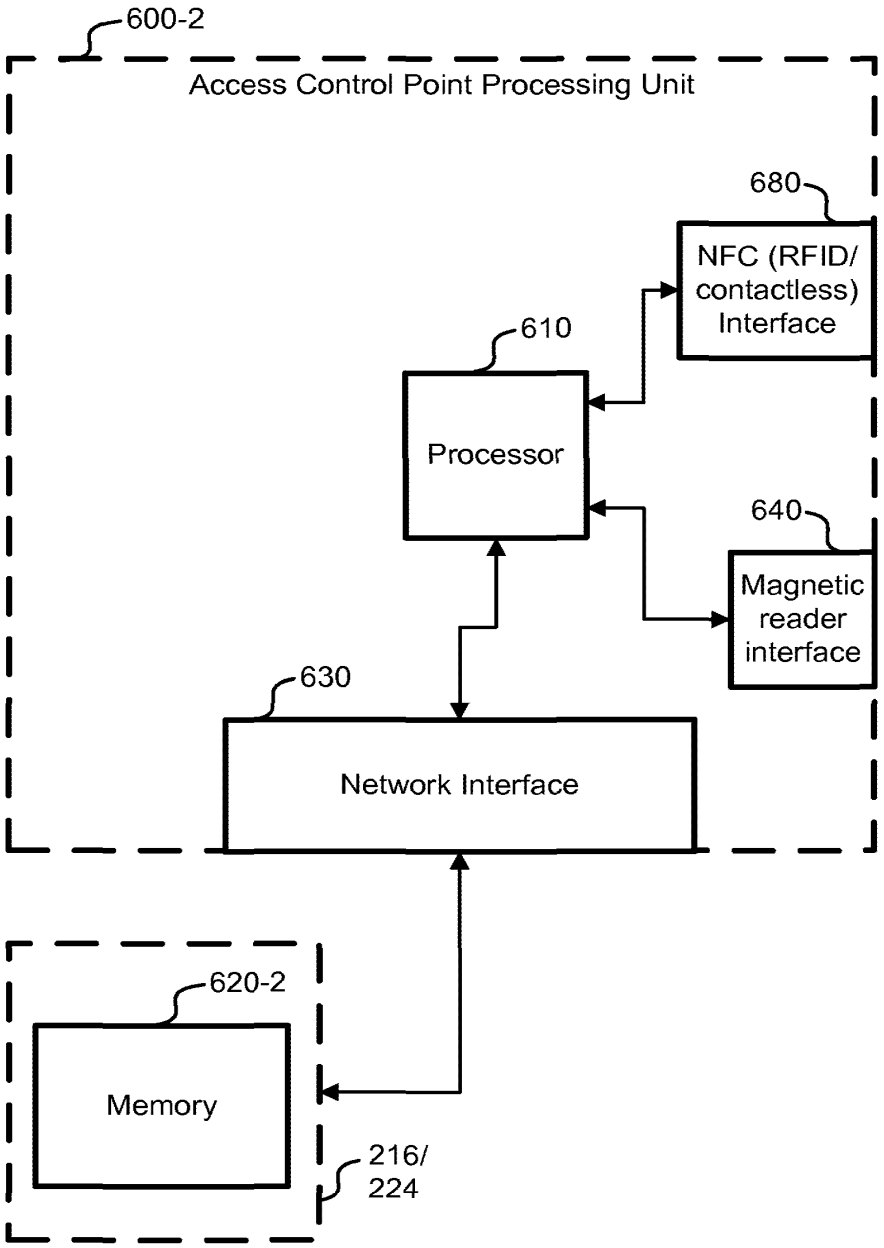

600-2
Access Control Point Processing Unit
680
NFC (RFID/ contactless) Interface
610
Processor
640
Magnetic reader interface
630
Network Interface
620-2
Memory
216/ 224

FIG. 6B

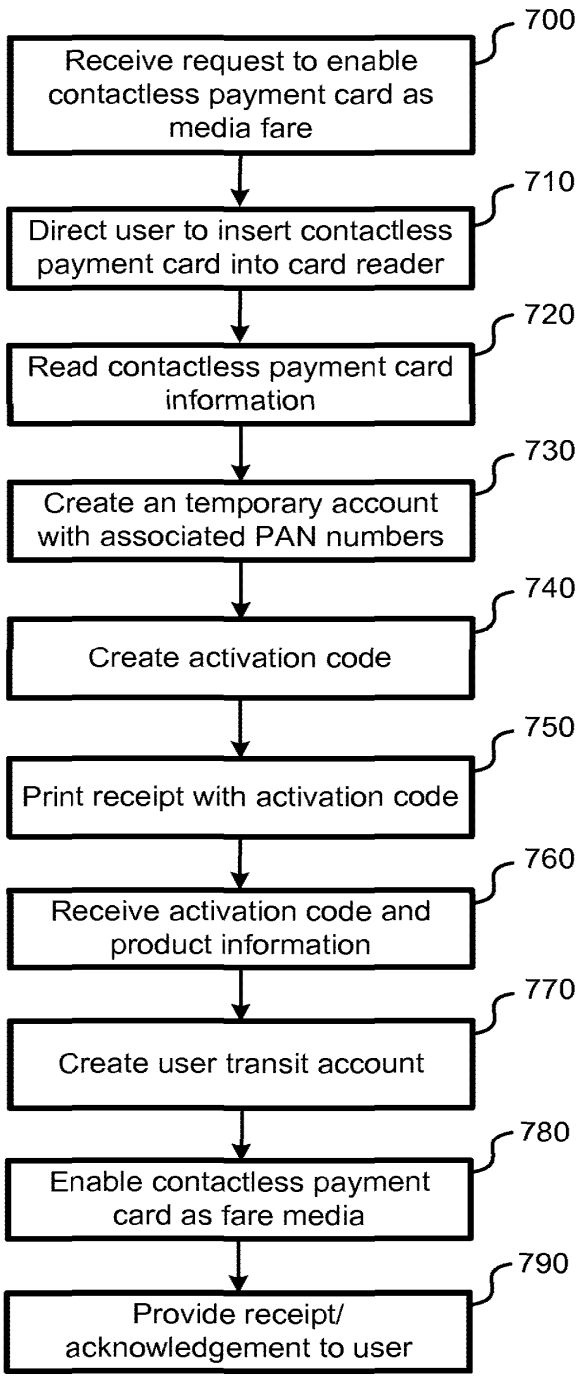

700
Receive request to enable contactless payment card as media fare
710
Direct user to insert contactless payment card into card reader
720
Read contactless payment card information
730
Create an temporary account with associated PAN numbers
740
Create activation code
750
Print receipt with activation code
760
Receive activation code and product information
770
Create user transit account
780
Enable contactless payment card as fare media
790
Provide receipt/ acknowledgement to user

FIG. 7A

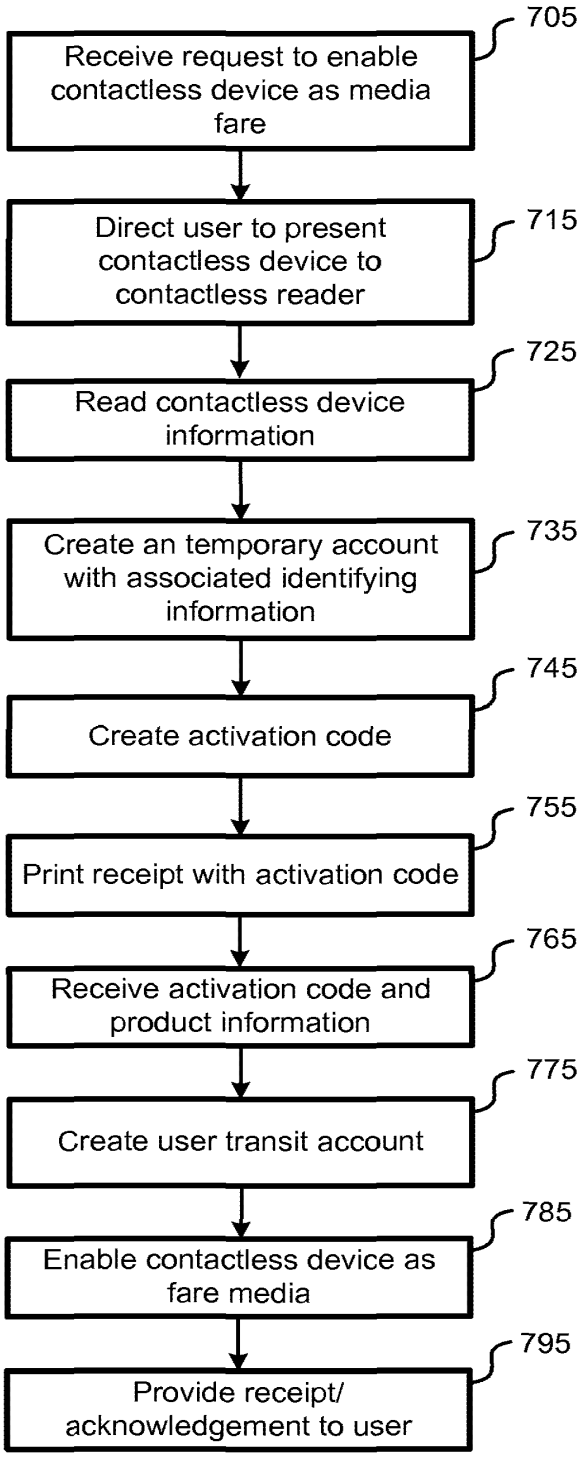

705
Receive request to enable contactless device as media fare
715
Direct user to present contactless device to contactless reader
725
Read contactless device information
735
Create an temporary account with associated identifying information
745
Create activation code
755
Print receipt with activation code
765
Receive activation code and product information
775
Create user transit account
785
Enable contactless device as fare media
795
Provide receipt/ acknowledgement to user

FIG. 7B

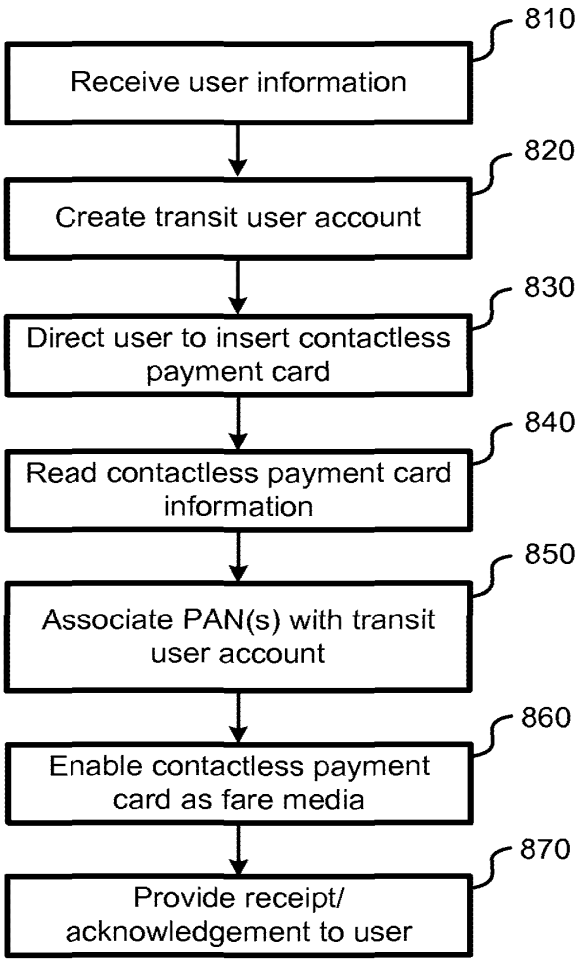

810
Receive user information
820
Create transit user account
830
Direct user to insert contactless payment card
840
Read contactless payment card information
850
Associate PAN(s) with transit user account
860
Enable contactless payment card as fare media
870
Provide receipt/ acknowledgement to user

FIG. 8A

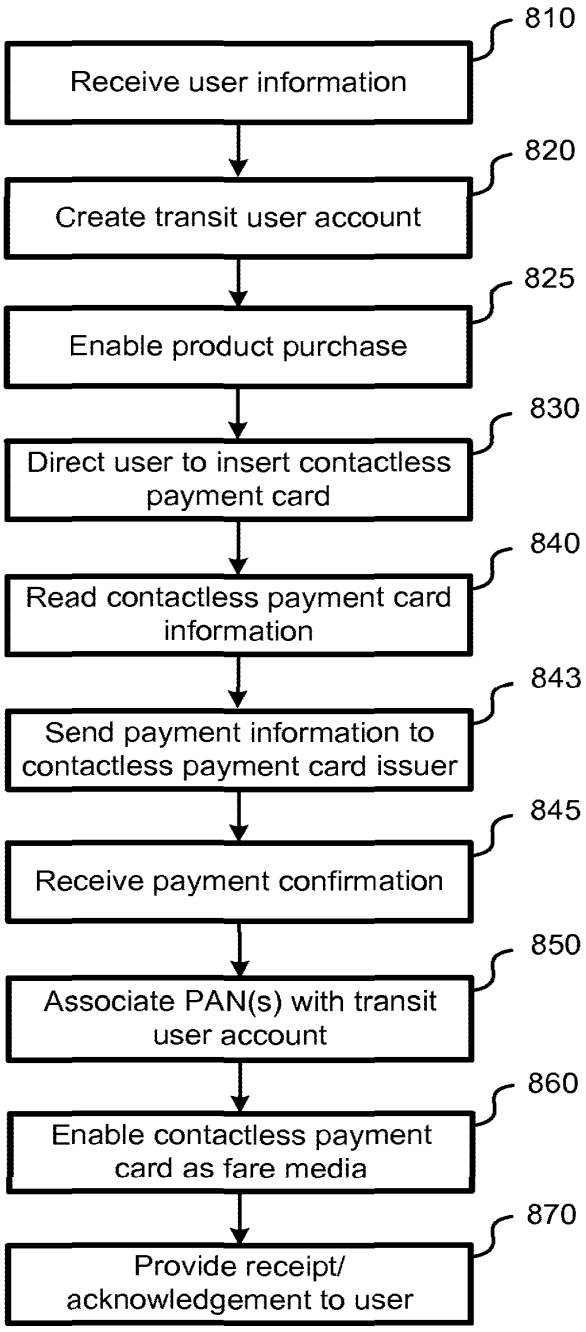

810
Receive user information
820
Create transit user account
825
Enable product purchase
830
Direct user to insert contactless payment card
840
Read contactless payment card information
843
Send payment information to contactless payment card issuer
845
Receive payment confirmation
850
Associate PAN(s) with transit user account
860
Enable contactless payment card as fare media
870
Provide receipt/ acknowledgement to user

FIG. 8B

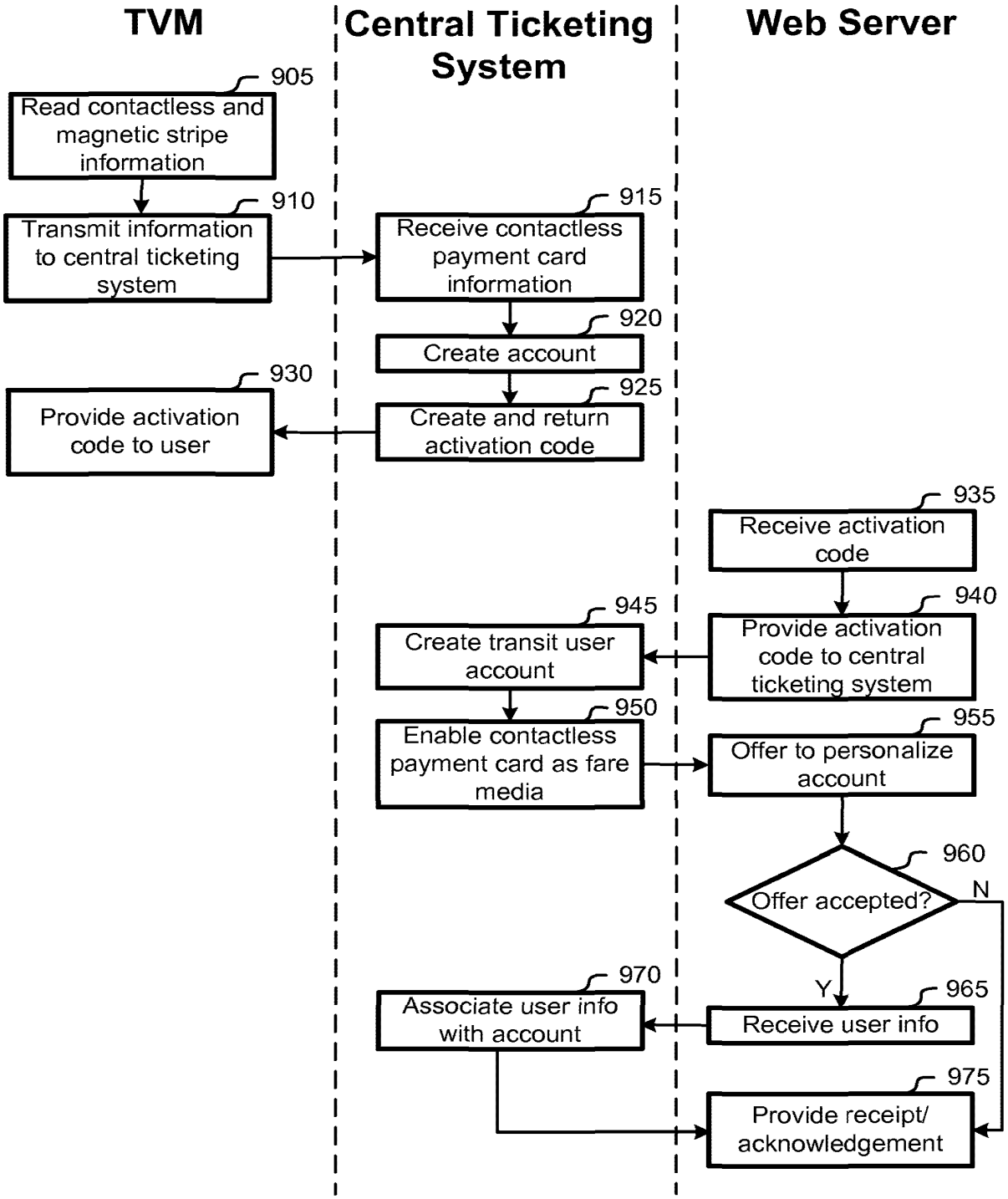

TVM
Central Ticketing System
Web Server
905
Read contactless and magnetic stripe information
910
Transmit information to central ticketing system
915
Receive contactless payment card information
920
Create account
925
Create and return activation code
930
Provide activation code to user
935
Receive activation code
940
Provide activation code to central ticketing system
945
Create transit user account
950
Enable contactless payment card as fare media
955
Offer to personalize account
960
Offer accepted?
N
Y
965
Receive user info
970
Associate user info with account
975
Provide receipt/ acknowledgement

FIG. 9

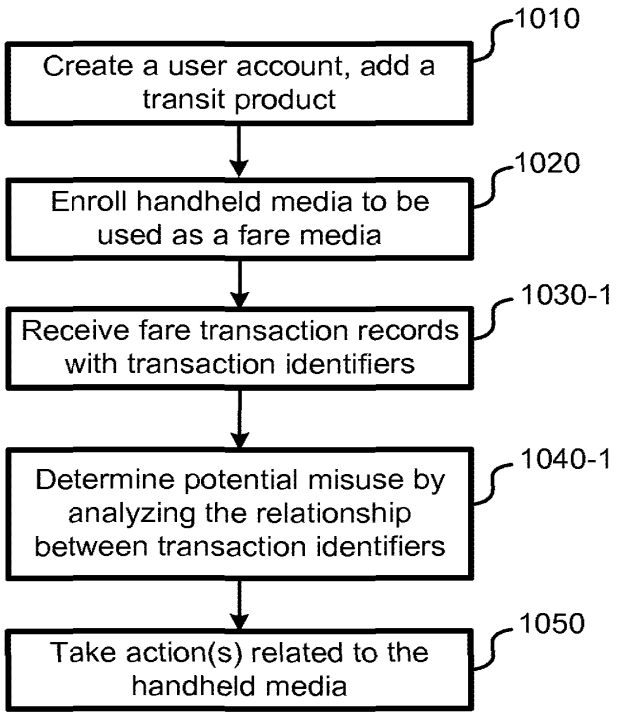

1010
Create a user account, add a transit product
1020
Enroll handheld media to be used as a fare media
1030-1
Receive fare transaction records with transaction identifiers
1040-1
Determine potential misuse by analyzing the relationship between transaction identifiers
1050
Take action(s) related to the handheld media

FIG. 10A

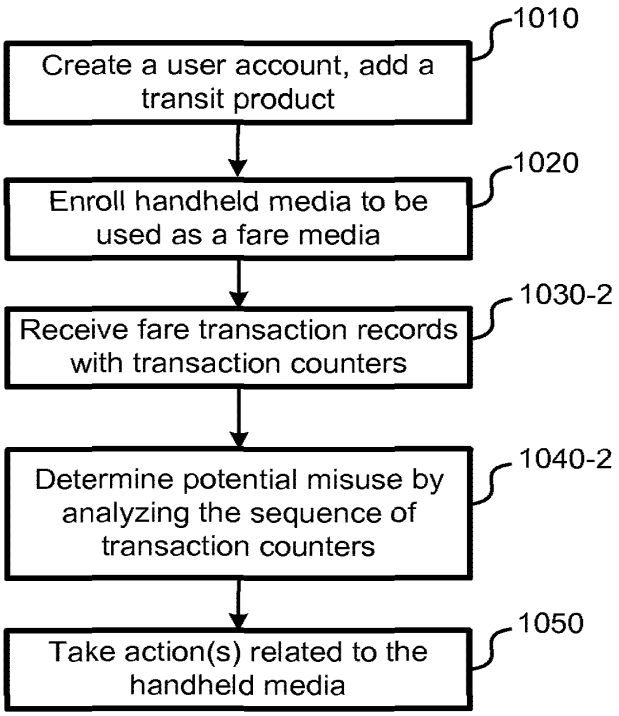

1010
Create a user account, add a transit product
1020
Enroll handheld media to be used as a fare media
1030-2
Receive fare transaction records with transaction counters
1040-2
Determine potential misuse by analyzing the sequence of transaction counters
1050
Take action(s) related to the handheld media

FIG. 10B

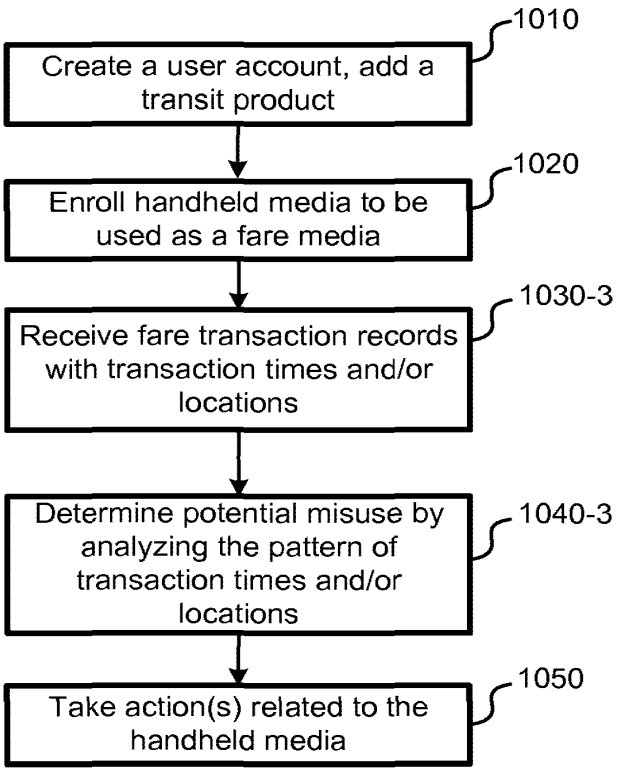

1010
Create a user account, add a transit product
1020
Enroll handheld media to be used as a fare media
1030-3
Receive fare transaction records with transaction times and/or locations
1040-3
Determine potential misuse by analyzing the pattern of transaction times and/or locations
1050
Take action(s) related to the handheld media

FIG. 10C

DETERMINING COMPANION AND JOINT CARDS IN TRANSIT

[0001] This application claims priority to Provisional U.S. Patent Application Number 61/406,821 filed October 26, 2010, entitled "Determining Companion and Joint Cards in Transit," of which the entire disclosure is hereby incorporated by reference for all purposes.

CROSS-REFERENCES TO RELATED APPLICATIONS

[0002] The present application is also related to U.S. Patent Application No. 12/877,691, filed on September 8, 2010, entitled "Association of Contactless Payment Card Primary Account Number," which is incorporated herein by reference for all purposes.

BACKGROUND

[0003] As transit systems throughout the world continue to mature, so do the technologies that support them. Many transit systems use impersonalized fare media that carry a value, such as stored-value cards, but other transit systems are taking a more personalized, account-based approach. Account-based transit systems can provide transit users with a personalized account, which can store product and funding information. Because value is associated with an account rather than a fare media, a transit system can disable a lost or stolen fare media and issue a new fare media to a transit user without the loss of any value to either the transit user or the transit system.

[0004] Because fare media does not store a value in these account-based transit systems, items other than those issued by a transit system may be enabled for use as fare media. Payment cards, for example, can be configured for use in such account-based transit systems. For transit systems utilizing wireless, or contactless, technology, contactless payment cards may be used. Occasionally, this process may be not be straight forward if multiple fare media become associated with the same primary account number, or if multiple users use the same fare media to access a transit product meant to be used by a single person.

BRIEF SUMMARY

[0005] Embodiments of methods and machines are disclosed for detecting potential misuse of handheld media, such as contactless payment cards and/or other devices having near-field communication (NFC) capabilities, for use as fare media in a transit and/or transportation system. Embodiments include reading contactless data from a contactless device and associating it with information received from another source on the device. For example, associating a primary account number (PAN) and/or other information received from a contactless payment card's

contactless interface with a PAN obtained from a magnetic stripe of the contactless payment card. The information can then be further associated with one or more products and/or a transit user account. A plurality of transaction identifiers may be collected from fare transactions at the transit station's access control points, and potential misuse of the PAN and/or handheld media may be determined, at least in part, by analyzing the relationship between a plurality of the transaction identifiers.

[0006] An example method for detecting potential misuse of a primary account number associated with a handheld media in a transit system having one or more access points, according to the description, may include creating a user account for managing transactional information, where the user account includes at least one transit product. The method may also include enrolling the handheld media for use as fare media for at least one of the transit products, where the PAN is stored in the user account. A plurality of fare transaction records are received from one or more access points of the transit system, and each fare transaction record may include the PAN associated with the handheld media and a transaction counter. The method may additionally include determining that a potential misuse of a handheld media associated with the PAN has occurred. The determination may be based, at least in part, on a sequence of the transaction counters from the fare transaction records. Finally, the method includes taking an action related to using the handheld media as fare media for the transit product.

[0007] The example method for detecting potential misuse of a PAN associated with a handheld media may include one or more of the following features. The handheld media may be a smart card having near-field communication capabilities, and the transaction counter may increment at least every time the handheld media is used at the access points and may be stored on the handheld media. The potential misuse may be determined by identifying gaps in the sequence of the plurality of transaction counters. The potential misuse may also be determined by determining that the sequence of transaction counters is not ascending. The potential misuse may also be determined by comparing the sequence of transaction counters to a user profile and identifying deviations. Additionally, each fare transaction record may also include a transaction time and a transaction location, and the potential misuse may also be determined, at least in part, on a pattern of the transaction times and locations from the fare transaction records.

[0008] Another example method for detecting potential misuse of a primary account number associated with a handheld media in a transit system having one or more access points, according to the description, may include creating a user account for managing transactional information,

where the user account includes at least one transit product. The method may also include enrolling the handheld media for use as fare media for at least one of the transit products, where the PAN is stored in the user account. A plurality of fare transaction records are received from one or more access points of the transit system, and each fare transaction record may include the PAN associated with the handheld media and a transaction time and location. The method may additionally include determining that a potential misuse of a handheld media associated with the PAN has occurred. The determination may be based, at least in part, on a pattern of the transaction times and locations from the fare transaction records. Finally, the method may also include taking an action related to using the handheld media as fare media for the transit product.

[0009] The example method for detecting potential misuse of a primary account number associated with a handheld media may include one or more of the following features. The potential misuse may be determined by indentifying multiple fare transactions that take place within a predetermined time window. The potential misuse may also be determined by indentifying fare transactions at distant locations that occur within a predetermined time window. The potential misuse may also be determined by indentifying first and second fare transactions where travel time between the locations exceeds a difference between the transaction times of the transactions. The potential misuse may also determined by comparing the pattern of the transaction times and locations to a user profile and identifying deviations. Finally, each transaction record may also include a plurality of transaction counters, and the potential misuse may also be determined, at least in part, on a sequence of the transaction counters.

[0010] An example server for detecting potential misuse of a PAN associated with a handheld media in a transit system, according to the description may include a network interface configured to communicate with a network, an input interface configured to receive information from one or more of the access points of the transit system, and a processor communicatively coupled with the network interface, the input interface, and a memory. The memory may contain instructions that cause the server to create a user account for managing transactional information in the memory. The user account may include a transit product, and a handheld media may be enrolled for use as fare media for the transit product. The PAN may be stored in the user account. The memory also may contain instructions that cause the server to receive, from the input interface, a plurality of fare transaction records, where each fare transaction record includes the PAN associated with the handheld media and a transaction identifier. The memory may also contain instructions that cause the server to determine potential misuse of a handheld media associated with the PAN based, at

least in part, on a relationship between some of the transaction identifiers from the fare transaction records. Finally, the memory may also contain instructions that cause the server to take an action related to using the handheld media as fare media for using the transit product.

[0011] The example server for detecting potential misuse of a PAN associated with a handheld media in a transit system may include one or more of the following features. Each transaction identifier may include a transaction counter, and the potential misuse may be determined, at least in part, on a sequence of the transaction counters. Each transaction identifier may include a transaction time and location, and the potential misuse may be determined, at least in part, on a pattern of the transaction times and locations. The action related to using the handheld media as fare media for using the transit product may include denying future use as fare media of any handheld media associated with the PAN. The action related to using the handheld media as fare media for using the transit product may also include charging the user account a fee for one or more of the fare transaction records. Finally, the server may also include an output interface configured to send notifications associated with potential misuse of the handheld media associated with the PAN, and the action related to using the handheld media as fare media for using the transit product comprises sending, from the output interface, a notification regarding the potential misuse of the handheld media associated with the PAN.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] FIG. 1 is a block diagram of an embodiment of a transit system providing transit user accounts for management of transactions of a user of the transit system.

[0013] FIG. 2 is a block diagram of an embodiment of a transit station system.

[0014] FIG. 3 is a simplified illustration of front and back views of a contactless payment card that can be enabled as fare media in a transit system, according to certain embodiments.

[0015] FIG. 4 is a perspective view of an embodiment of a transit vending machine that can be used to enable contactless devices, such as a contactless payment card, for use as fare media.

[0016] FIG. 5 is a block diagram of an embodiment of a transit vending machine that can be used to enable contactless devices, such as a contactless payment card, for use as fare media.

[0017] FIG. 6A is a simplified block diagram of an embodiment of an access control point processing unit of a transit system.

[0018] FIG. 6B is a simplified block diagram of an alternative embodiment of an access control point processing unit of a transit system.

[0019] FIG. 7A is a diagram of a method for enabling a contactless payment card to be used as fare media in a transit system, according to some embodiments.

[0020] FIG. 7B is a diagram of an alternative method for enabling a contactless payment card to be used as fare media in a transit system, according to some embodiments.

[0021] FIG. 8A is a block diagram of yet another method for enabling a contactless payment card for use as fare media in a transit system, according to some embodiments.

[0022] FIG. 8B is an embodiment of a method that incorporates the enablement of a contactless payment card for use as fare media with the payment of a transit and/or transportation product using the contactless payment card.

[0023] FIG. 9 is a swim-lane diagram of yet another embodiment of a method for enabling a contactless payment card for use as fare media.

[0024] FIG. 10A is a block diagram of an embodiment for detecting potential misuse of a fare media using transaction identifiers.

[0025] FIG. 10B is a block diagram of an embodiment for detecting potential misuse of a fare media using transaction counters as transaction identifiers.

[0026] FIG. 10C is a block diagram of an embodiment for detecting potential misuse of a fare media using transaction times and/or locations as transaction identifiers.

DETAILED DESCRIPTION

[0027] In the following description, for the purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of various embodiments. It will be apparent, however, to one skilled in the art that various embodiments may be practiced without some of these specific details. In other instances, well-known structures and devices are shown in block diagram form.

[0028] The ensuing description provides exemplary embodiments only, and is not intended to limit the scope, applicability, or configuration of the disclosure. Rather, the ensuing description of the exemplary embodiments will provide those skilled in the art with an enabling description for implementing an exemplary embodiment. It should be understood that various changes may be made in the function and arrangement of elements without departing from the spirit and scope of the disclosed systems and methods as set forth in the appended claims.

[0029] Specific details are given in the following description to provide a thorough understanding of the embodiments. However, it will be understood by one of ordinary skill in the art that the embodiments may be practiced without these specific details. For example, circuits,

systems, networks, processes, and other components may be shown as components in block diagram form in order not to obscure the embodiments in unnecessary detail. In other instances, known circuits, processes, algorithms, structures, and techniques may be shown without unnecessary detail in order to avoid obscuring the embodiments.

[0030] Also, it is noted that individual embodiments may be described as a process which is depicted as a flowchart, a flow diagram, a data flow diagram, a structure diagram, or a block diagram. Although a flowchart may describe the operations as a sequential process, many of the operations can be performed in parallel or concurrently. In addition, the order of the operations may be re-arranged. A process is terminated when its operations are completed, but could have additional steps not included in a figure. A process may correspond to a method, a function, a procedure, a subroutine, a subprogram, etc. When a process corresponds to a function, its termination can correspond to a return of the function to the calling function or the main function.

[0031] Furthermore, embodiments may be implemented by hardware, software, firmware, middleware, microcode, hardware description languages, or any combination thereof. When implemented in software, firmware, middleware or microcode, the program code or code segments to perform the necessary tasks may be stored in a machine readable medium. A processor(s) may perform the necessary tasks.

[0032] The term "payment brand" as used herein includes, but is not limited to payment card networks, such as VISA®, MASTERCARD®, AMERICAN EXPRESS®, and DISCOVER®. These networks may issue payment cards, such as reloadable prepaid cards, directly or though a separate card issuer, such as an authorized issuing bank. Furthermore, payment-branded cards as described herein may be "co-branded," meaning that the cards may be accepted, issued, and/or authorized by a transit agency or other entity in addition to a bank and/or payment brand.

[0033] Account-based transit systems are uncommon among current transit systems. Because transit systems require quick transactions, it is easier to use stored-value fare media (e.g., fare media, such as a transit fare card, that can store a value and a trip history on the card). However, encoding the value or transit product onto a fare media, rather than associate the value or fare media to a transit user, has its limitations. If the fare media is lost or stolen, it is difficult to remove the value from the lost or stolen fare media and restore it to a transit user. On the other hand, an account-based transit system can enable a transit user to enroll a variety of items as fare media. The fare media can be disabled if lost or stolen, without any lost value to the account.

And the account may be linked to a funding source to conveniently increase the account value and purchase additional products.

[0034] **FIG. 1** illustrates a block diagram of an embodiment of a transit system 100, in communication with other systems, providing transit user accounts for management of transactions of users of the transit system 100. The transit system can include various forms of transit, including subway, bus, ferry commuter rail, para-transit, etc., or any combination thereof. The transit user account can comprise information regarding a certain user of the transit system 100, such as a name, address, phone number, email address, user identification (such as a unique identifier of the user or other user ID), passcode (such as a password and/or personal identification number (PIN)), an identification code associated with a fare media used to identify a user and/or a transit user account (such as a primary account number (PAN)), information regarding user preferences and user opt-in or opt-out selections for various services, product(s) associated with the transit user account, a value and/or credit associated with the product(s), information regarding a funding source 165 for the transit user account, and more. The transit user account can further comprise funding and transaction information, such as product information, a funding source, and a payment amount. A transit user may request a transit user account and provide the information listed above by phone (such as a call to a customer service center 190 maintained and/or provided by the transit service provider of the transit system 100), on the Internet, at ticket booth, at a ticket venting machine, or by other means. A central ticketing system 112, which can comprise of one or more servers and/or other computing systems having processors, memories, and network interfaces for processing and communicating information. The central ticketing system 112 can use the information provided by the user to create the transit user account, which can be stored and/or maintained on a database, such as a central data store 114 of a central control system 110. It will be recognized that such a transit system 100 can be enabled for use in applications beyond transit, such as transportation systems (e.g., airline systems, car rental systems, etc.).

[0035] A funding source 165 for a transit user account can provide funding to purchase products of the transit services system. It can be external to the central control system 110 and maintained, for example, by a financial institution 160. Such a funding source 165 may include a savings or checking account, a prepaid account, a credit account, an e-commerce account (such as a PAYPAL® account), or more, which can transfer funds via automated clearing house (ACH) or other means. If a transit user account comprises information regarding a funding source 165 for

the account, the central ticketing system 112 can use the information to fund purchases or other transactions of a user of the transit system 100. These transactions can be made at stations, on the Internet, by phone, text, email, or a variety of other different ways, and transaction information can then be sent to the central ticketing system 112 to update the transit user account associated with the transactions and reconcile payments and purchases with the funding source 165. The central ticketing system 112 can communicate with the financial institution 160 (or other entity maintaining the funding source 165) through a financial network 150.

[0036] The central ticketing system's reconciliation with a funding source 165 may vary depending on one or more products associated with the transit user account and the functionality desired by a transit services provider. For example, the transit user account may include a running balance mirroring a balance of the funding source 165. In such a case, transactions, such as passage of a user at an access control point (such as a turnstile, faregate, platform validator, para-transit vehicle, bus, conductor handheld unit, or fare box at a entry, exit, or other location of a transit station) can be recorded and/or tracked by the central ticketing system 112 and reconciled, on a per-transaction basis and/or collectively with other transactions. Along these lines, the central ticketing system 112 may reconcile payment for the transactions with the funding source 165 as the transactions are received and/or on a scheduled basis, such as on an hourly or daily basis.

[0037] Additionally or alternatively, when transit products or services are associated with a transit user account, the central ticketing system 112 can draw funds from a funding source 165 less frequently. For example, a transit product can include a certain number of rides or an unlimited number of rides for a certain period of time. In this case, the central ticketing system 112 can track transactions associated with the passage of a user at an access control point (i.e., transactions in the transit system associated with a ride), but may only need to reconcile with the funding source 165 once, for the purchase of the transit product.

[0038] The transit user account may further include information regarding a user's preferences with regard to funding. For example, the transit user account may be configured to automatically draw a certain amount of funds from the funding source 165 each month to pay for a certain transit product or service, or to add value and/or credits to an existing transit product or service. The value and/or credits can include a monetary credit, a usage credit, and/or a usage period. Additionally or alternatively, the transit user account can be configured to automatically withdraw a certain amount of funds from the funding source 165 to add additional value and/or credits to an

existing product when the value and/or credits of the existing product drops below a certain threshold level. Various other configurations are allowable by the transit user account. It will be understood that other systems of the transit system 100, such as a station system 130, may draw funds from a funding source 165. Moreover, because cash payments can also be used to fund transactions associated with a transit user account, the transit user account may not require funding source 165.

[0039] Transactions of a user, such as passage at a transit access control points, can frequently occur at stations of the transit system 100, although it will be understood that access control points can exist elsewhere, such as on busses or trains. Station systems 130 can gather information regarding transactions and communicate the information to the central ticketing system 112 using a wide area network (WAN) 140. The WAN 140 can include one or more networks, such as the Internet, that may be public, private, or a combination of both. The WAN 140 could be packet-switched or circuit-switched connections using telephone lines, coaxial cable, optical fiber, wireless communication, satellite links, and/or other mechanisms for communication. Communication between the station systems 130 and the central control system 110 may be in real time or periodic. Thus, the usage of fare media throughout the transit system 100 can be tracked.

[0040] In this embodiment, a central ticketing system 112 and a central data store 114 are shown for the central control system 110. As discussed above, central ticketing system 112 receives periodic reports upon how credits or debits are being processed throughout the transit system 100. Additionally, changes in schedules, ticket prices, and delay notifications can be communicated from the central ticketing system 112 to the station systems 130 via the WAN 140.

[0041] A mobile device 180 may be communicatively coupled with the central control system 110. Such a mobile device may be a smart phone or other mobile phone (including a near-field-communication (NFC)-enabled mobile phone), a tablet personal computer (PC), a personal digital assistant (PDA), an e-book reader, or other device. In transit system 100, a communicative link from mobile device 180 to central ticketing system 112 can be provided by a mobile carrier network 170 in communication with WAN 140. Mobile device 180 can thereby communicate with the central ticketing system 112 to access and/or manage information of a transit user account. Furthermore, the central ticketing system 112 can send messages to the mobile device 180, providing transit, account, and/or advertisement information to a user of the transit system

100 in possession of the mobile device 180. Such messages may be based on, among other things, opt-in or opt-out selections and/or other user preferences as stored in a transit user account.

[0042] A transit user can use mobile device 180 to download a transit application from a transit application source 120. The transit application source 120 may be an application store or website provided by a mobile carrier, the hardware and/or software provider of the mobile device 180, and/or the transit service provider. The transit application can be uploaded or otherwise provided to transit application source 120 by the transit service provider. According to some embodiments, the transit application can provide additional functionality of mobile device 180, including enabling an NFC-enabled mobile device to be used as fare media and access control points of the transit system 100.

[0043] **FIG. 2** shows a block diagram of an embodiment of a transit station system 130. As discussed above, transit system 100 can include various forms of transit, such as subway, bus, ferry, commuter rail, para-transit, and more. Because different forms of transit may require different functionality, various transit station systems 130 may have some or all of the components shown in the block diagram. A local area network (LAN) 240 couples the various systems together and could include point-to-point connections, packet switched connections, wireless connections, and/or other networking techniques.

[0044] A station server 224 can be coupled to the WAN 140 to allow communication with the central ticketing system 112. Processing of local information can be performed on the station computer server 224. For example, fare information, schedule information, delay update information, and other transit related information can be processed at the station server 224 and communicated to the various other machines in the transit system 100.

[0045] A ticket booth computer 220, access control points 208, and transit vending machines (TVMs) 212 can communicate with the central ticketing system 112 through the station computer server 224 or directly with the central ticketing system 112 through LAN 240 or WAN 140 (e.g., the Internet). According to some embodiments, access control points 208 collect information from a user at various locations in the transit station system 130, and can come in various forms such as turnstiles, faregates, platform validators, para-transit vehicles, busses, conductor handheld units, and/or fare boxes. The access control points 208 can communicate with the station server 224 and/or central ticketing system 112 to determine whether to grant a user access when fare media has been presented at the access control points 208. If access control points communicate with a station server 224 during such transactions, identification codes of fare media, which can

be used to link a transaction with a transit user account, may be stored on lists in the station data store 216. Additionally, "hotlists", or lists of information identifying users, handheld media, PAN's, and/or user accounts may be stored on these lists. These lists can be updated on a regular basis to reflect other transactions of the fare media throughout the transit system 100. In other embodiments, identification codes of fare media 250 are stored at access control points 208.

[0046] Access control points 208 of the transit system 100 can be configured to read information from one or more sources of information on a fare media 250. To do so, access control points 208 can employ one or more technologies, such as WIFI, BLUETOOTH®, bar-code and/or other optical scanning. Access control points 208 may also employ near-field communication (NFC) technologies to read information from RFID tags, NFC-enabled mobile devices (such as certain personal digital assistants (PDAs), mobile phones, and other portable and/or personal electronics), contactless payment cards, and other contactless devices. The access control points 208 may also be configured to record, store, and/or transmit data regarding characteristics of the fare transactions, or transaction identifiers.

[0047] The access control points 208, TVMs 212, and one or more ticket booth computers 220, can communicate with the station server 224 via the LAN 204. This communication can be transmitted via a physical connection or wireless connection via one or more antennas 228. Transactions at access control points 208, TVMs 212, and one or more ticket booth computers 220 can be communicated to the station server 224, stored at station data store 216, and/or transmitted to central ticketing system, which can update information in a transit user account accordingly.

[0048] Various portable and/or handheld media with a unique identifier can be used as fare media, whether or not the media is issued by a transit services provider. Such media can include identification cards, payment cards, personal electronic devices, bar codes and items having bar codes, contactless devices, and more. Contactless devices can include media having a unique identification code readable by access control points 208 though NFC signals (e.g., radio frequency (RF) signals). By way of example, but not by limitation, such contactless devices can include devices comprising RFID tags and/or RFID-tagged items, contactless payment cards (including but not limited to credit cards, prepaid cards, debit cards, or other bank cards or contactless smart cards.), contactless identification cards and/or fobs, and NFC-enabled mobile devices.

[0049] Fare media 250 can have multiple sources of information, which may be read automatically by certain systems and devices in the transit system 100, depending on desired functionality. For contactless devices, such sources can include an IC, memory, and/or contactless interface of the device. Additionally or alternatively, contactless devices and other forms of fare media 250 can include a magnetic stripe, a bar code, and/or data imprinted and/or embossed on the device, which can serve as additional sources of information. Contactless and other sources of information can serve as repositories of account information related to, for example, a financial or user account associated with the fare media 250 (which may not be associated with the transit system 100).

[0050] TVMs 212 may interact directly with a fare media 250 through, for example, a contactless connection 232. Although communication of the contactless connection 232 may be two way, fare media 250 may simply communicate an identification code to TVM 212. This can be done, for example, to authenticate a contactless device for use as fare media 250 in the transit system 100. A contactless device does not have to be issued by a transit service provider in order to be authenticated and used as fare media 250 in the transit system, as long as the information communicated by the fare media 250 to the TVM 212 (and subsequently to access control points 208 for passage in the transit system 100) serves to uniquely identify the fare media 250. Such an authentication process is provided in greater detail below.

[0051] All or part of the information communicated by the fare media 250 can be used as an identification code to identify the transit fare media 250. This identification code can comprise one or more fields of data including or based on information such as a name, a birth date, an identification number (such as a PAN), a social security number, a drivers license number, a media access control (MAC) address, an electronic serial number (ESN), an international mobile equipment identifier (IMEI), and more. Because the identification code is unique, it can be associated with a transit user account, and utilized by a user at a TVM 212 to access and/or update information associated with the transit user account.

[0052] In some instances, an identification code may be assigned by a transit service provider and written to the fare media 250, such as an NFC-enabled mobile device 280. For example, a transit application running on an NFC-enabled phone can generate or otherwise provide an identification code to be transmitted from the phone at access control points 208 of the transit system 100. In other instances, if TVM 212 is utilized to enable a user to create a transit user account, the TVM 212 may also write an identification code to an unused portion of a memory of

the fare media, such as integrated circuit chip file space on a smart card or an NFC component on the NFC-enabled mobile device 280.

[0053] **FIG. 3** illustrates front and back views of an embodiment of a contactless payment card 310 that can be enabled as fare media 250 in the transit system 100. Such contactless payment cards are widely available, can be issued by any of a wide variety of issuing banks, and can include a payment brand. The contactless payment card 310 can include an integrated circuit (IC) 313 configured to, among other things, store account information, such as a PAN, expiry date, name associated with an account, etc. The IC 313 can adhere to one or more relevant standards, such as the Europay, MasterCard, and VISA (EMV) standard, and can be coupled with an antenna 315 for communicating information wirelessly to a contactless card reader (not shown). Contactless payment cards 310 frequently adhere to standards set by the International Organization for Standardization and/or International Electrotechnical Commission (ISO/IEC), such as ISO/IEC 14443 or ISO/IEC 15693 standards for contactless smart card communications. The IC 313 and antenna 315 can be embedded in the payment card and are frequently not visible to a card user.

[0054] The contactless payment card 310 can include features and/or data common to other payment cards, as defined in other ISO/IEC standards, such as ISO/IEC 7810 and ISO/IEC 7813. This can include a magnetic stripe 317, a payment brand logo 318, an account number 314 (such as a PAN, which can be printed and/or embossed on the contactless payment card 310) and a cardholder name 316.

[0055] EMV is an emerging global standard for the inter-operation of IC-enabled payment cards. The EMV standards define the interaction at the physical, electrical, data and application levels between IC cards and IC card processing devices for financial transactions. There are standards based on ISO/IEC 7816 for contact cards, and standards based on ISO/IEC 14444 for contactless cards. The cards following the EMV standard have additional information stored on the card 310. This information includes the PAN 320, an expiry date 321, a service code 322, an issuer discretionary data space 323, a transaction counter 324, and a calculated verification value based on an algorithm that includes the transaction counter 324 as a dynamic value 325. EMV transactions may also include other parameters outside of the track data.

[0056] For each use of the contactless interface antenna 315 on an EMV-compliant contactless payment card 310, the card 310 increments the transaction counter 324 value by one. The counter is incremented by the IC 313 on the card 310. Therefore, the counter increments whether or not

there is an associated retail transaction forwarded to an financial institution 160. Using the EMV card 310 as a contactless fare media would cause the transaction counter 324 to increment, even though financial institution that issued the card is not involved in the transaction.

[0057] In **FIGs. 4 and 5**, a perspective view and block diagram of an embodiment of a TVM 212 are shown. A vending machine processor 500 is coupled to the other components of the TVM 212 and transmits and receives signals to and from the other subsystems to cause the other components to perform their intended functions. Fare cards can be purchased and/or reloaded with value at the TVM 212. A coin/bill system 504, magnetic stripe card reader 412, and contactless card reader 418 are used to make payments for transactions at the TVM 212. Additionally or alternatively, a contactless card reader 418 may be coupled with a magnetic stripe card reader 412 to enable simultaneous reading of contactless and magnetic stripe information. A keypad 416 is provided adjacent to the credit/debit card reader 412 to enter numerical information such as a PIN code for a debit card. A coin slot 436 and bill loader 428 are used to accept cash. Change is returned in a change/receipt slot 420 and coin return 424. Reloadable fare cards and receipts, including receipts having a activation code, are also provided in the change/receipt slot. TVM 212 may further dispense single-ride fare cards through card dispenser 444, which is coupled with a card storage unit (not shown) storing reloadable prepaid cards for distribution. Information regarding transactions may be communicated through a LAN 240 by the vending machine processor 500 using, for example, a network interface (not shown).

[0058] Information regarding transactions may be communicated to various entities. For example, a contactless PAN, a magnetic stripe PAN, and/or other information may be communicated to the central ticketing system 112 to create a transit user or temporary account. Additionally or alternatively, a PAN and other payment information may be transmitted to a card issuer or other financial institution 160 for payment of a transit product. The financial institution 160 can receive communication from TVM 51 via financial network 150, central ticketing system 42, and/or WAN 140. Moreover, a financial account associated with a contactless payment card 310 may comprise a funding source 165 maintained by a financial institution 160.

[0059] A display system 404 prompts the card holder through the refill/purchase process. For example, the screen prompts the purchaser to touch a start button/icon on a touch screen display of the display system 404 to begin the process. A textual display portion 406 can display textual instructions for the user after the process has begun. Additionally or alternatively, an audio system 442, including a speaker, can produce audio commands. The user can be given a menu of

choices of how to proceed. For example, the menu may include choices to purchase or reload a reloadable fare card, purchase a single-ride fare card, purchase a product, setup a transit user account, and/or associate a contactless device, such as a contactless payment card, with a transit user account. It will be understood that, additionally or alternatively to a touch screen display, other input interfaces may be utilized to accept input from a user. This can include, but is not limited to a touchpad, keyboard, mouse, trackball, audio input interface, joystick, etc.

[0060] If the user chooses an option requiring payment, the user may be instructed, by menu prompts, pre-recorded video and/or audio, on how to proceed with the payment. The user can be given a choice to pay in cash or by a payment card. For cash purchases, the user is instructed to insert coins or bills into the coin slot 436 or the bill loader 428. For payment card purchases, the user is instructed to insert payment card into the magnetic stripe card reader 412, or touch a contactless payment card 310 to contactless card reader 418.

[0061] Different processes may be implemented if the user chooses to enable a contactless payment card 310 as fare media 250. For example, the user can be instructed to touch a contactless payment card 310 to contactless card reader 418. Additionally, the user would be instructed to insert the contactless payment card 310 into the magnetic stripe card reader 412 and/or input the imprinted and/or embossed PAN 314 by using the keypad 416, the display system 404 (if it includes touchscreen capabilities), or both. Alternatively, for TVMs 212 with a contactless card reader 418 coupled with a magnetic stripe card reader 412, a user can be instructed to insert the contactless payment card 310 into the magnetic stripe card reader 412, allowing the TVM 212 to read both the contactless and magnetic stripe information from the contactless payment card 310. The TVM 212 can be configured to provide additional functions such as allowing the user to purchase a product, activate the contactless payment card 310 as fare media 250, and/or create a transit user account, by, for example, accepting additional input through any one of the user interfaces described above. Additionally or alternatively, the TVM 212 can simply print out an activation code on a receipt and provide the receipt to the user from the change/receipt slot 420. The transit system 100 can associate the activation code with information collected from the contactless payment card 310, enabling the user to perform any of the additional functions listed above at a TVM 212, ticket booth, website and/or other system at a subsequent point in time.

[0062] It will be understood that any or all of the features and/or capabilities of the TVM 212 described above may be included in other locations and/or devices of the transit system 100. A

user may therefore register a contactless device, such as a contactless payment card 310, as fare media at other locations of the transit system 100. For example ticket booth computers 220 can be coupled with contactless card readers and/or magnetic stripe card readers, allowing a user to perform any or all of the functions described above by providing a contactless payment card 310 to a transit worker at a ticket booth. Additionally or alternatively, other devices may be configured to read contactless and magnetic stripe information from a contactless payment card 310 and transmit the information to a central ticketing system 112 of the transit system 100, without having the additional functionality of a TVM 212. Such devices further can be configured to print a receipt with an activation code, enabling a user to complete, at a later point in time, the process of activating a contactless payment card 310 for use as fare media 250. Moreover, these procedures may be carried out at a sales office, automated teller machine, and/or other manned or unmanned locations.

[0063] **FIG. 6A** is a simplified block diagram of an embodiment of an access control point processing unit 600-1, which can be coupled with and/or integrated into access control points 208 of a transit system 100 and can control certain physical properties of access control points 208 such as to allow or deny passage of a user. Among other things, the access control point processing unit 600-1 can be used to read an identification code, such as a contactless PAN and/or other contactless information, from fare media. The access control processing unit may also record transaction identifiers, such the time and location of the transaction. The access control point processing unit 600-1 also can determine whether to permit passage of a user at the access control point 208. Interfaces such as an NFC interface 680 (which can read RFID and contactless information), and/or magnetic reader interface 640, can be used to receive information from fare media 250, including an identification code. Alternative embodiments contemplate access control processing units 600 without a magnetic reader interface 640. Once the identification code is received, it can then be sent to processor 610.

[0064] In addition to performing any decryption and/or verifying any security features, the processor 610 can compare the identification code against lists stored in memory 620-1 and/or other data store to determine whether to allow passage of the user at the access control point 208. Lists can be generated and maintained from a central system, such as the central ticketing system 112. The central system can send updated list information to station server 224 via WAN 140 or directly with the central ticketing system 112 through WAN 140 (e.g., the Internet) or LAN 240. The station server 224 can store updated list at the station data store 216 and/or communicate the

updated list information via LAN 240 to access control point processing unit 600-1, which receives the information at network interface 630. U.S. Patent Application No. 12/833,404, entitled "Reloadable Prepaid Card Distribution, Reload, And Registration In Transit," (hereafter, the "'404 Application") which is incorporated herein, details how the transit system 100 and access control point processing units 600 may use lists to determine whether to allow passage of the user at access control points 208. Once the determination is made, the processor 610 can cause the access control point processing unit 600-1 to physically allow or deny passage of a user at the access control point 208.

[0065] The access control point processing unit 600-1 can also log transaction information in memory 620-1 and/or communicate the transaction information to station server 224 with a network interface 630. The station server 224 can, in turn, send the transaction information to the central ticketing system 112, which can store the information in central data store 114. The transaction information can be used to update transit user accounts associated with the transactions and to settle with a funding source 165.

[0066] **FIG 6B** is a simplified block diagram of an alternative embodiment of an access control point processing unit 600-2. As illustrated, a memory 620-2 may be located at a source external to access control point processing unit 600-2. The external source can include, for example, station server 224 or station data store 216. In such an embodiment, the processor 610 may communicate with the external source in deciding whether to allow or deny passage of a user at an access control point 208, or the decision may be made by station server 224. In either case, it is desirable to make the decision quickly, often in 500 milliseconds or less. Thus, in this embodiment, it can be desirable that the connection between access control point processing unit 600-2 and the external source having memory 620-2 have sufficient speed and minimal latency to provide for a quick decision. Methods of allowing or denying access to a user at access control points 208, as well as methods of processing transactions received from access control points 208, are described in more detail in the '404 Application.

[0067] **FIG. 7A** is a diagram of an embodiment of a method for enabling a contactless payment card 310 to be used as fare media 250 in a transit system 100 providing account-based transactions. Beginning at block 700, a request is received to enable a contactless payment card 310 as fare media. For example, a user may select a menu option at a TVM 212 to make such a request. At block 710, a user is directed to insert a contactless payment card 310 into a card reader.

[0068] At block 720, card information is read. As described above, a device such as a TVM 212 may include a magnetic stripe card reader 412 integrated and/or coupled with a contactless card reader 418 such that the device can read the magnetic stripe and contactless information at the same time. Alternative embodiments contemplate variations on reading card information. For instance, where card readers are not integrated, the user may be directed to tap a contactless card reader 418 and insert the card into a magnetic stripe card reader 412 separately, in which case, the contactless and magnetic stripe information correspondingly is read in discrete steps.

[0069] In some instances, the contactless PAN may match the PAN of the magnetic stripe. However, to overcome the problems introduced by multiple cards with an identical PAN, a unique "fingerprint" of the contactless payment card 310 can be identified. To do so, additional track data components can be used to decipher one contactless PAN from another. For instance, track data includes name and expiry data. Additionally, some card issuers place a sequence code into the track data to make the contactless payment card 310 uniquely distinguishable. Thus, in addition to reading the contactless PAN and the PAN of the magnetic stripe, the device in which a user inserts and/or taps a contactless payment card 310 can be configured to read additional contactless track data, such as a sequence code, account holder name, and/or expiry date. Access control points 208 of the transit system 100 can be similarly configured to read the additional contactless track data to be able to access the uniquely distinguishable information.

[0070] Because the PAN of the magnetic stripe is typically identical to the imprinted and/or embossed PAN 314, a device may be configured to receive the imprinted and/or embossed PAN 314 rather than the PAN of the magnetic stripe. For instance, a TVM 212 can be configured to allow a user to manually enter the imprinted and/or embossed PAN 314 using a keypad 416 or touchscreen. Moreover, a device may have visual scanning capabilities to read the imprinted and/or embossed PAN 314 directly. It will be understood that other information such as an expiry date or account holder name, can be read from the magnetic stripe and/or otherwise received by the transit system.

[0071] At block 730, a temporary account with associated PAN numbers, and any additional contactless track data, is created. The account simply can comprise an association of the contactless data with the other provided information. At block 740, an activation code is created, and at block 750, a receipt with the activation code is provided to the user.

[0072] At block 760, the activation code is provided, along with product information. The activation code and product information is associated with the information received earlier, and, at

block 770, a user transit account is created. The transit user account can comprise the information of the temporary account in addition to the product information provided at block 760. It may also include additional information provided by a user, as well as the activation code. For example, after receiving a receipt with the activation code, a user can provide the activation code at a website and purchase a product, such as a monthly pass.

[0073] A user may provide additional information to personalize the transit user account. For example, a user may provide a name, phone number, address, email address, social security number (SSN) or other government-issued identifier, a drivers license number, a username, a passcode (such as a personal identification number (PIN) or a password), other identification verification information, and/or funding information. Depending on the desired functionality of the transit system, a user also may input information regarding opt-in or opt-out selections for additional services, user preferences, and/or additional product(s) for purchase to be associated with a transit user account. The account further may include other data generated by the transit service provider.

[0074] At block 780, the contactless payment card 310 is enabled as fare media, and a receipt and/or acknowledgement is provided to the user at block 790. Enabling the contactless payment card 310 for use as fare media within the transit system 100 can comprise sending the contactless information (e.g. uniquely-identifying information) of the contactless payment card 310 to a central database, such as the central data store 114 and/or multiple remote databases, such as the station data store 216, with which access control points 208 can communicate. Additionally or alternatively, the contactless information may be propagated to the access control points 208 themselves. Thus, in subsequent transactions where the contactless information is read from the contactless payment card 310 at an access control point 208, the access control point 208 can recognize the information as being related to a valid transit user account and allow a transit user access accordingly.

[0075] It will be understood that embodiments contemplate numerous variations to the method shown in FIG. 7A. For example, although providing a receipt with a activation code is desirable, it is not required. Rather than provide an activation code, a method include simply receiving the imprinted and/or embossed PAN, which a user can provide a subsequent registration over the Internet, at a ticket booth, or at another location of the transit system 100. Additionally or alternatively, embodiments contemplate allowing a user to link information received from the contactless payment card 310 to an existing user account. For instance, a user can provide user

information contained in the transit user account, such as a username and/or passcode, at any time before or after information is read from the contactless payment card 310, allowing a the contactless and other information to be associated with the user account.

[0076] **FIG. 7B** illustrates how a method similar to that shown in FIG. 7A can be extended to apply more broadly to contactless devices. Access control points 208 can be configured to read wireless information from contactless devices other than contactless payment cards 310, such as NFC-enabled mobile devices, RFID tags/stickers, contactless identification cards, etc. These devices may have contactless information uniquely identifying the device that may differ from information from another source of the device. Accordingly, a transit, transportation, or similar system can be configured to enable such contactless devices for use within the system in a manner similar to that of contactless payment cards 310.

[0077] **FIG. 8A** is a block diagram of an embodiment of another method for enabling a contactless payment card 310 for use as fare media 250 in transit system 100. FIG. 8A illustrates how a user account may be created before information is read from the contactless payment card 310. FIG. 8A also demonstrates how the creation of the transit user account and the enablement of the contactless payment card 310 as fare media 250 can be done in a single session, without requiring additional steps at a later point in time.

[0078] At block 810, user information is received, and at block 820, a transit user account is created. Similar to the user information described above, the user information can comprise any of a variety of information, including product and payment information, among other things. At block 830, a user is directed to insert a contactless payment card 310. And at block 840, information is read from the contactless payment card, including contactless information. The information may also include information from a magnetic stripe, bar code, imprinted and/or embossed characters, and/or other sources of information.

[0079] At block 850, the contactless information, including a PAN, is associated with the transit user account. A PAN provided by another data source of the contactless payment card can also be associated with the transit user account. After which, at block 860, the contactless payment card 310 is enabled as fare media. And at block 870, a receipt and/or other acknowledgement is provided to the user. It will be understood that certain blocks, such as blocks 840-870, can be repeated at any time to allow a user with an existing transit user account to enable a handheld media, such as a contactless payment card or other NFC-enabled device, to be used as fare media.

Such occasions can arise, for example, when a card issuer provides a user with a new contactless payment card before the expiry of an existing payment card.

[0080] **FIG. 8B** is an embodiment of a method that incorporates the enablement of a contactless payment card 310 for use as fare media 250 with the payment of a transit and/or transportation product using the contactless payment card 310. In addition to the steps shown in FIG. 8A, the embodiment of FIG. 8B includes block 825, enabling product purchase. This can include, for example, allowing a user to select a transit and/or transpiration product from a menu. Additionally, block 843, payment information, such as the PAN, expiry date, and other information is sent to a card issue for verification. At block 845, payment confirmation is received. As with all methods described herein, numerous variations may be made. For example, at any of a variety of points during the process, a user may be allowed to select whether or not to enable the contactless payment card 310 for use as fare media 250. It will be understood further that other embodiments described herein can incorporate payment of a product with the contactless payment card 310 similarly.

[0081] **FIG. 9** is a swim-lane diagram of yet another embodiment of a method for enabling a contactless payment card 310 for use as fare media 250. FIG. 9 illustrates how the method may be performed by a TVM 212, a central ticketing system 112, and a web server. The web server can host a web site for receiving input from a user. Such a web server can be maintained or otherwise communicatively connected with the central ticketing system 112. Moreover, the web server comprise part of the central control system 110 of a transit system 100.

[0082] At block 905 the TVM 212 reads the contactless and magnetic stripe information from a contactless payment card 310. At block 910 all, or at least a part, of the information is communicated to the central ticketing system 112. At block 915, the central ticketing system 112 receives the information, and at block 920, creates the account. At block 925, the central ticketing system 112 can then create and return an activation code. At block 930, the TVM 212 provides the activation code to the user.

[0083] With the activation code, the user can then access a website hosted by the web server to complete the enablement process. At block 935, the web server receives the activation code. This can be done, for example, simply by providing a website with a small form to fill out and submit, including a text box for the activation code. Product and payment information may also be received by the web server. At block 940, the web server provides the activation code to the central ticketing system 112.

[0084] At block 945, the central ticketing system 112 creates a transit user account with, among other things, information received at block 935. At block 950, the central ticketing system enables the contactless payment card 310 as fare media in the transit system 100. The central ticketing system 112 can notify the web server that the contactless payment card 310 has been enabled.

[0085] At block 955, or alternatively at an earlier point in the process, the web server can further offer to personalize the transit user account. At block 960, if the offer is rejected, the web site can, at block 975, simply relay receipt and/or acknowledgement information to the user. Otherwise, at block 965, the web server can receive additional information from the user by, for example, providing an additional online form, which is submitted by the user. The information is relayed to the central ticketing system 112, and at block 965, associated with the transit user account. At block 970, the web server provides receipt and/or acknowledgement information to the user.

[0086] Processing of contactless payment cards in the transit system can be based on the PAN as a unique identification code. The PAN is available to an access control point 208 configured to read contactless track data from the contactless payment card 310. The PAN can be extracted from the track data and used to identify the card for account-based processing. Under most circumstances, the PAN imprinted and/or embossed on the front of the card is the same as the PAN found in the track data and stored on in the card's 310 integrated circuit 313.

[0087] If the contactless PAN stored in memory of the IC 313 of a contactless payment card 310 is different than the PAN imprinted and/or embossed 314 on the front of the card, additional difficulties arise. For example, it would be particularly difficult to allow a transit user to use the Internet to register the contactless payment card 310 for use as a fare media 250. Because access control points 208 are configured to read the contactless PAN from the contactless payment card 310, it would not avail the transit user to enter the imprinted and/or embossed PAN 314.

[0088] One way to solve this and other problems may be solved by providing the imprinted and/or embossed PAN 314 and the contactless pan beforehand. For example, a transit user can swiping and/or dipping the contactless payment card 310 at a TVM 212 or other device of the transit system 100 configured to read information the magnetic stripe 317, which frequently includes a PAN that including a PAN that matches the imprinted and/or embossed PAN 314. The device can also read the contactless PAN from the IC 313. The transit system can then associate the contactless PAN with the imprinted and/or embossed PAN 314, enabling a user to access the

Internet subsequently and enter the imprinted and/or embossed PAN 314. The transit system 100 can then associate any additional user and/or product information with the contactless PAN, and enable the contactless payment card 310 for use as fare media in the transit system 100. More details describing this process are provided below.

[0089] Usually, the PAN 314 on one contactless card 310 will be different and distinct from the PANs on other payment cards, thus enabling the transit system to treat each PAN 314 as a unique identifier associated with each user account. However, there will be variations that the transit system 100 may need to contemplate. Bank card issuers have their own issuing rules and procedures, which may result in multiple cards 310 with the same PAN 314. Also, fraud and theft may result in illegitimate handheld media encoded with a stolen PAN 314 that could be used as a fare media 250. When different cards/devices have the same PAN there is a problem correctly associating the registered card with the purchased fare products. Accordingly, some embodiments disclosed herein include methods allowing for such determination and providing ways to combat a possible scam or fraud.

[0090] Contactless bank cards can be used in account-based transit fare collection in two modes: (1) pay as you go; and (2) where the card is registered and fare products are purchased and associated with that bank card account number. In the second case, when the bank card account number is read, for exampe at a contactless interface 680, and processed in the transit system 100 as a fare media 250, it is associated with the account-based fare product. This association can be made by the transit system 100 using hardware, software, or a combination of the two.

[0091] A problem arises when contactless account number (PAN) are not be unique amongst cardholders. Fraud may be prevented by not allowing random bank cards/devices to be registed against account-based products and/or requiring that cards used for passes and discounted fare products must be of agency issued media. But this would be limiting and not be convenient for the patron. Alternatively, a fare collection system could demand that card issuers do not issue single PANs 314 on multiple cards/devices. But this may not be practical. Many card issuers exist, each with their own process for card numbering, and they are unlikely to conform to the needs of a transit agency.

[0092] One variation of this problem can include multiple parties linked to one financial account, such as a husband and wife, a parent and child, or multiple business partners, each having access to the joint account. Each joint-account holder could be issued a payment card 310 associated with the joint account, and each card 310 could have the same PAN 314 embossed on

the card and/or stored in the track data (e.g., magnetic stripe 317) and/or IC 313. To further illustrate, if a transit user with a transit user account purchases a single, flat-fare monthly pass and associates the PAN 314 of a contactless payment card 310 with his/her transit user account, each additional contactless payment card having the same PAN 314 could also be used as fare media 250 for the monthly pass. Thus, if the multiple contactless payment cards 310 are distributed among several people, each person essentially would receive a monthly pass when only one monthly pass was purchased. In another variation, a single account holder may be issued multiple devices which provide access to one or more accounts. For example, a user may be issued multiple payment cards 310 and/or companion devices, such as another style of contactless payment card, an RFID-enabled sticker, a key chain tag, a FOB, etc. In another variation, an account holder may receive a replacement card prior to the time that an enrolled payment card 310 expires. This could result in a period of time between the time when the replacement card is activated and when the original card 310 expires when both cards could be validly read as a fare media 250 at a access control point 208.

[0093] Another problem may involve only a single card 310 that is used by multiple people as a fare media 250. In one variation, a user account may contain a type of transit product that allows for unlimited access to the transit system during a limited time, such as a monthly or weekly pass. In this case, a single payment card 310 may be used as a fare media by multiple users at one or more access control points. For example, the card owner could use the card 310 in conjunction with the NFC interface 680 of a single access control point 208 to allow additional transit users to enter an access control point 208 either before or after the card owner. In another variation, the card owner could use the payment card 301 himself/herself, and then pass the card 310 back to other transit patrons on the other side of the access control point 208 for reuse. In yet another variation, the transit product associated with the user account could be non-transferrable. In this case, a payment card 310 could be cancelled by the issuing bank at the request of the owner, then sold for use solely as a fare media 250 to another user until expiration of the transit product.

[0094] In addition to misuse by legitimate holders of the payment card 310, fraud and theft can also lead to multiple handheld media devices that are associated with the same PAN 314. In one variation, a payment card 310 could be stolen from a user, and a replacement card could be mailed from the issuing bank. If the replacement card had the same PAN 314, then both the stolen card 310 and the replacement card could be used as a fare media 250. In another variation, the payment card 310 itself may not be stolen; however, the stored data including the PAN 314 could

be stolen from the card 310, associated with another handheld media, and used as a fare media 250 without the knowledge of the card owner. This situation could be particularly worrisome to the transit system 100 if the thief were to only use the card 310 as a fare media 250. Unless the thief were to also use the PAN 314 in retail transactions, the issuing bank and the card owner would have no means of knowing that the payment card data had been stolen. Without being able to benefit from the issuing bank's existing fraud-detection schemes, the transit agency 100 would need its own method of detecting when a handheld media with a PAN 314 associated with a user account is being potentially misused.

[0095] In the above circumstances, the contactless payment card issuer knows how to associate each card variation and can charge the single bank account as appropriate. The transit system 100, however, will not be able to automatically decipher most of these circumstances. Because the transit system 100 allows for account-based transactions, the inability to take into account the above circumstances can be problematic in many ways. Ideally, the issuer would have to communicate to the transit agency regarding multiple card scenarios and fraud detection. This is not a practical solution due to the tremendous number of transit systems around the world and the number of payment cards in circulation. Regardless, the transit agency may be interested in determining whether more than one person is using a handheld media associated with a PAN 314 authorized as a fare media 250. As illustrated by the situations above, using the PAN 314 alone may not be sufficient to detect potential misuse. Additional data from the transaction may be necessary for the transit system 100 to perform this type of operation without assistance from the issuing bank.

[0096] According to certain embodiments of the present invention, this problem may be solved by using invented procedures and processes of automation to detect and stop multiple cards 310 and/or devices from using the same stored account-based fare product. This can include fraud detection mechanisms looking for exceptions and odd travel patterns on a single PAN 314 by analyzing additional transaction identifying data.

[0097] FIG. 10A illustrates one embodiment of a method wherein the transit system 100 may collect additional information that is characteristic of each individual fare transaction. This additional information may be referred to as a transaction identifier, and it can be used to detect potential misuse of a payment card as a transit fare. In this method, a user account is created for managing transactional information wherein at least one transit product is purchased and/or designated for use at block 1010. At block 1020, a handheld media is enrolled for use as a fare

media 250 for the transit product according to the various methods described above. The handheld media could be a payment card 310, a smart phone, a portable media player, a FOB, and/or the like. The handheld media may use contact with the access control point when used as a fare media, for instance with a magnetic stripe or a electrical contact. Alternatively, the handheld media may use a contactless connection with the access control point 208, such as with NFC-enabled devices, Bluetooth, RF, IR, or barcode devices. In one embodiment, the fare media is contactless payment card 310 using the EMV data standard.

[0098] The handheld media can be associated with all of the transit products associated with the user account, or the handheld media can be associated with one or more single transit products. In one embodiment, the transit product is an unlimited ride pass that is valid for a finite period of time, such as a monthly, weekly, or yearly pass. Alternatively, the transit product could include a limited-ride pass such as ten-ride pass. In this case, it would still be desirable for the transit system to detect potential misuse of a PAN 314 in order to protect its customers, to inspire customer loyalty, and/or to prevent the transfer of transit products between different users.

[0099] Next, at block 1030-1, the transit system 100 may receive a listing of transaction identifiers from one or more of the access control points 208. Each transaction identifier may be associated with a single use of a handheld media as a fare media 250. One or more transaction identifiers may be received and stored for each fare transaction involving a fare media 250, resulting in a plurality of transaction identifiers associated with a single PAN 314 over time. A transaction identifier may be a single piece of data, such as the time of the transaction. Alternatively, a transaction identifier may be comprised of more than one characteristic of the transaction. For example, a transaction identifier may include the time or location of the transaction, a user code, a one-time-use password, biometric data from the user, and/or track data from the card other than the PAN 314. In some embodiments, the misuse detection algorithms may also use other inputs in addition to the transaction identifiers, such as user inputs from the transit system 100, an authorized user, or law enforcement. These algorithms could incorporate other data, such as surveillance data or information from a financial institution. It will be understood that combinations of each of these data sources could also be incorporated to detect potential misuse.

[0100] The list of transaction identifiers may be stored and/or analyzed locally at the station server 224, or the list of transaction identifiers may be stored and/or analyzed remotely at the central ticketing system 112. If the transaction identifiers are analyzed remotely at the central

ticketing system 112, they may be transmitted from the station systems 130 individually as they are collected from the access control points 208. Or, in another embodiment, the transaction identifiers may be stored locally at the access control points 208 or at the station server 224 or at a comparable local system. In this case, a list of transaction identifiers associated with a PAN 314 could then be transmitted to the central ticketing system 112 periodically in batches during off-peak travel times to reduce network traffic. These batches could be sent periodically, such as every 15 minutes, or they could be sent when a predetermined number of fare transactions have taken place. The transaction identifiers could be stored and/or transmitted in a dedicated list, or they could each be packaged in with other data. For example, if the transaction counters 324 in the EMV data are used as transaction identifiers, then they could be stored in the EMV data format in a cryptogram that is received from the payment card 310. The encrypted packets could be decrypted locally at the station systems 130, and the transaction counters 324 could be analyzed or transmitted to the central ticketing system 112. Alternatively, the encrypted data packets themselves could be transmitted to the central ticketing system 112 for decryption and analysis. It will be understood that a fare transaction record analyzed for potential misuse may include any arrangement of the data described above.

[0101] At block 1040-1, after a number of fare transactions have been recorded for a given PAN 314, the transaction identifier list can be analyzed to determine if there is potential misuse involving the PAN 314. To detect potential misuse, the transit system 100 could examine the relationship between at least a subset of the recorded transaction identifiers to identify patterns that are associated with misuse. In one embodiment, the transaction identifiers could be compared to an expected pattern for a typical transit system patron. In another embodiment, the transaction identifiers could be compared to an expected pattern of use for the user associated with the user account. Alternatively, the transaction identifiers could be analyzed to detect abnormalities in the use of the fare media associated with the PAN 314, such as transactions that would indicate that multiple cards are being used with a single PAN 314.

[0102] At block 1050 the transit system 100 may take an action related to using the handheld media as a fare media 250 in association with the transit product. Various actions can be taken, as described later in this disclosure.

[0103] FIG. 10B illustrates one embodiment similar to that of FIG. 10A, wherein the transaction identifier is comprised of the transaction counter 324 from an EMV data packet that is incremented during each contactless use as a fare media. At block 1030-2, the fare transaction

records may include the transaction counter 324 as read from a payment card 310. The transaction counters 324 could be stored in the EMV data format in a cryptogram that is received from the payment card 310, and this entire cryptogram could be sent to the transit system 100 as a transaction fare record. Alternatively, the encrypted packets could be decrypted locally at the station systems 130, and the transaction counters 324 could be analyzed or transmitted to the central ticketing system 112.

[0104] At block 1040-2 potential misuse may be detected by analyzing the sequence of at least a subset of the transaction counters 324. Specifically, determining that potential misuse has occurred may be based on the relationship between the transaction counter 324 values. The detection algorithm may look for sequences of transaction counter values that appear to deviate from the expected pattern of values that would occur during normal use of a payment card 310. Normal use could include use as a fare media 250, use as in retail transactions, or a combination of the two. In most situations where the payment card 310 is also used for retail transactions, the algorithm may need to account for gaps in the transaction counter sequence depending on the time between uses as a fare media 250. The algorithm may also need to account for situations where the card 310 is reissued and used the transaction counter 324 is reset. Other variations in the transaction counter 324 sequence due to normal card use are contemplated by this invention.

[0105] In one embodiment, potential misuse may discovered by detecting large gaps in the transaction counter sequence that are not proportional to the time between uses as a fare media 250. In most cases, the transaction counter sequence should steadily increase, and the increments should go up in small numbers when the card 310 is used regularly as a fare media 250. For example, a set of transaction counters 324 sequentially recorded by a transit system that might not indicate potential misuse could be "5, 6, 8, 10, 13." Another example might be "125, 127, 128, 132." The small gaps in these sequences may indicate normal retail use between uses as a fare media 250. If the sequence reveals large gaps in the transaction counters 324, this may indicate that two cards 310 associated with the same PAN 314 are being used as a fare media 250 for the same transit product. For example, the sequence could be "12, 14, 15, 52, 53, 55." In this case, the gap between 15 and 52 could be used to determine that two different cards 310 with the same PAN 314 are being used. On the other hand, if there is a large amount of time between transaction number 15 and transaction number 52, then the gap may be attributed to normal retail use of the payment card 310 and not indicative of potential misuse. Therefore, some embodiments may determine whether the gap in the transaction counter sequence is proportional

to the amount of time between fare transactions involving the card 310. For example, the determination could take into account the average gap size in the transaction counter sequence to gauge when a gap is large enough to indicate potential misuse. Thus, a sequence of "5, 16, 30, 44, 45, 60" may not indicate potential misuse even though the gaps are large between each transaction. This situation may instead indicate that the user is involved in a large number of retail transactions on a regular basis between fare transactions, even if the fare transactions are not relatively far apart in time.

[0106] Alternatively or additionally, the determination of potential misuse may also be made by detecting patterns of transaction counters 324 that do not continually increase. Even if a payment card 310 is involved in retail transactions in addition to being used as a fare media 250, the transaction counter 324 would typically increase, even with gaps in the sequence. For example, a sequence of transaction counters 324 such as "5, 6, 189, 9, 191, 192, 12" could indicate that more than card 310 with the same PAN 314 is being used, one with a transaction count near "5", and one with a transaction count near "191". The detection may also anticipate situations where the large gaps occur, or where a sequence jumps from high numbers to low numbers as a result of legitimate single-card use. An example sequence could be "250, 253, 255, 1, 4." Such situations may arise when a card is reissued by the financial institution or when the transaction counter 324 rolls over. In these cases, the detection algorithm may consider other inputs, such as the card expiry date 321, a known transaction counter limit, a notification from the user, and/or the like.

[0107] More sophisticated misuse of a payment card 310 might be more difficult to detect. For example, two users could be using cards 310 with the same PAN 314 and could coordinate the cards' use to prevent glaring out-of-sequence transaction counters 324. This could result in a transaction counter 324 sequence such as "80, 81, 83, 83, 84, 86, 87." In this case, the algorithm may need to look for more subtle errors in the sequence. Therefore, the determination of misuse may also look for duplicate numbers or sequences that do not show signs of normal retail transactions. In another embodiment, the determination of potential misuse could detect repeated patterns, such as "120, 122, 123, 120, 122, 123." Repeated patterns may indicate a careful collaboration between users of duplicate cards 310, or could indicate that a card 310 has been electronically pick-pocketed or skimmed, and a duplicate card 310 is being used without the card owner's knowledge. A determination that potential misuse does not necessarily implicate the card owner may be valuable in determining an appropriate action to take in response at block 1050 described later in this disclosure.

[0108] A determination of potential misuse involving the transaction counters 324 can also be made by developing use profiles of different transaction counter sequences, and then comparing the recorded sequences with the profiles. Recorded sequences that deviate sufficiently from an expected profile could indicate potential misuse. A profile may consist of certain transaction counter sequence patterns that are common. Alternatively, a profile may consist of descriptive information about expected profile patterns, such as average gap size, average transaction counter limit, and/or total number of retail transactions for each fare transaction. The profiles could be derived from multiple users and combined to create an average user profile. Alternatively, a profile could be derived from the usage statistics from users that are similar to the suspect user. In another embodiment, a profile may be based on the actual use of each individual user's transaction history. In this case, the determination algorithm may identify types a card use which deviate from the historical usage pattern of the particular user. Other methods of generating a comparison profile are contemplated by various embodiments, and may involve combinations of the various methods described above.

[0109] Alternatively or additionally, other embodiments may use different data as a transaction identifier to detect potential misuse. FIG. 10C illustrates an embodiment wherein the time and/or location of a transaction is used as the transaction identifier. At block 1030-3, time and location data could be collected from the access control points 208 of the transit system 100 as a handheld media is used as a fare media 250. The data could be collected and packaged together in a data packet along with the data read from the handheld media. Alternatively, the time and location data could be stored and/or transmitted separately from the handheld media data. In another variation, the time and location data could be received from the handheld media itself, for example from a smart phone enabled with GPS location information. In any case, the transaction fare records made available to the transit system 100 may include transaction time and /or location data with an associated PAN 314.

[0110] At block 1040-3, potential misuse is determined, at least in part, by analyzing the pattern of transaction times and/or locations. The determination of potential misuse may identify travel patterns that are illogical, unlikely, out of character compared to a user profile, and/or physically impossible. In one embodiment, the determination may be made by detecting transaction times that are unlikely to occur. For example, multiple trips during the same day, although physically possible, may be unlikely. This situation may indicate that multiple users are handing off the same handheld media for use throughout the day. A large number of uses over a short period of

time may indicate that a PAN 314 has been stolen and associated with a large number of handheld media. In another embodiment, the transaction time may be analyzed in conjunction with the transaction location. For example, fare transactions near the same time at distant locations may be indicative of two handheld media associated with the same PAN 314 being used by two different users for the same transit product. While some time and location combinations may be physically impossible, others may be possible but unlikely. In these cases, the potential for misuse may be determined to be proportional to the time and distance between locations. For example, uses at transit stations that are 30 miles apart may indicate potential misuse if the uses were 20 minutes apart. On the other hand, uses at two stations that are 30 miles apart may not indicate potential misuse if the uses occur more than 60 minutes apart.

[0111] In one embodiment, the time and/or location data may be compared to an expected user profile, and potential misuse may be determined by detecting deviations from the expected user profile. The profiles could be derived from multiple users and combined to create an average user profile. Alternatively, a profile could be derived from the usage statistics from users that are similar to the suspect user account. In another embodiment, the profile may be based on the actual use of each individual user's transaction history. In this case, the determination algorithm may identify types of card use which deviate from the historical usage pattern of the particular user. For example, if a particular user only travels between two transit stations on weekdays, then travel between different stations, or from a different starting station, may indicate potential misuse. Similarly, usage statistics from a single user account that do not establish any recognizable and/or predictable pattern may indicate that a card 310 is being exchanged by multiple users contrary to the rules of the transit product. Other methods of generating a comparison profile are contemplated by various embodiments, and may involve combinations of the various methods described above.

[0112] Using a transaction counter 324 or the transaction time and/or location as the transaction identifier in the determination of potential misuse, as described in embodiments hereinabove, are not meant to be limiting. Other embodiments may include other data that may be used as transaction identifiers. It may also be advantageous to combine data together as transaction identifiers to increase the effectiveness of the misuse detection. In one embodiment, the transaction identifier may include both a transaction counter 324 and the transaction time and/or location. For example, if the times and locations of a series of fare transactions indicate that the potential for misuse exists, the transaction counter 324 may be used to verify or dismiss the

suspicious behavior. In another example, the transaction counter 324 might indicate potential misuse when the counter sequence contains a large gap or resets to a lower number. In this case, the times and locations of the transactions may be analyzed to either confirm the suspicious activity or to indicate that a valid user may instead be using a valid replacement card 310, that the user is making a large number of retail purchases, or that the card's transaction counter 324 has rolled over. It will be understood that further combinations of transaction data beyond those explicitly describe herein are also contemplated by these and other embodiments.

[0113] Block 1050 of FIGS. 10A-10C illustrates that in certain embodiments an action may be taken related to using a handheld media associated with the user account as a fare media 250. The type of action taken may be related to the type and/or severity of potential misuse. It may also depend on a customer preference or on the duration or extent of the potential misuse. For example, in some embodiments the potential misuse may be a type that could be unknown to an authorized user. In this case, the transit system could send a notification to the user alerting him/her to the possibility of fraud via text message, voice mail, email, telephone, traditional mail, and/or any other means of communication. A user preference may also be used to decide how to deal with potential misuse detected in the user's account. For instance, the user could specify that a notification be sent to the user. Notification could also be sent to the issuing bank in cases where the handheld media is a payment card. The user could also specify that more immediate action be taken to prevent further misuse and protect the user's account and the transit system 100.

[0114] In some embodiments, immediate action could include taking steps to restrict the use of the transit product, or to restrict the use of any handheld media with PANs 314 associated with the transit product. In one embodiment, the PAN 314 could be "hotlisted" to restrict the use of the associated handheld media at the access control points 208. This restriction could happen immediately when potential misuse is detected at the access control point 208, or the restricted PANs 314 could be sent our in batches periodically from the transit system 100. The restriction could prevent a PAN 314 from being used at all, including for any current transaction when potential misuse is detected. Alternatively, the restriction could allow any current transactions to proceed, but could restrict future transactions. The restriction could also be partial, allowing only a certain number of uses of the transit product during a time period. For example, a user account with a monthly transit pass could be restricted to ten uses per week, or to two uses per day.

[0115] In cases where the potential for misuse is less certain, the action taken may include manual inspection and/or further processing. For example, the times and locations associated with a PAN 314 may seem to indicate that although it would not be impossible for a single user to be using the PAN 314, it would be unlikely. In this case, the detection algorithm could flag the account as one possibly requiring more scrutiny. The travel patterns associated with the account could then be manually inspected by a human operator, or the travel patterns could be further analyzed by different types of detection methods to verify any potential misuse. If the further inspection or processing determines that the potential misuse is likely, then the account may be "hotlisted" as described above. Alternatively or additionally, the user and/or issuing bank institution could be notified. In one embodiment, a flagged account may collect more transaction identifiers from each subsequent transaction for processing. The detection algorithm could also use a larger subset of the transaction history or could compare the transaction identifiers with additional user profiles. It will be understood that other embodiments may use a combination of these and other techniques in taking an action after the detection of potential misuse.

[0116] In cases where it is determined that the user is allowing others to use his/her PAN 314 to access that transit system 100, either the transit system 100 or the user may specify that the additional uses be charged to the user account without restricting use of the card 310. For example, a user may swipe a payment card 310 multiple times at an access control point 208, allowing multiple users to enter the transit system 100 with his/her monthly pass. The first use of the card 310 could be allowed under the monthly pass, and each additional use could be charged to the user as an additional single-ride use. Charging for additional uses may result in a charge to the user account, or if the handheld media is a payment card 310, the additional charges may be charged directly to the payment card 310. Charging the payment card 310 in this manner may be the result of preference set by the user in the user account, and it may combined with other actions, such as restricting the PAN's 314 use or notifying the user.

[0117] In the foregoing description, for the purposes of illustration, methods were described in a particular order. It should be appreciated that in alternate embodiments, the methods may be performed in a different order than that described. It should also be appreciated that the methods described above may be performed by hardware components or may be embodied in sequences of machine-executable instructions, which may be used to cause a machine, such as a general-purpose or special-purpose processor or logic circuits programmed with the instructions to perform the methods. These machine-executable instructions may be stored on one or more

machine readable mediums, such as CD-ROMs or other type of optical disks, floppy diskettes, ROMs, RAMs, EPROMs, EEPROMs, magnetic or optical cards, flash memory, or other types of machine-readable mediums suitable for storing electronic instructions. Alternatively, the methods may be performed by a combination of hardware and software.

[0118] Although many of the embodiments disclosed hereinabove use a contactless payment card 310, this is only one type of handheld media that is contemplated by this invention. It will be understood that many other types of handheld media may be used as a fare media 250, and that all of the embodiments described herein can utilize various forms of handheld media, in addition, and as an alternative to, contactless payment cards.

[0119] While illustrative and presently preferred embodiments of the disclosed systems, methods, and machine-readable media have been described in detail herein, it is to be understood that the inventive concepts may be otherwise variously embodied and employed, and that the appended claims are intended to be construed to include such variations, except as limited by the prior art.

CLAIMS

1. A method for detecting potential misuse of a primary account number (PAN) associated with a handheld media in a transit system having one or more access points, the method comprising:

creating a user account for managing transactional information, the user account comprising a transit product;

enrolling the handheld media for use as fare media for the transit product, wherein the PAN is stored in the user account;

receiving, from the one or more access points of the transit system, a plurality of fare transaction records, wherein each fare transaction record in the plurality of fare transaction records comprises:

the PAN associated with the handheld media; and

a transaction counter;

determining a potential misuse of a handheld media associated with the PAN, wherein the determination is based, at least in part, on a sequence of a plurality of transaction counters corresponding to the plurality of fare transaction records; and

taking an action related to using the handheld media as fare media for using the transit product.

2. The method of claim 1, wherein the handheld media is a smart card having near-field communication capabilities, wherein the transaction counter is stored on the handheld media, and wherein the transaction counter increments at least every time the handheld media is used at the one or more access points.

3. The method of claim 1 or claim 2, wherein the potential misuse is determined by identifying gaps in the sequence of the plurality of transaction counters.

4. The method of claim 1 or claim 2, wherein the potential misuse is determined by determining that the sequence of the plurality of transaction counters is not ascending.

5. The method of claim 1 or claim 2, wherein the potential misuse is determined by comparing the sequence of the plurality of transaction counters to a user profile and identifying deviations.

6. The method of claim 1 or claim 2, wherein:

each fare transaction record further comprises a transaction time and a transaction location; and

the potential misuse is further determined, at least in part, on a pattern of the transaction times and locations of a plurality of the transaction times and locations corresponding to the plurality of fare transaction records.

7. The method claim 6, wherein the potential misuse is determined by identifying a gap in the sequence of the plurality of transaction counters that is larger than a corresponding time gap by a calculated amount.

8. A method for detecting potential misuse of a primary account number (PAN) associated with a handheld media in a transit system having one or more access points, the method comprising:

creating a user account for managing transactional information, the user account comprising a transit product;

enrolling the handheld media for use as fare media for the transit product, wherein the PAN is stored in the user account;

receiving, from the one or more access points of the transit system, a plurality of fare transaction records, wherein each fare transaction record in the plurality of fare transaction records comprises:

the PAN associated with the handheld media;

a transaction time; and

a transaction location;

determining a potential misuse of a handheld media associated with the PAN, wherein the determination is based, at least in part, on a pattern of the transaction times and locations of a plurality of the transaction times and locations corresponding to the plurality of fare transaction records; and

taking an action related to using the handheld media as fare media for using the transit product.

9. The method of claim 8, wherein the potential misuse is determined by indentifying multiple fare transactions that take place within a predetermined time window.

10. The method of claim 8, wherein the potential misuse is determined by indentifying fare transactions at distant locations that occur within a predetermined time window.

11. The method of claim 8, wherein the potential misuse is determined by indentifying first and second fare transactions wherein travel time between the locations of the first and second fare transactions exceeds a difference between the transaction times of the first and second fare transactions.

12. The method of claim 8, wherein the potential misuse is determined by comparing the pattern of the transaction times and locations to a user profile and identifying deviations.

13. The method of claim 8, wherein:

each fare transaction record further comprises a transaction counter; and

the potential misuse is determined, at least in part, on a sequence of a plurality of transaction counters.

14. A server for detecting potential misuse of a primary account number (PAN) associated with a handheld media in a transit system having one or more access points, the server comprising:

a network interface configured to communicate with a network;

an input interface configured to receive information from the one or more access points of the transit system;

a processor communicatively coupled with the network interface, the input interface, and a memory;

the memory having instructions that, when executed by the processor, cause the server to:

create a user account for managing transactional information in the memory, the user account comprising a transit product;

enroll the handheld media for use as fare media for the transit product, wherein the PAN is stored in the user account in the memory;

receive, from the input interface, a plurality of fare transaction records, wherein each fare transaction record in the plurality of fare transaction records comprises:

the PAN associated with the handheld media; and

a transaction identifier;

determine, by the processor, a potential misuse of a handheld media associated with the PAN, wherein the determination is based, at least in part, on a relationship between a plurality of transaction identifiers of the plurality of fare transaction records; and

take an action related to using the handheld media as fare media for using the transit product.

15. The server of claim 14, wherein the determination of potential misuse of the handheld media associated with the PAN comprises a determination that more than one individual is using the handheld media associated with the PAN.

16. The server of claim 14, wherein:

each transaction identifier comprises a transaction counter; and;

the potential misuse is determined, at least in part, on a sequence of a plurality of transaction counters.

17. The server of claim 14, wherein:

each transaction identifier comprises a transaction time and a transaction location; and

the potential misuse is determined, at least in part, on a pattern of the transaction times and locations of a plurality of the transaction times and transaction locations.

18. The server of any one of claims 14 to 17, wherein the action related to using the handheld media as fare media for using the transit product comprises denying future use as fare media of any handheld media associated with the PAN.

19. The server of any one of claims 14 to 17, wherein the action related to using the handheld media as fare media for using the transit product comprises charging the user account a fee for one or more of the plurality of fare transaction records.

20. The server of any one of claims 14 to 17,

further comprising an output interface configure to send notifications associated with potential misuse of the handheld media associated with the PAN; and

wherein the action related to using the handheld media as fare media for using the transit product comprises sending, from the output interface, a notification regarding the potential misuse of the handheld media associated with the PAN.

21. A method for detecting potential misuse of a primary account number (PAN) associated with a handheld media in a transit system having one or more access points, the method being substantially as described herein with reference to the accompanying drawings.

22. A server for detecting potential misuse of a primary account number (PAN) associated with a handheld media in a transit system having one or more access points, the server being substantially as described herein with reference to the accompanying drawings.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 December 2005 (15.12.2005)

PCT

(10) International Publication Number
WO 2005/119607 A2

(51) International Patent Classification[7]: G07F 19/00

(21) International Application Number: PCT/US2005/019988

(22) International Filing Date: 3 June 2005 (03.06.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/576,894 3 June 2004 (03.06.2004) US
60/591,998 28 July 2004 (28.07.2004) US

(71) Applicant *(for all designated States except US)*: **TYFONE, INC.** [US/US]; 1490 Clifton Street, Portland, Oregon 97201 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **SPITZER, Thomas N.** [US/US]; 1490 Clifton Street, Portland, Oregon 97201 (US). **TADEPALLI, Prabhakar** [US/IN]; 290 Phase II, Adarsh Palm Meadows, Airport Whitefield Road, Bangalore, Karnataka 560066 (IN). **NARENDRA, Siva G.** [IN/US]; 7180 SW 84th Avenue, Portland, Oregon 97223 (US).

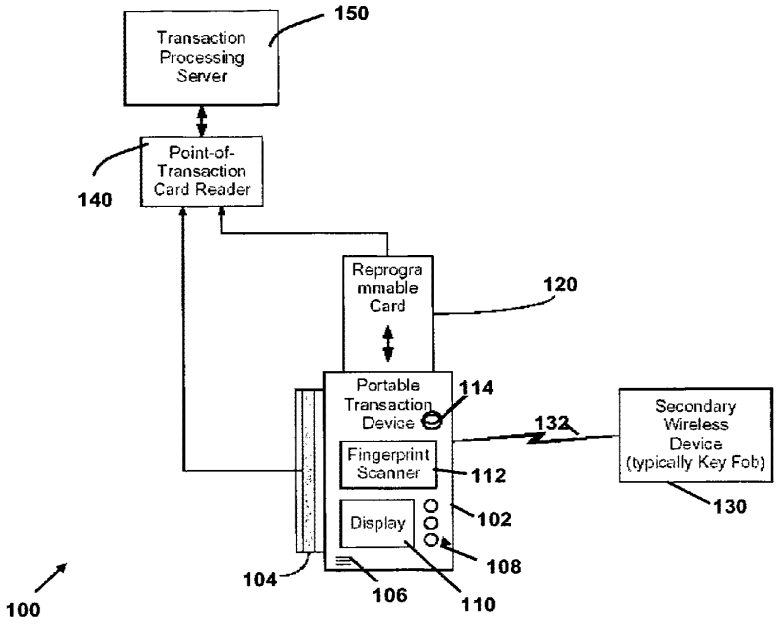
(74) Agent: **LEMOINE, Dana B.**; LeMoine Patent Services, PLLC, c/o Portfolio IP, P.O. Box 52050, Minneapolis, Minnesota 52050 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR SECURING FINANCIAL TRANSACTIONS



(57) Abstract: A financial transaction system utilizes multi-factor authentication to secure financial transactions.

WO 2005/119607 A2

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SYSTEM AND METHOD FOR SECURING FINANCIAL TRANSACTIONS

Field

The present invention relates generally to portable transaction devices, and more specifically to portable transaction devices having various security features.

Background

Instances of financial card fraud and identity theft have increased dramatically in recent years, particularly with the rapid increase of online and electronic transactions. Solutions of varying efficacy have been proposed to protect financial information and otherwise guard against fraud and theft. Firewalls protect computer systems against unauthorized access; however, they cannot be completely assured of the identities of individuals accessing the network. Various electronic devices may be employed to verify the identity of individuals; however, these devices often permit authentication information to be accessed. Some systems provide significantly improved security, but at the expense of requiring substantial changes to point-of-sale devices or other parts of the transactional infrastructure.

Brief Description of the Drawings

Figures 1 and 2 show transaction systems with multi-factor authentication;

Figure 3 shows a block diagram of a programmable card;

Figure 4 shows a block diagram of a secondary wireless device;

Figure 5 shows a computer and base station;

Figure 6 shows usage models for various embodiments of the present invention;

Figure 7 shows an intelligent electronic device capable of printing checks;

Figures 8-10 show various methods for financial card transaction verification in accordance with various embodiments of the present invention;

Figure 11 shows a flexible form factor for a programmable financial card;

Figure 12 shows an exploded perspective view of the programmable financial card of Figure 11;

Figure 13 shows usage models for a secondary wireless device in card-present transactions and card-not-present transactions;

Figure 14 shows an architecture diagram for a transaction system with multi-factor authentication;

Figure 15 shows usage models for electronic money transfer;

Figure 16 shows usage models for pre-paid card recharge; and

Figure 17 shows business methods.

Description of Embodiments

In the following detailed description, reference is made to the accompanying drawings that show, by way of illustration, various embodiments of an invention. These embodiments are described in sufficient detail to enable those skilled in the art to practice the invention. It is to be understood that the various embodiments of the invention, although different, are not necessarily mutually exclusive. For example, a particular feature, structure, or characteristic described in connection with one embodiment may be implemented within other embodiments without departing from the spirit and scope of the invention. In addition, it is to be understood that the location or arrangement of individual elements within each disclosed embodiment may be modified without departing from the spirit and scope of the invention. The following detailed description is, therefore, not to be taken in a limiting sense, and the scope of the present invention is defined only by the appended claims, appropriately interpreted, along with the full range of equivalents to which the claims are entitled. In the drawings, like numerals refer to the same or similar functionality throughout the several views.

The present disclosure relates generally to use of a portable transaction device having various security features. The security features may be employed to particular advantage in financial transactions, so as to enhance security beyond that currently available in transactions conducted with financial cards,