[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.

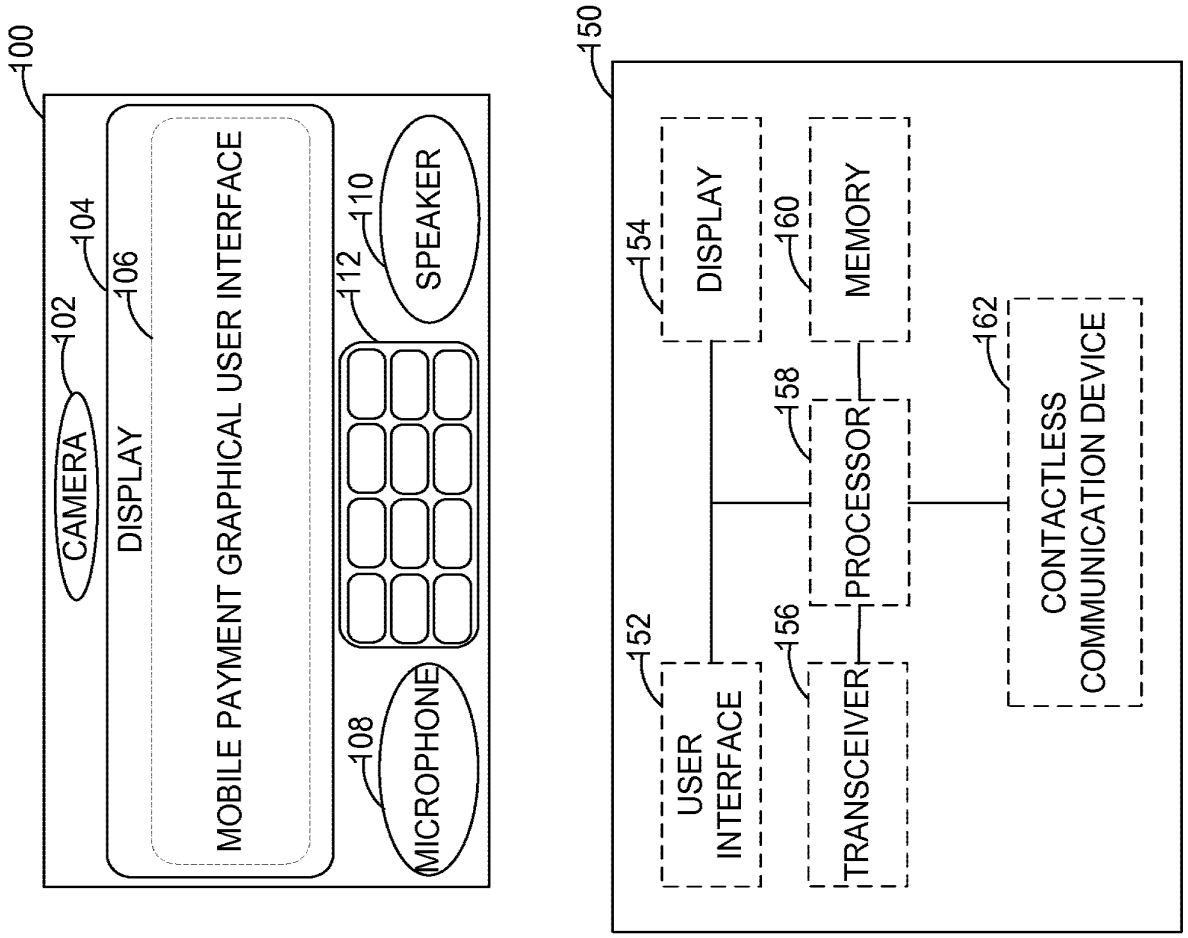

100
CAMERA
102
DISPLAY
104
MOBILE PAYMENT GRAPHICAL USER INTERFACE
106
MICROPHONE
108
SPEAKER
110
112
150
USER INTERFACE
152
TRANSCEIVER
156
PROCESSOR
158
DISPLAY
154
MEMORY
160
CONTACTLESS COMMUNICATION DEVICE
162

FIG. 1

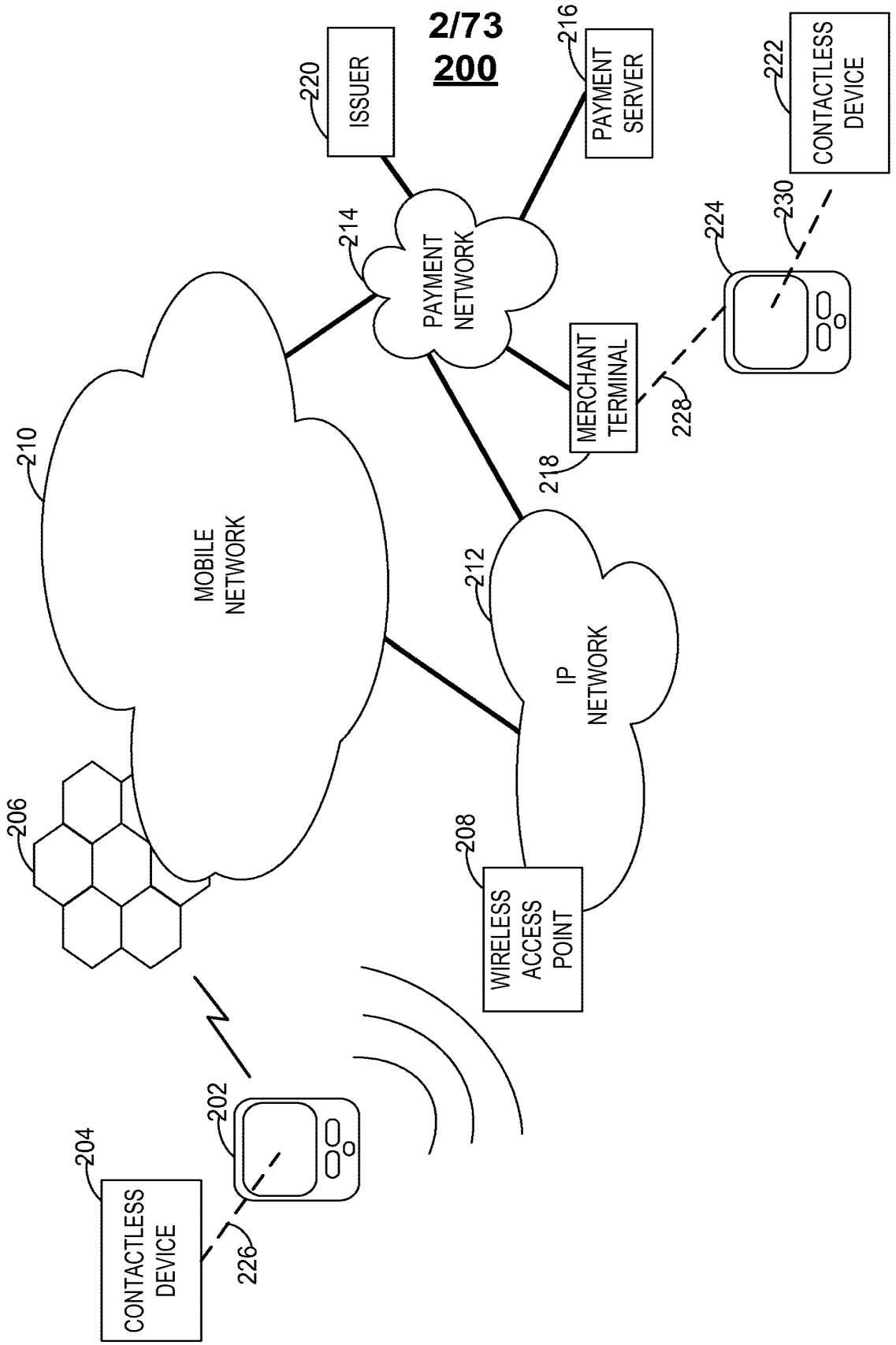

200
ISSUER
220
PAYMENT SERVER
216
CONTACTLESS DEVICE
222
PAYMENT NETWORK
214
MERCHANT TERMINAL
218
224
230
228
MOBILE NETWORK
210
IP NETWORK
212
206
208
WIRELESS ACCESS POINT
202
204
CONTACTLESS DEVICE
226

FIG. 2

300

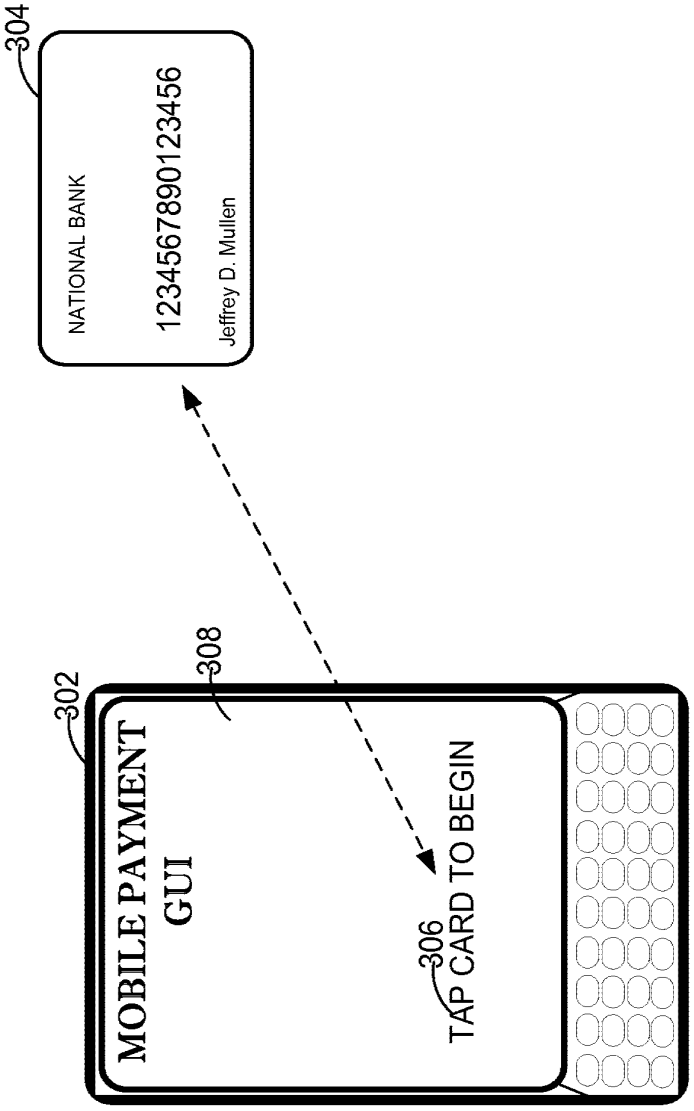

304
NATIONAL BANK
1234567890123456
Jeffrey D. Mullen
302
308
MOBILE PAYMENT GUI
306
TAP CARD TO BEGIN

FIG. 3

400

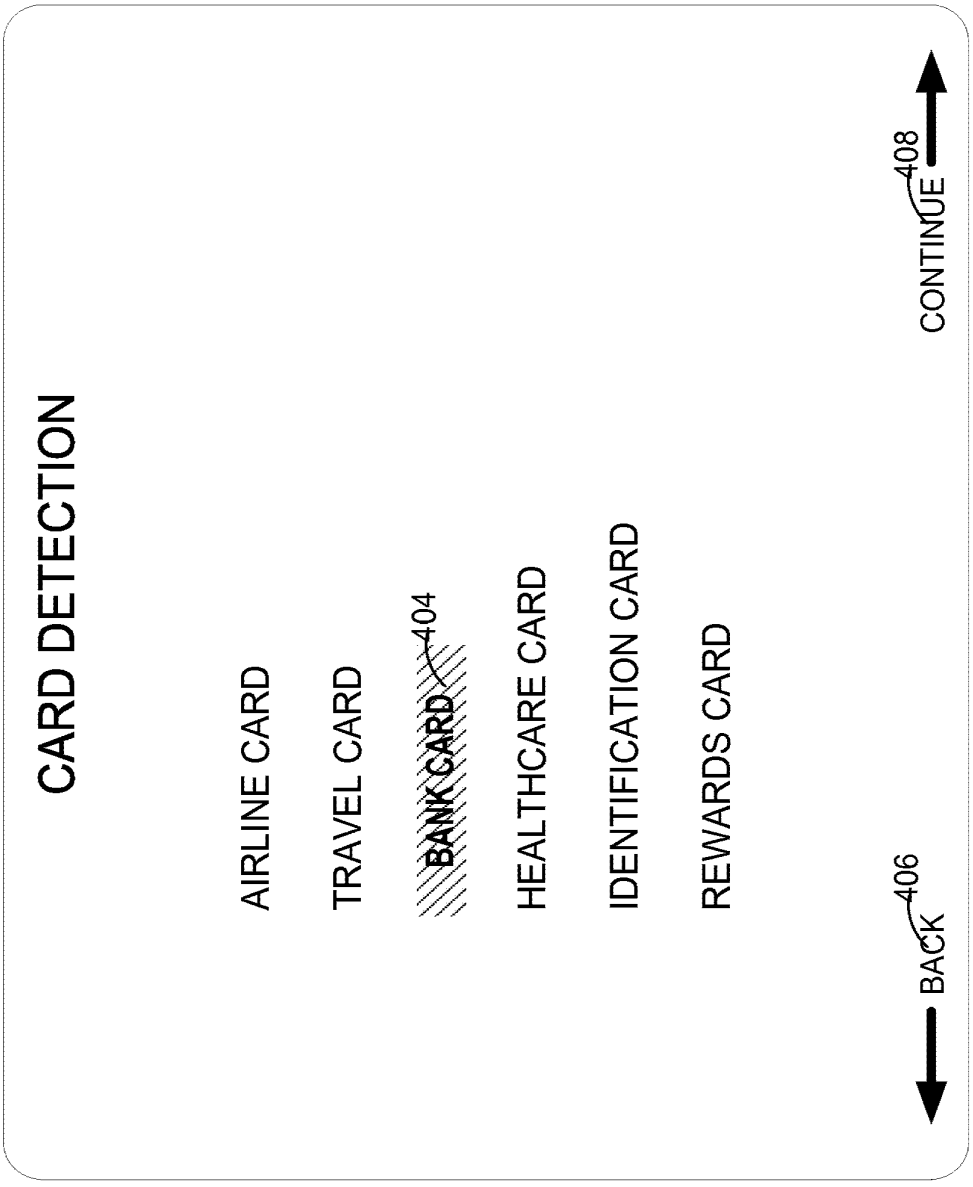

CARD DETECTION
AIRLINE CARD
TRAVEL CARD
BANK CARD
404
HEALTHCARE CARD
IDENTIFICATION CARD
REWARDS CARD
BACK
406
CONTINUE
408

FIG. 4

500

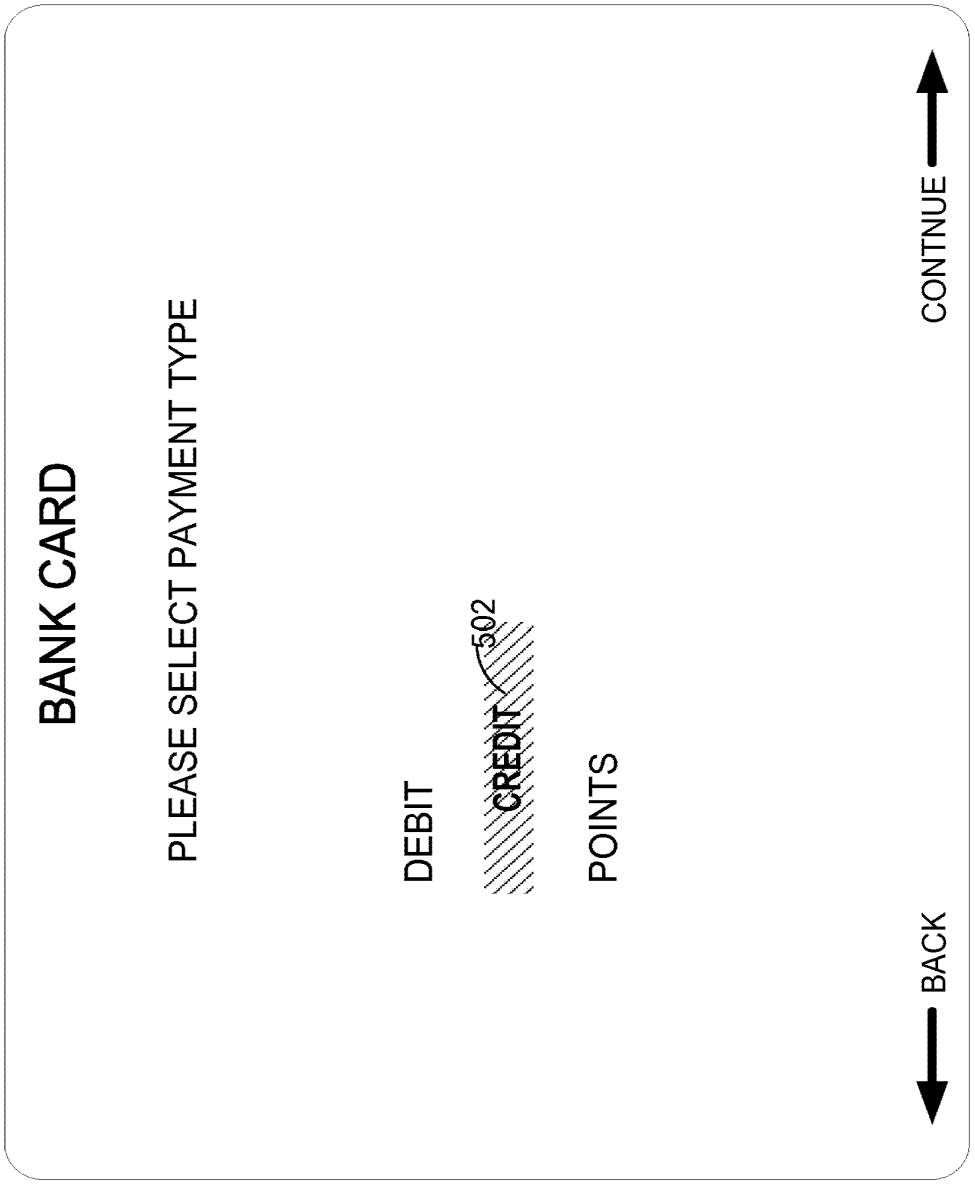

BANK CARD
PLEASE SELECT PAYMENT TYPE
DEBIT
CREDIT
502
POINTS
CONTNUE
BACK

FIG. 5

600

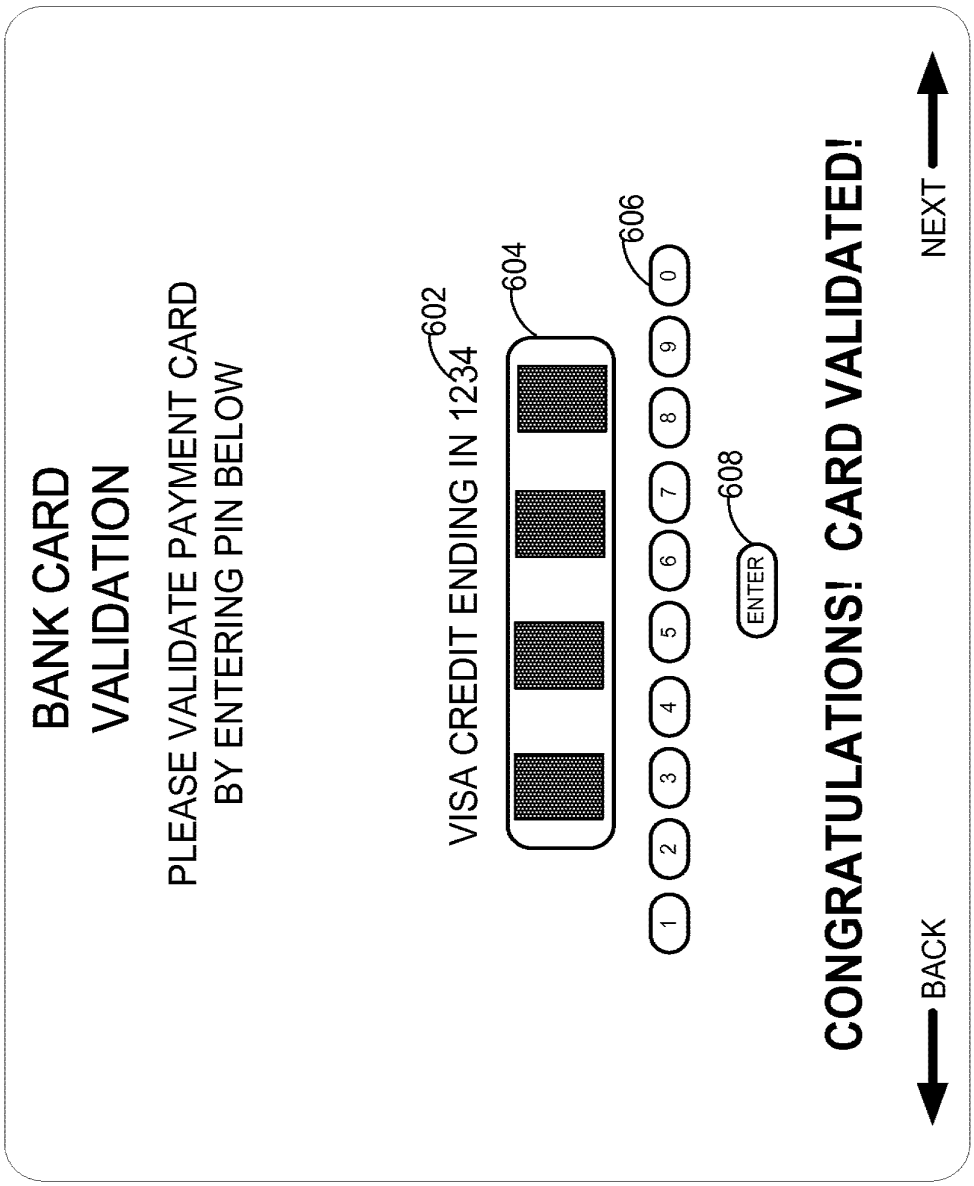

BANK CARD
VALIDATION
PLEASE VALIDATE PAYMENT CARD
BY ENTERING PIN BELOW
VISA CREDIT ENDING IN 1234
602
604
606
1
2
3
4
5
6
7
8
9
0
ENTER
608
CONGRATULATIONS! CARD VALIDATED!
BACK
NEXT

FIG. 6

700

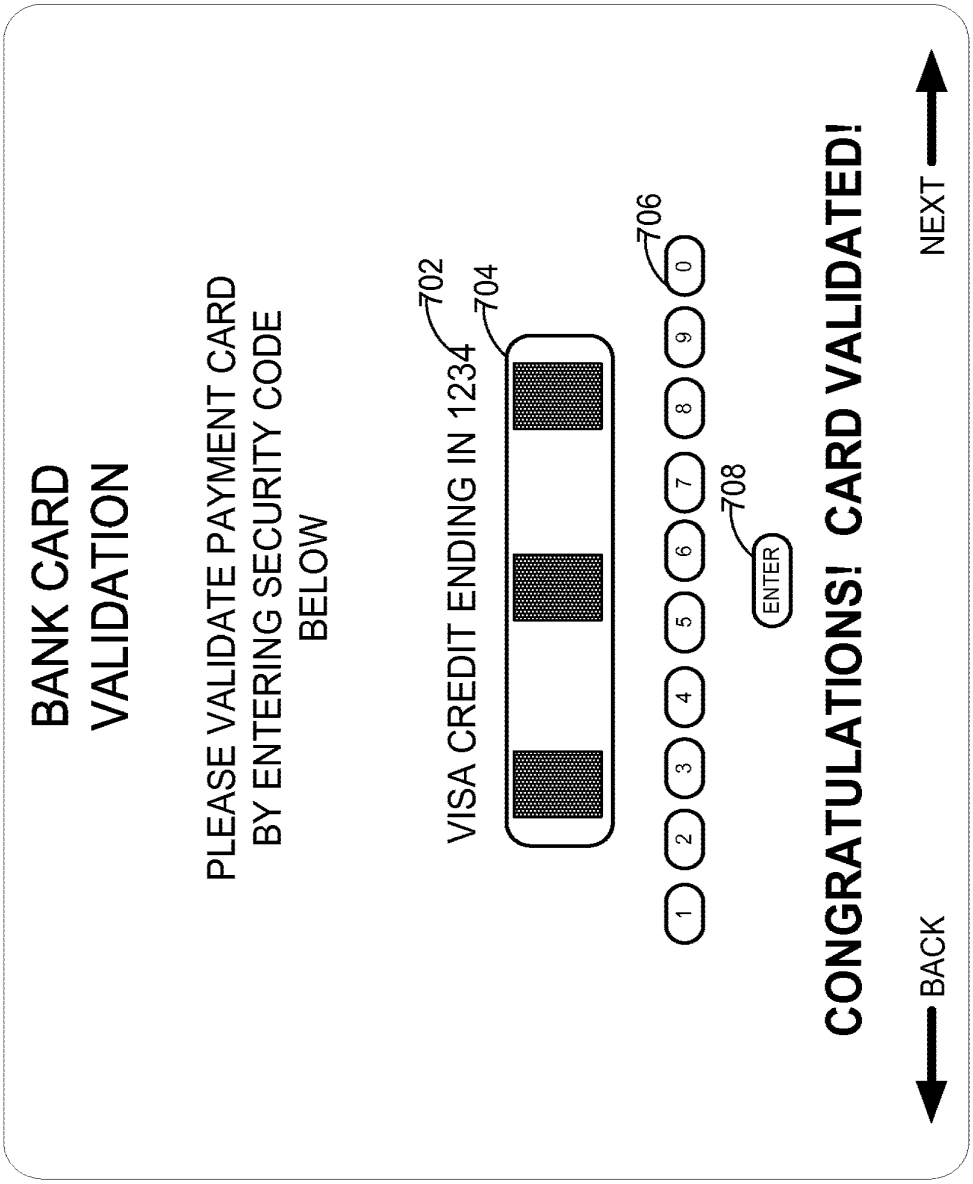

BANK CARD VALIDATION
PLEASE VALIDATE PAYMENT CARD BY ENTERING SECURITY CODE BELOW
VISA CREDIT ENDING IN 1234
702
704
706
708
1
2
3
4
5
6
7
8
9
0
ENTER
CONGRATULATIONS! CARD VALIDATED!
BACK
NEXT

FIG. 7

800

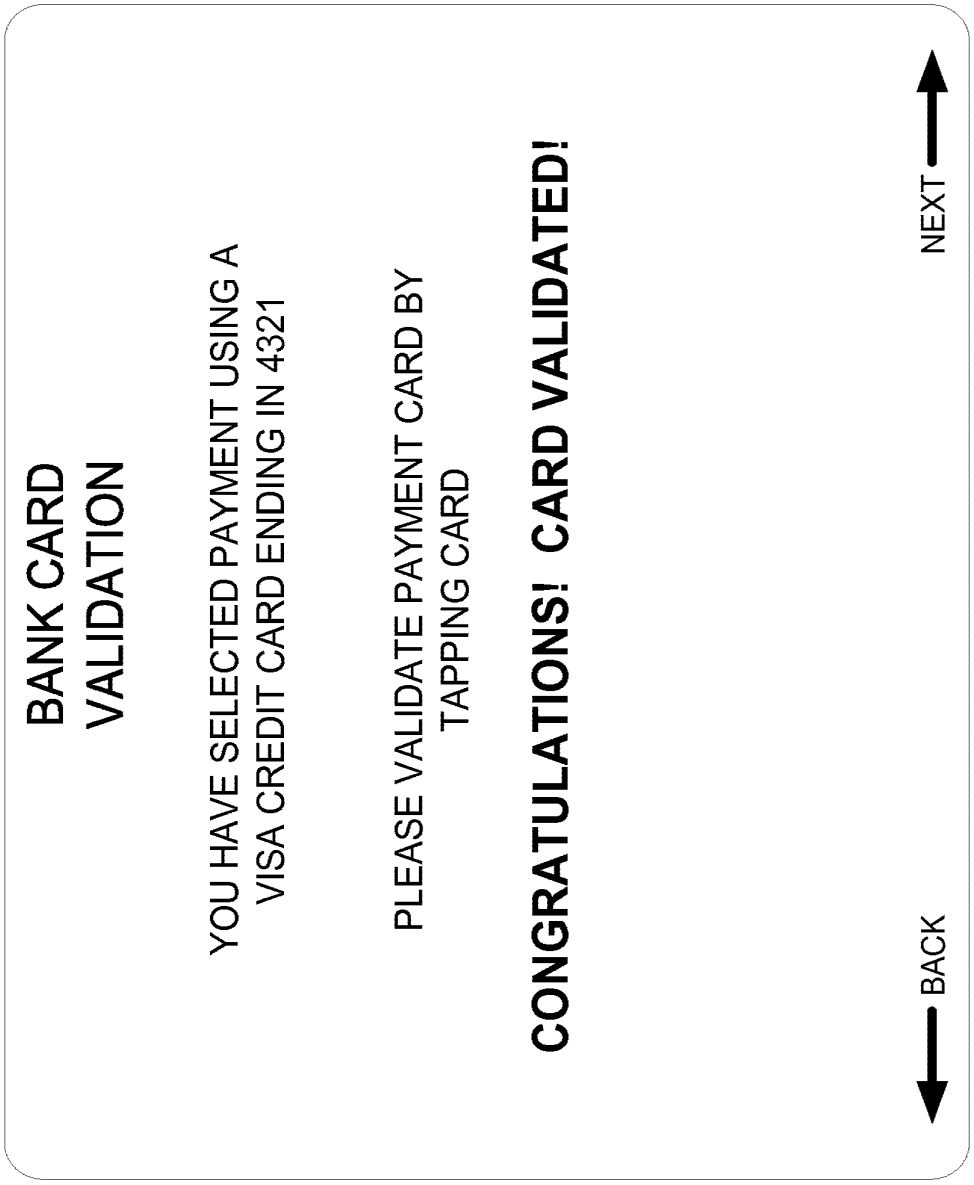

BANK CARD
VALIDATION
YOU HAVE SELECTED PAYMENT USING A
VISA CREDIT CARD ENDING IN 4321
PLEASE VALIDATE PAYMENT CARD BY
TAPPING CARD
CONGRATULATIONS! CARD VALIDATED!
BACK
NEXT

FIG. 8

900

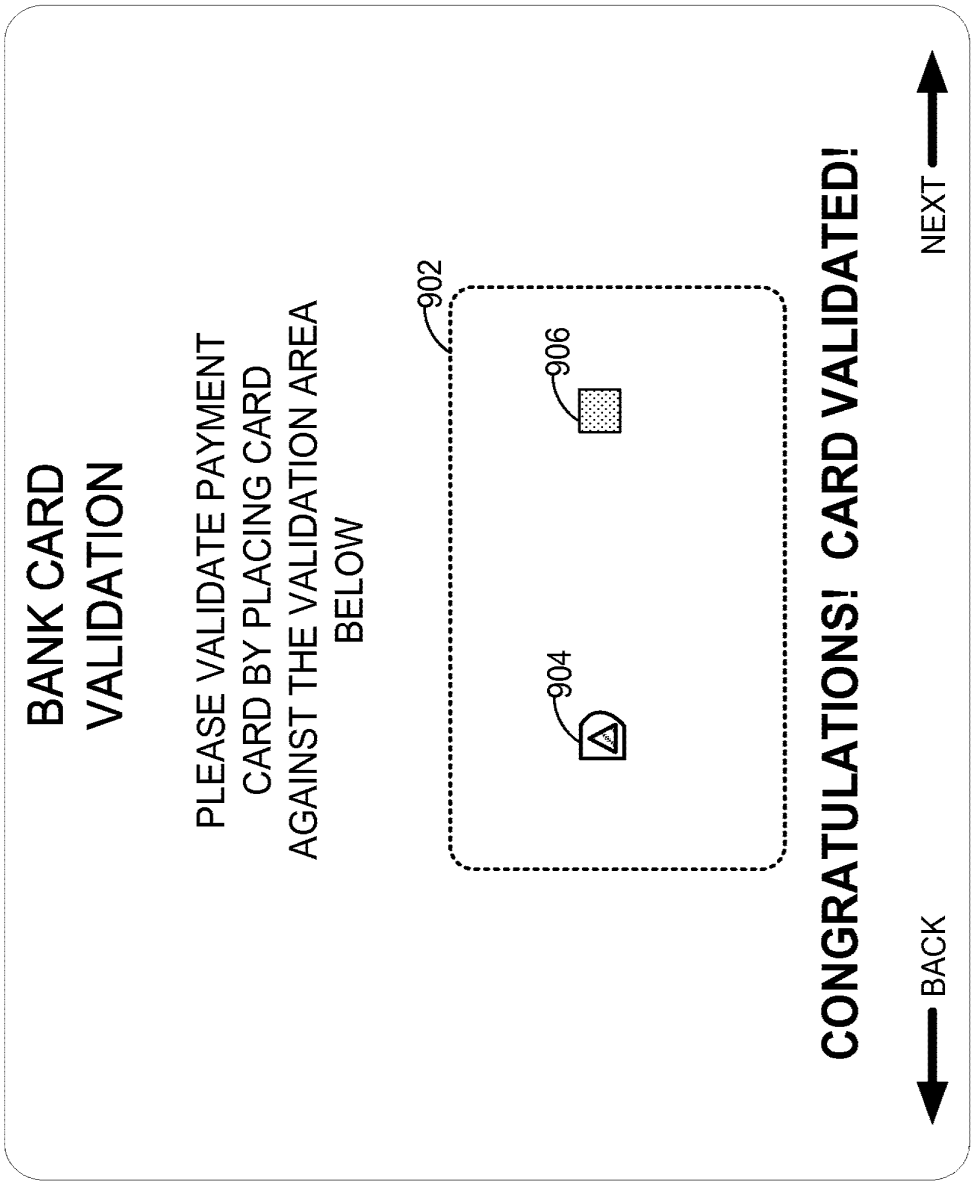

BANK CARD
VALIDATION
PLEASE VALIDATE PAYMENT
CARD BY PLACING CARD
AGAINST THE VALIDATION AREA
BELOW
902
906
904
CONGRATULATIONS! CARD VALIDATED!
BACK
NEXT

FIG. 9

10/73

1000

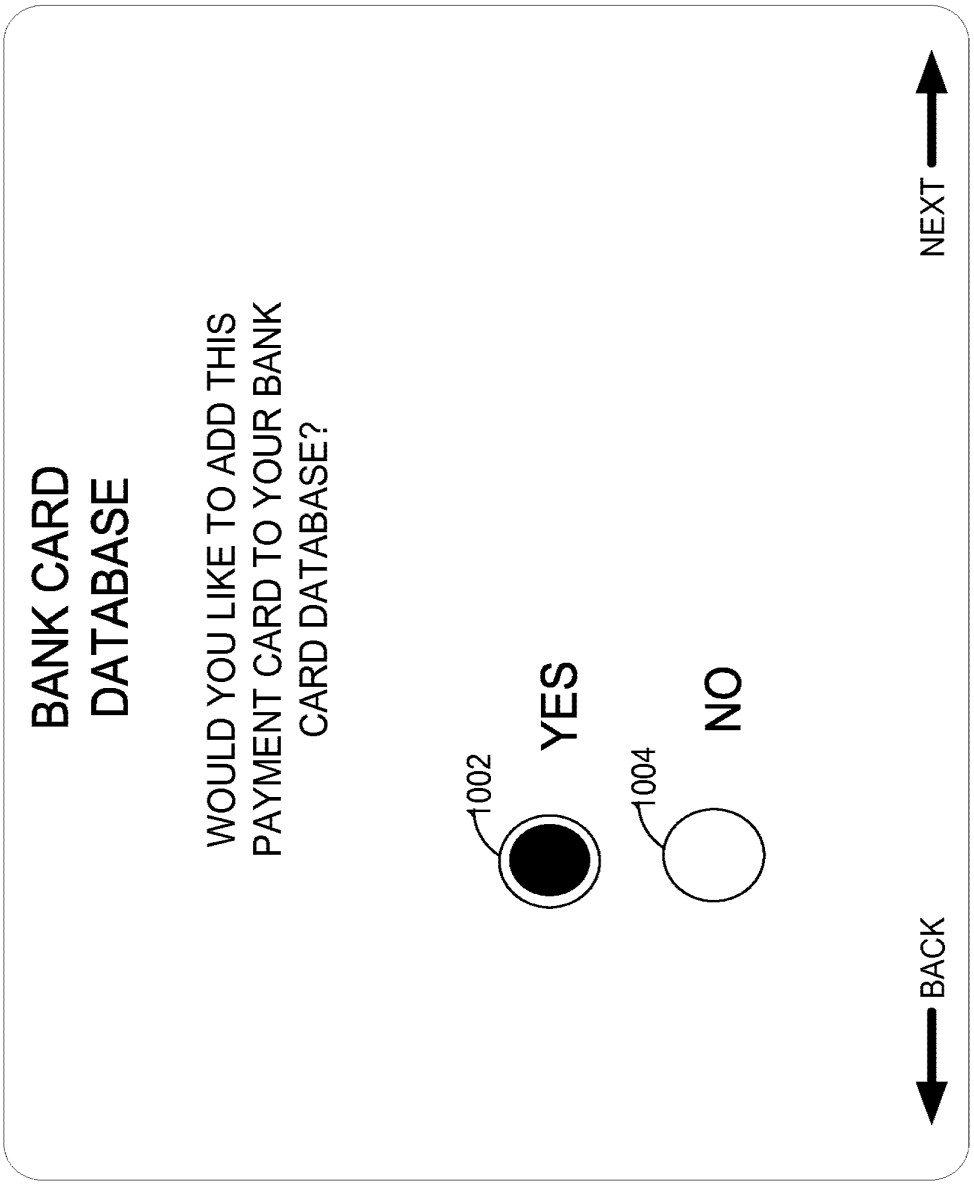


FIG. 10

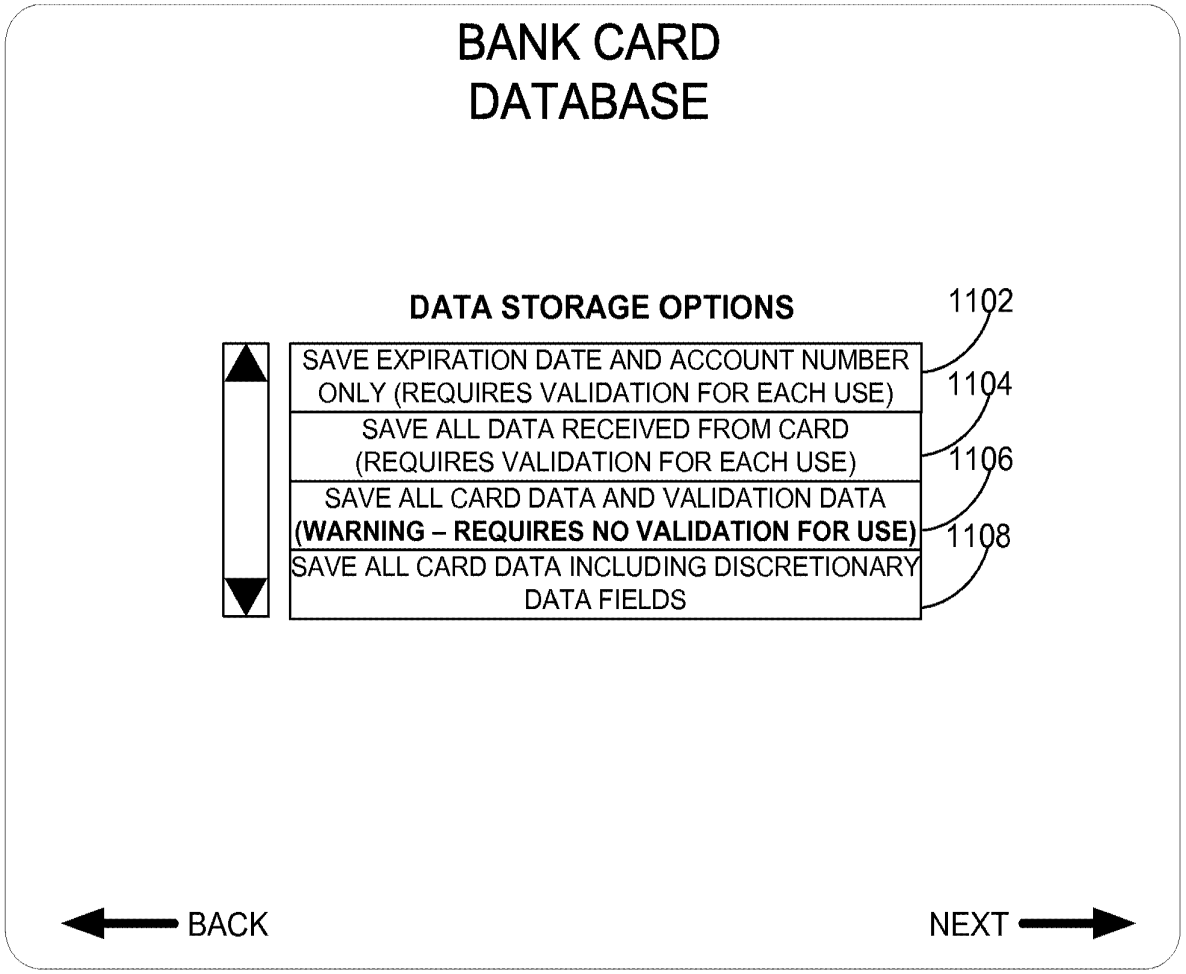


FIG. 11

IPR2025-01152
Apple EX1002 Page 1015

1200

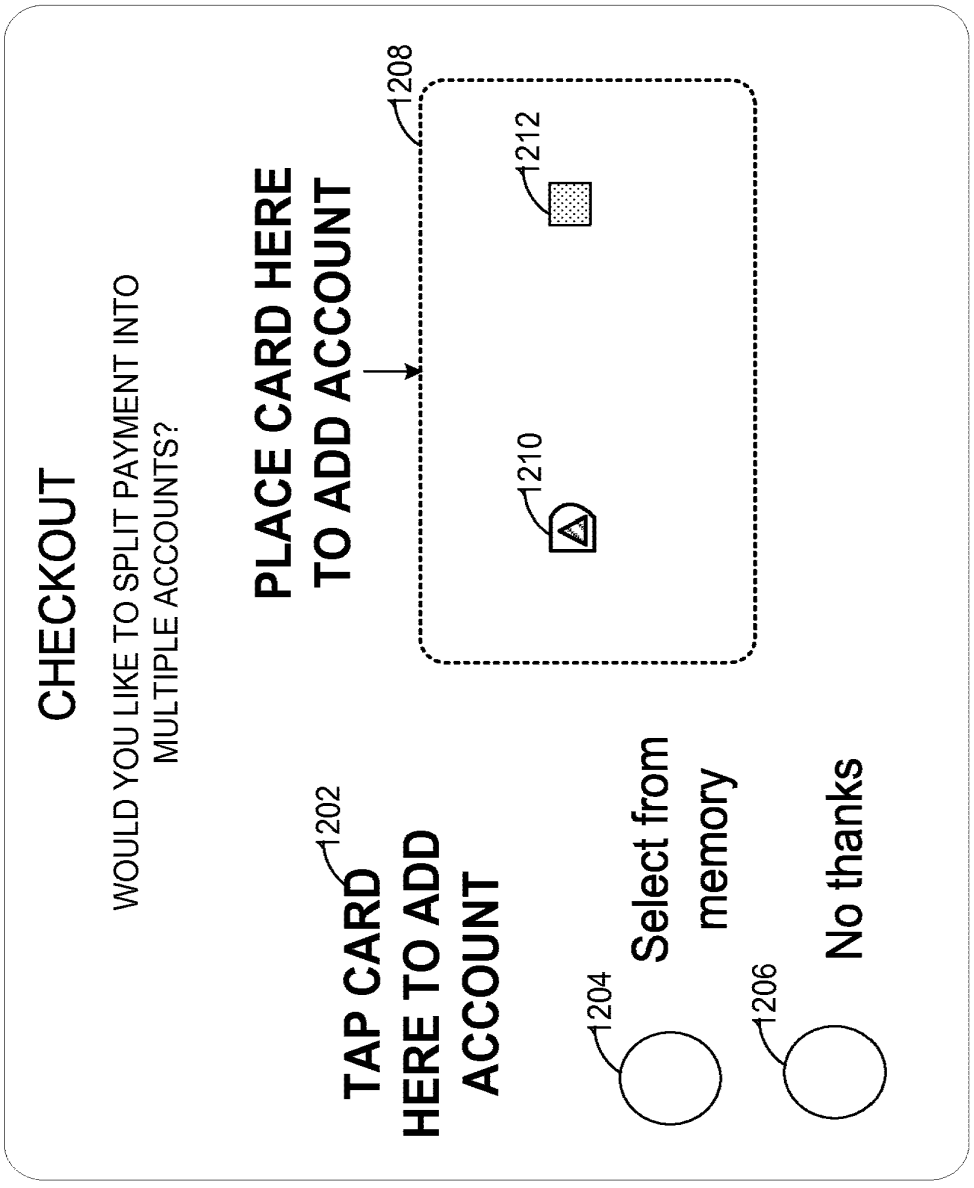

CHECKOUT
WOULD YOU LIKE TO SPLIT PAYMENT INTO MULTIPLE ACCOUNTS?
PLACE CARD HERE TO ADD ACCOUNT
1208
1212
1210
1202
TAP CARD HERE TO ADD ACCOUNT
1204
Select from memory
1206
No thanks

FIG. 12

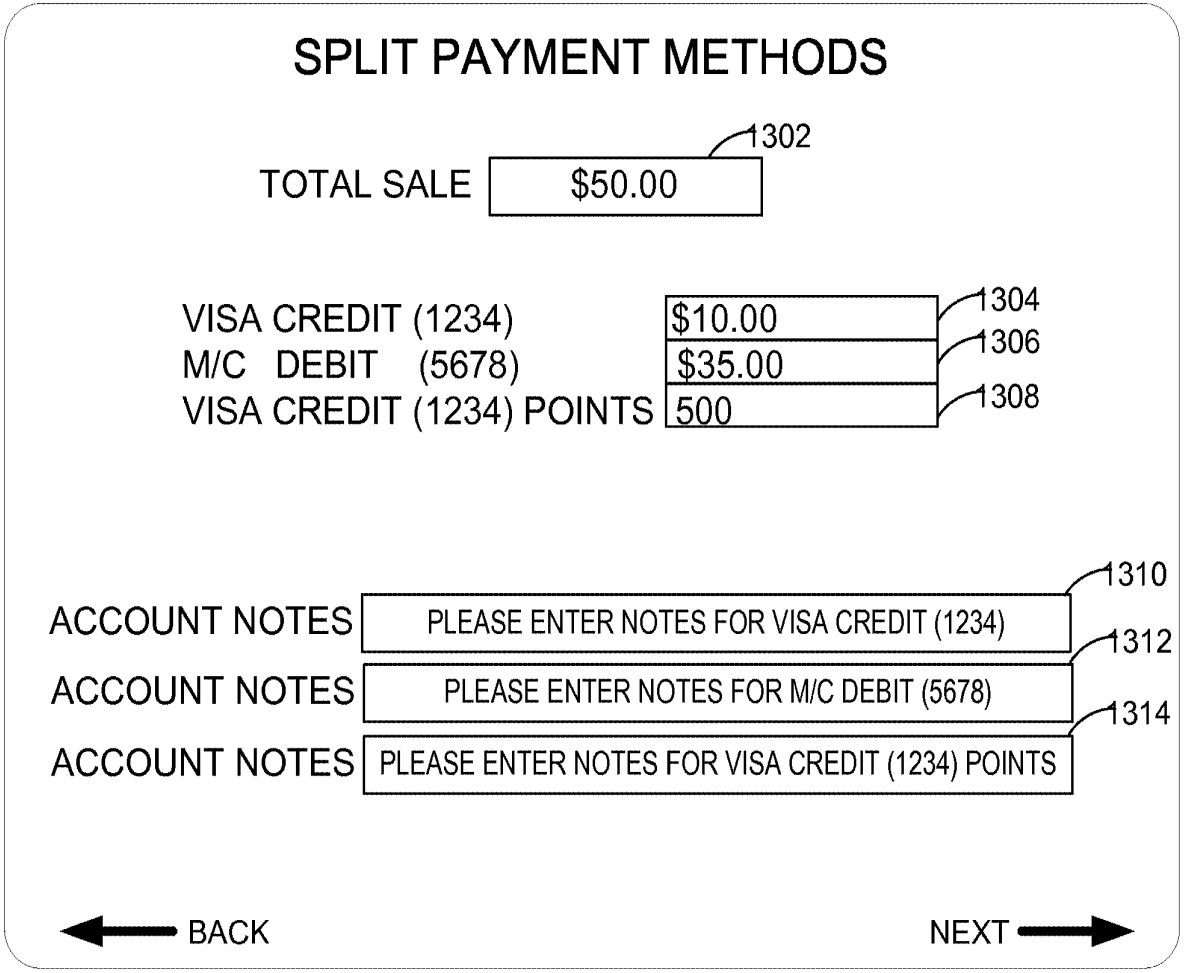
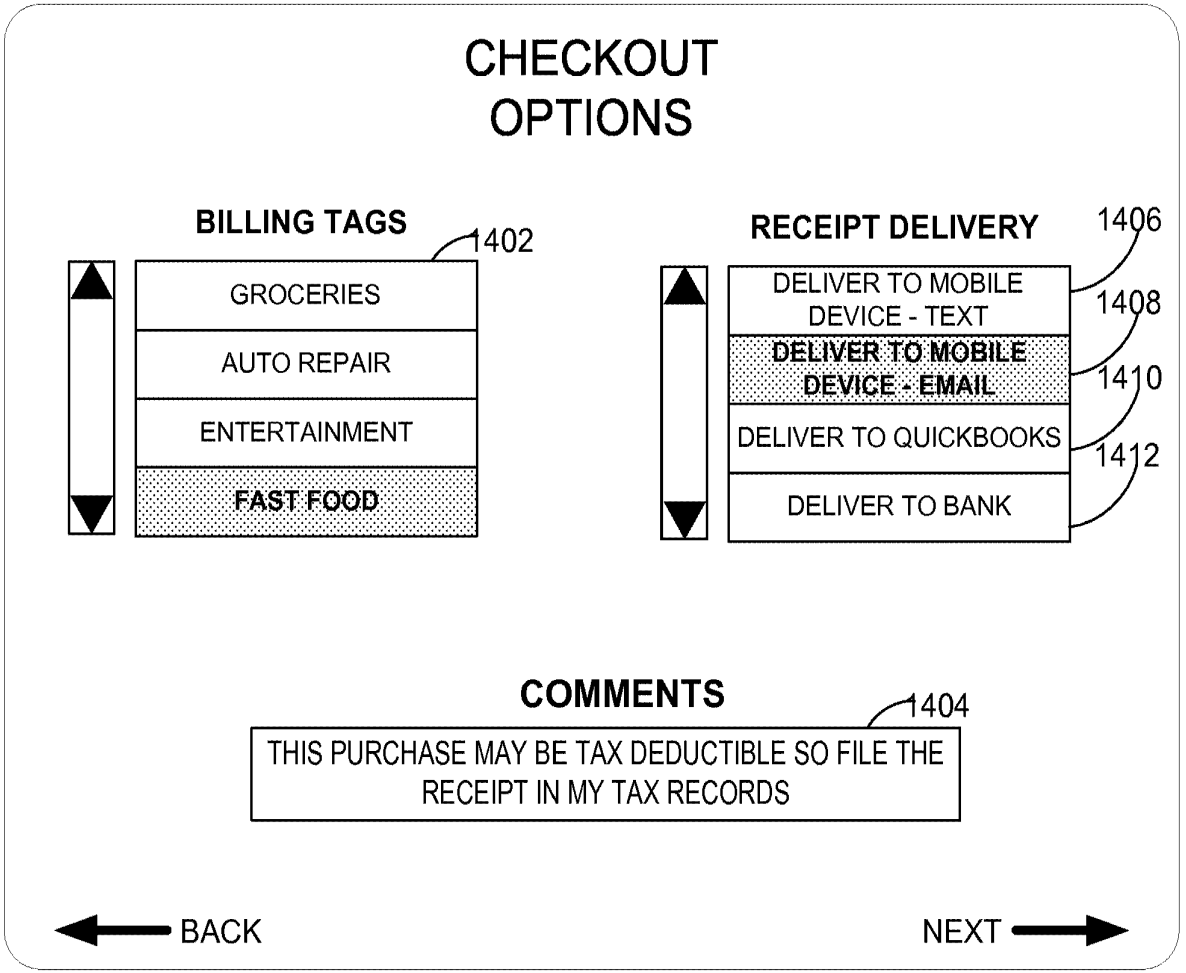

SPLIT PAYMENT METHODS
1302
TOTAL SALE
$50.00
VISA CREDIT (1234)
$10.00
1304
M/C DEBIT (5678)
$35.00
1306
VISA CREDIT (1234) POINTS
500
1308
1310
ACCOUNT NOTES
PLEASE ENTER NOTES FOR VISA CREDIT (1234)
1312
ACCOUNT NOTES
PLEASE ENTER NOTES FOR M/C DEBIT (5678)
1314
ACCOUNT NOTES
PLEASE ENTER NOTES FOR VISA CREDIT (1234) POINTS
BACK
NEXT

FIG. 13



1400

FIG. 14

IPR2025-01152
Apple EX1002 Page 1018

1500

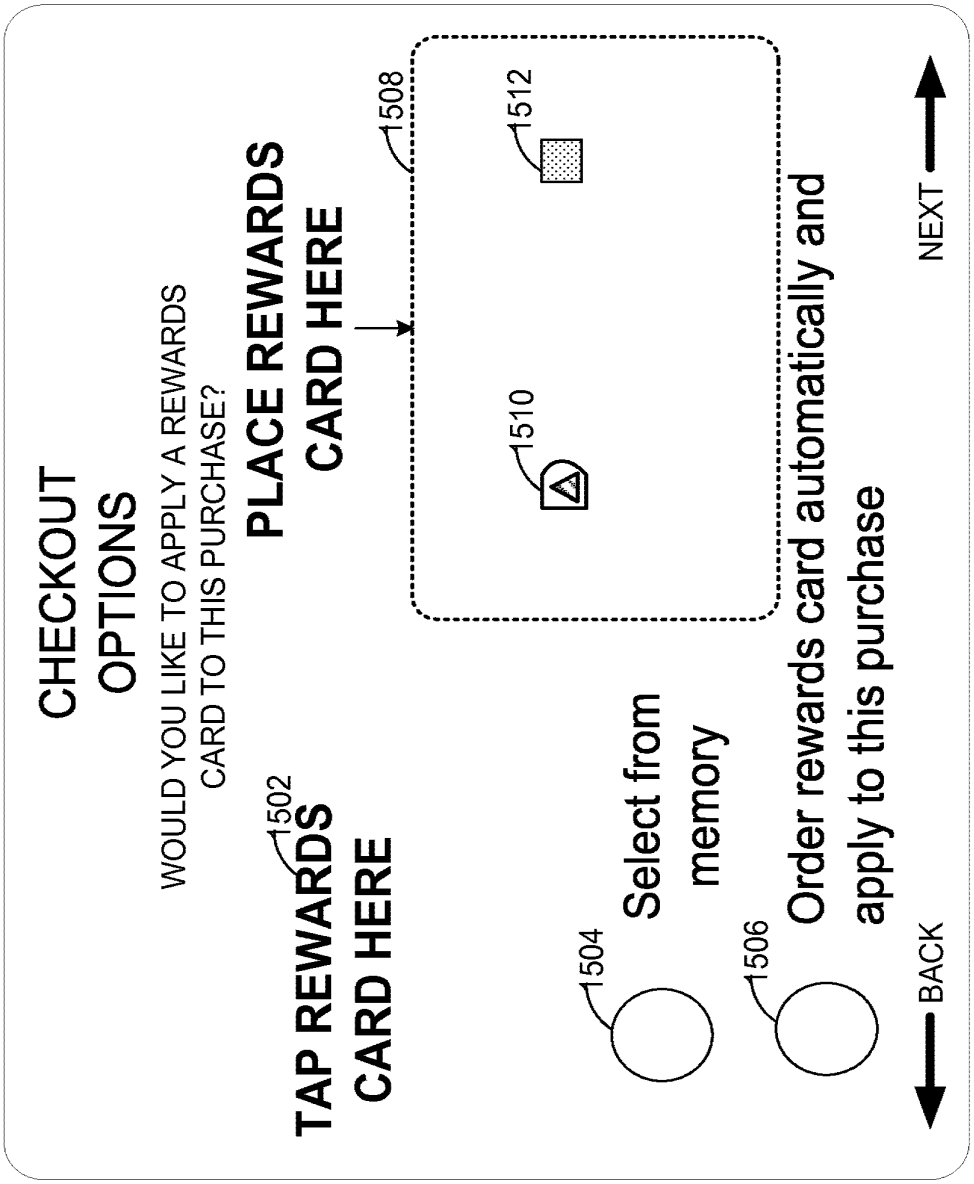


FIG. 15

IPR2025-01152
Apple EX1002 Page 1019

16/73

1600

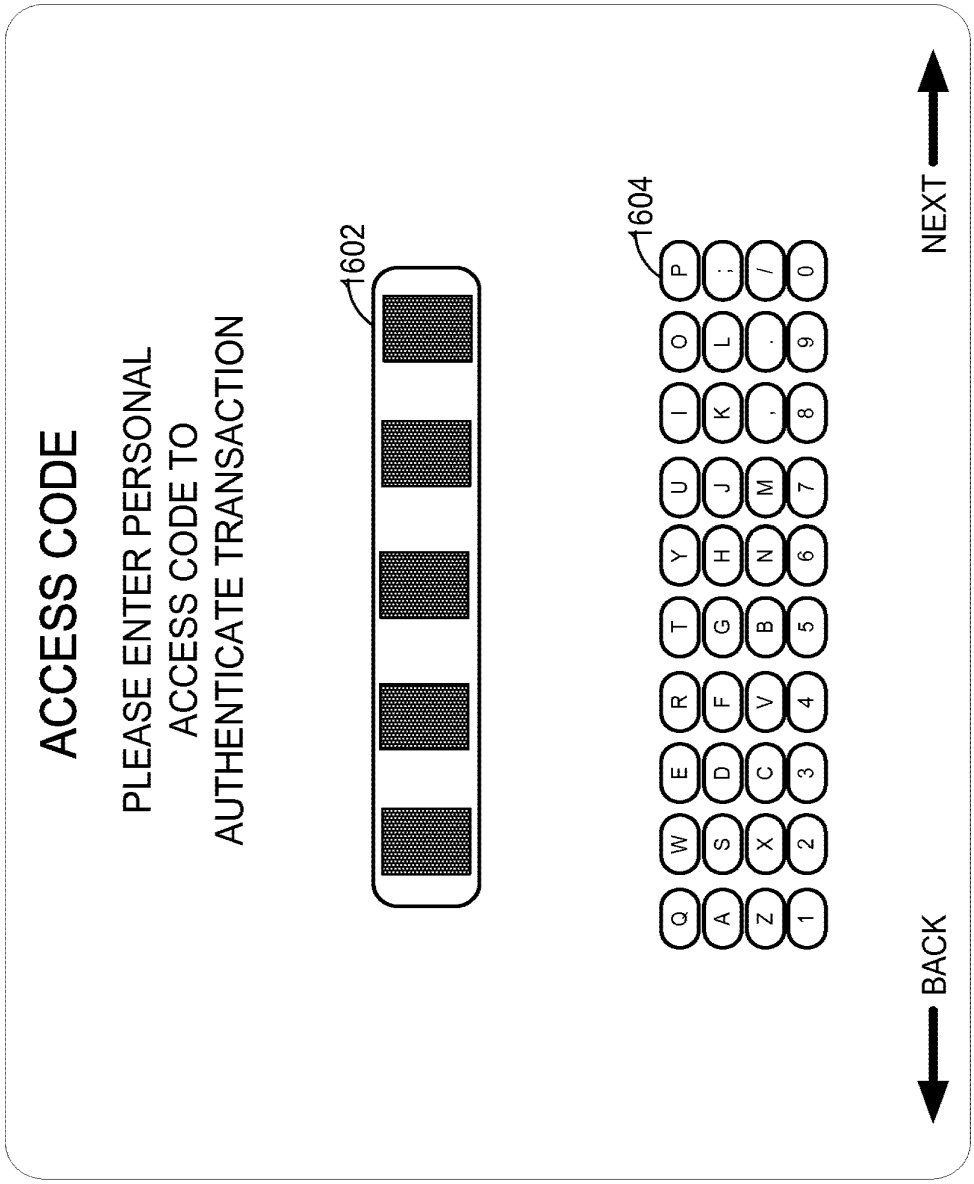


FIG. 16

1700

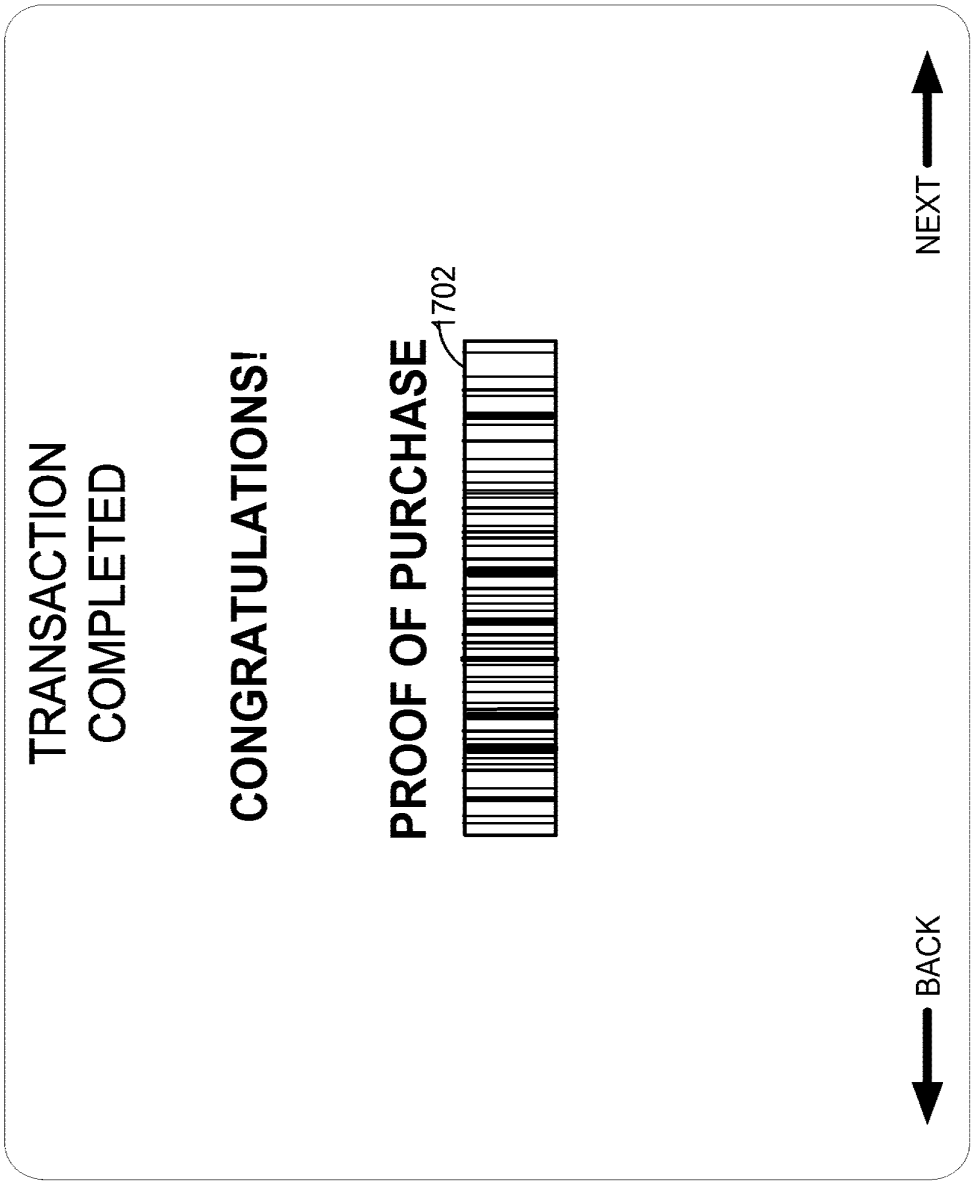

TRANSACTION COMPLETED
CONGRATULATIONS!
PROOF OF PURCHASE
1702
NEXT
BACK

FIG. 17

18/73

1800



FIG. 18

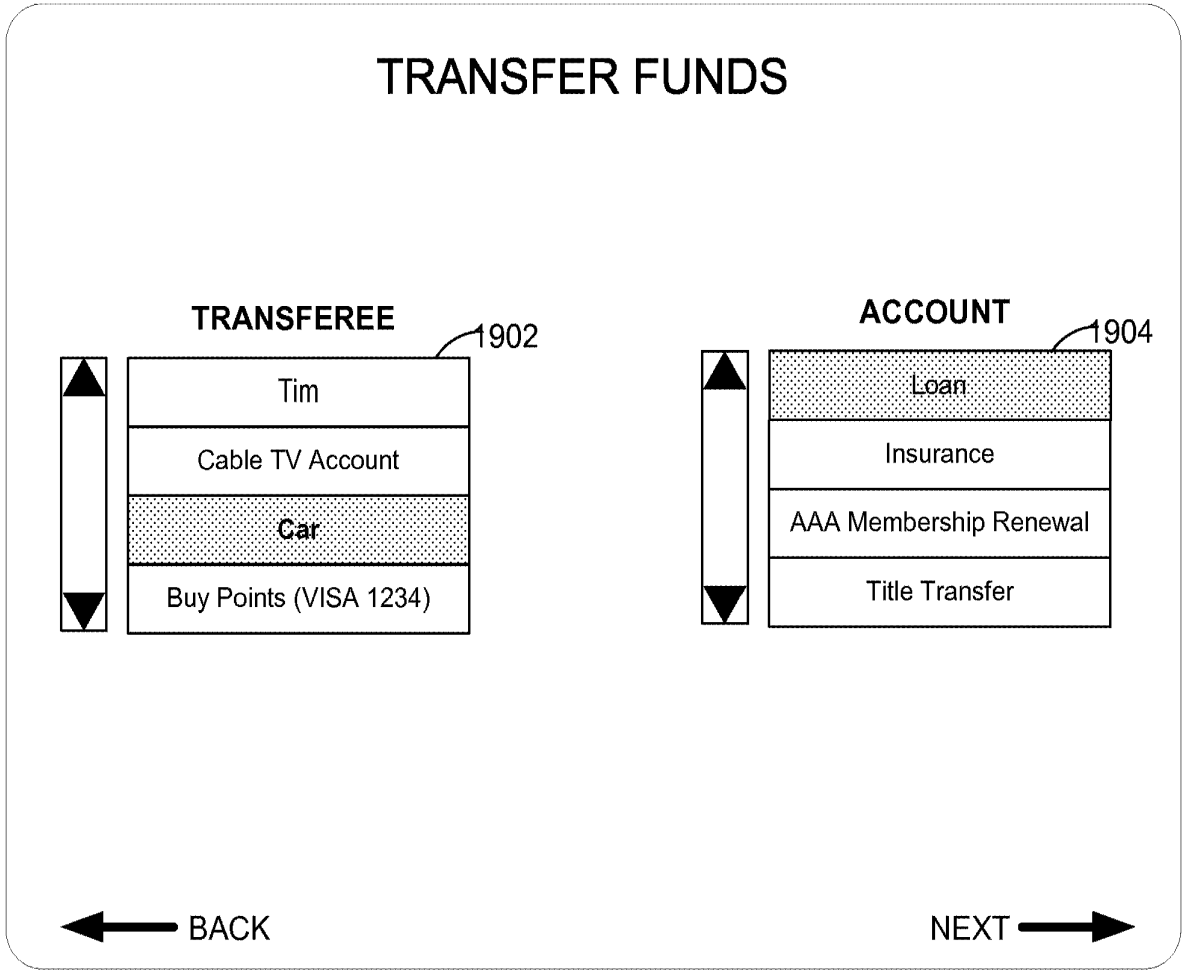


FIG. 19

IPR2025-01152
Apple EX1002 Page 1023

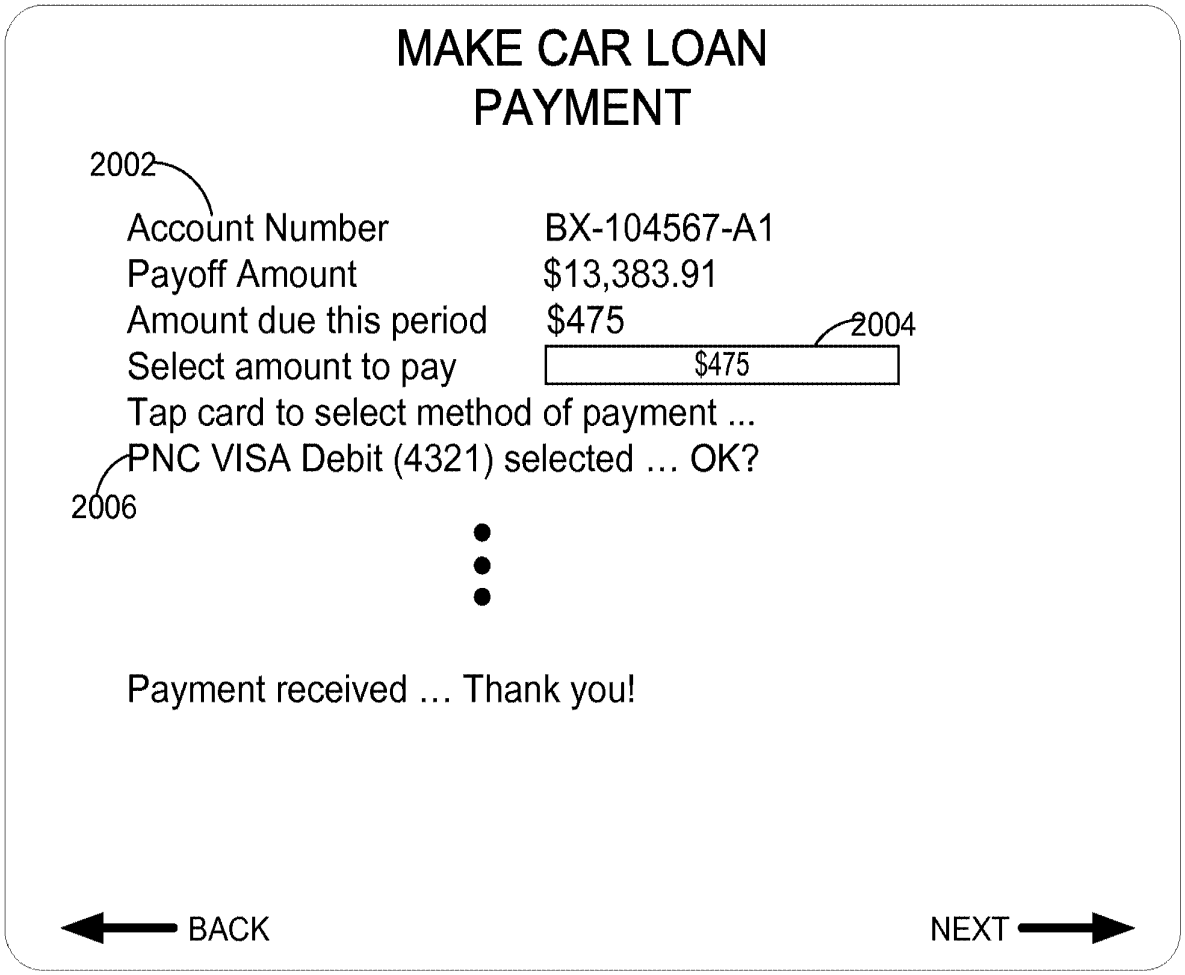

MAKE CAR LOAN PAYMENT
2002
Account Number
BX-104567-A1
Payoff Amount
$13,383.91
Amount due this period
$475
2004
Select amount to pay
$475
Tap card to select method of payment ...
PNC VISA Debit (4321) selected … OK?
2006
Payment received … Thank you!
BACK
NEXT

FIG. 20

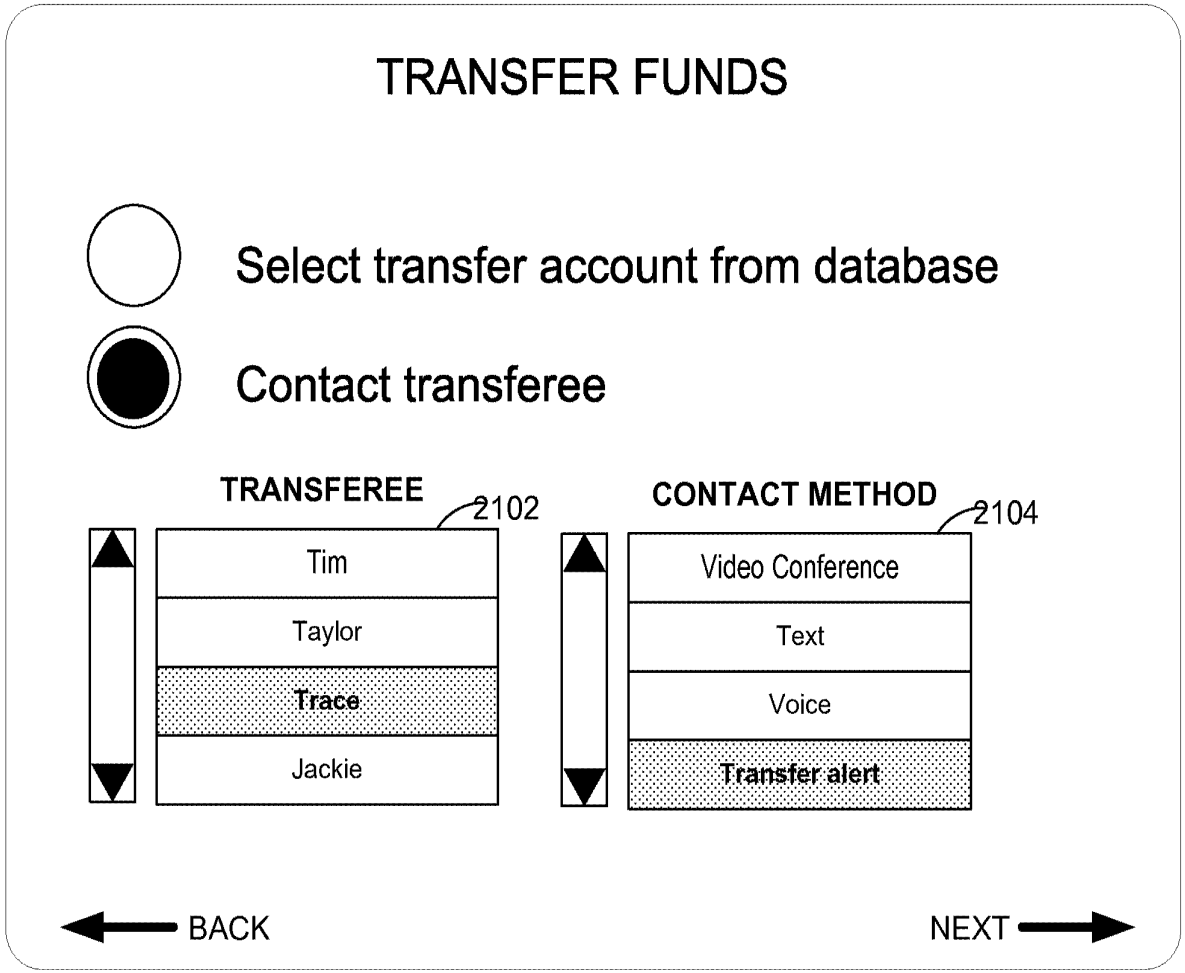
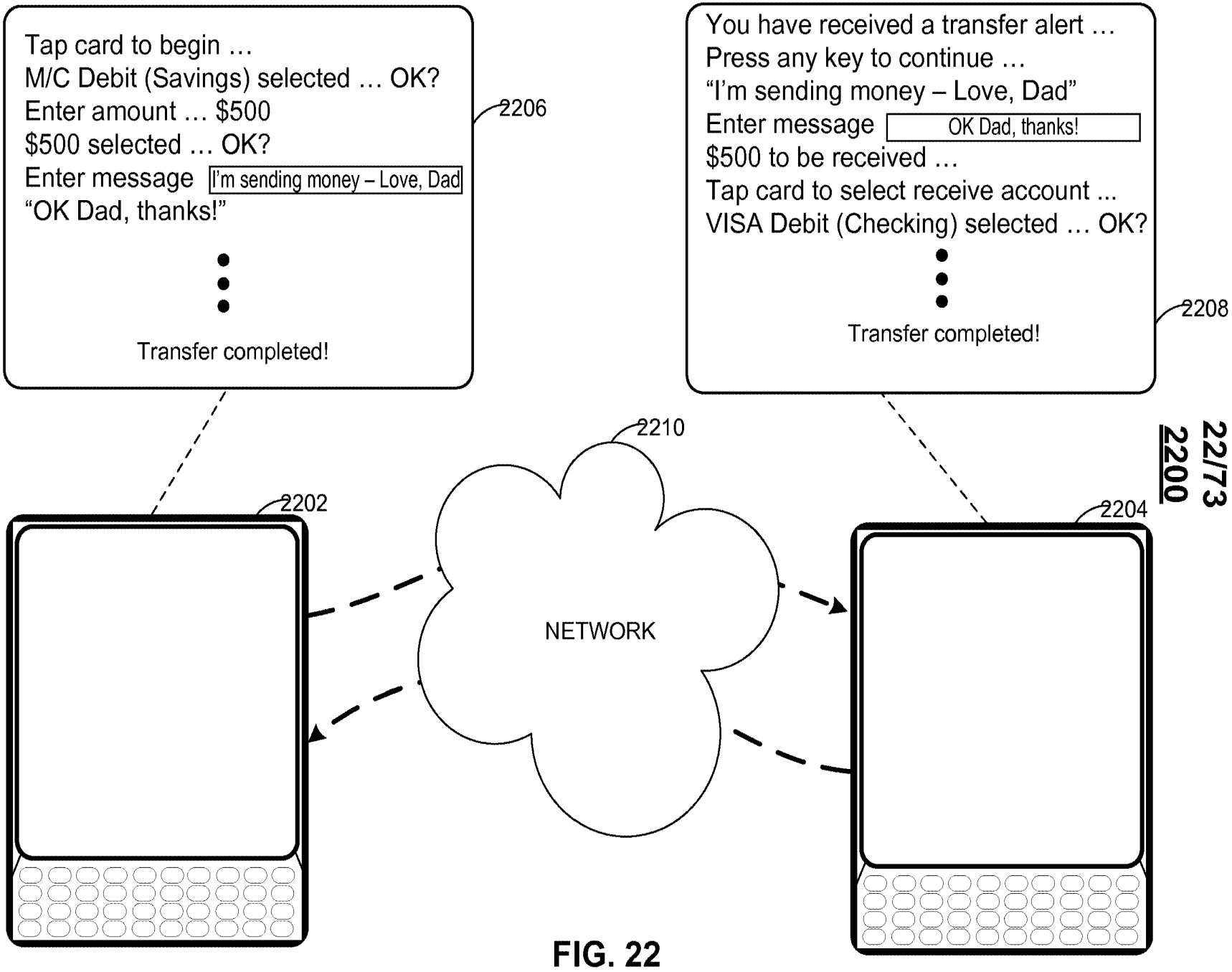

TRANSFER FUNDS
Select transfer account from database
Contact transferee
TRANSFEREE
2102
Tim
Taylor
Trace
Jackie
CONTACT METHOD
2104
Video Conference
Text
Voice
Transfer alert
BACK
NEXT

FIG. 21



22/73

2200

FIG. 22

2300

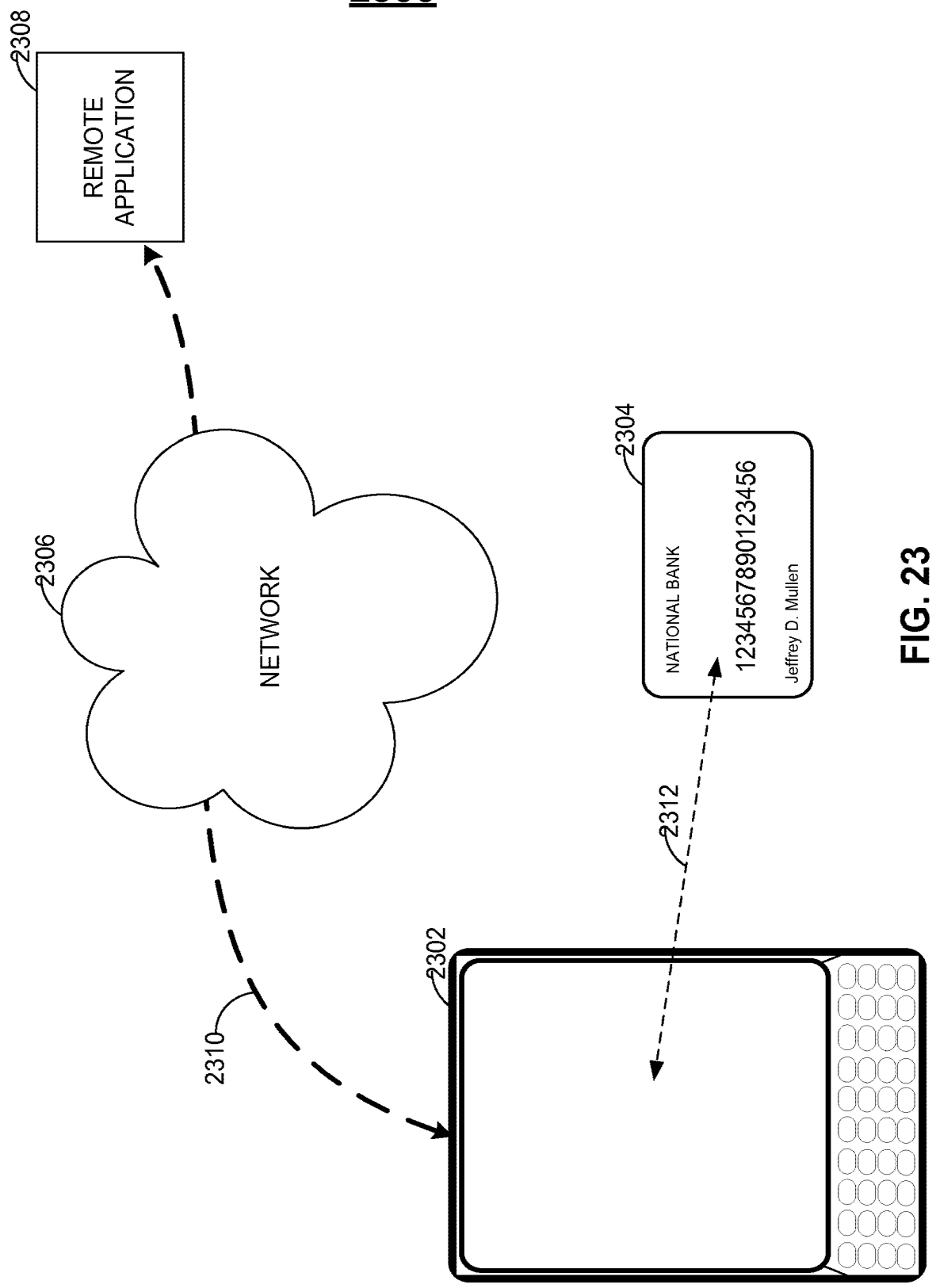

2308
REMOTE APPLICATION
2306
NETWORK
2304
NATIONAL BANK
1234567890123456
Jeffrey D. Mullen
2312
2302
2310

FIG. 23

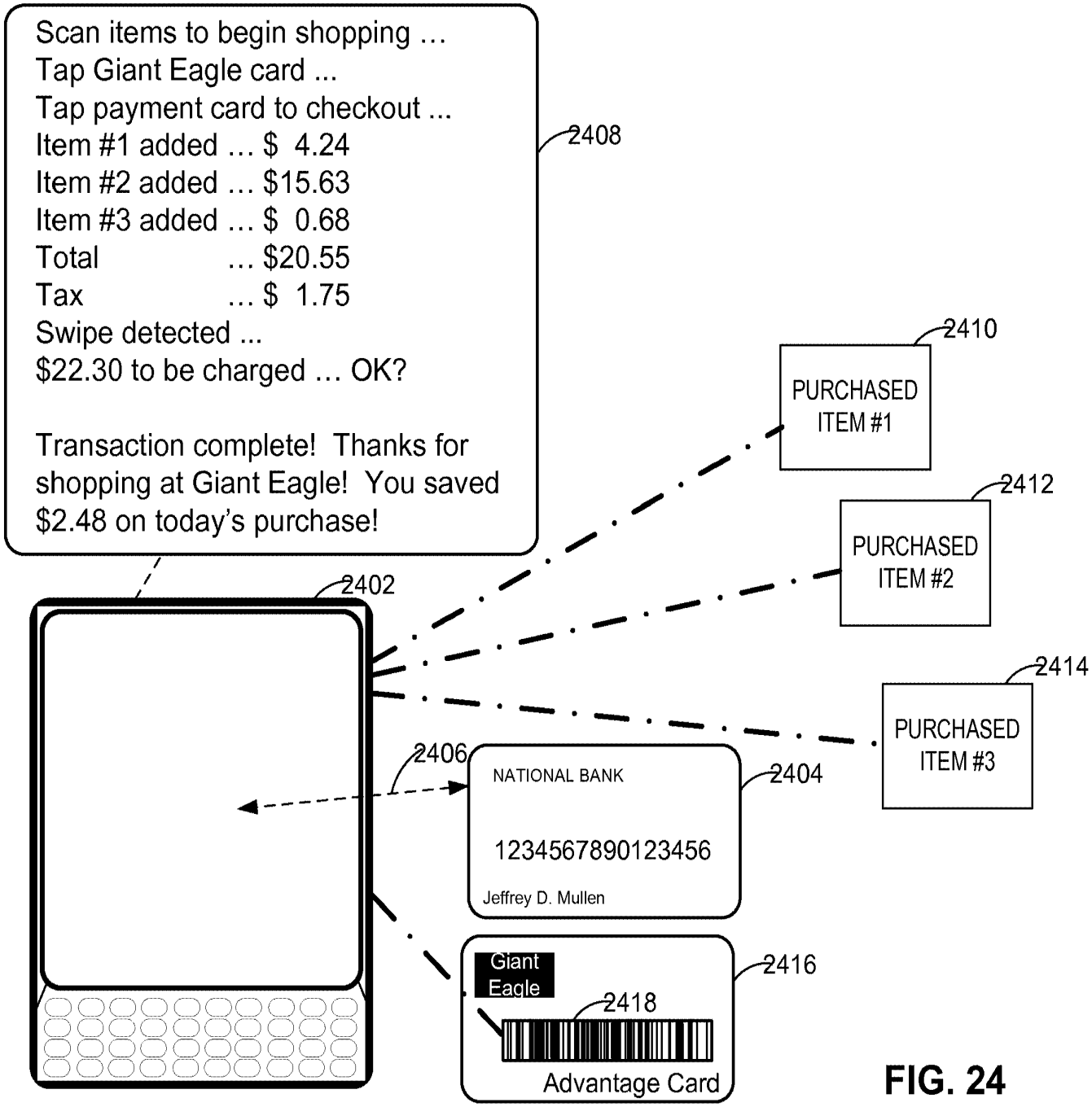

Scan items to begin shopping …
Tap Giant Eagle card ...
Tap payment card to checkout ...
Item #1 added … $ 4.24
Item #2 added … $15.63
Item #3 added … $ 0.68
Total … $20.55
Tax … $ 1.75
Swipe detected ...
$22.30 to be charged … OK?
Transaction complete! Thanks for shopping at Giant Eagle! You saved $2.48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

FIG. 24

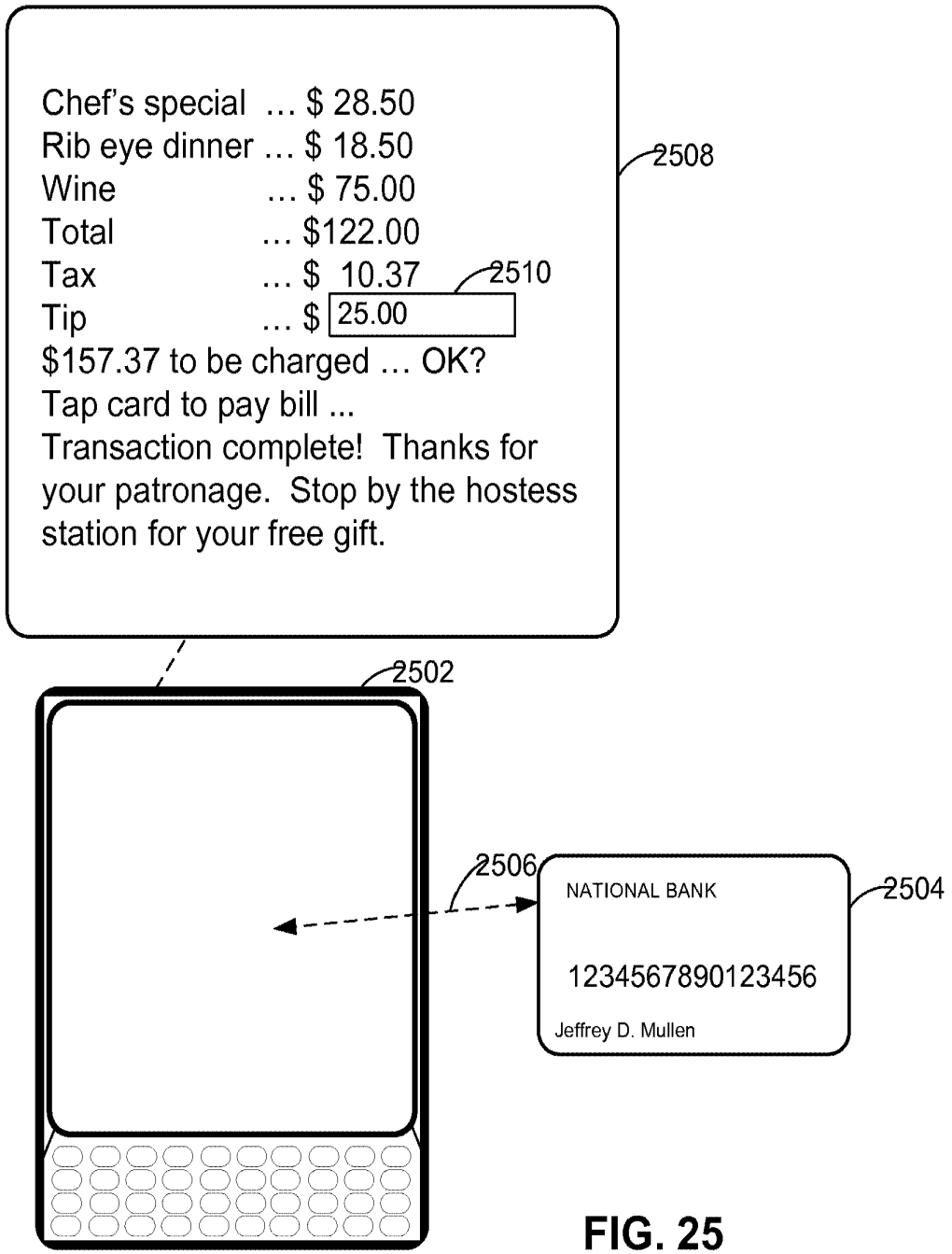

2500
Chef's special ... $ 28.50
Rib eye dinner ... $ 18.50
Wine ... $ 75.00
Total ... $122.00
Tax ... $ 10.37
Tip ... $ 25.00
$157.37 to be charged ... OK?
Tap card to pay bill ...
Transaction complete! Thanks for your patronage. Stop by the hostess station for your free gift.
2508
2510
2502
2506
NATIONAL BANK
1234567890123456
Jeffrey D. Mullen
2504

FIG. 25

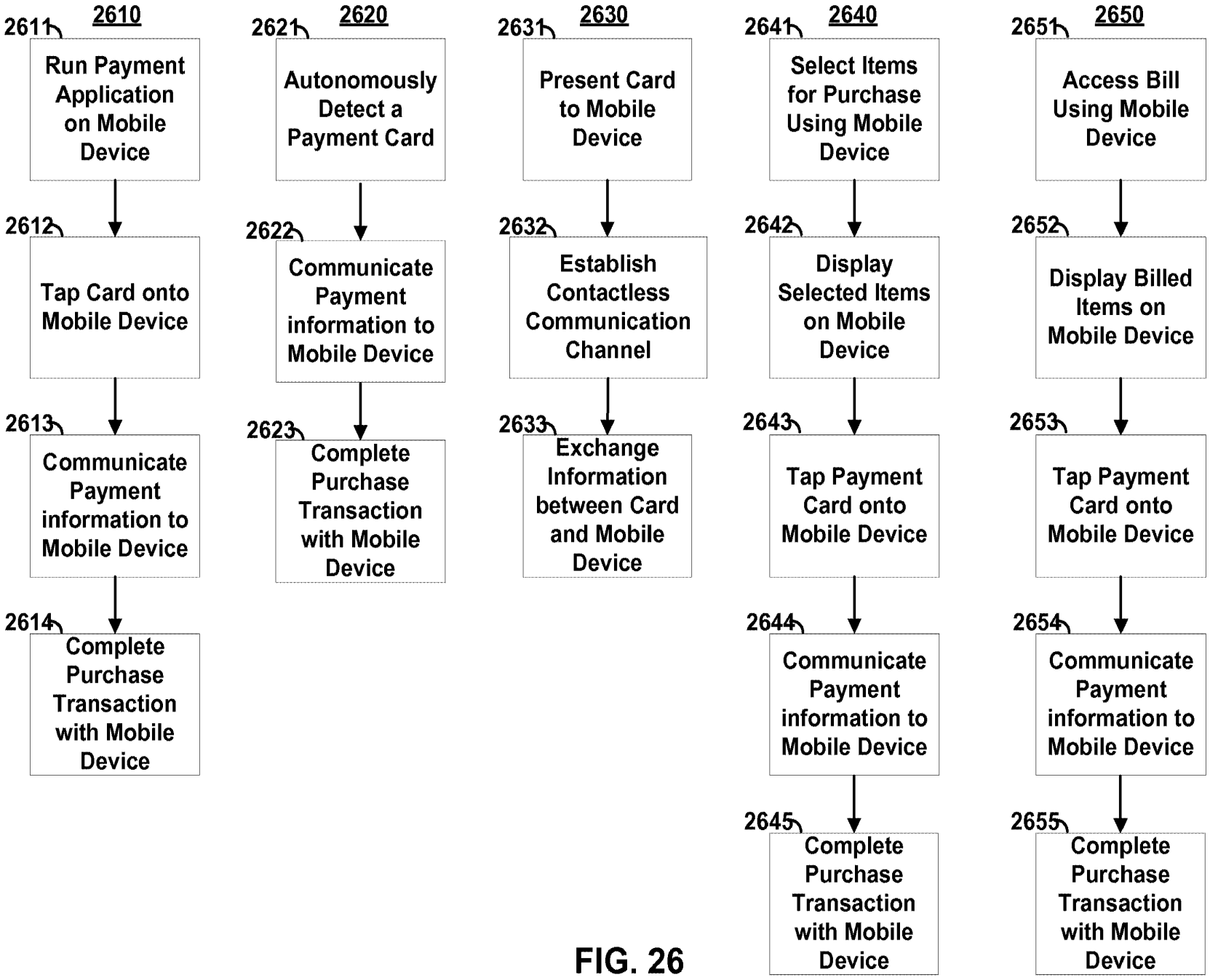


FIG. 26

IPR2025-01152
Apple EX1002 Page 1030

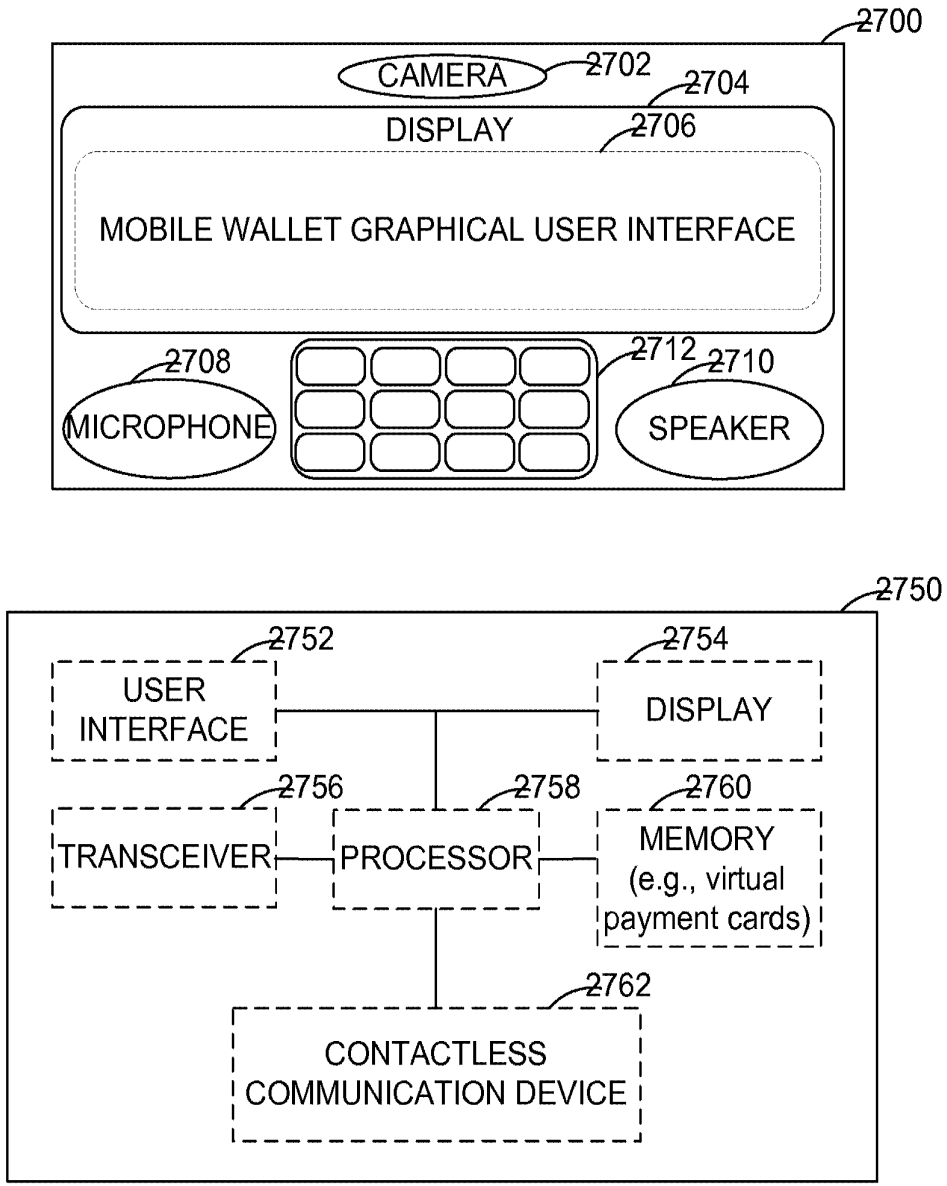


FIG. 27

IPR2025-01152
Apple EX1002 Page 1031

28/73

2800

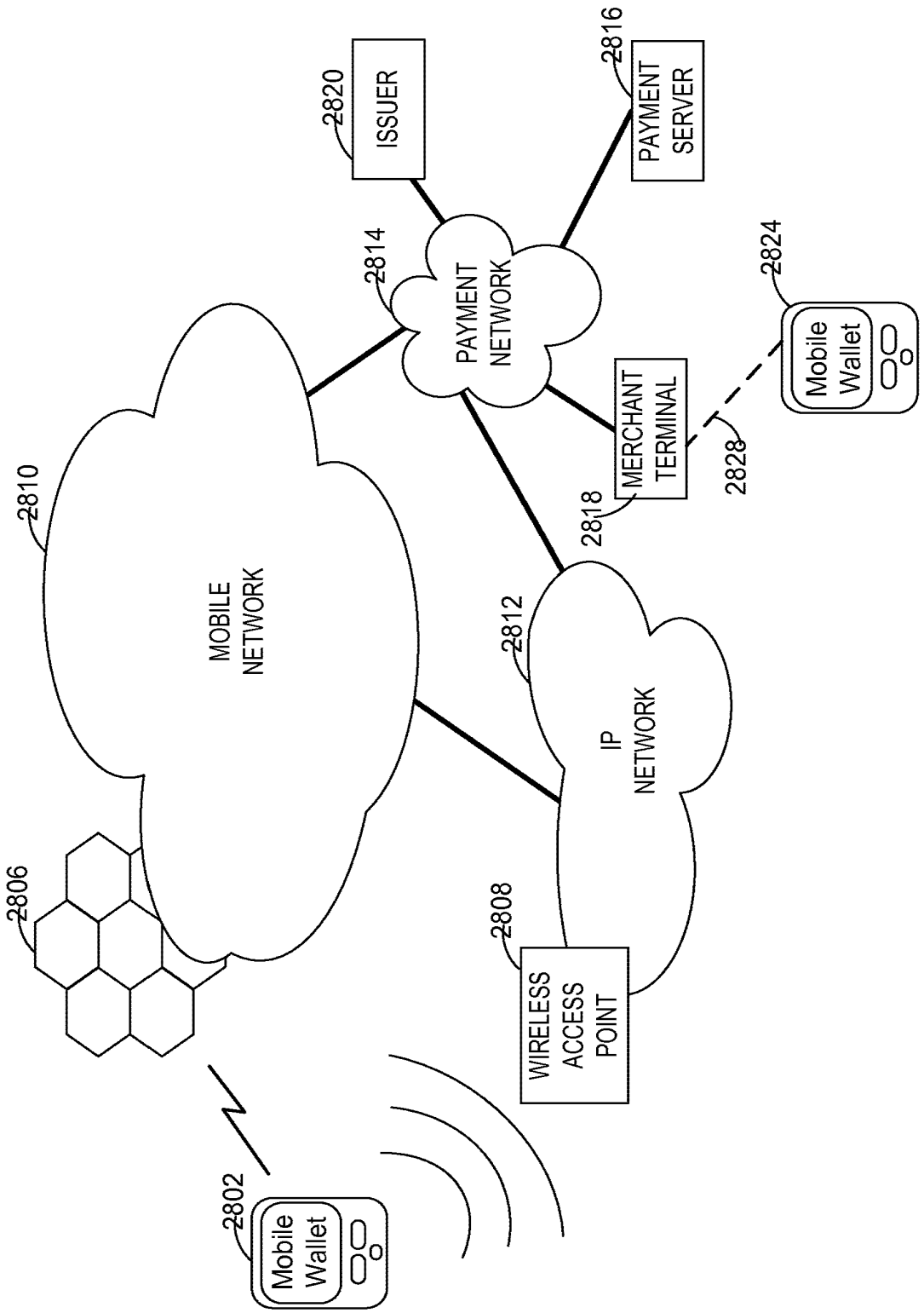


FIG. 28

2900

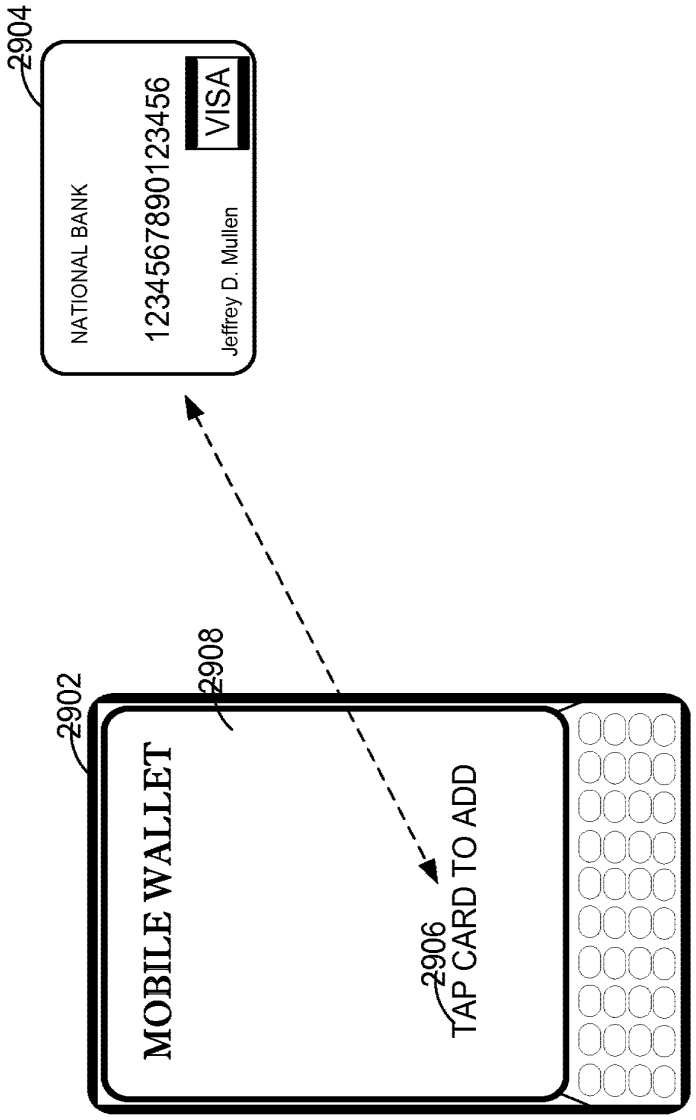

2904
NATIONAL BANK
1234567890123456
VISA
Jeffrey D. Mullen
2902
2908
MOBILE WALLET
2906
TAP CARD TO ADD

FIG. 29

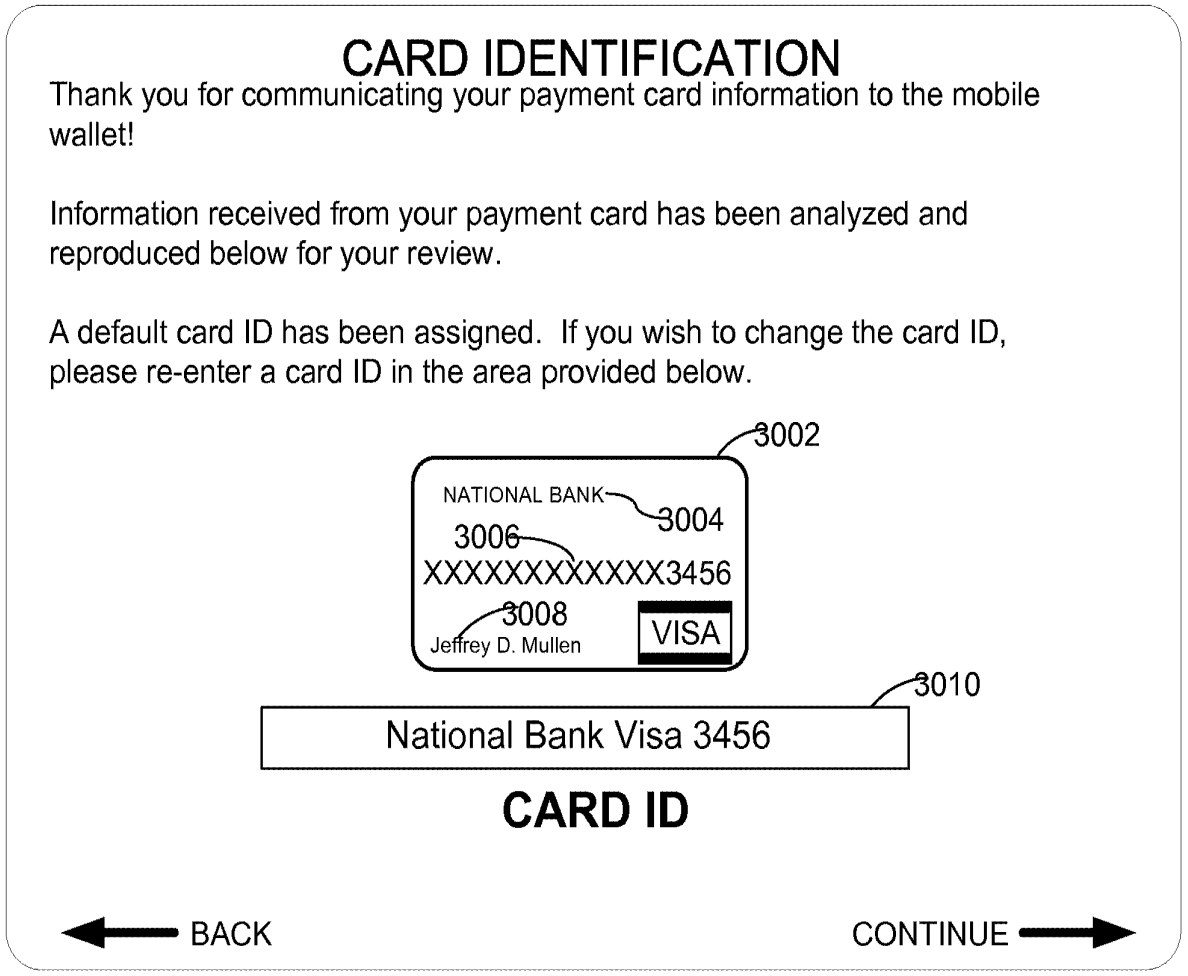

CARD IDENTIFICATION
Thank you for communicating your payment card information to the mobile wallet!
Information received from your payment card has been analyzed and reproduced below for your review.
A default card ID has been assigned. If you wish to change the card ID, please re-enter a card ID in 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

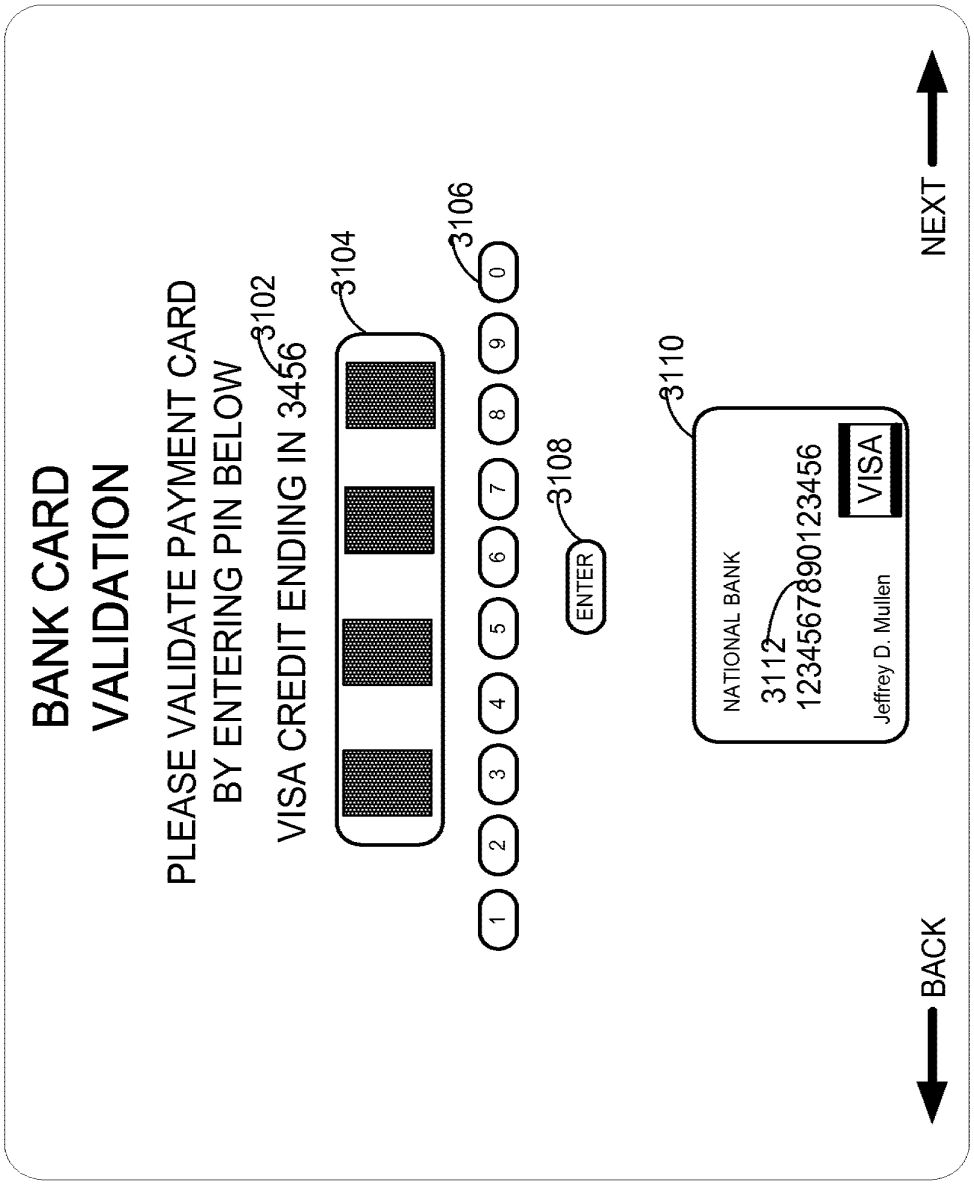

BANK CARD
VALIDATION
PLEASE VALIDATE PAYMENT CARD
BY ENTERING PIN BELOW
VISA CREDIT ENDING IN 3456
3102
3104
3106
1
2
3
4
5
6
7
8
9
0
ENTER
3108
3110
NATIONAL BANK
3112
1234567890123456
Jeffrey D. Mullen
VISA
NEXT
BACK

FIG. 31

3200

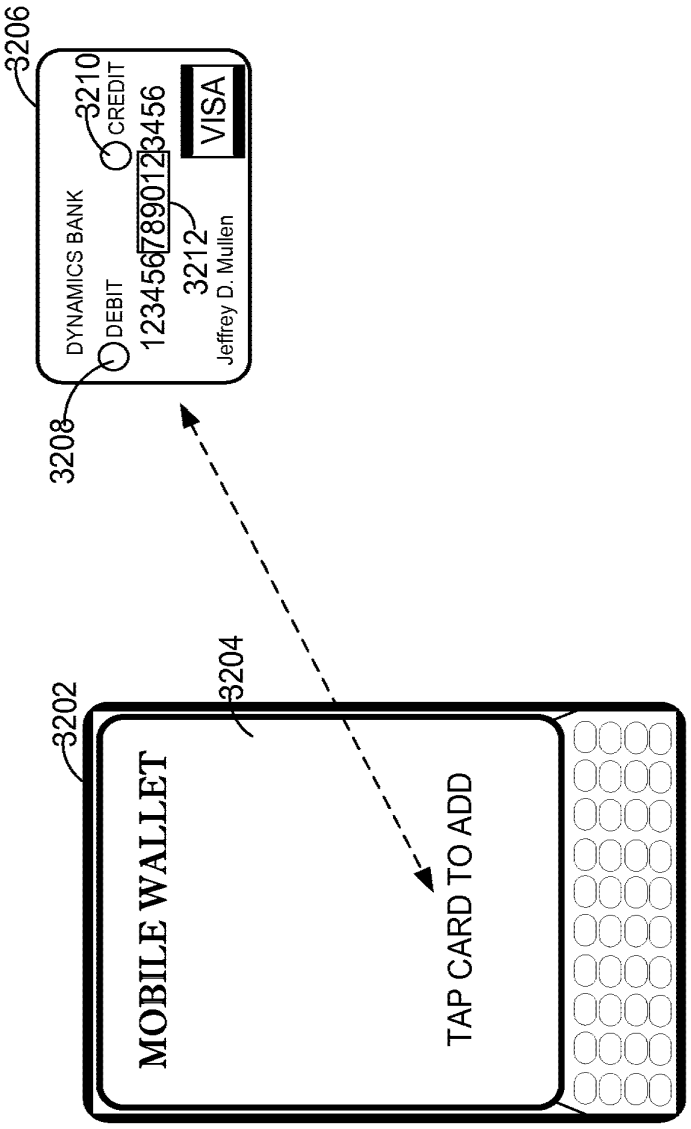

3206
3210
CREDIT
3456
VISA
DYNAMICS BANK
DEBIT
123456789012
3212
Jeffrey D. Mullen
3208
3204
3202
MOBILE WALLET
TAP CARD TO ADD

FIG. 32

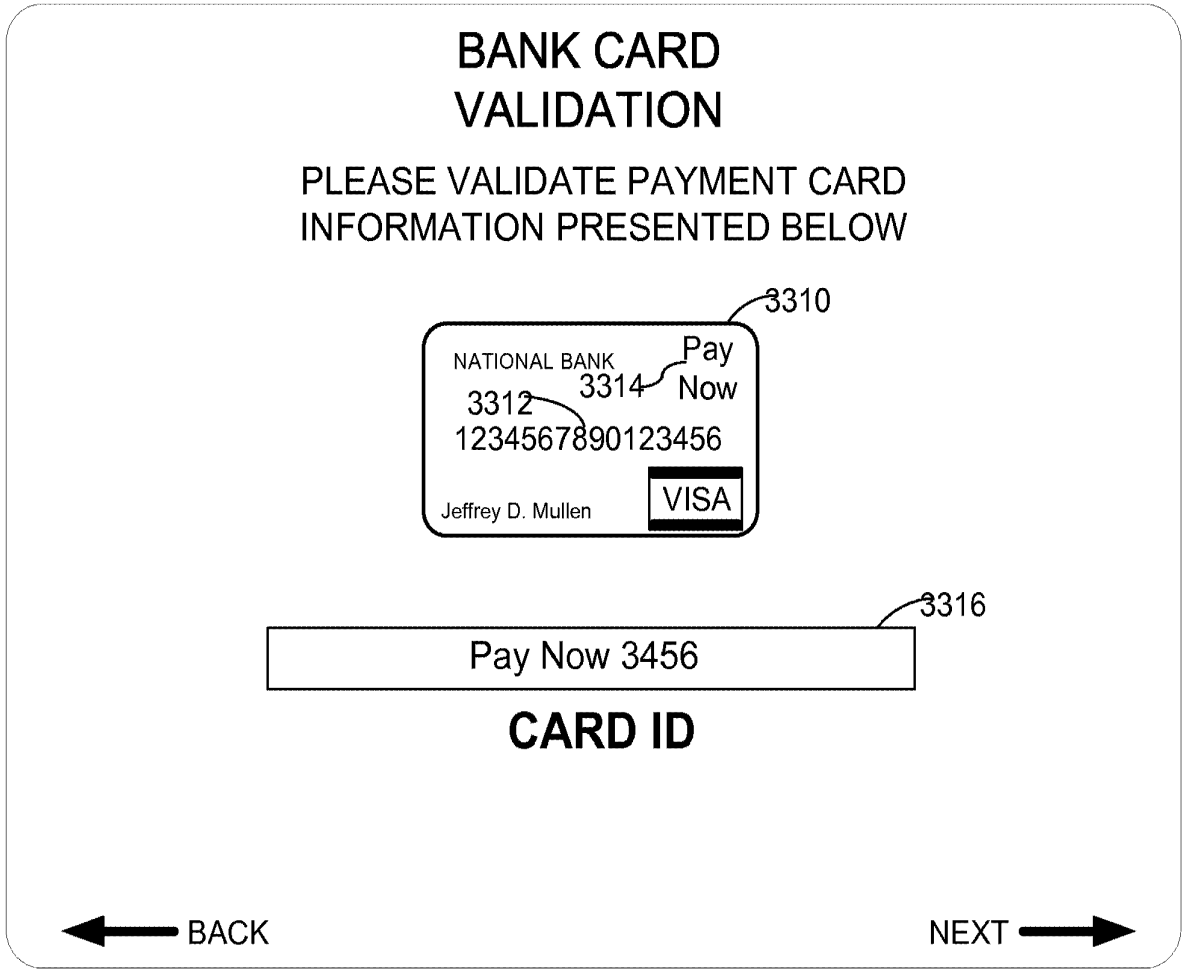

BANK CARD
VALIDATION
PLEASE VALIDATE PAYMENT CARD
INFORMATION PRESENTED BELOW
3310
NATIONAL BANK
Pay
Now
3314
3312
1234567890123456
Jeffrey D. Mullen
VISA
3316
Pay Now 3456
CARD ID
BACK
NEXT

FIG. 33

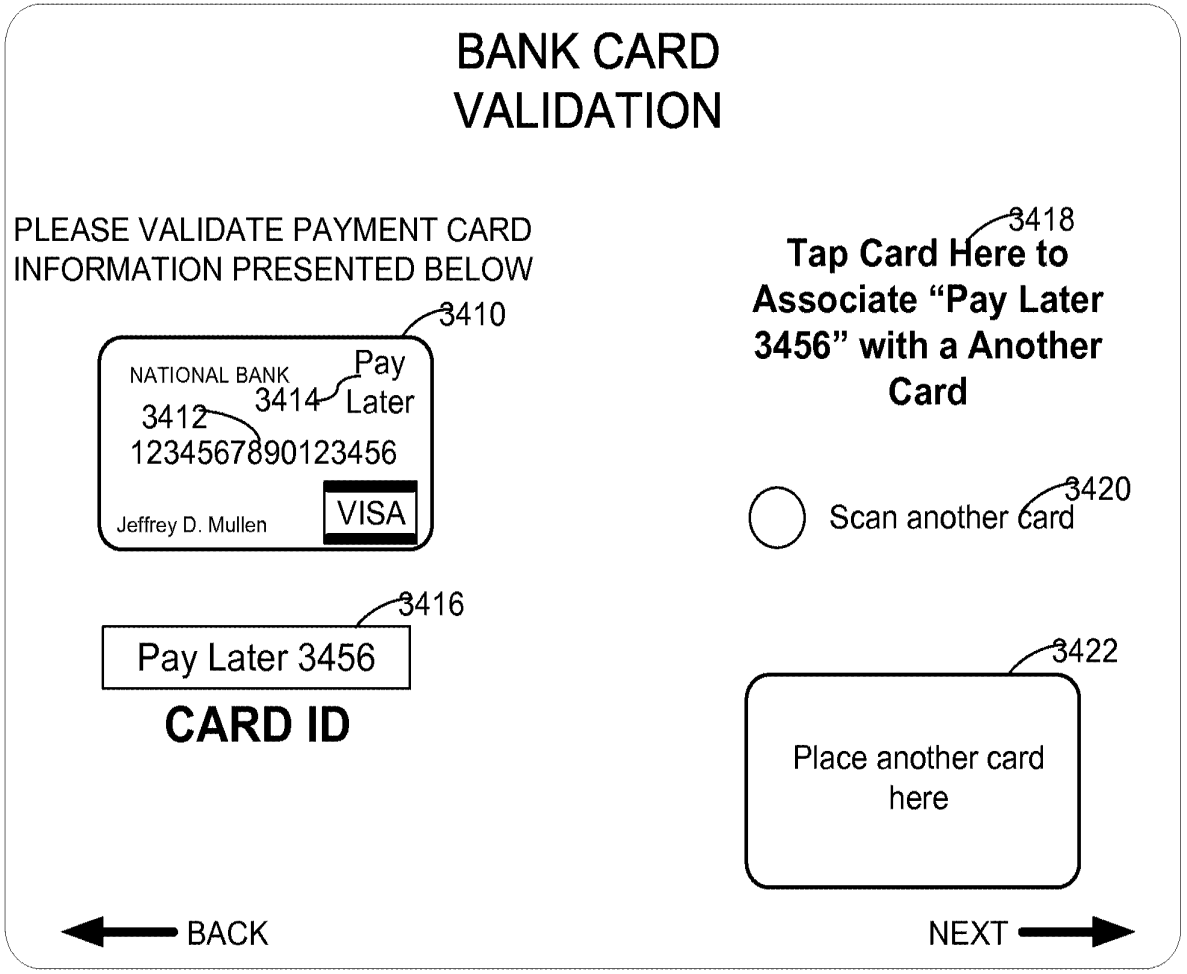

BANK CARD VALIDATION
PLEASE VALIDATE PAYMENT CARD INFORMATION PRESENTED BELOW
3410
NATIONAL BANK
Pay Later
3414
3412
1234567890123456
Jeffrey D. Mullen
VISA
3416
Pay Later 3456
CARD ID
3418
Tap Card Here to Associate "Pay Later 3456" with a Another Card
Scan another card
3420
3422
Place another card here
BACK
NEXT

FIG. 34

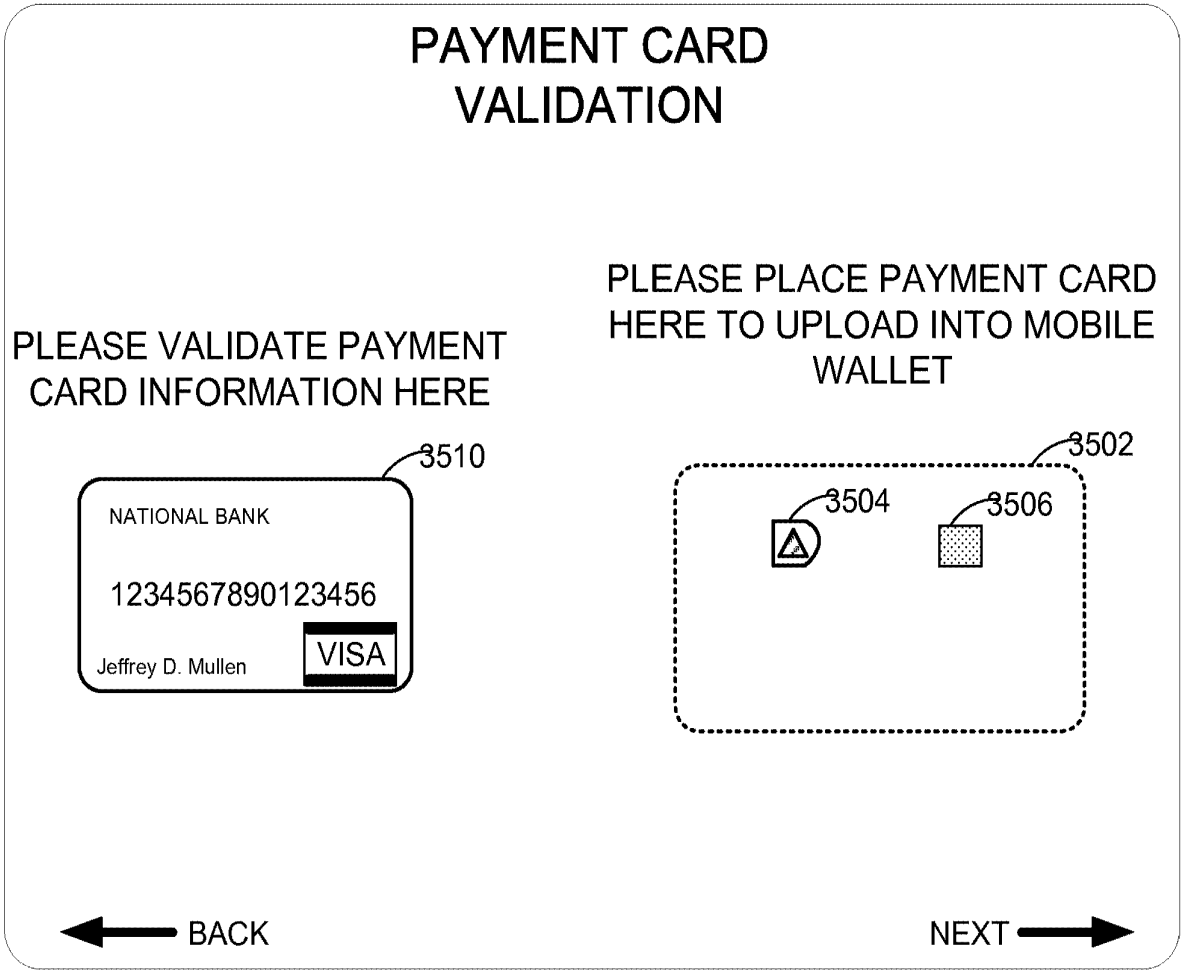


FIG. 35

IPR2025-01152
Apple EX1002 Page 1039

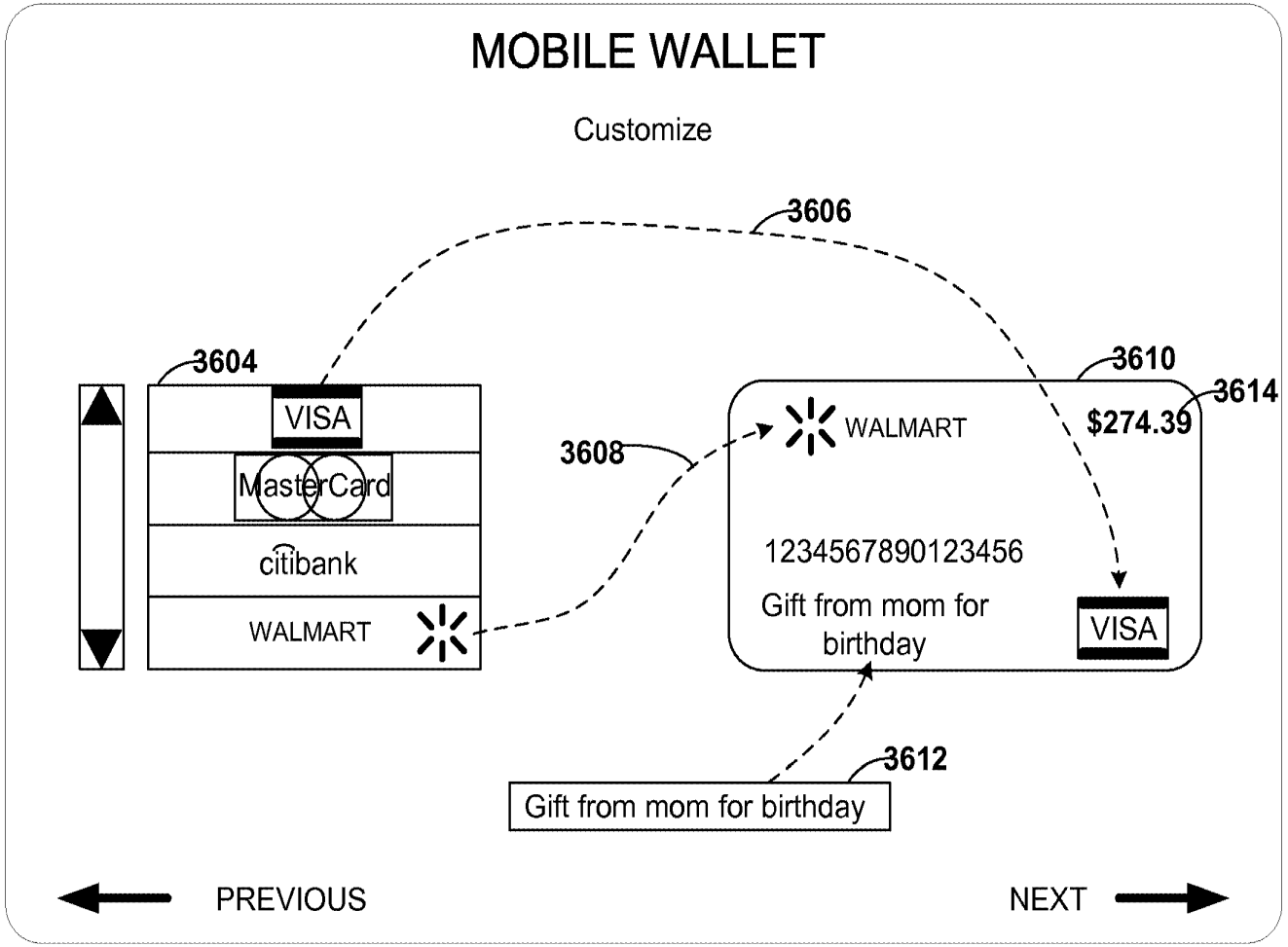


FIG. 36

IPR2025-01152
Apple EX1002 Page 1040

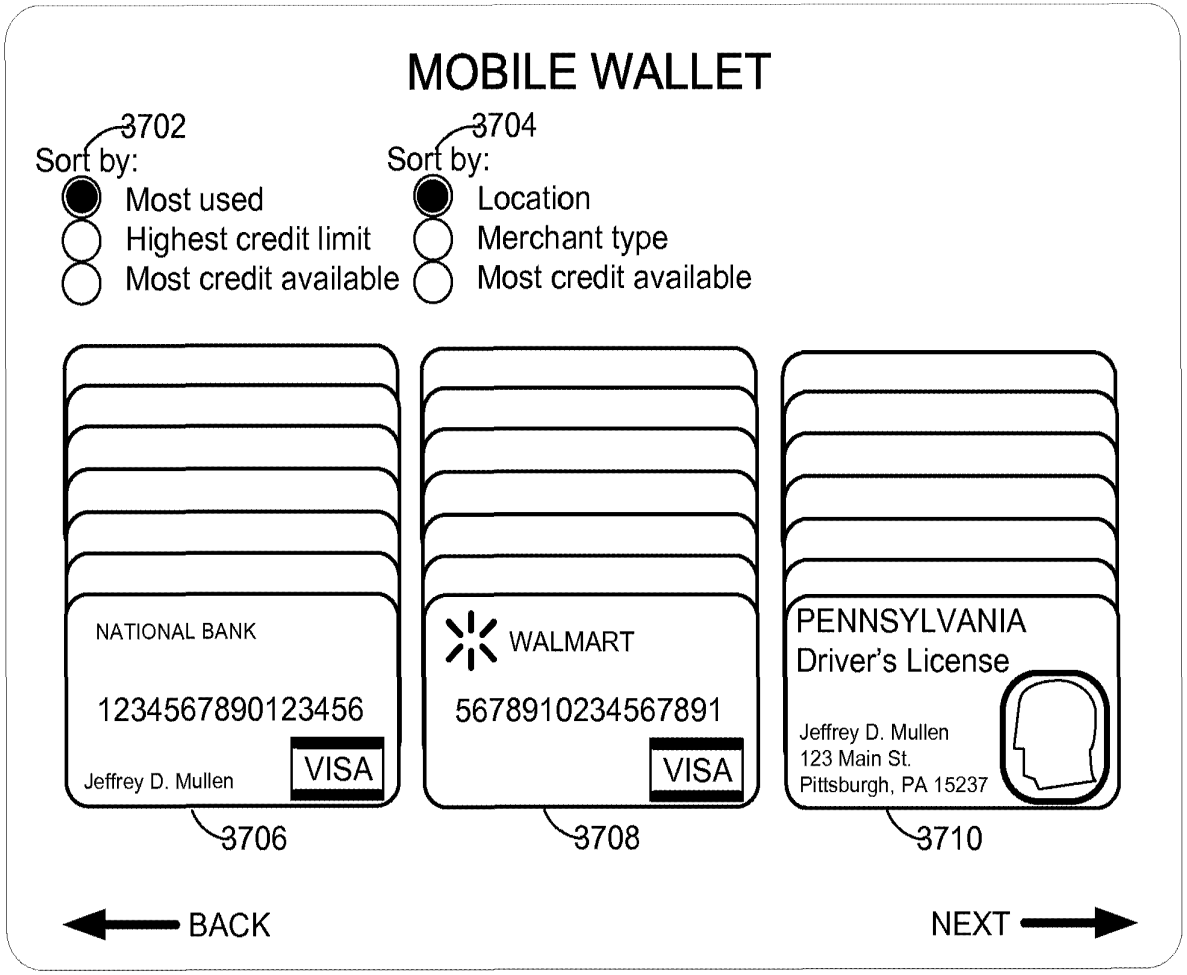

MOBILE WALLET
3702
Sort by:
Most used
Highest credit limit
Most credit available
3704
Sort by:
Location
Merchant type
Most credit available
NATIONAL BANK
1234567890123456
Jeffrey D. Mullen
VISA
3706
WALMART
5678910234567891
VISA
3708
PENNSYLVANIA
Driver's License
Jeffrey D. Mullen
123 Main St.
Pittsburgh, PA 15237
3710
BACK
NEXT

FIG. 37

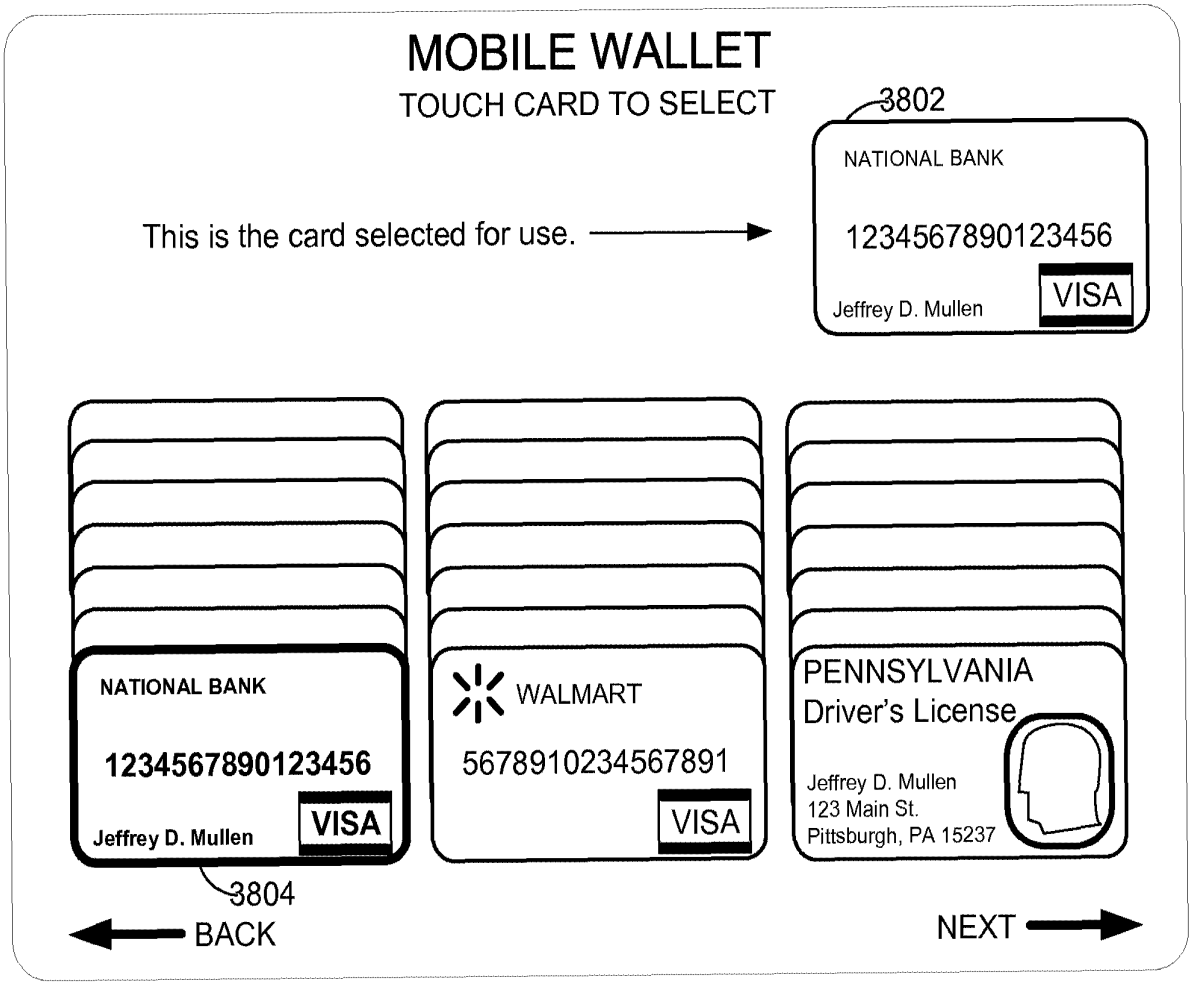

MOBILE WALLET
TOUCH CARD TO SELECT
3802
NATIONAL BANK
This is the card selected for use.
1234567890123456
Jeffrey D. Mullen
VISA
NATIONAL BANK
1234567890123456
Jeffrey D. Mullen
VISA
3804
WALMART
5678910234567891
VISA
PENNSYLVANIA
Driver's License
Jeffrey D. Mullen
123 Main St.
Pittsburgh, PA 15237
BACK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

FIG. 38

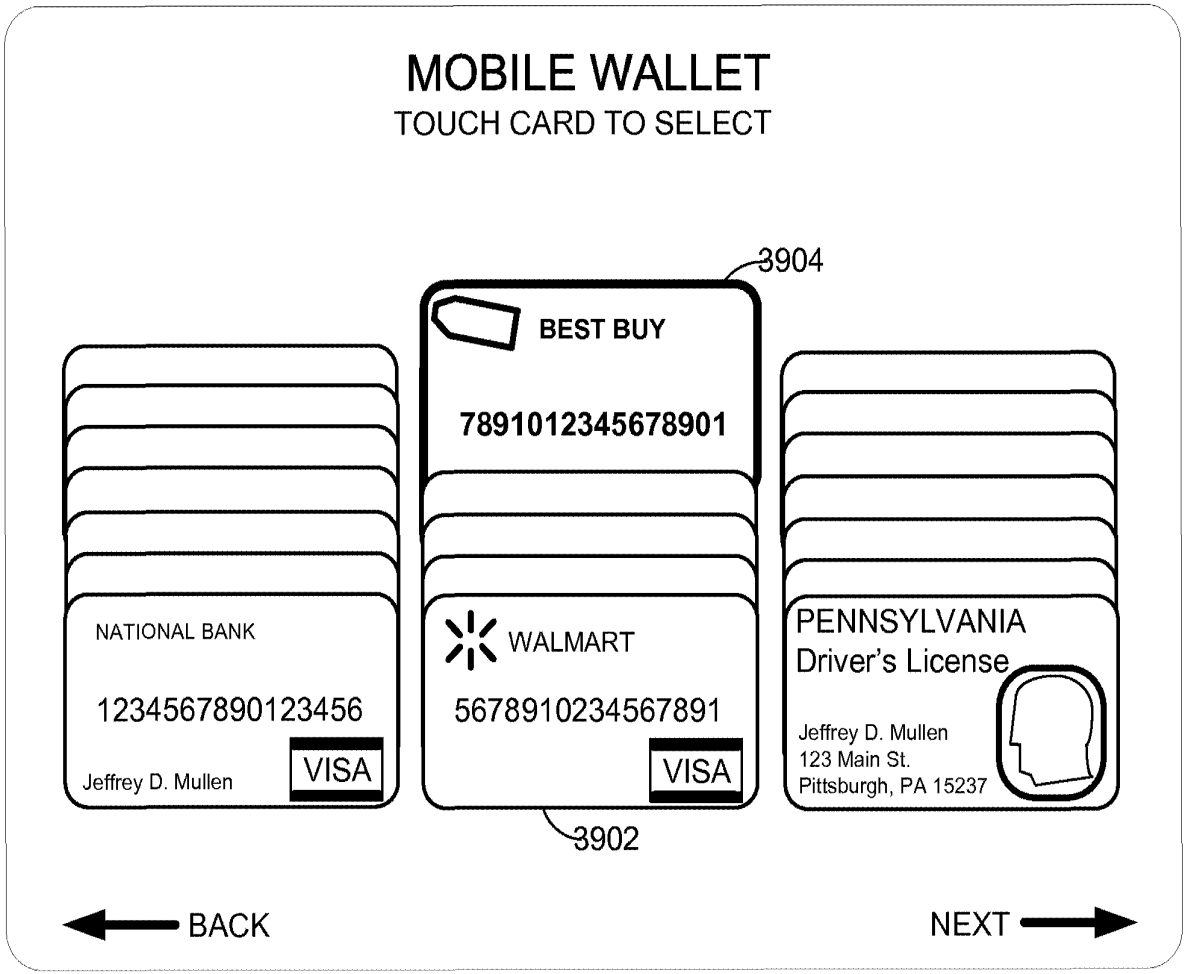

MOBILE WALLET
TOUCH CARD TO SELECT
3904
BEST BUY
7891012345678901
NATIONAL BANK
1234567890123456
Jeffrey D. Mullen
VISA
WALMART
5678910234567891
VISA
PENNSYLVANIA
Driver's License
Jeffrey D. Mullen
123 Main St.
Pittsburgh, PA 15237
3902
BACK
NEXT

FIG. 39

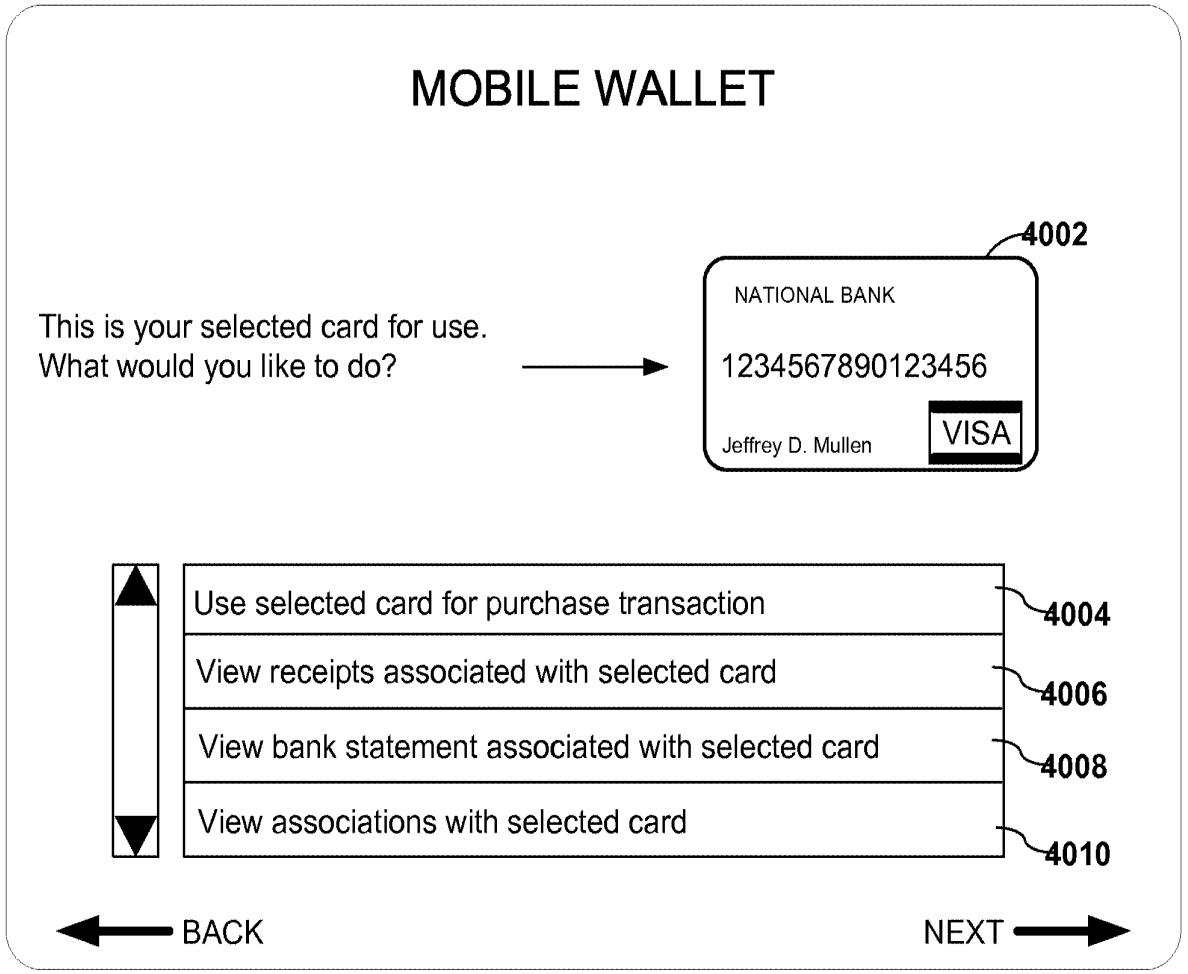


FIG. 40

IPR2025-01152
Apple EX1002 Page 1044

4100

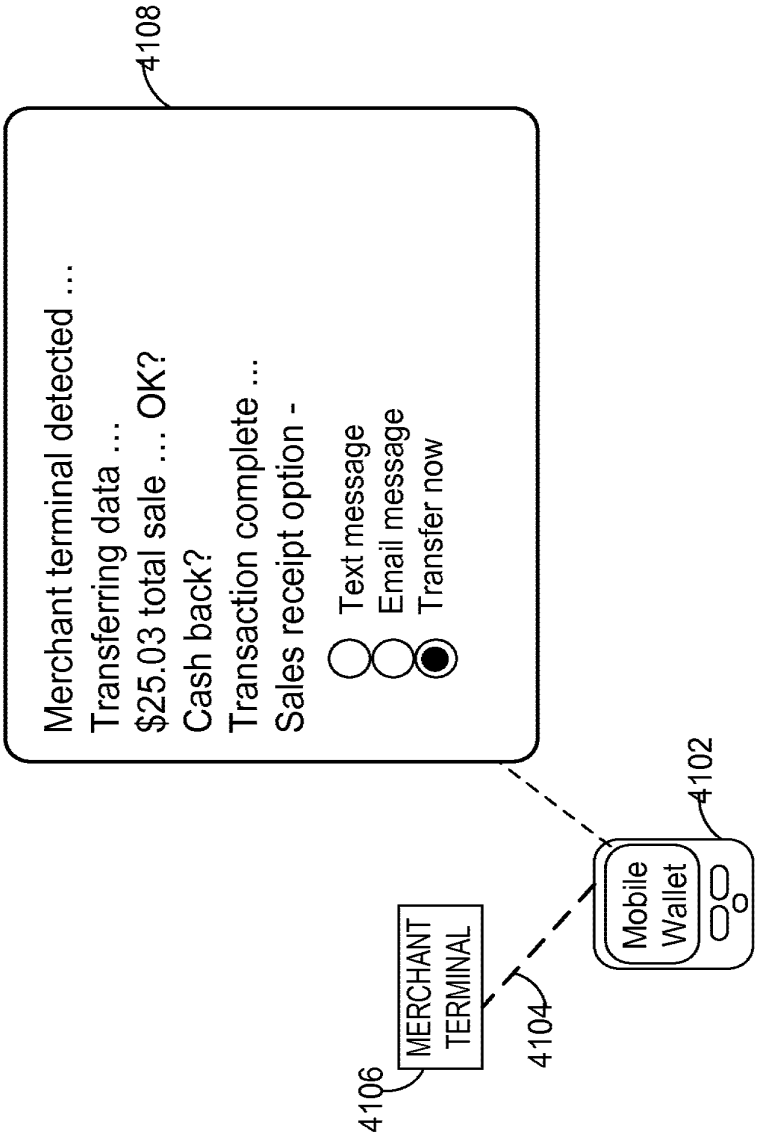


FIG. 41

IPR2025-01152
Apple EX1002 Page 1045

4200

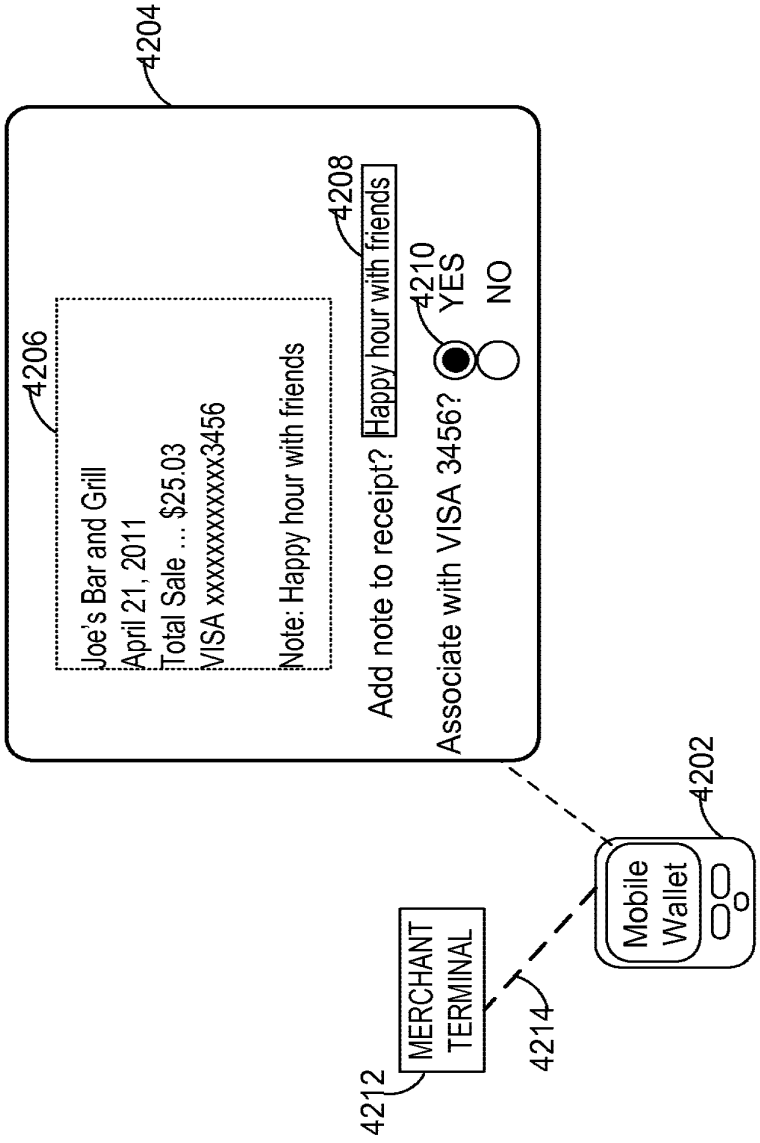


FIG. 42

IPR2025-01152
Apple EX1002 Page 1046

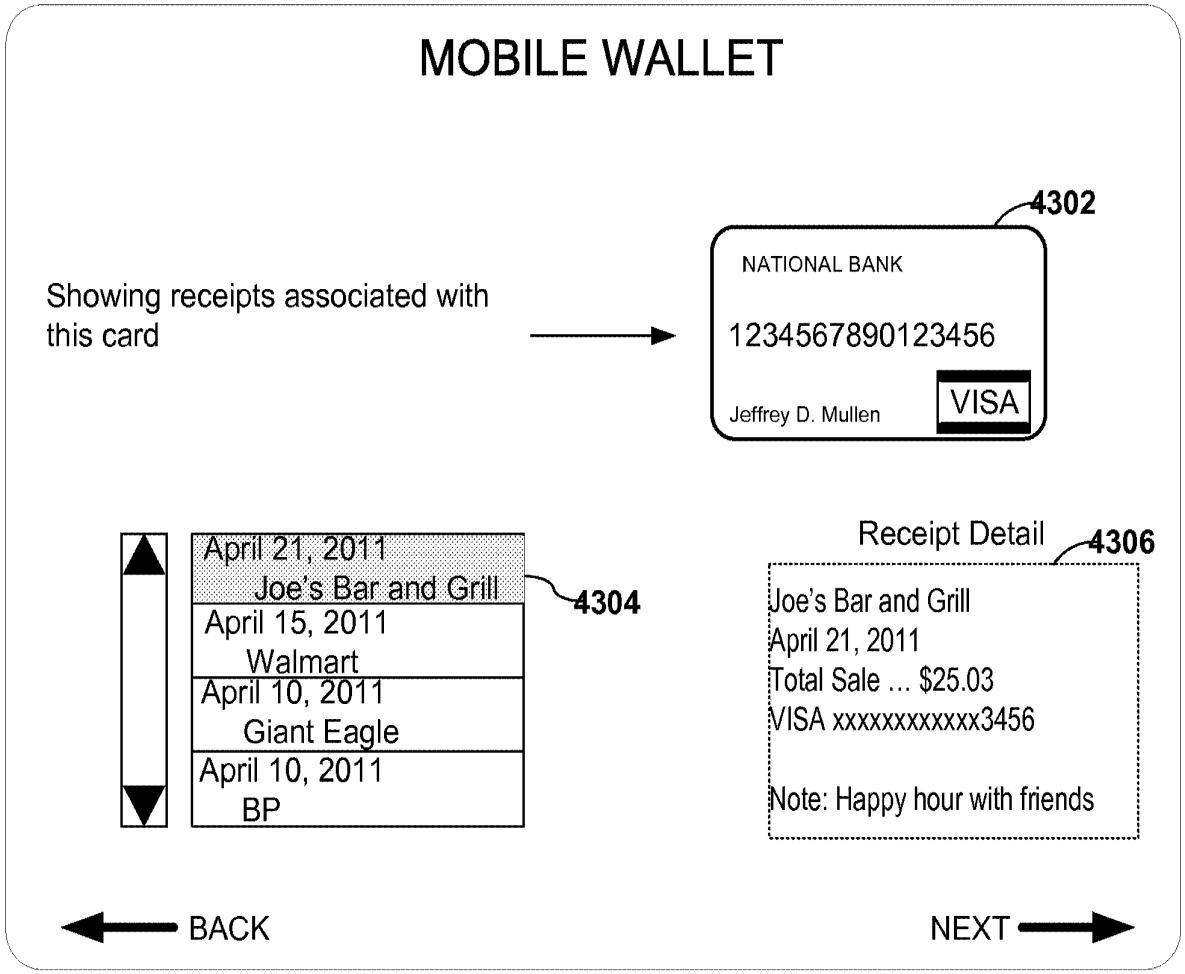

MOBILE WALLET
Showing receipts associated with this card
4302
NATIONAL BANK
1234567890123456
Jeffrey D. Mullen
VISA
April 21, 2011
Joe's Bar and Grill
April 15, 2011
Walmart
April 10, 2011
Giant Eagle
April 10, 2011
BP
4304
Receipt Detail
4306
Joe's Bar and Grill
April 21, 2011
Total Sale ... $25.03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

FIG. 43

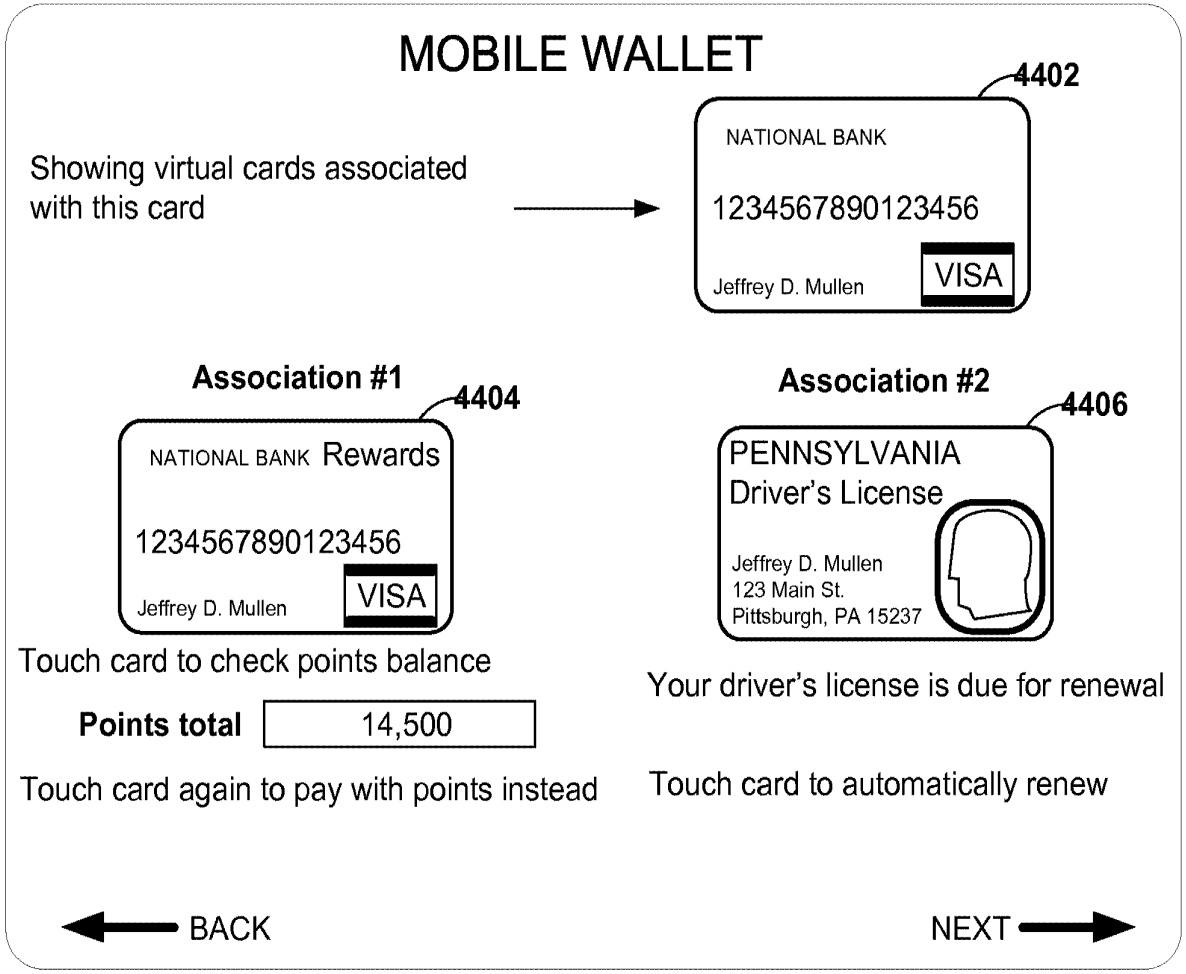


FIG. 44

IPR2025-01152
Apple EX1002 Page 1048

45/73
4500

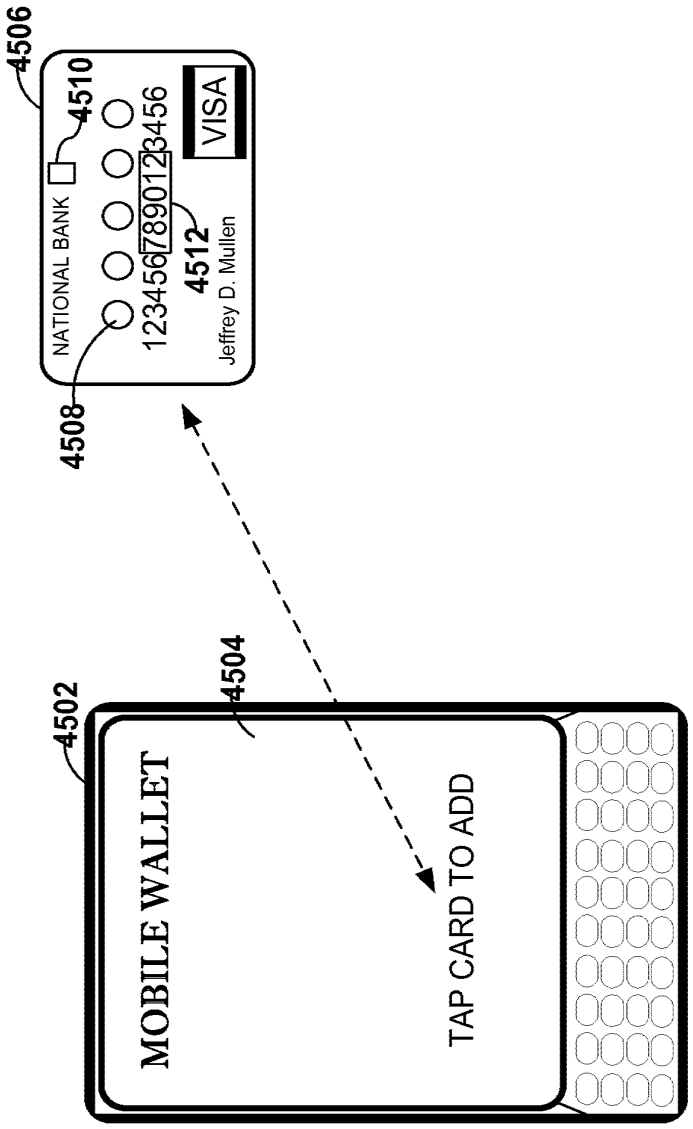


FIG. 45

4600

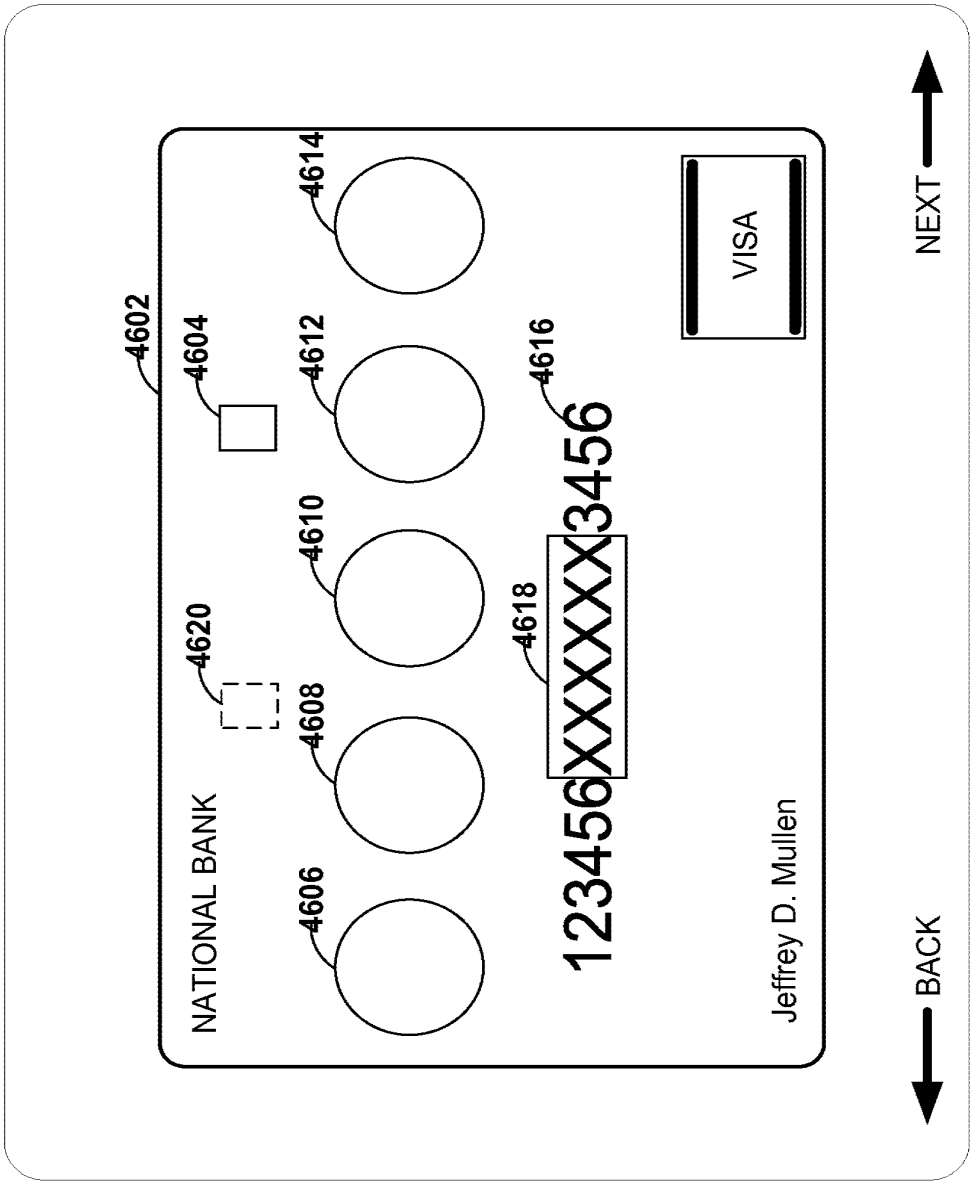

4602
4604
4606
4608
4610
4612
4614
4616
4618
4620
NATIONAL BANK
123456XXXXXX3456
Jeffrey D. Mullen
VISA
NEXT
BACK

FIG. 46

47/73

4700

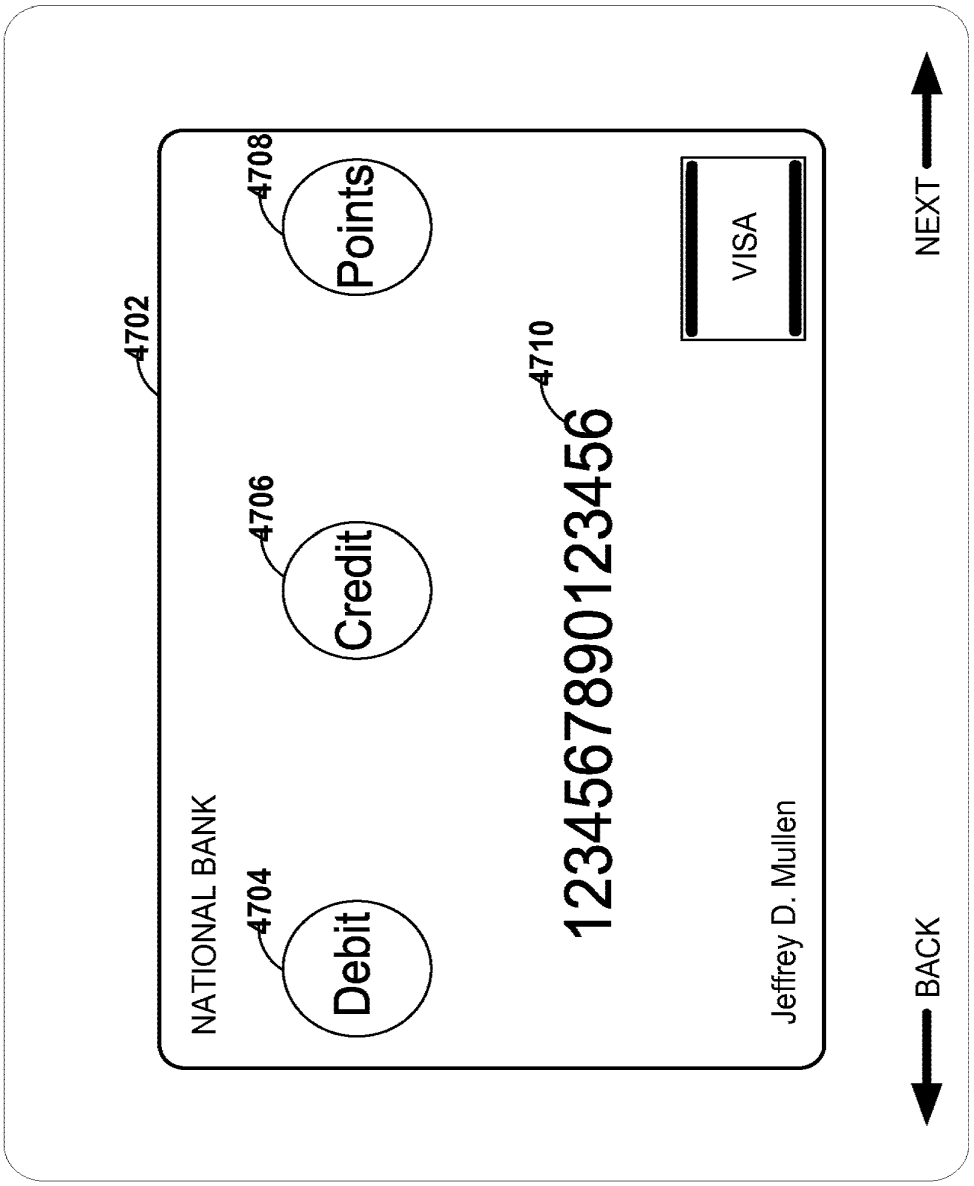


FIG. 47

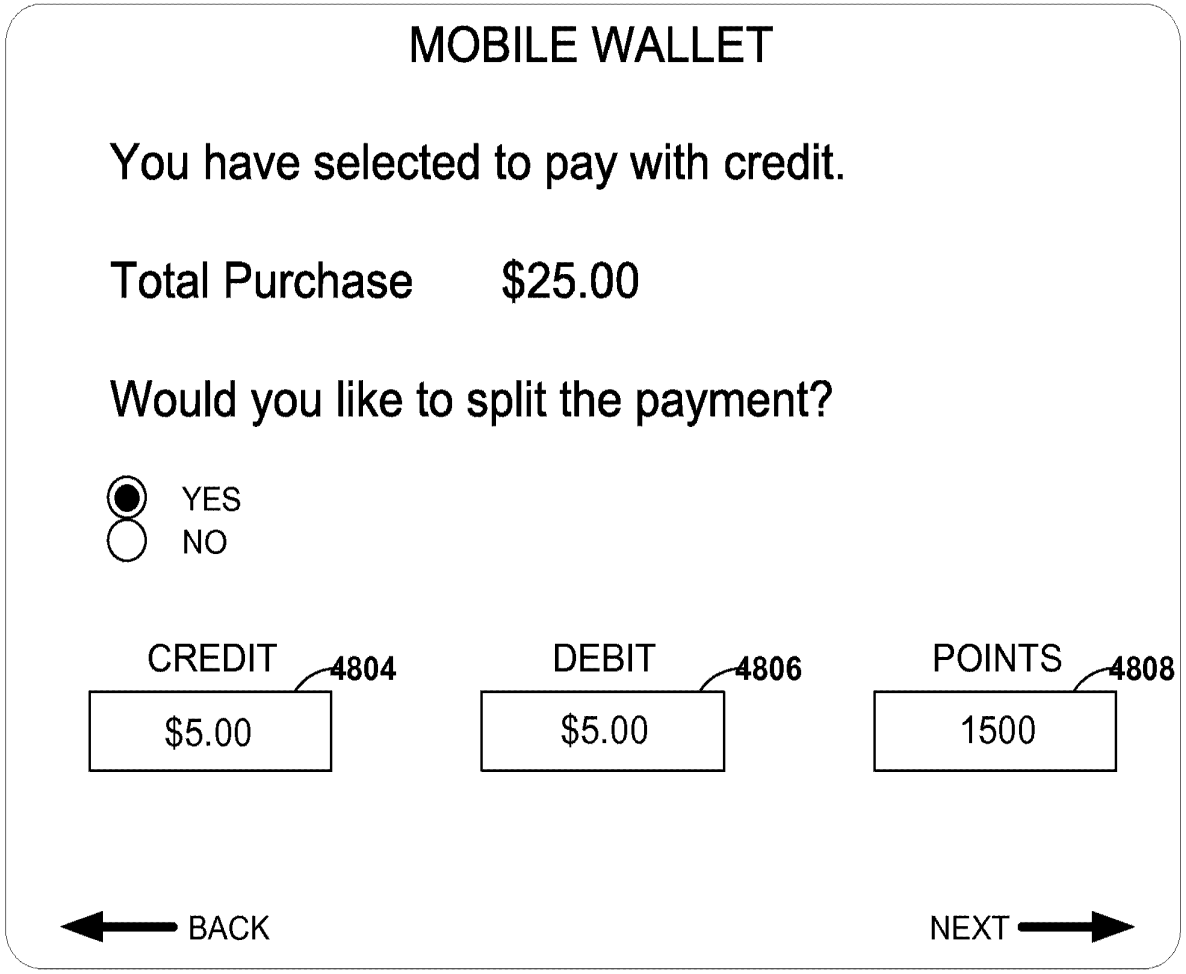

MOBILE WALLET
You have selected to pay with credit.
Total Purchase $25.00
Would you like to split the payment?
YES
NO
CREDIT
4804
$5.00
DEBIT
4806
$5.00
POINTS
4808
1500
BACK
NEXT

FIG. 48

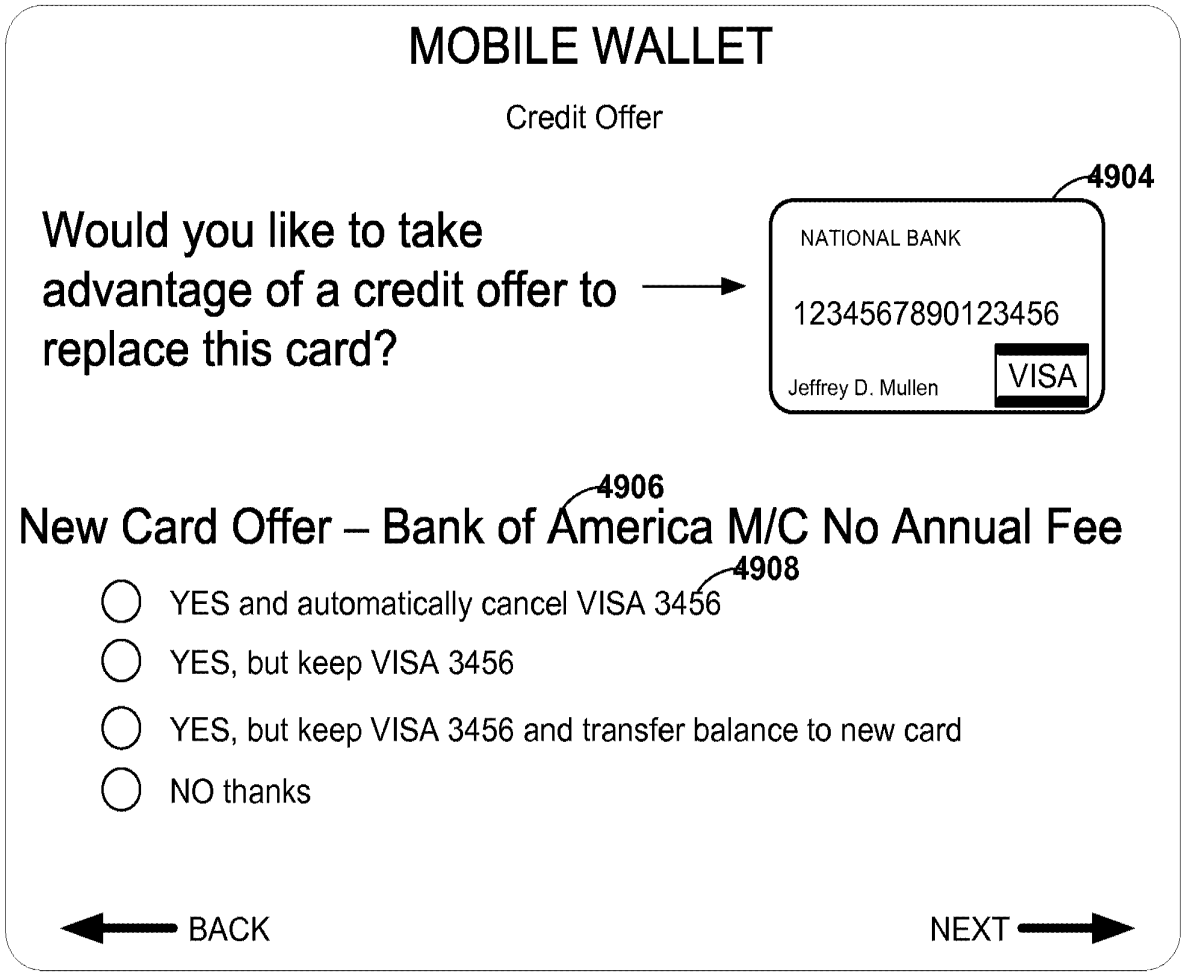

MOBILE WALLET
Credit Offer
Would you like to take advantage of a credit offer to replace this card?
4904
NATIONAL BANK
1234567890123456
Jeffrey D. Mullen
VISA
4906
New Card Offer – Bank of America M/C No Annual Fee
4908
YES and automatically cancel VISA 3456
YES, but keep VISA 3456
YES, but keep VISA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

FIG. 49

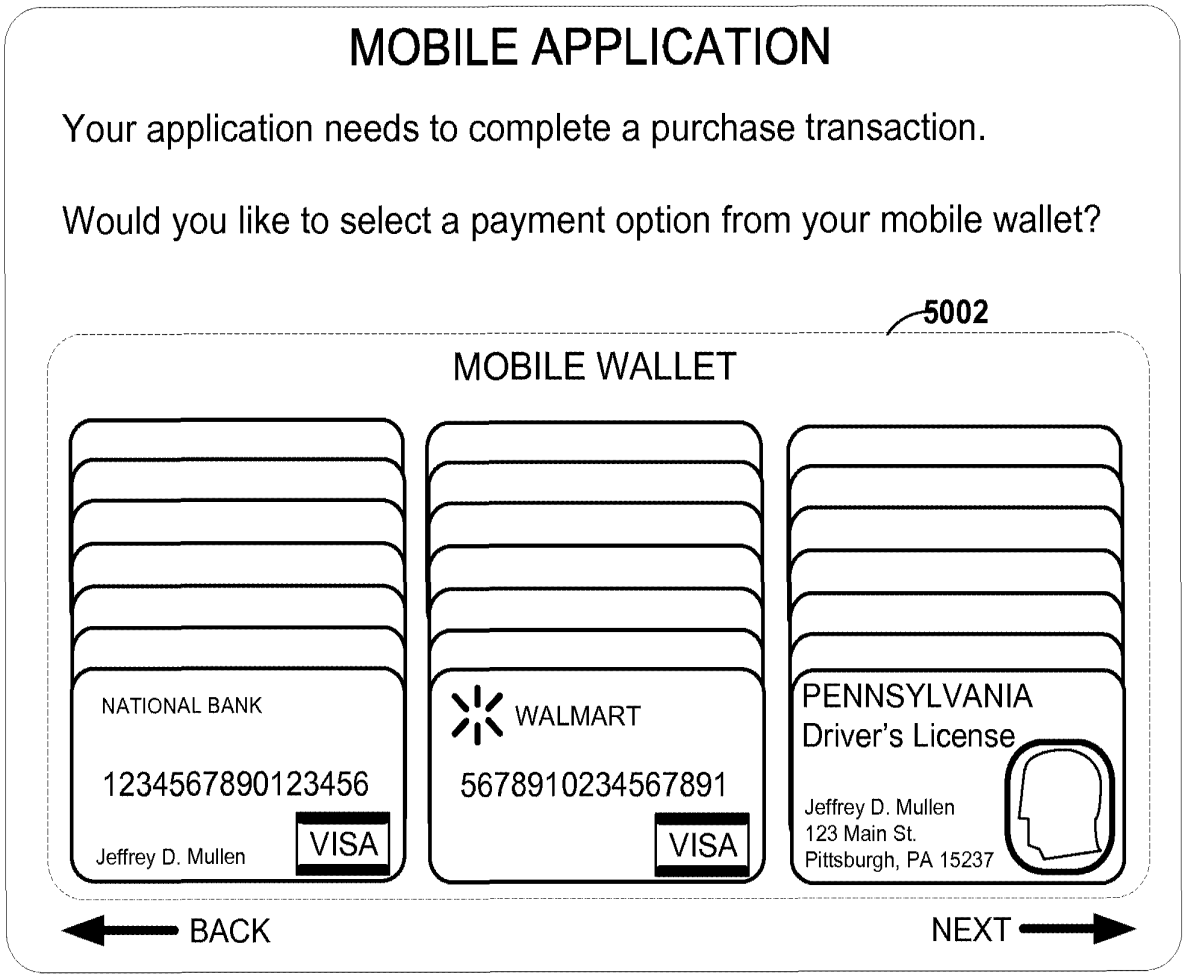

MOBILE APPLICATION
Your application needs to complete a purchase transaction.
Would you like to select a payment option from your mobile wallet?
5002
MOBILE WALLET
NATIONAL BANK
1234567890123456
Jeffrey D. Mullen
VISA
WALMART
5678910234567891
VISA
PENNSYLVANIA
Driver's License
Jeffrey D. Mullen
123 Main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

FIG. 50

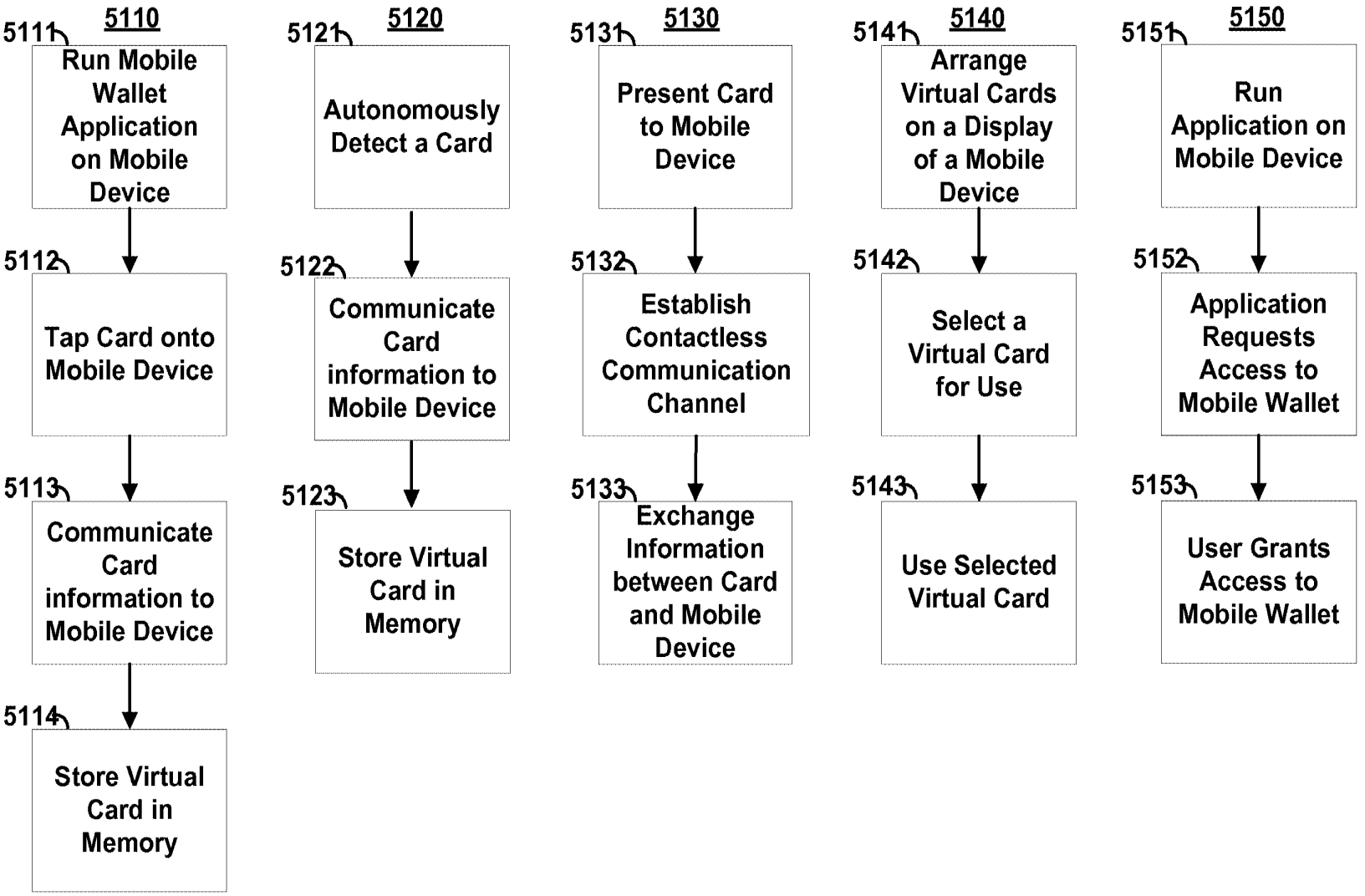


FIG. 51

IPR2025-01152
Apple EX1002 Page 1055

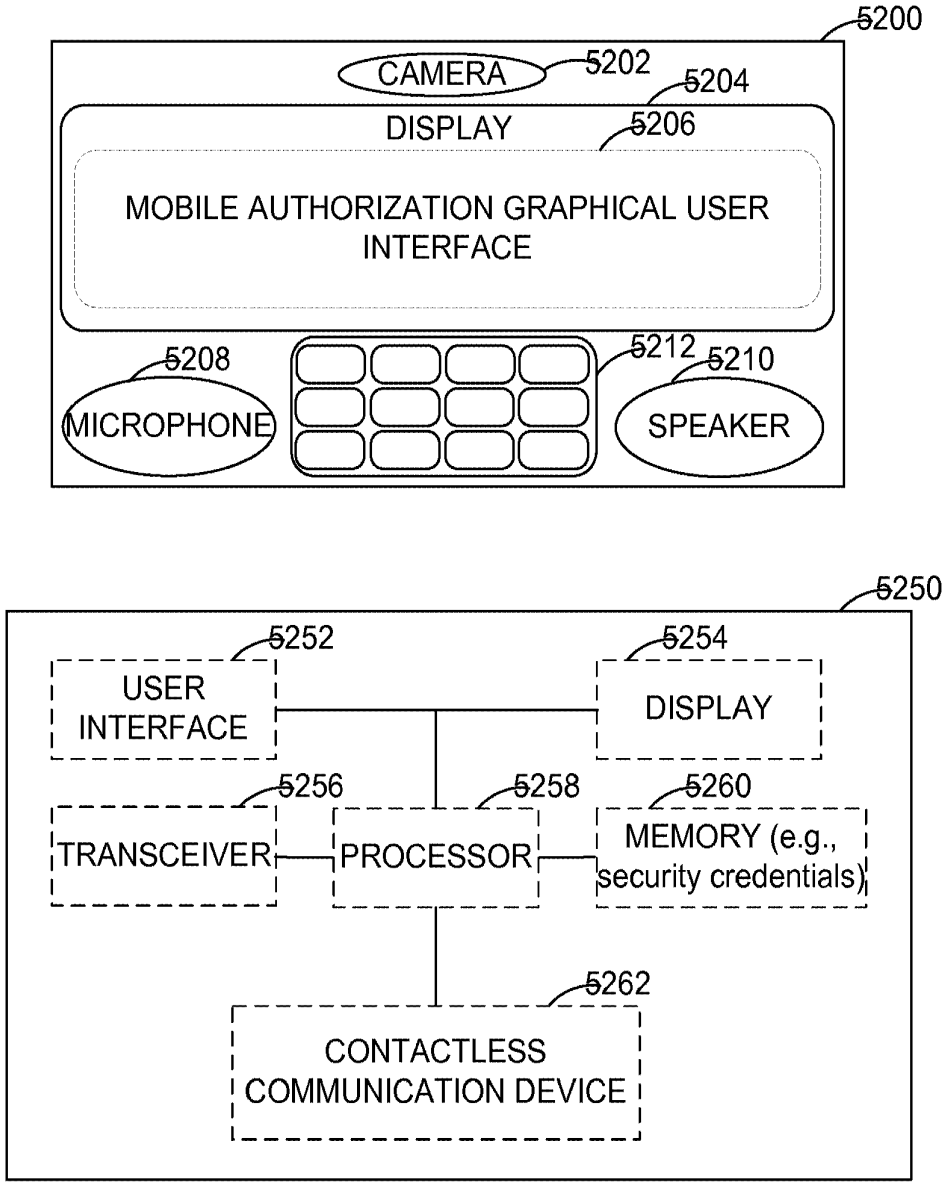
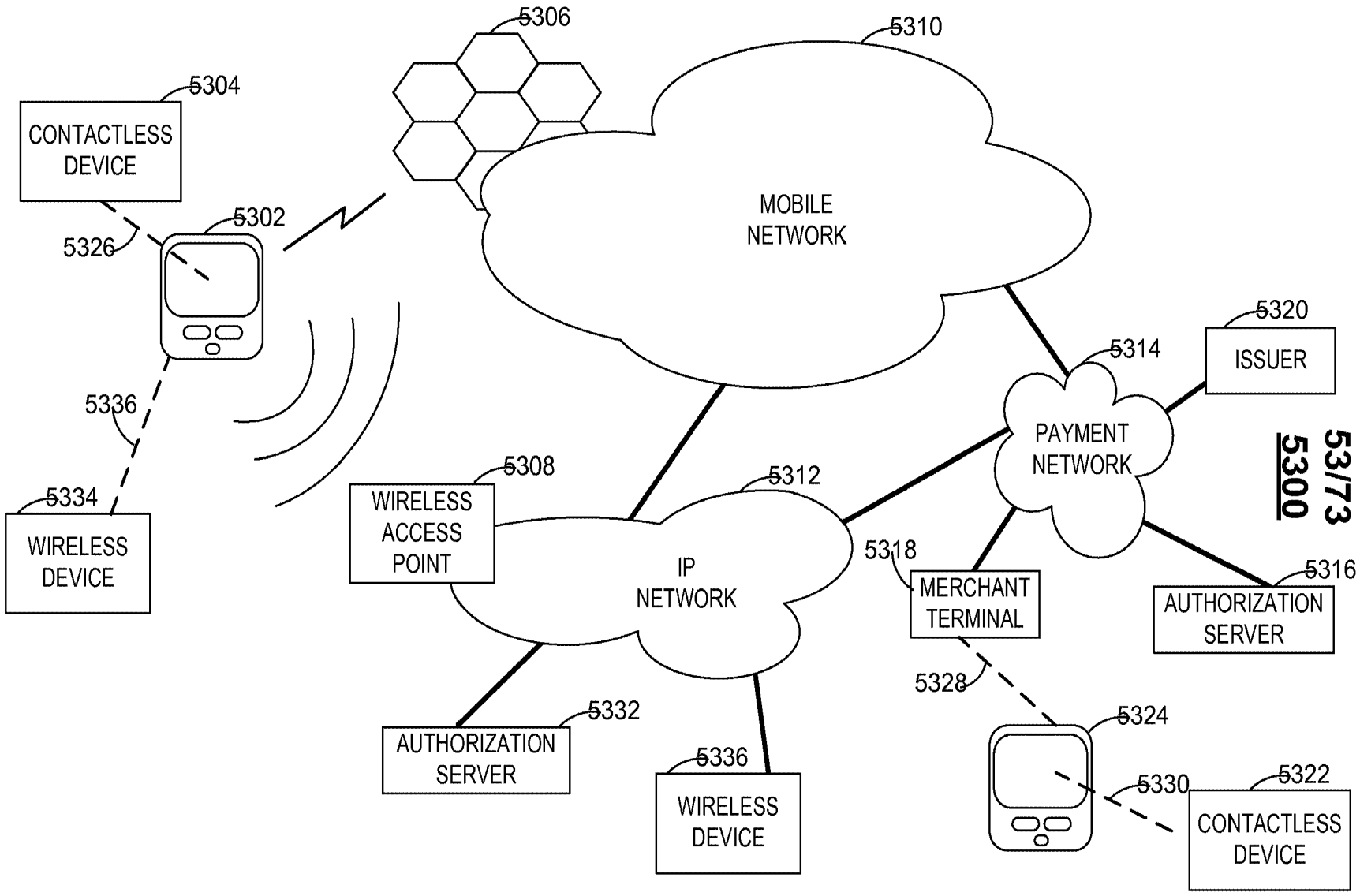

5200
CAMERA
5202
5204
DISPLAY
5206
MOBILE AUTHORIZATION GRAPHICAL USER INTERFACE
5208
MICROPHONE
5212
5210
SPEAKER
5250
5252
USER INTERFACE
5254
DISPLAY
5256
5258
5260
TRANSCEIVER
PROCESSOR
MEMORY (e.g., security credentials)
5262
CONTACTLESS COMMUNICATION DEVICE

FIG. 52



53/73
5300

FIG. 53

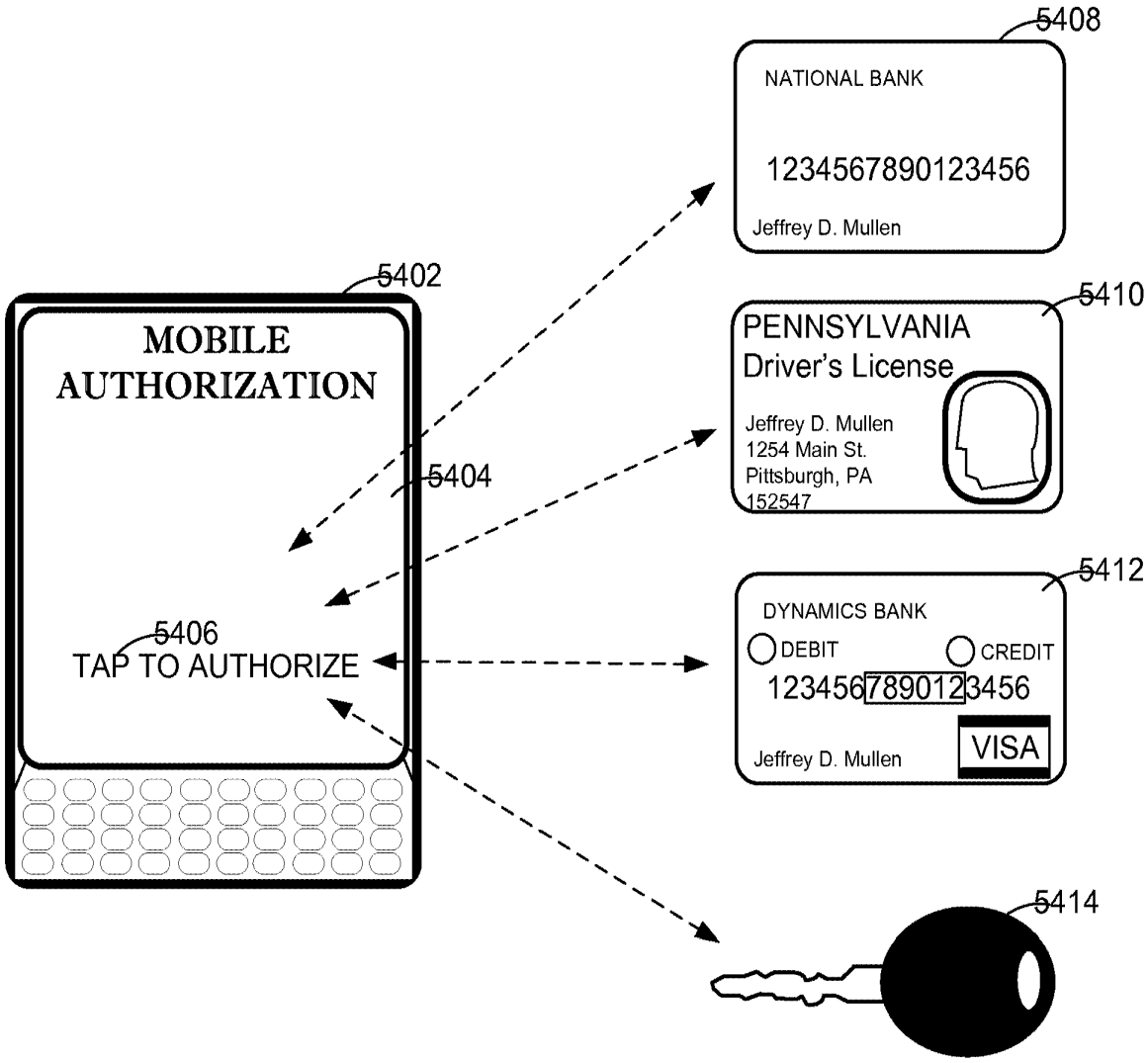

5408
NATIONAL BANK
1234567890123456
Jeffrey D. Mullen
5402
MOBILE
AUTHORIZATION
5404
5410
PENNSYLVANIA
Driver's License
Jeffrey D. Mullen
1254 Main St.
Pittsburgh, PA
152547
5412
DYNAMICS BANK
DEBIT
CREDIT
123456789012 3456
Jeffrey D. Mullen
VISA
5406
TAP TO AUTHORIZE
5414

FIG. 54

5500

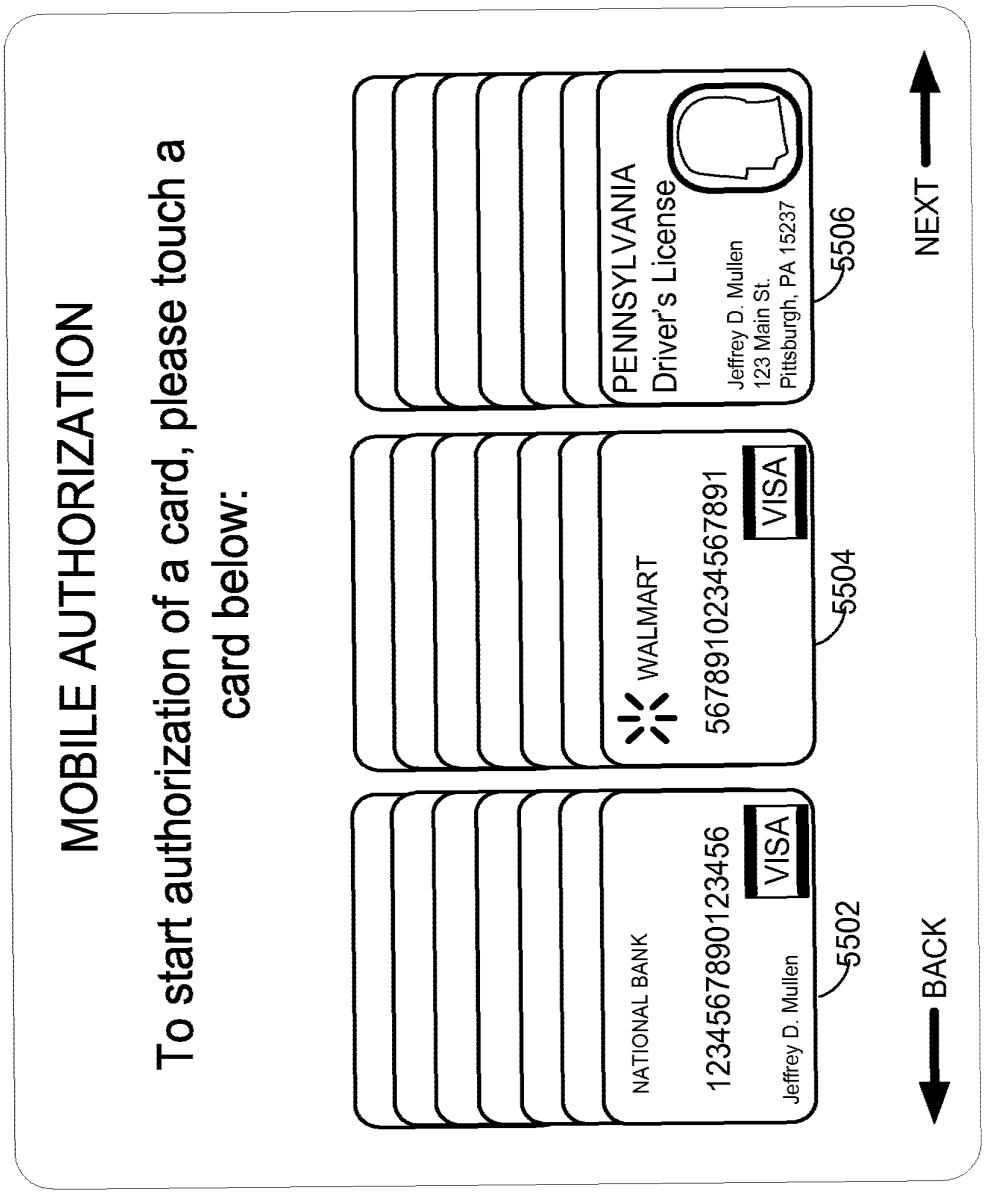


FIG. 55

IPR2025-01152
Apple EX1002 Page 1059

5600

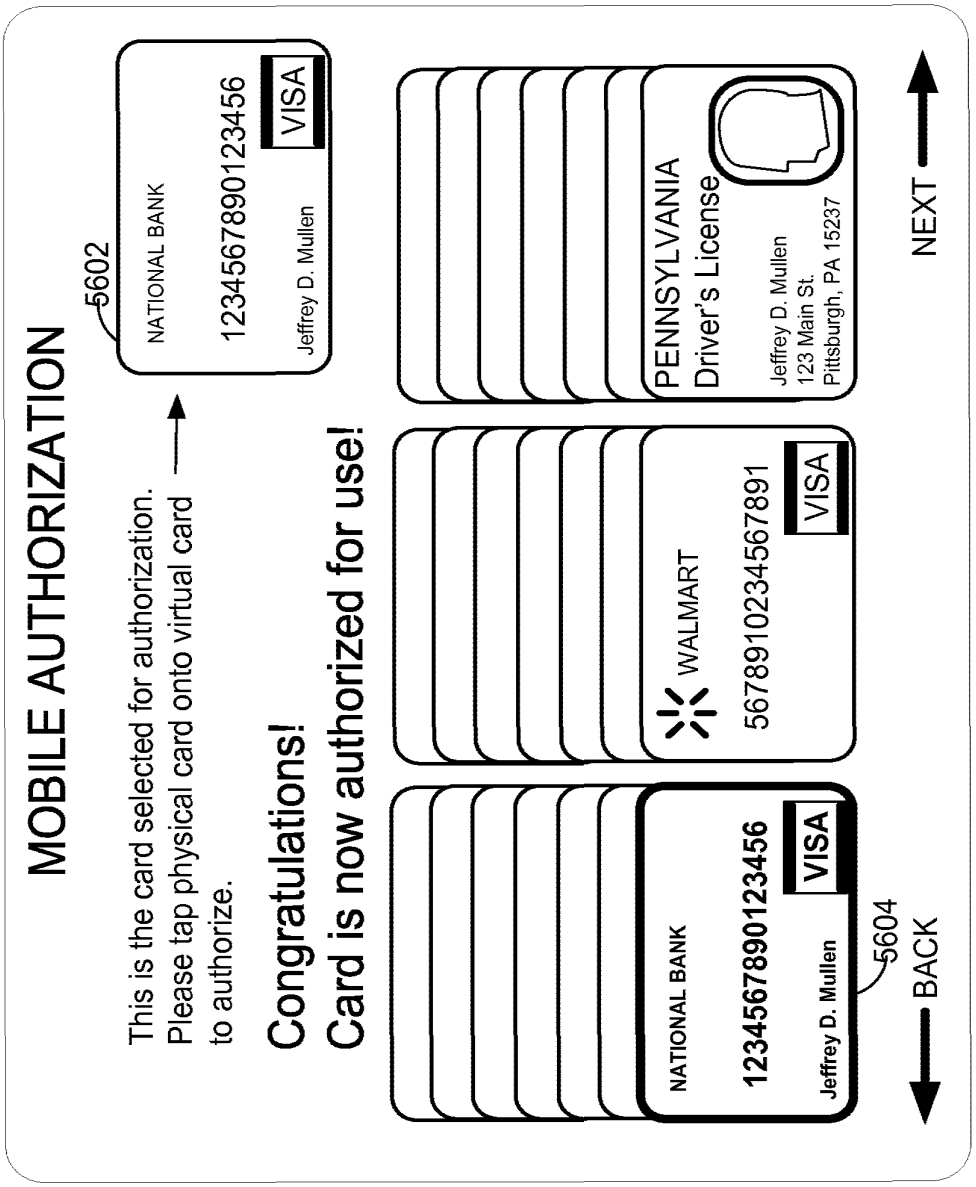


FIG. 56

IPR2025-01152
Apple EX1002 Page 1060

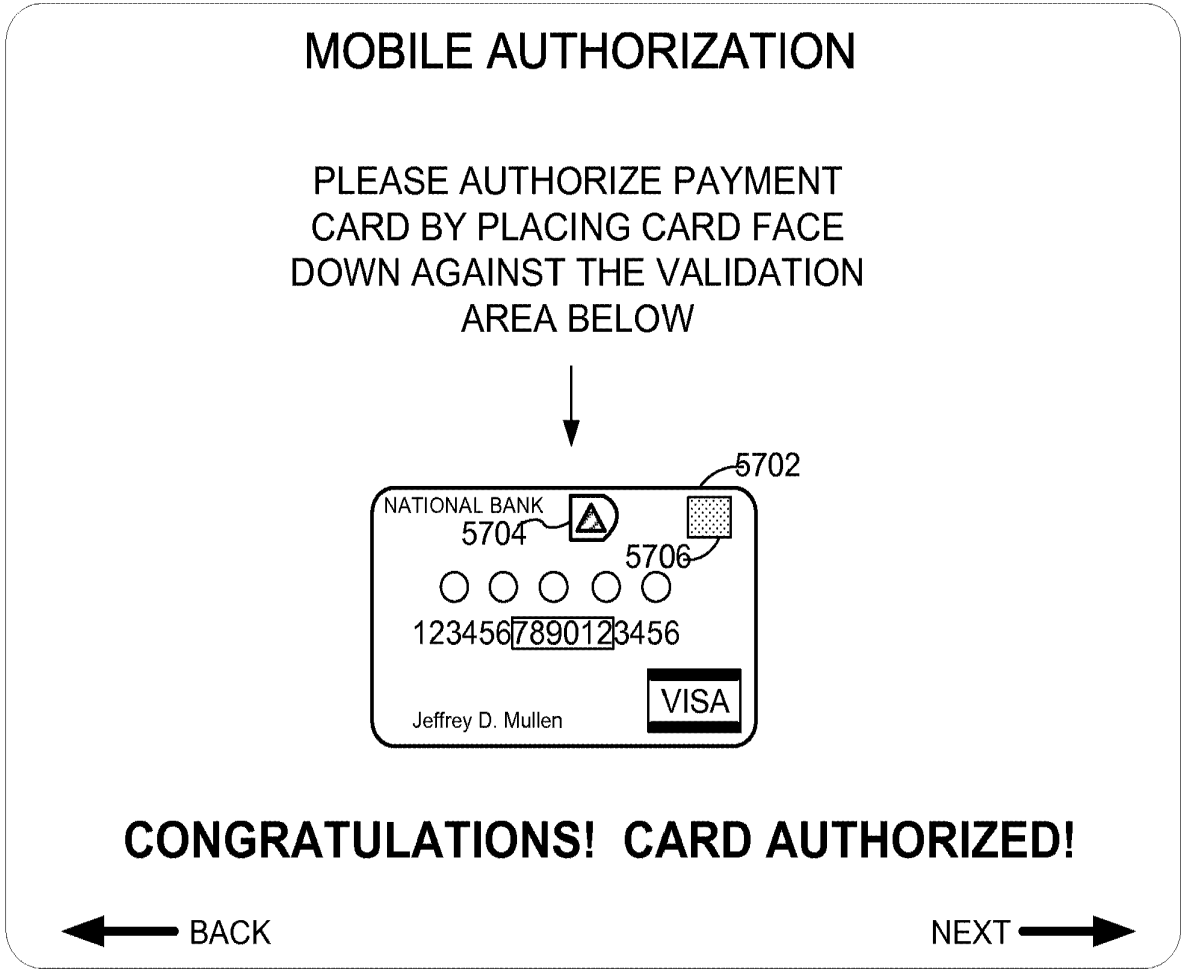
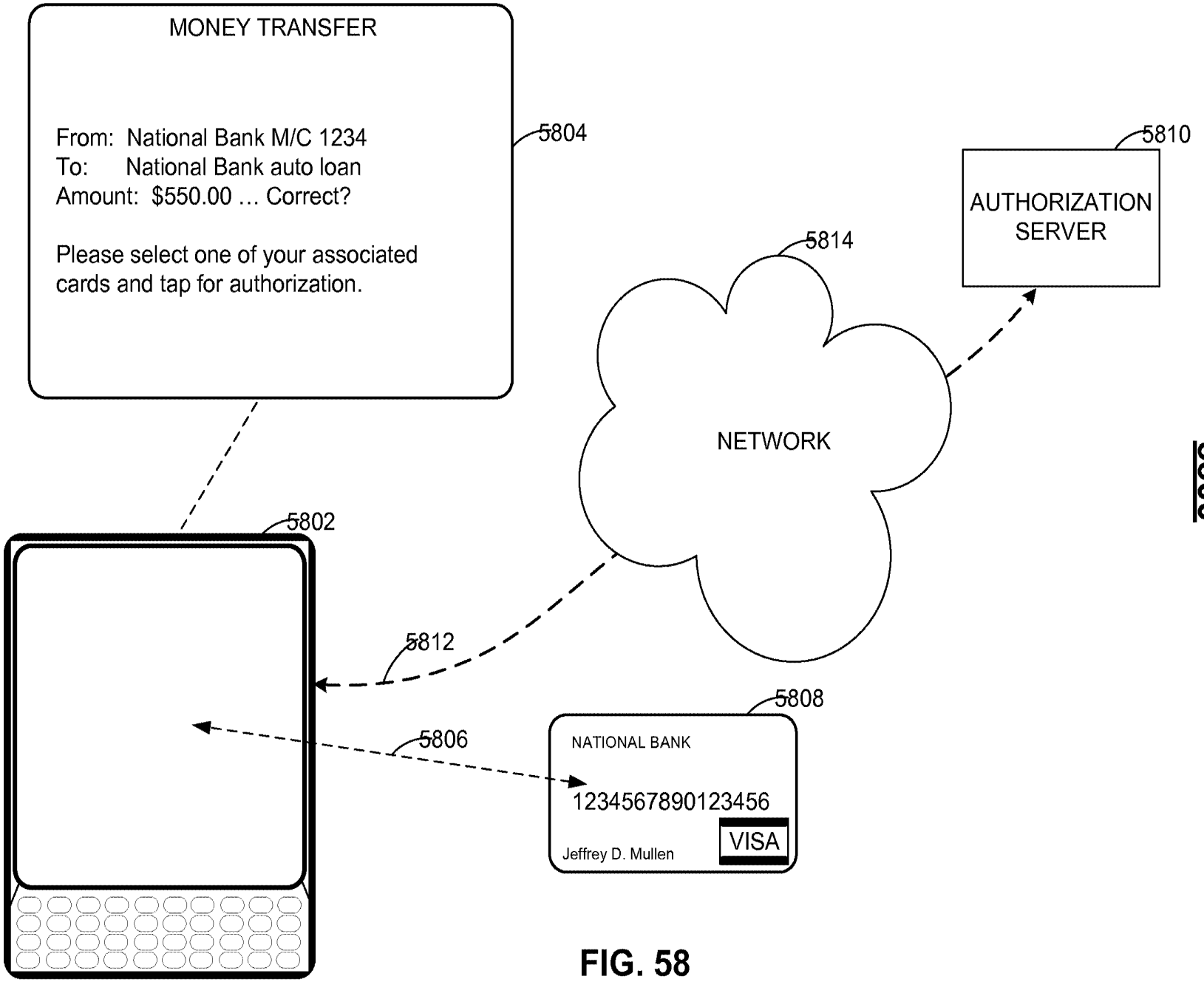


FIG. 57

IPR2025-01152
Apple EX1002 Page 1061



58/73
5800

FIG. 58

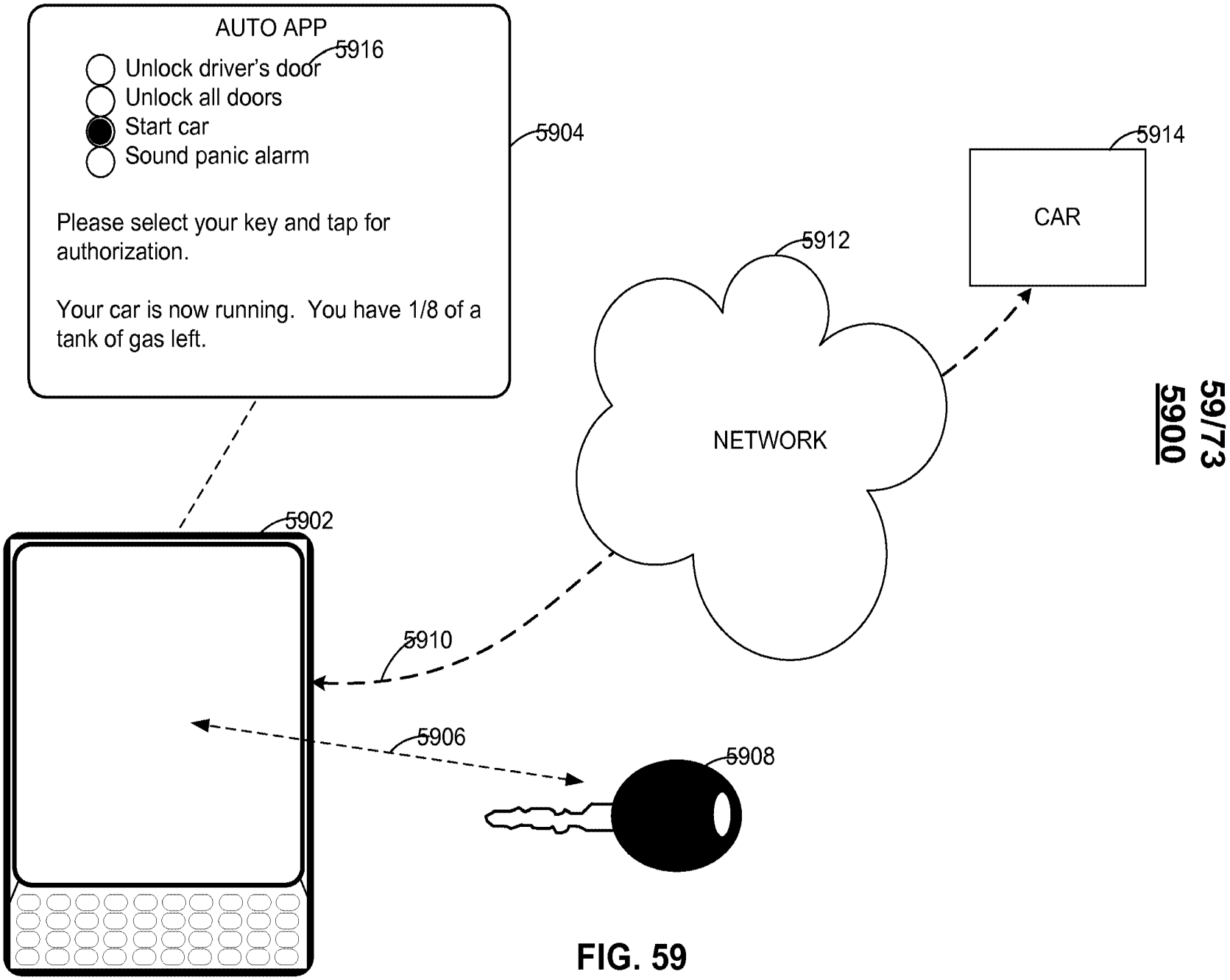
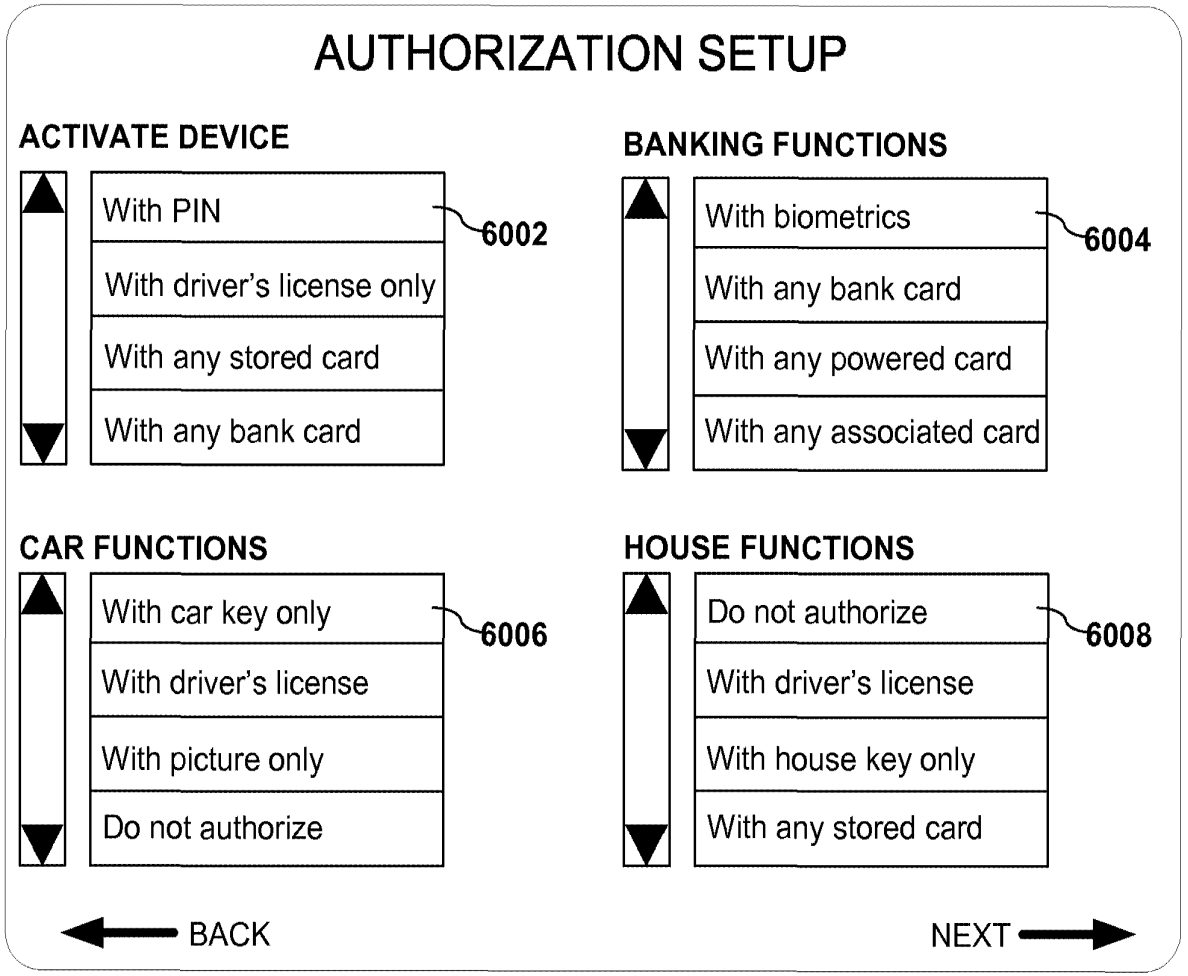

AUTO APP
5916
Unlock driver's door
Unlock all doors
Start car
Sound panic alarm
5904
Please select your key and tap for authorization.
Your car is now running. You have 1/8 of a tank of gas left.
5914
CAR
5912
NETWORK
5902
5910
5906
5908

FIG. 59


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

6000

FIG. 60

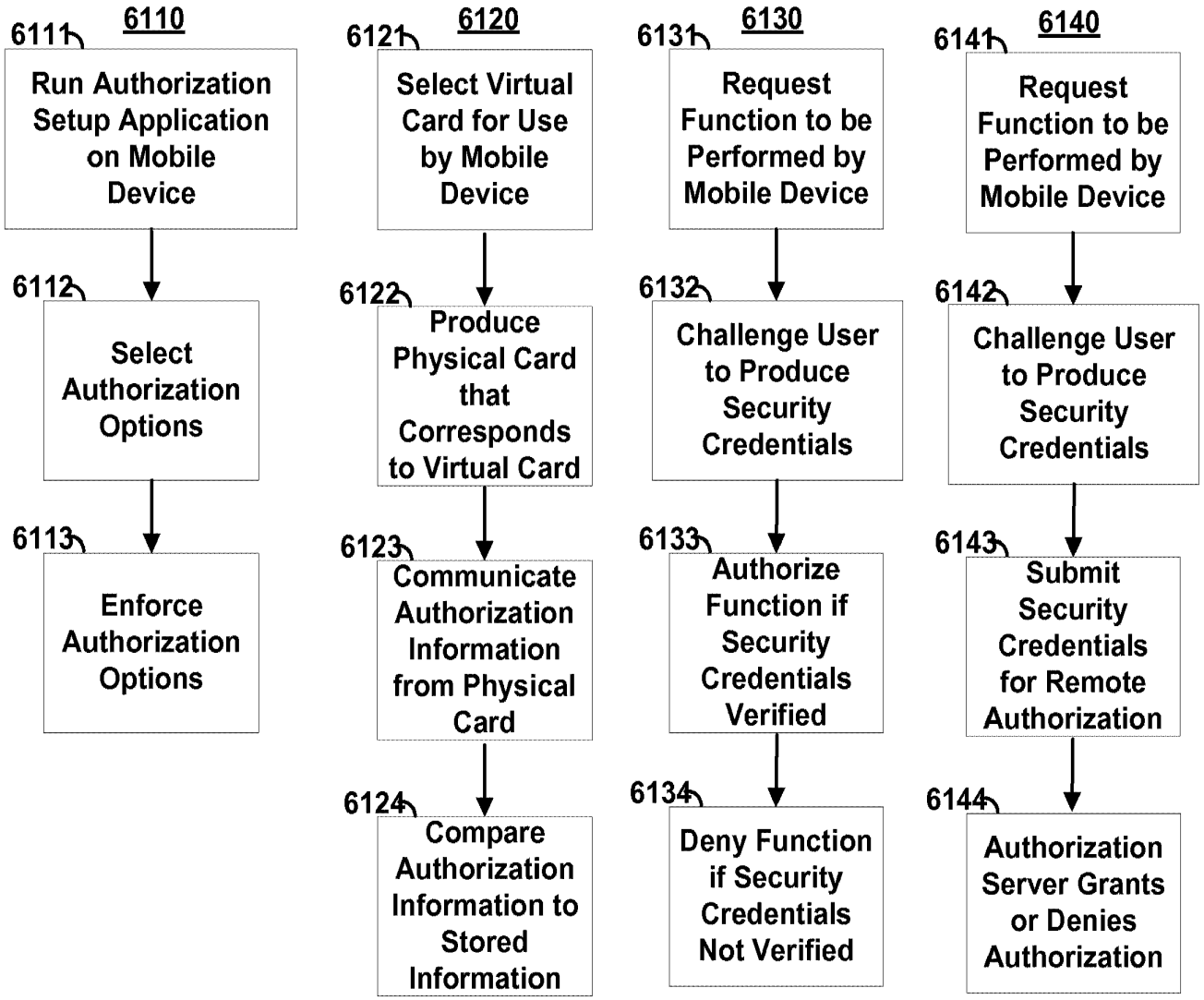


FIG. 61

IPR2025-01152
Apple EX1002 Page 1065

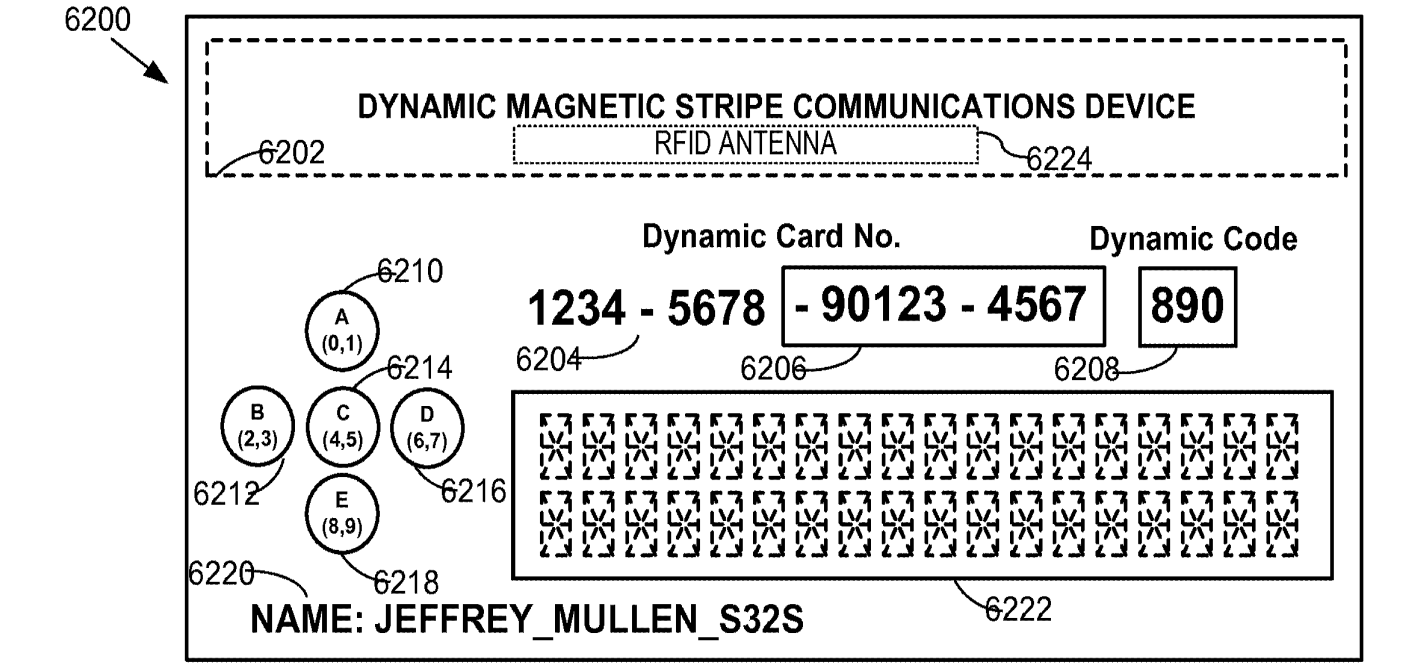

6200
DYNAMIC MAGNETIC STRIPE COMMUNICATIONS DEVICE
RFID ANTENNA
6202
6224
Dynamic Card No.
Dynamic Code
6210
A (0,1)
1234 - 5678
- 90123 - 4567
890
6204
6206
6208
6214
B (2,3)
C (4,5)
D (6,7)
6212
6216
E (8,9)
6220
6218
6222
NAME: JEFFREY_MULLEN_S32S
6250
6252
MEMORY
6254
PROCESSOR
6256
Display
Battery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

FIG. 62

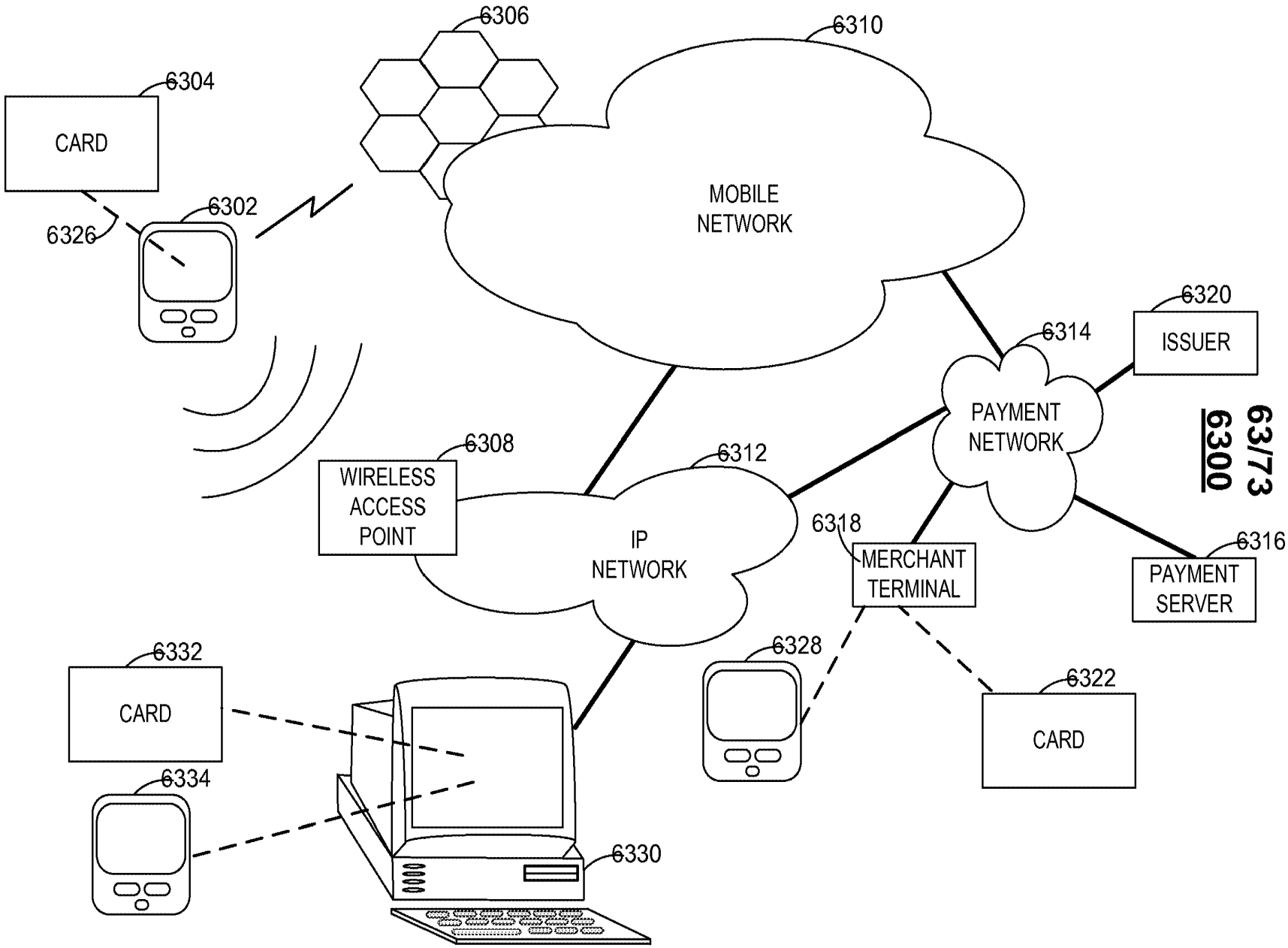

6306
6310
6304
CARD
6302
6326
MOBILE NETWORK
6320
ISSUER
6314
PAYMENT NETWORK
63/73
6300
6308
WIRELESS ACCESS POINT
6312
IP NETWORK
6318
MERCHANT TERMINAL
6316
PAYMENT SERVER
6332
CARD
6328
6322
CARD
6334
6330

FIG. 63

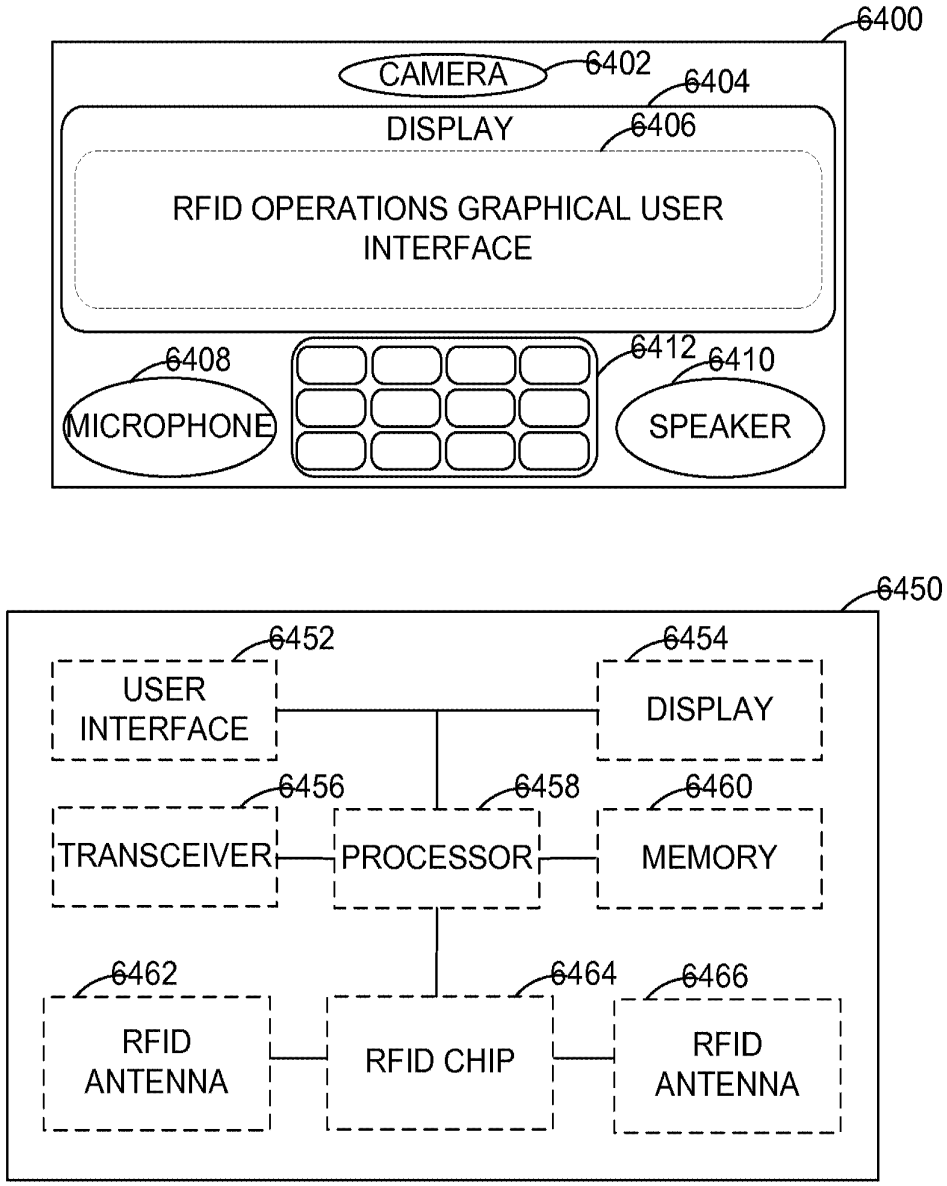


FIG. 64

IPR2025-01152
Apple EX1002 Page 1068

6500

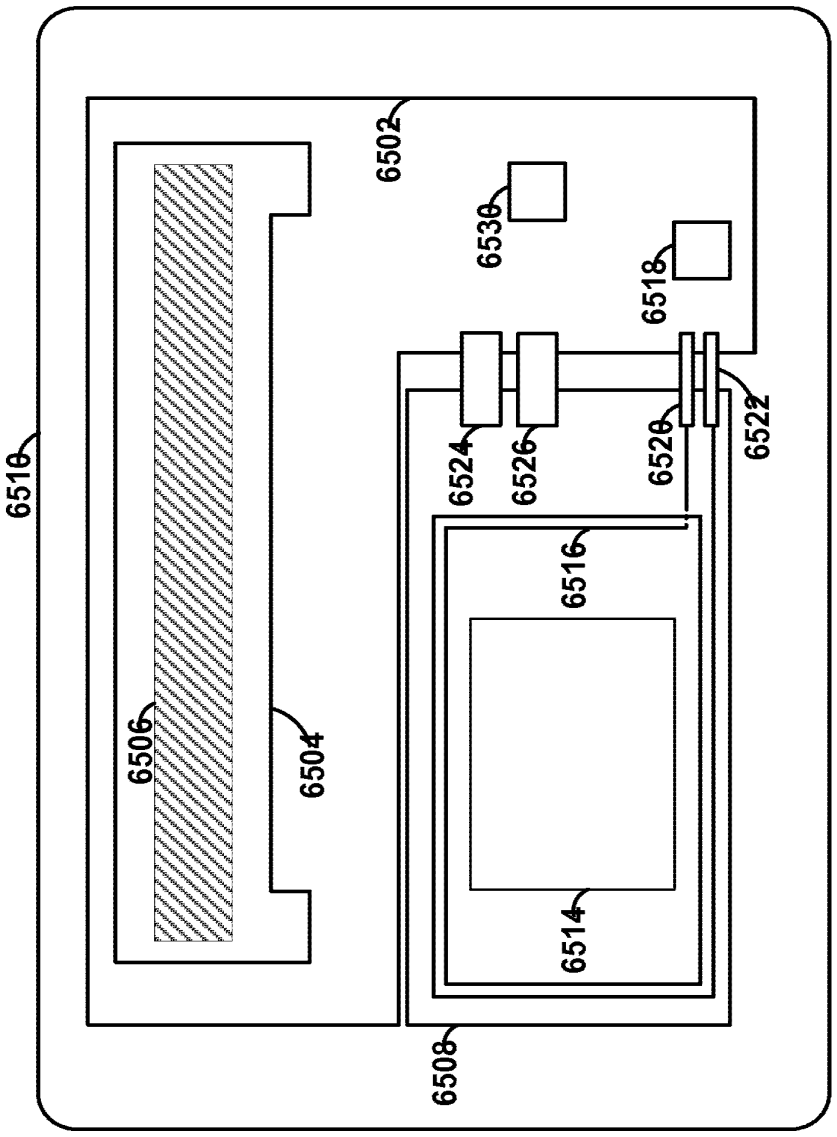

6502
6530
6518
6510
6524
6526
6528
6522
6516
6506
6504
6514
6508

FIG. 65

6600

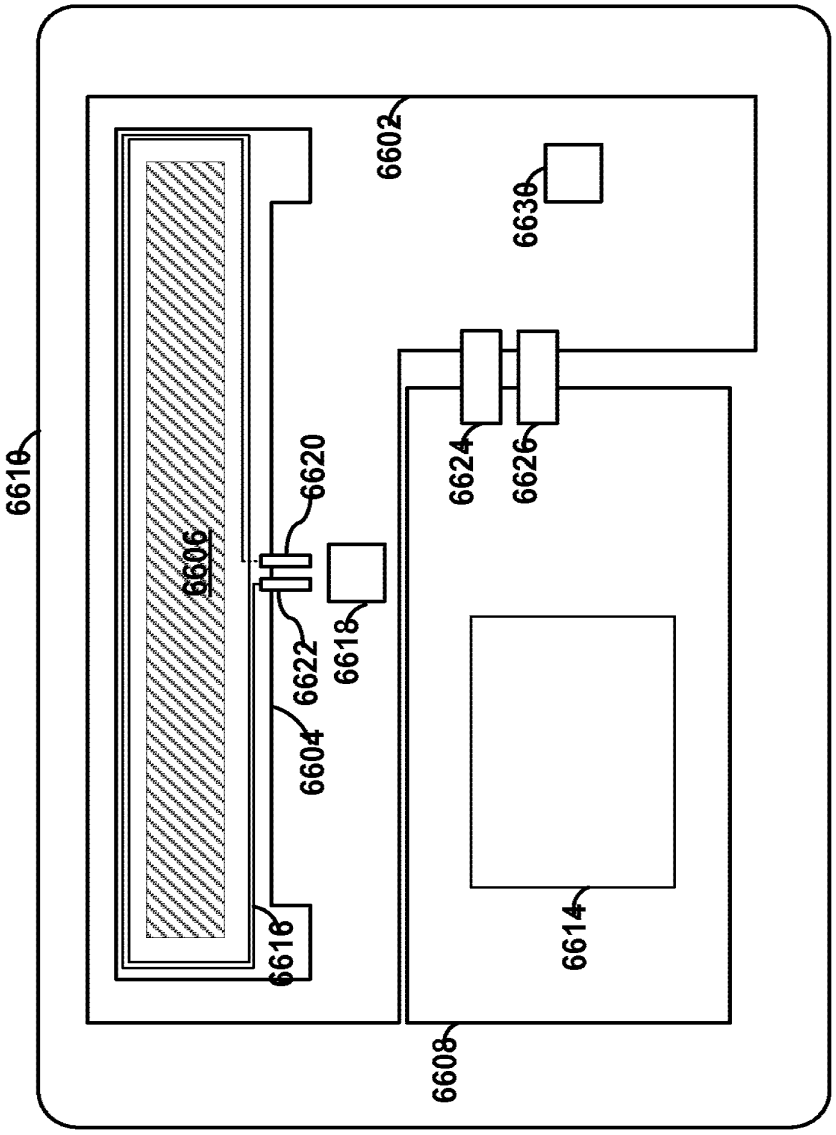

6602
6630
6624
6626
6620
6610
6606
6618
6622
6604
6618
6614
6608

FIG. 66

6700

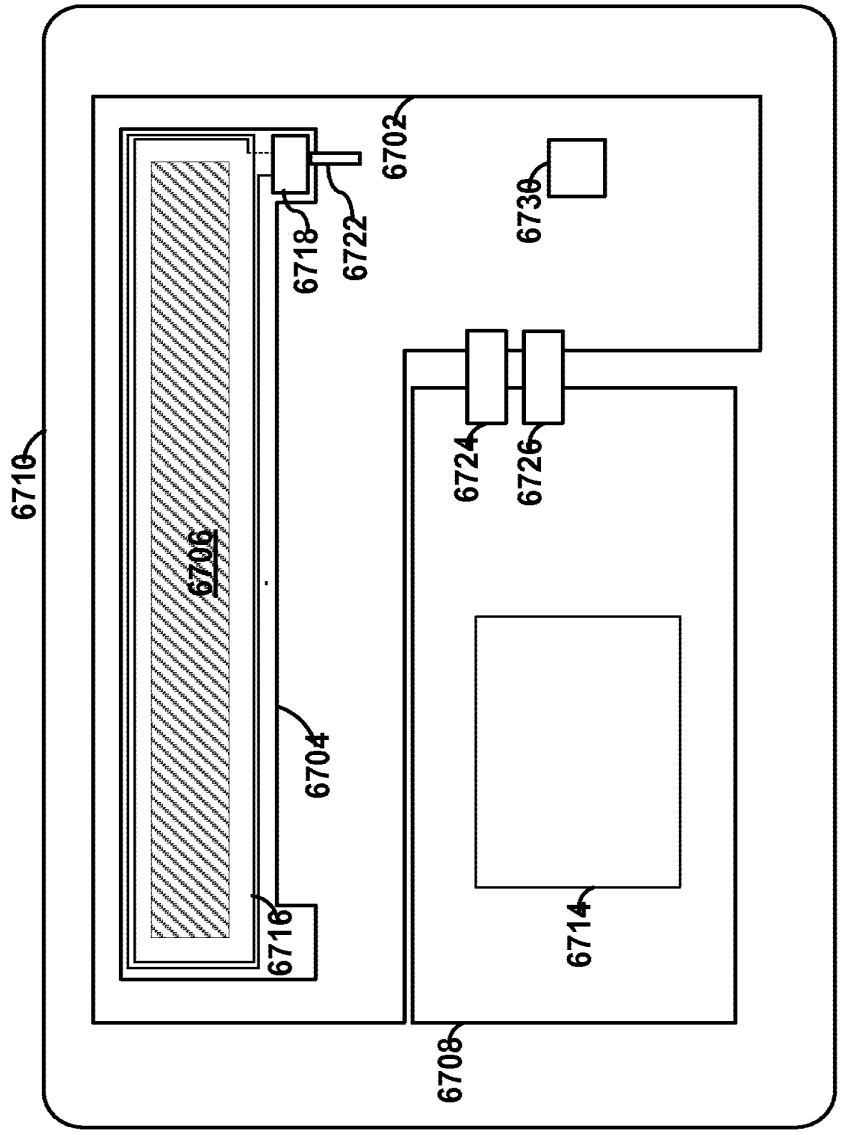


FIG. 67

6800

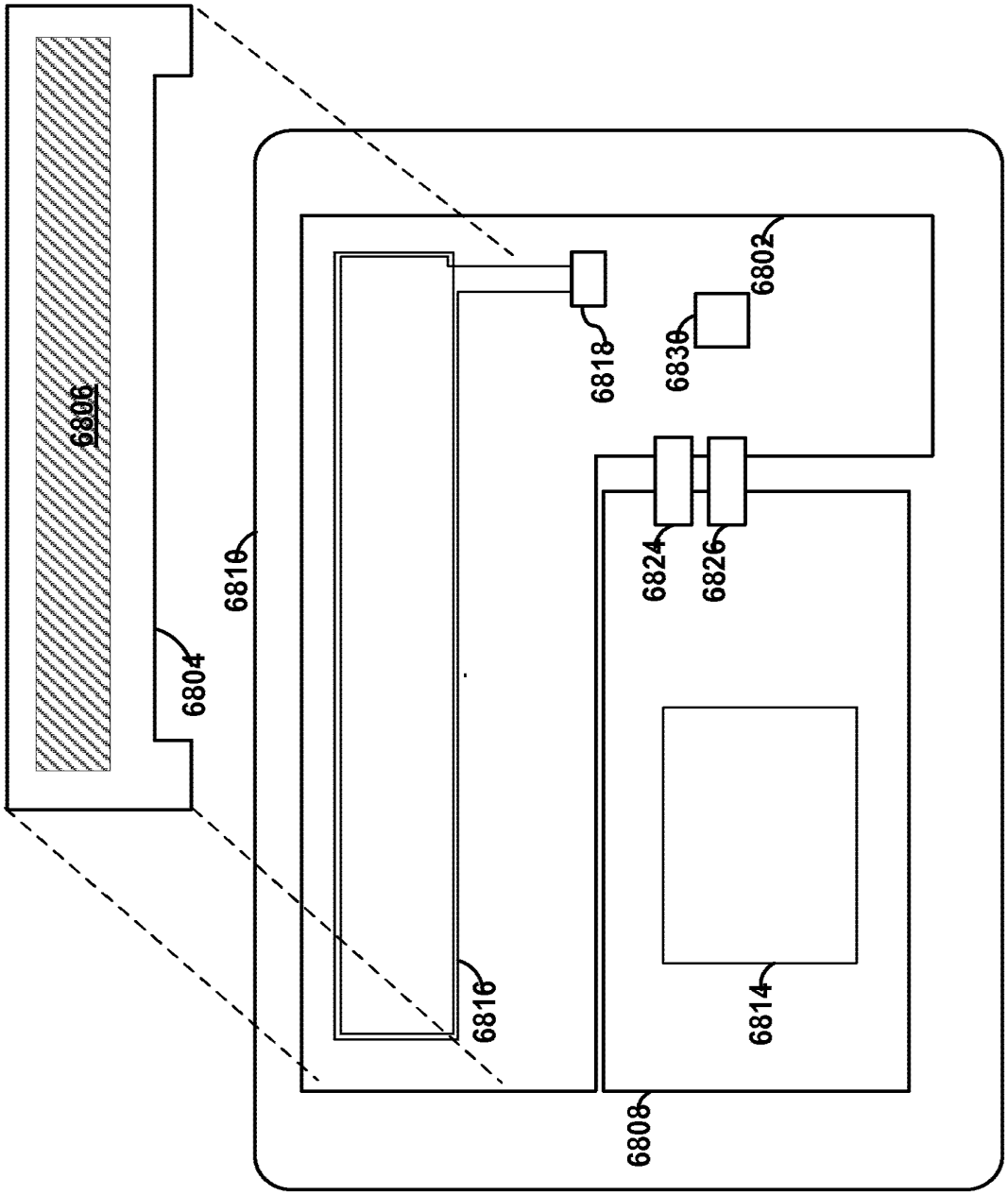


FIG. 68

6900

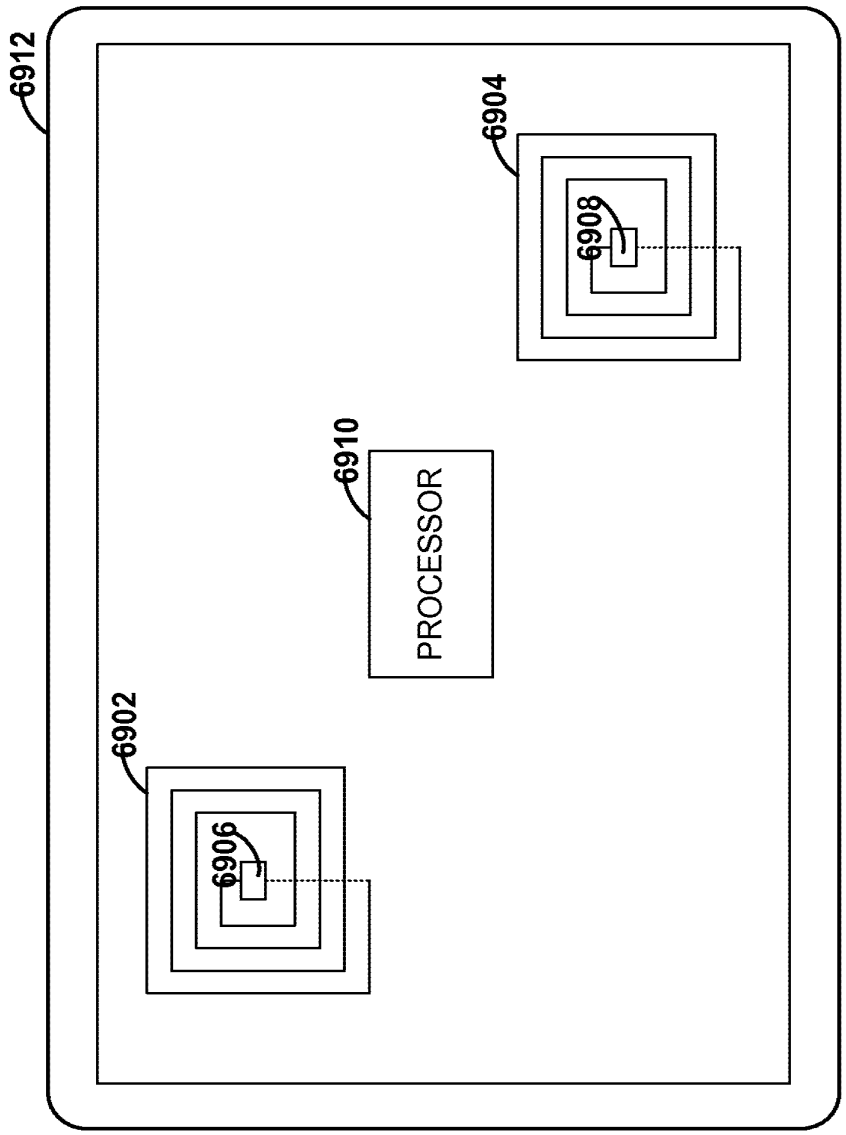


FIG. 69

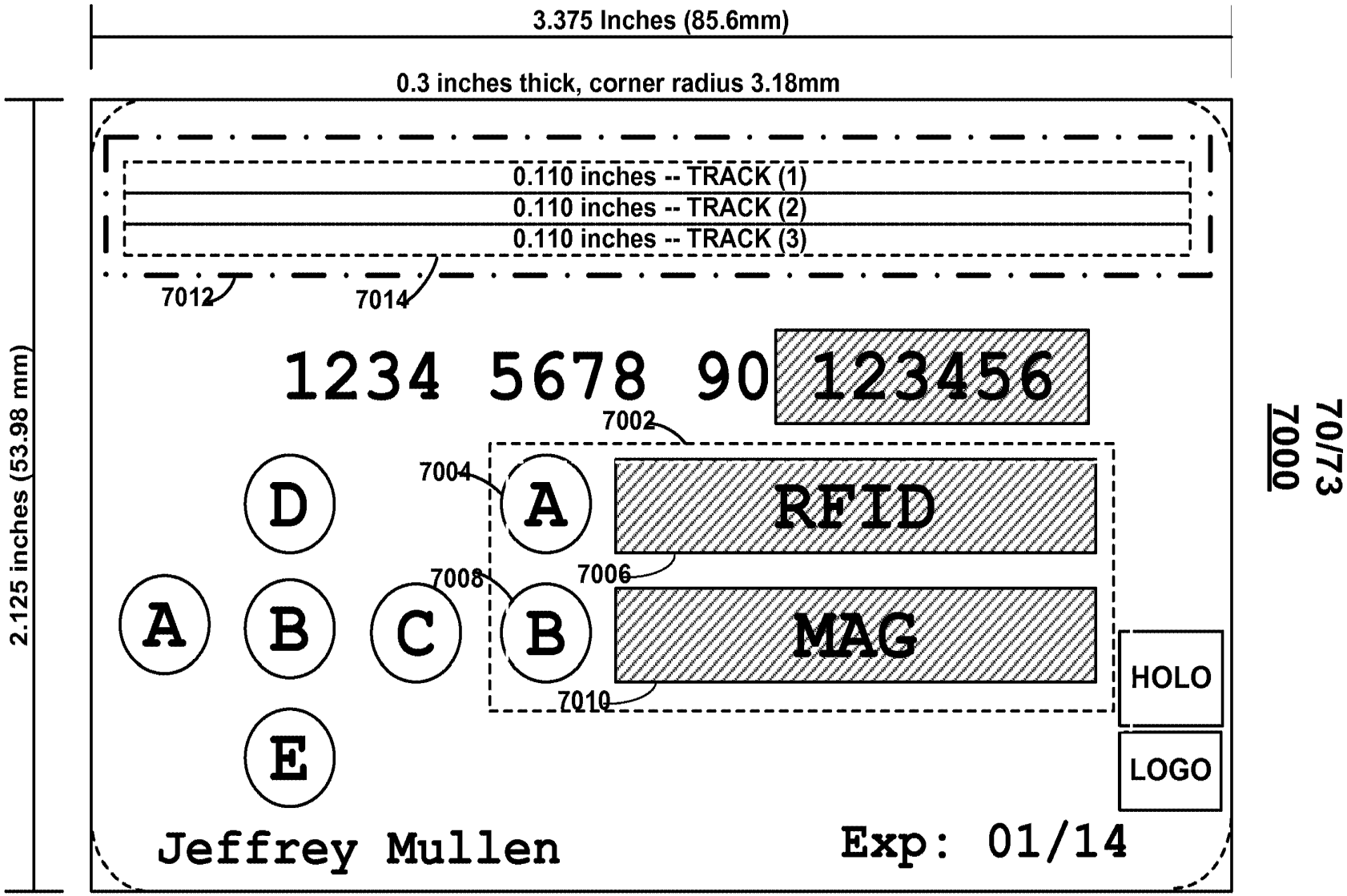

3.375 Inches (85.6mm)
0.3 inches thick, corner radius 3.18mm
2.125 inches (53.98 mm)
0.110 inches -- TRACK (1)
0.110 inches -- TRACK (2)
0.110 inches -- TRACK (3)
7012
7014
1234 5678 90
123456
7002
7004
A
REID
7006
7008
B
MAG
7010
D
A
B
C
E
HOLO
LOGO
Jeffrey Mullen
Exp: 01/14
7000
70/73

FIG. 70

71/73
7100

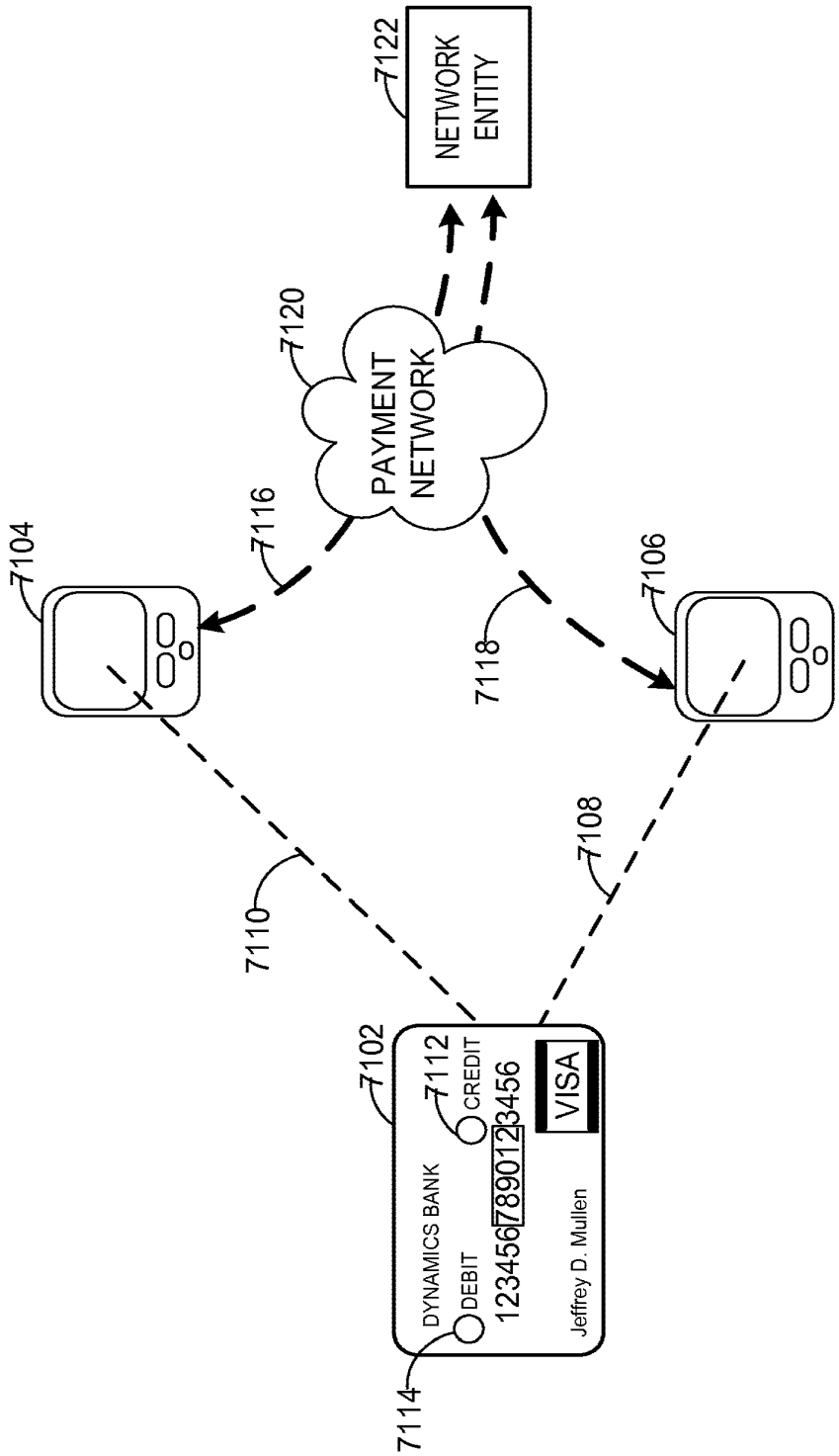


FIG. 71

7200

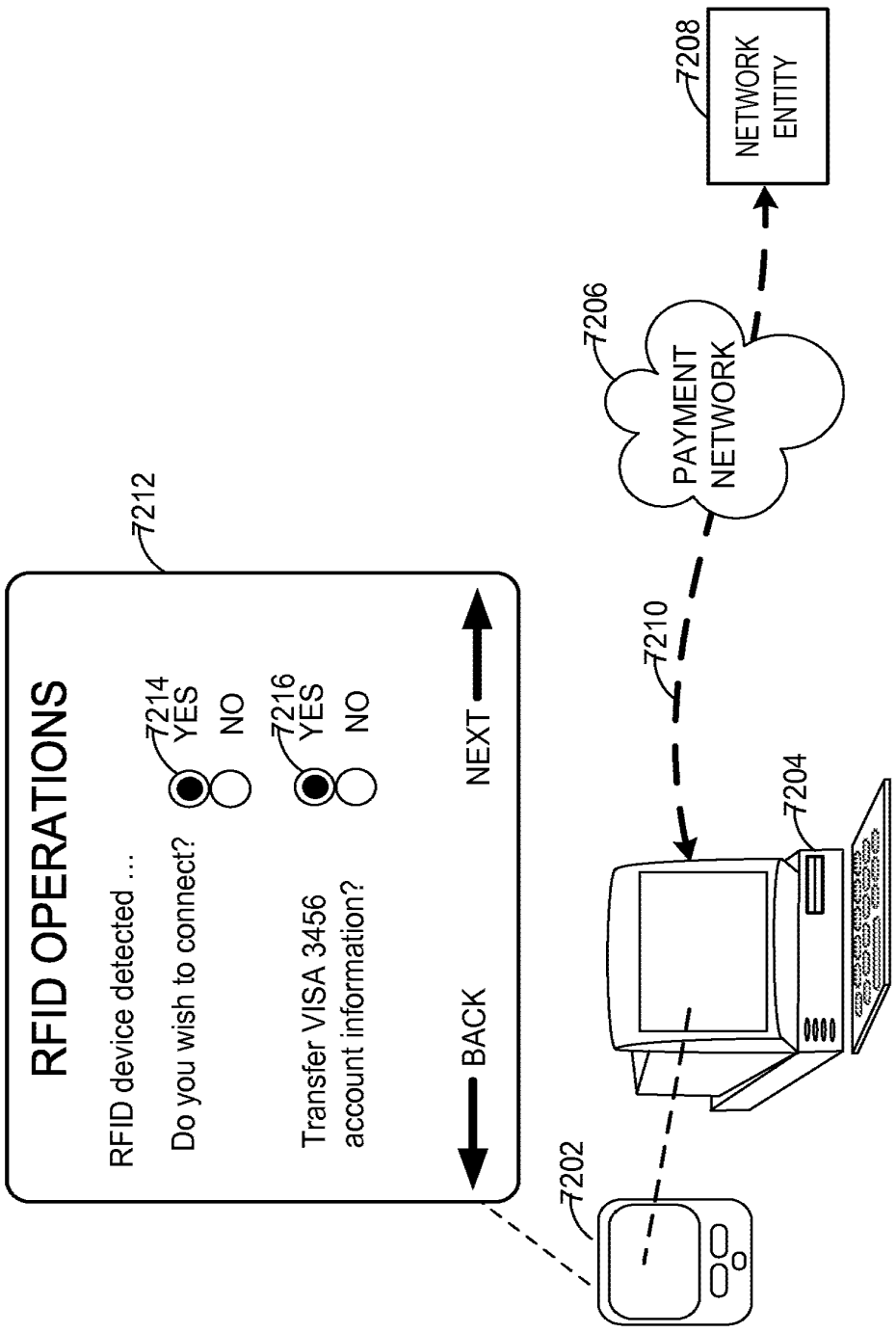


FIG. 72

IPR2025-01152
Apple EX1002 Page 1076

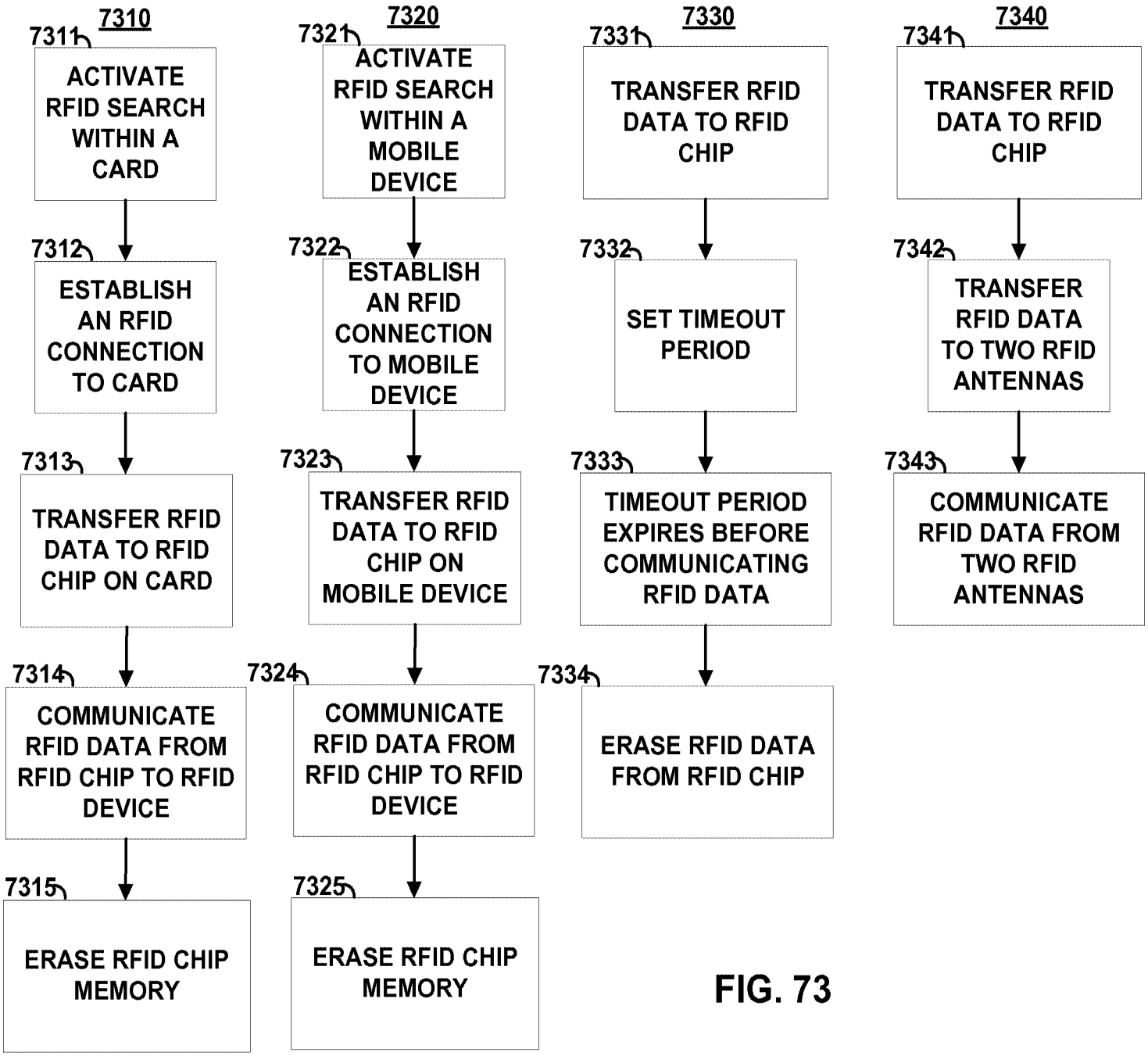


FIG. 73

IPR2025-01152
Apple EX1002 Page 1077

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.

IPR2025-01152
Apple EX1002 Page 1079

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.

IPR2025-01152
Apple EX1002 Page 1080

(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

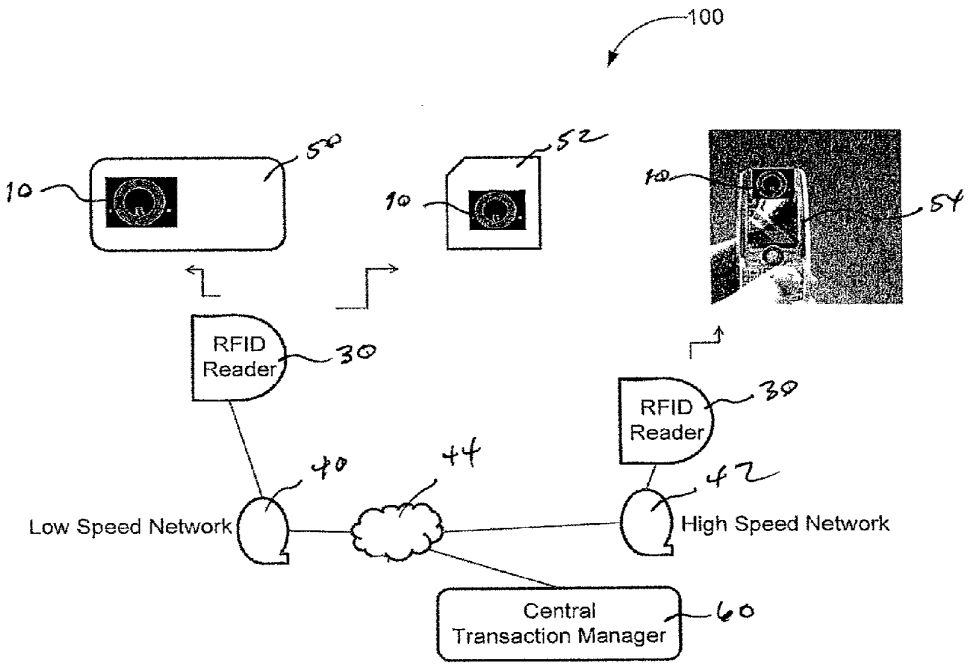


Figure 1

[Continued on next page]

WO 2010/043974 A1

IPR2025-01152
Apple EX1002 Page 1081

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.

IPR2025-01152
Apple EX1002 Page 1082

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

IPR2025-01152
Apple EX1002 Page 1083

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

IPR2025-01152
Apple EX1002 Page 1084

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

IPR2025-01152
Apple EX1002 Page 1085

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;

IPR2025-01152
Apple EX1002 Page 1086

[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

IPR2025-01152
Apple EX1002 Page 1087

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

IPR2025-01152
Apple EX1002 Page 1088

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

IPR2025-01152
Apple EX1002 Page 1089

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

IPR2025-01152
Apple EX1002 Page 1090

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.

IPR2025-01152
Apple EX1002 Page 1091

[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

IPR2025-01152
Apple EX1002 Page 1092

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

IPR2025-01152
Apple EX1002 Page 1093

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.

IPR2025-01152
Apple EX1002 Page 1094

[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,

IPR2025-01152
Apple EX1002 Page 1095

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

IPR2025-01152
Apple EX1002 Page 1096

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

IPR2025-01152
Apple EX1002 Page 1097

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.

IPR2025-01152
Apple EX1002 Page 1098

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.

IPR2025-01152
Apple EX1002 Page 1099

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.

IPR2025-01152
Apple EX1002 Page 1100

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

IPR2025-01152
Apple EX1002 Page 1101

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;

IPR2025-01152
Apple EX1002 Page 1102

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.

IPR2025-01152
Apple EX1002 Page 1103

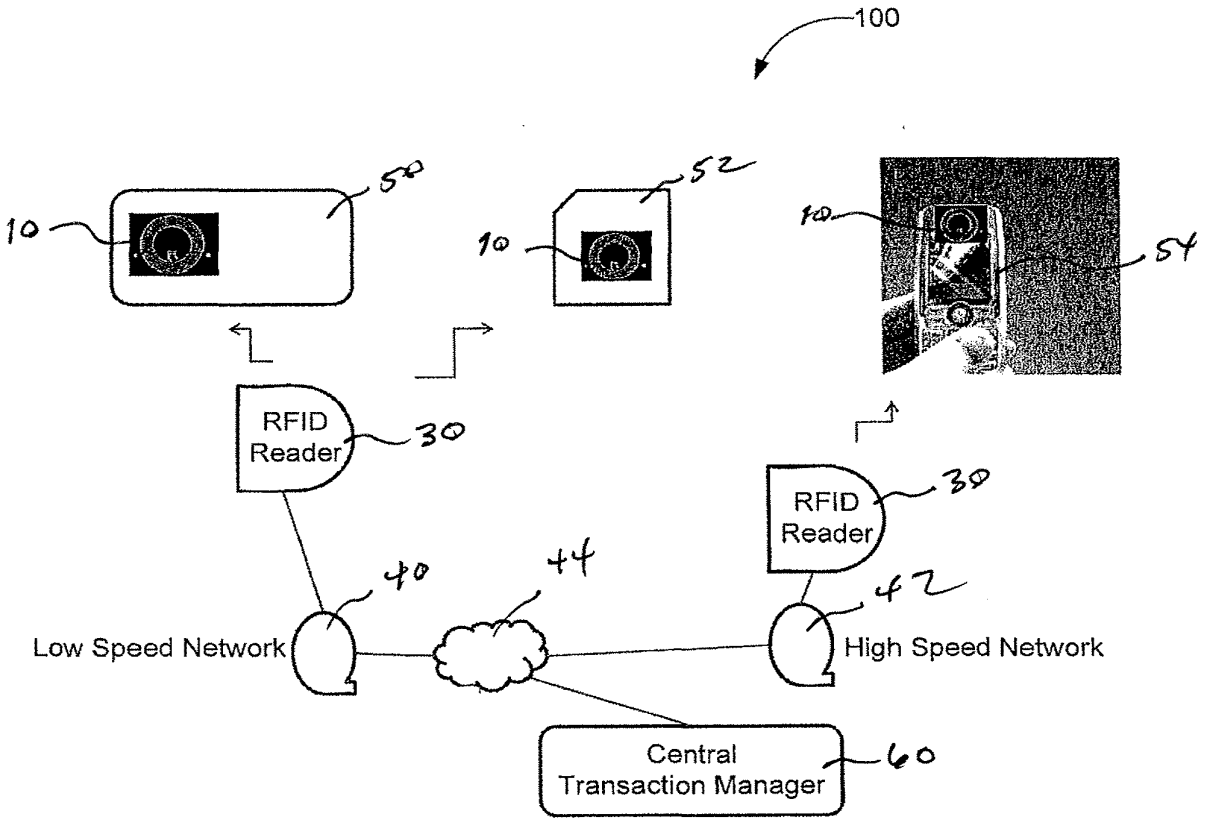

100
10
50
10
52
10
54
RFID Reader
30
RFID Reader
30
40
44
42
Low Speed Network
High Speed Network
Central Transaction Manager
60

Figure 1

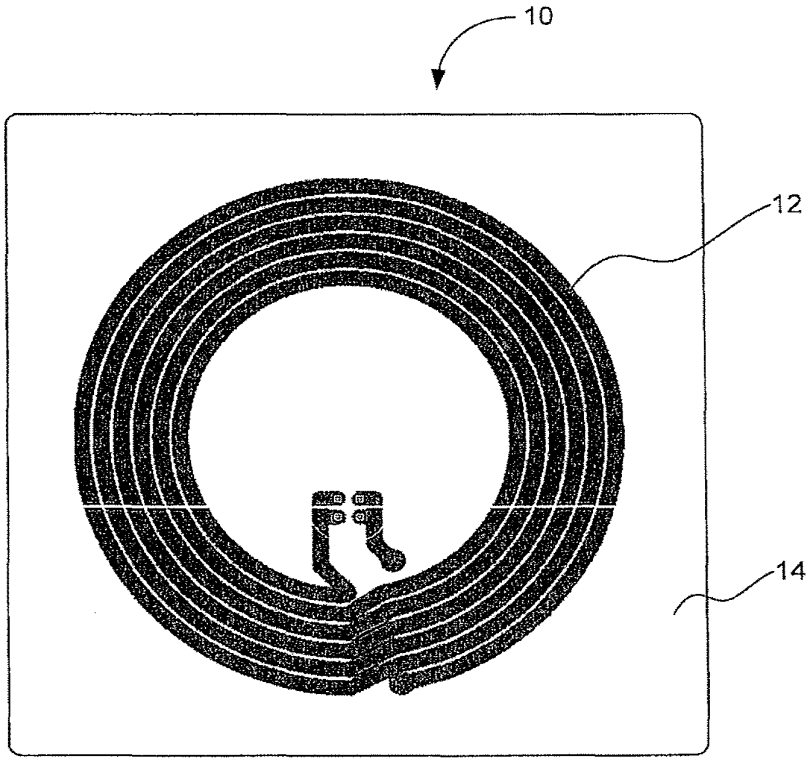


Figure 2

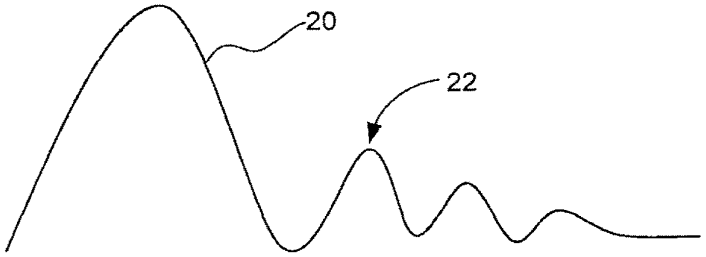


Figure 3

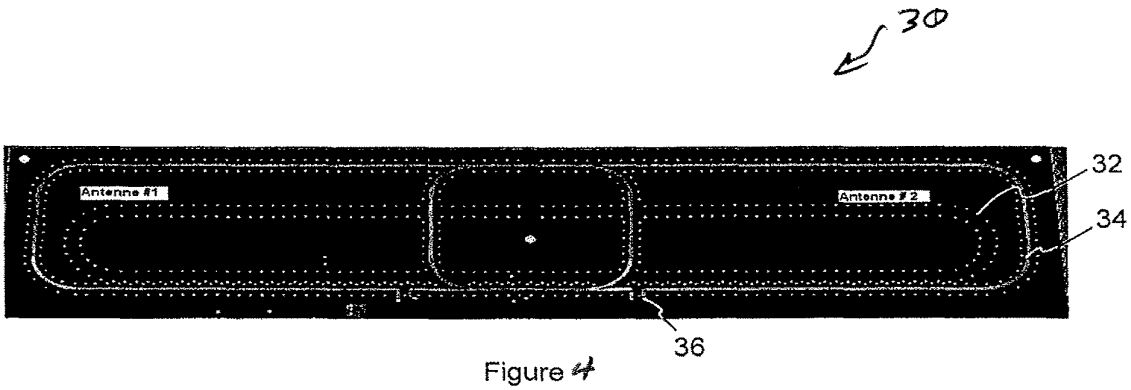


Figure 4

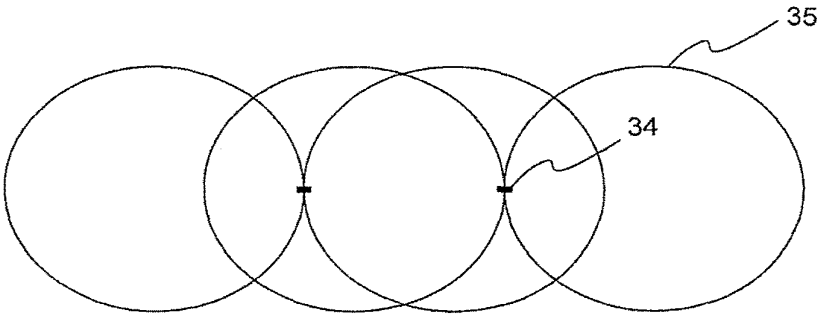


Figure 5A

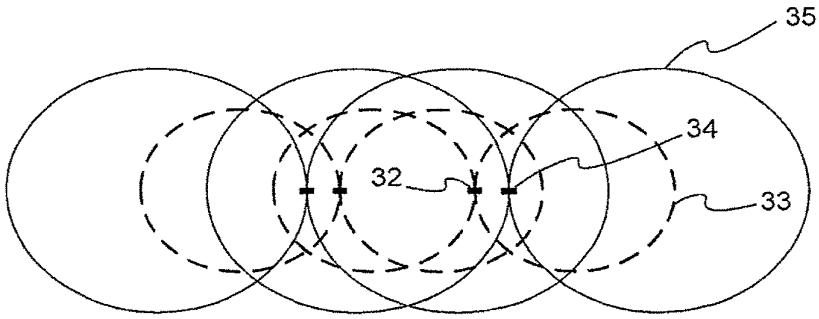


Figure 5B

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

IPR2025-01152
Apple EX1002 Page 1107

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

IPR2025-01152
Apple EX1002 Page 1108

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)

IPR2025-01152
Apple EX1002 Page 1109

(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

IPR2025-01152
Apple EX1002 Page 1110

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.

IPR2025-01152
Apple EX1002 Page 1111

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.

IPR2025-01152
Apple EX1002 Page 1112

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

(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

(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**

(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.

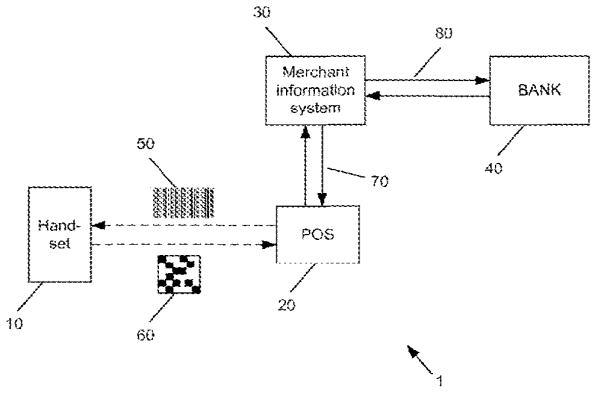


Fig. 1

GB 2478712 A

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

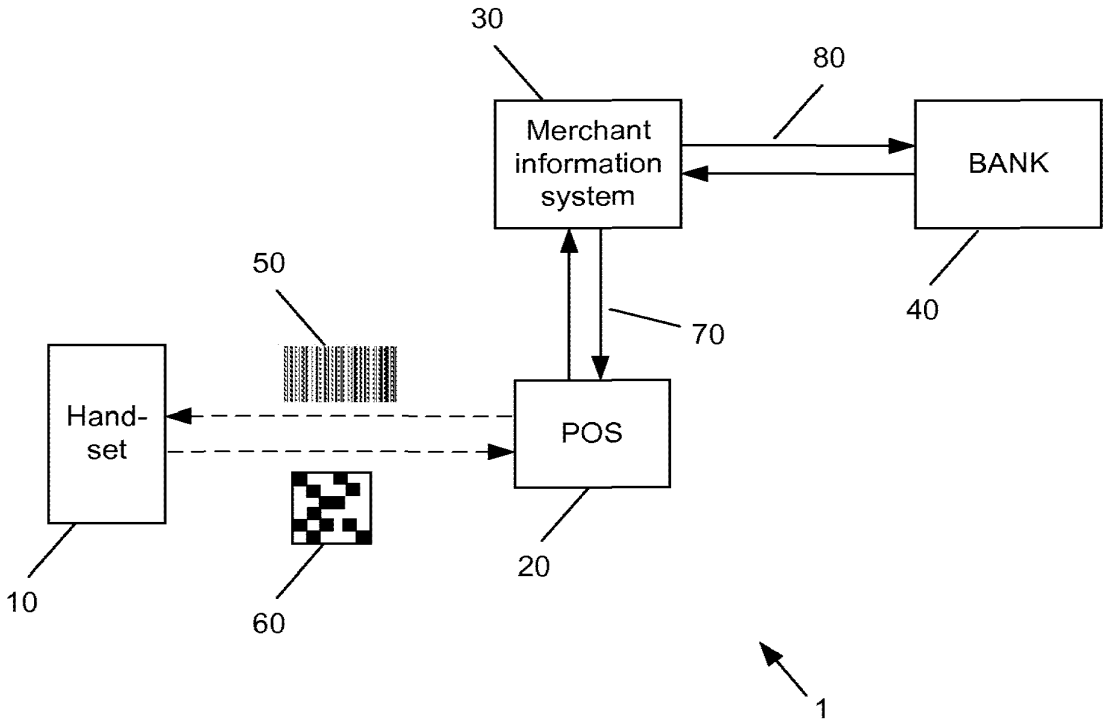

30
80
Merchant information system
BANK
50
40
70
Hand-set
POS
10
60
20
1

Fig. 1

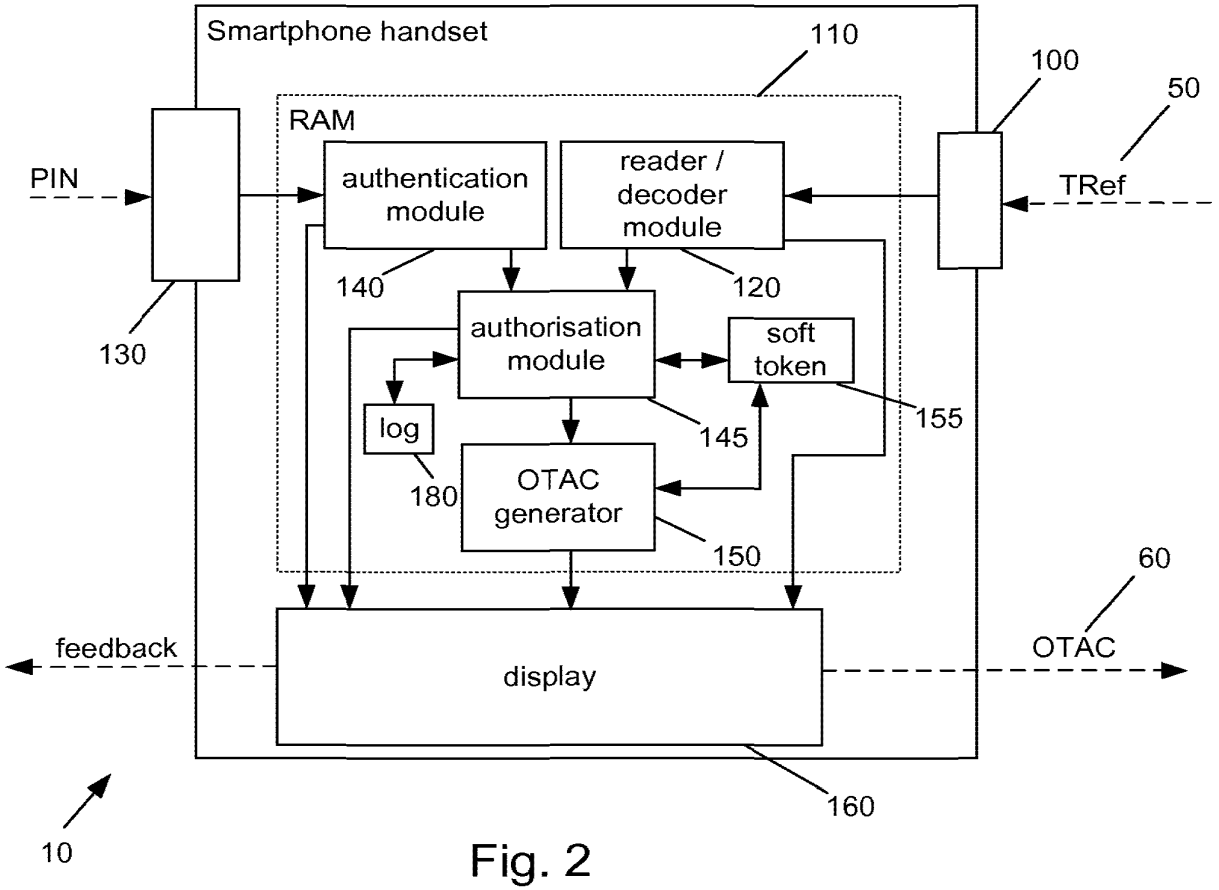

Smartphone handset
110
100
50
RAM
PIN
authentication module
reader / decoder module
TRef
140
120
130
authorisation module
soft token
log
155
145
180
OTAC generator
150
60
feedback
display
OTAC
160
10

Fig. 2

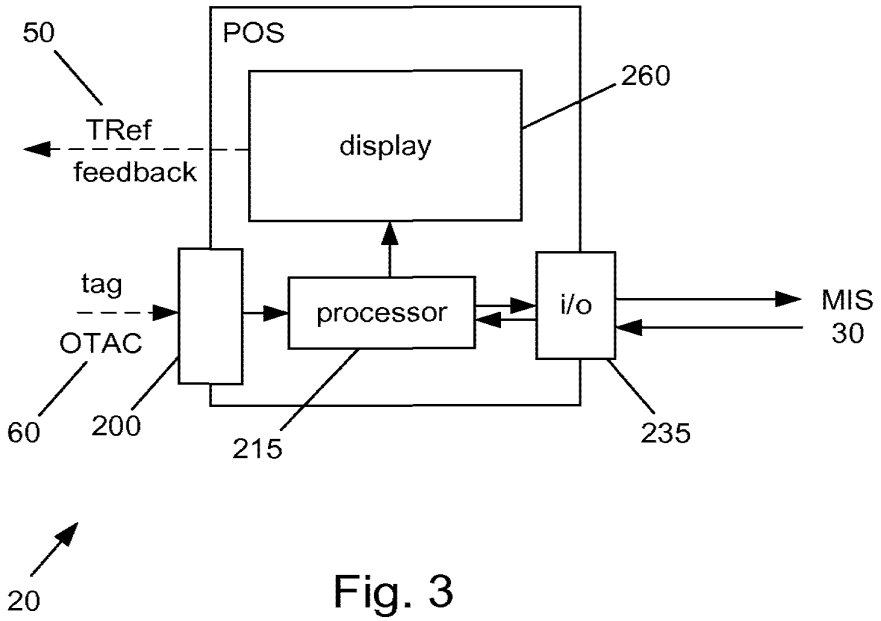

50
POS
260
TRef
feedback
display
tag
processor
i/o
MIS
30
OTAC
60
200
215
235
20

Fig. 3

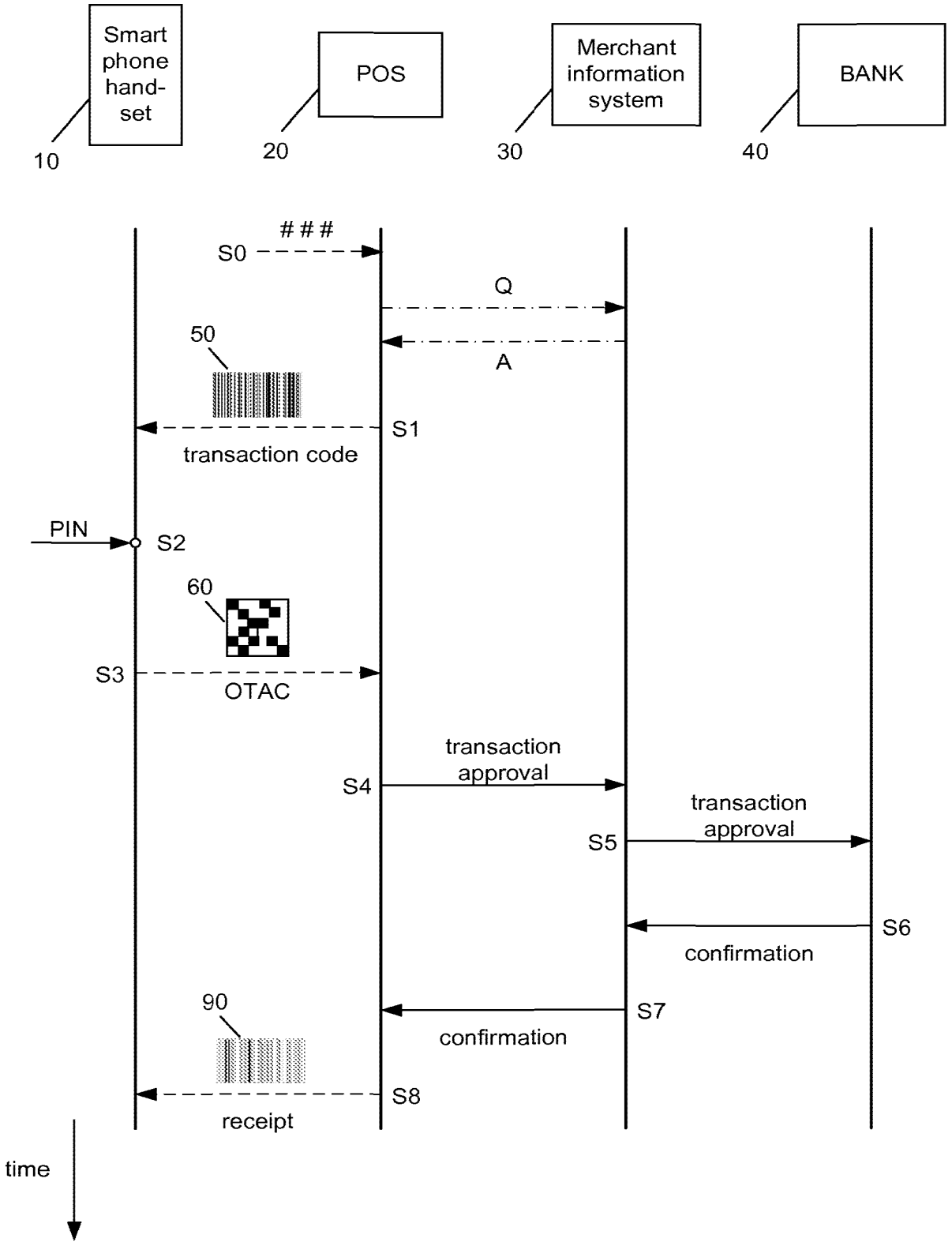
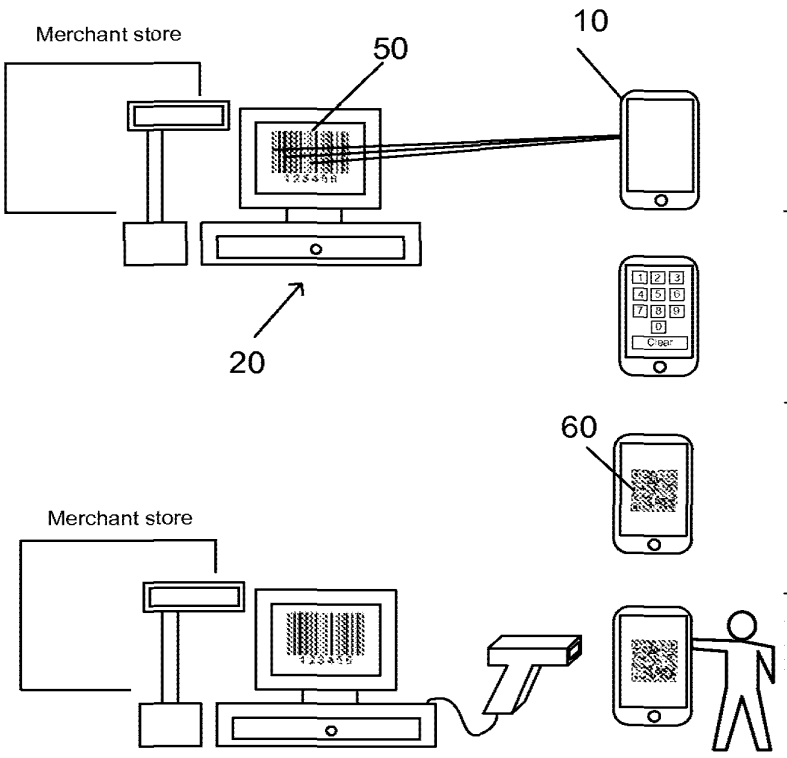

Smart phone hand-set
10
POS
20
Merchant information system
30
BANK
40
###
S0
Q
A
50
S1
transaction code
PIN
S2
60
S3
OTAC
transaction approval
S4
transaction approval
S5
S6
confirmation
90
S7
confirmation
S8
receipt
time

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

Intellectual Property Office is an operating name of the Patent Office

(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).

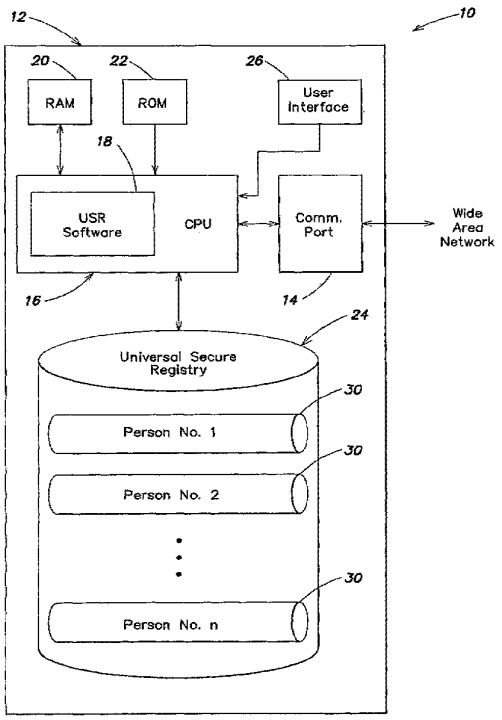
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, 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.

IPR2025-01152
Apple EX1002 Page 1177

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

IPR2025-01152
Apple EX1002 Page 1181

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

IPR2025-01152
Apple EX1002 Page 1184

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.

IPR2025-01152
Apple EX1002 Page 1191

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

IPR2025-01152
Apple EX1002 Page 1197

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.

IPR2025-01152
Apple EX1002 Page 1199

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

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.

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

IPR2025-01152
Apple EX1002 Page 1223

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.

IPR2025-01152
Apple EX1002 Page 1224

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.

IPR2025-01152
Apple EX1002 Page 1225

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.

IPR2025-01152
Apple EX1002 Page 1226

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:

IPR2025-01152
Apple EX1002 Page 1227

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:

IPR2025-01152
Apple EX1002 Page 1228

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;

IPR2025-01152
Apple EX1002 Page 1229

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.

IPR2025-01152
Apple EX1002 Page 1230

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.

IPR2025-01152
Apple EX1002 Page 1231

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

IPR2025-01152
Apple EX1002 Page 1232

system, and enabling or preventing with the second device the occurrence of the event based on the validation information and the additional information.

IPR2025-01152
Apple EX1002 Page 1233

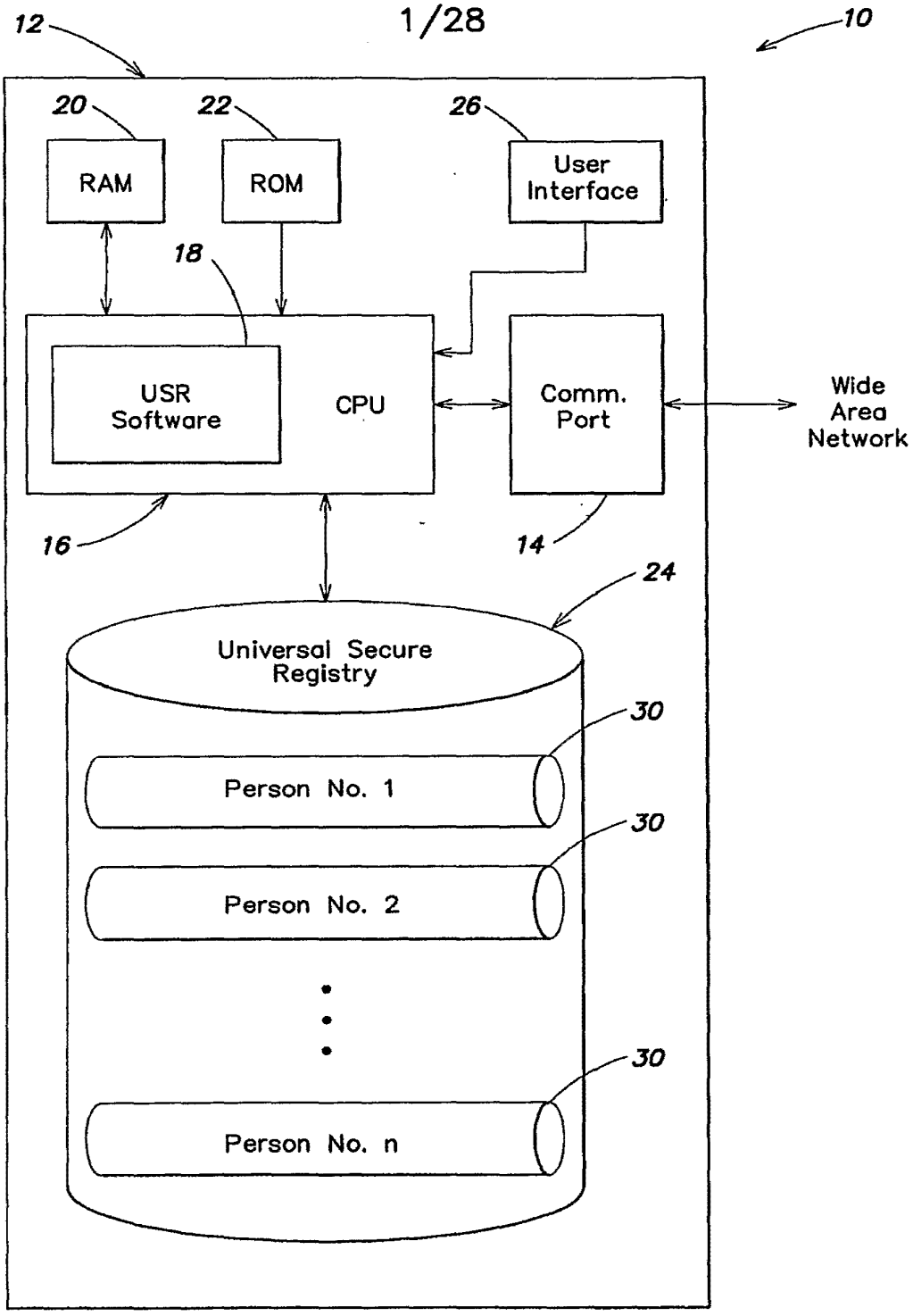


FIG. 1

IPR2025-01152
Apple EX1002 Page 1234

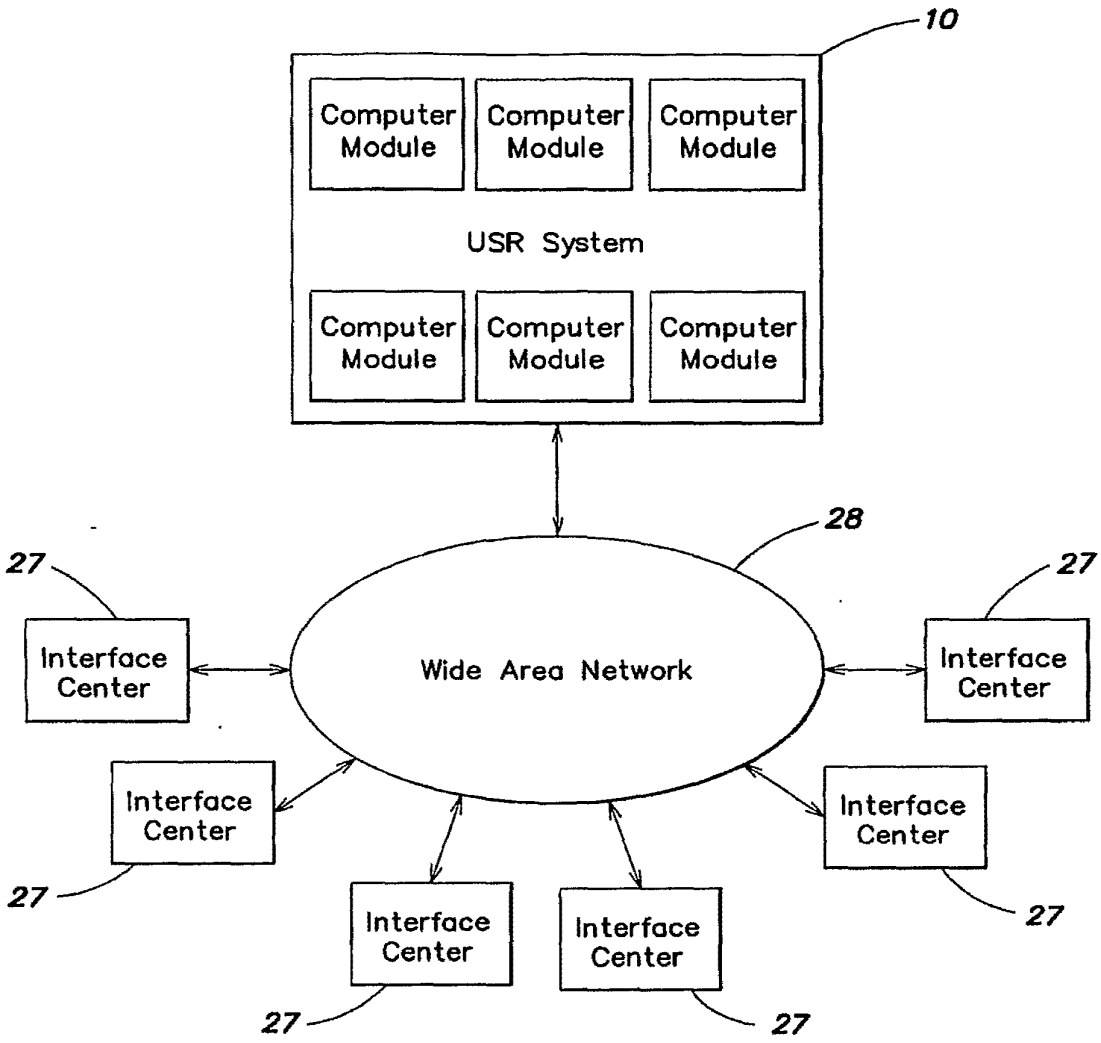


FIG. 2

IPR2025-01152
Apple EX1002 Page 1235

FIG. 3

SUBSTITUTE SHEET (RULE 26)

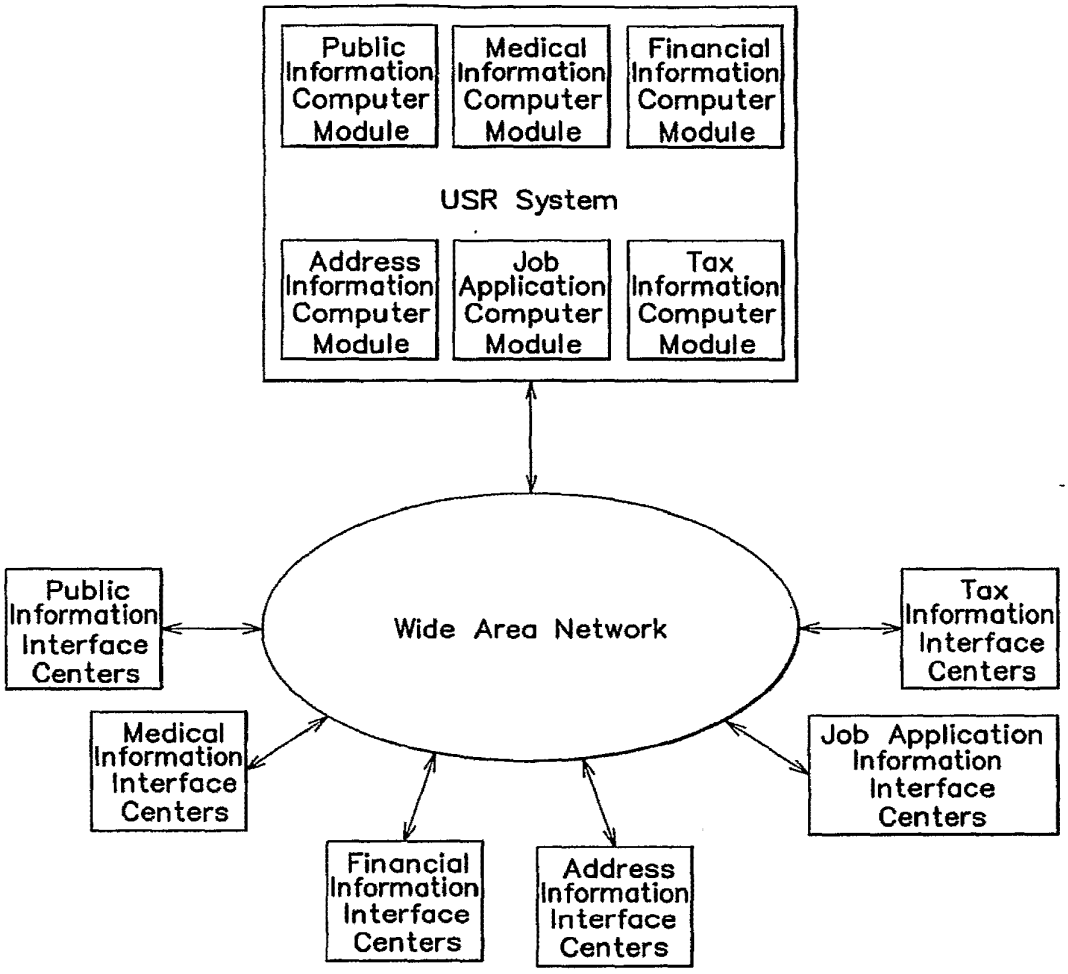


FIG. 4

IPR2025-01152
Apple EX1002 Page 1237

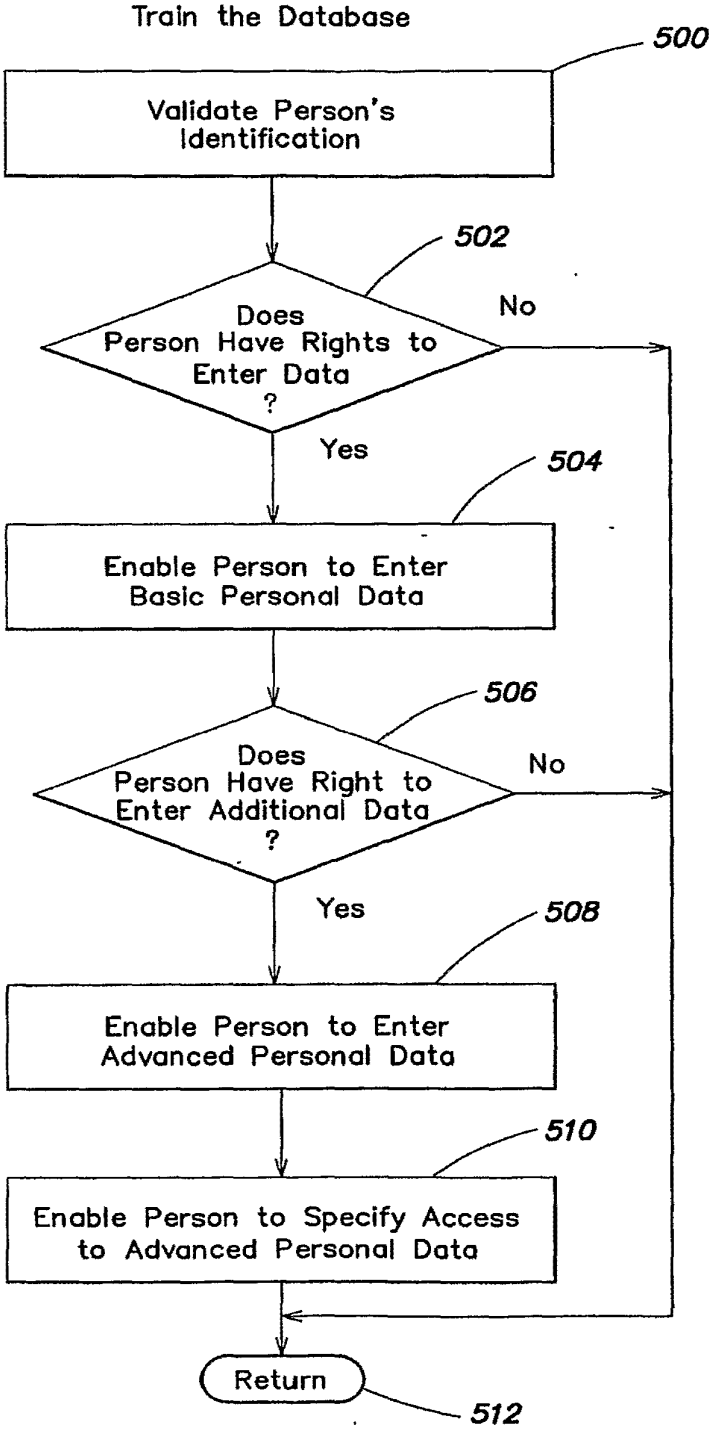


FIG. 5

IPR2025-01152
Apple EX1002 Page 1238

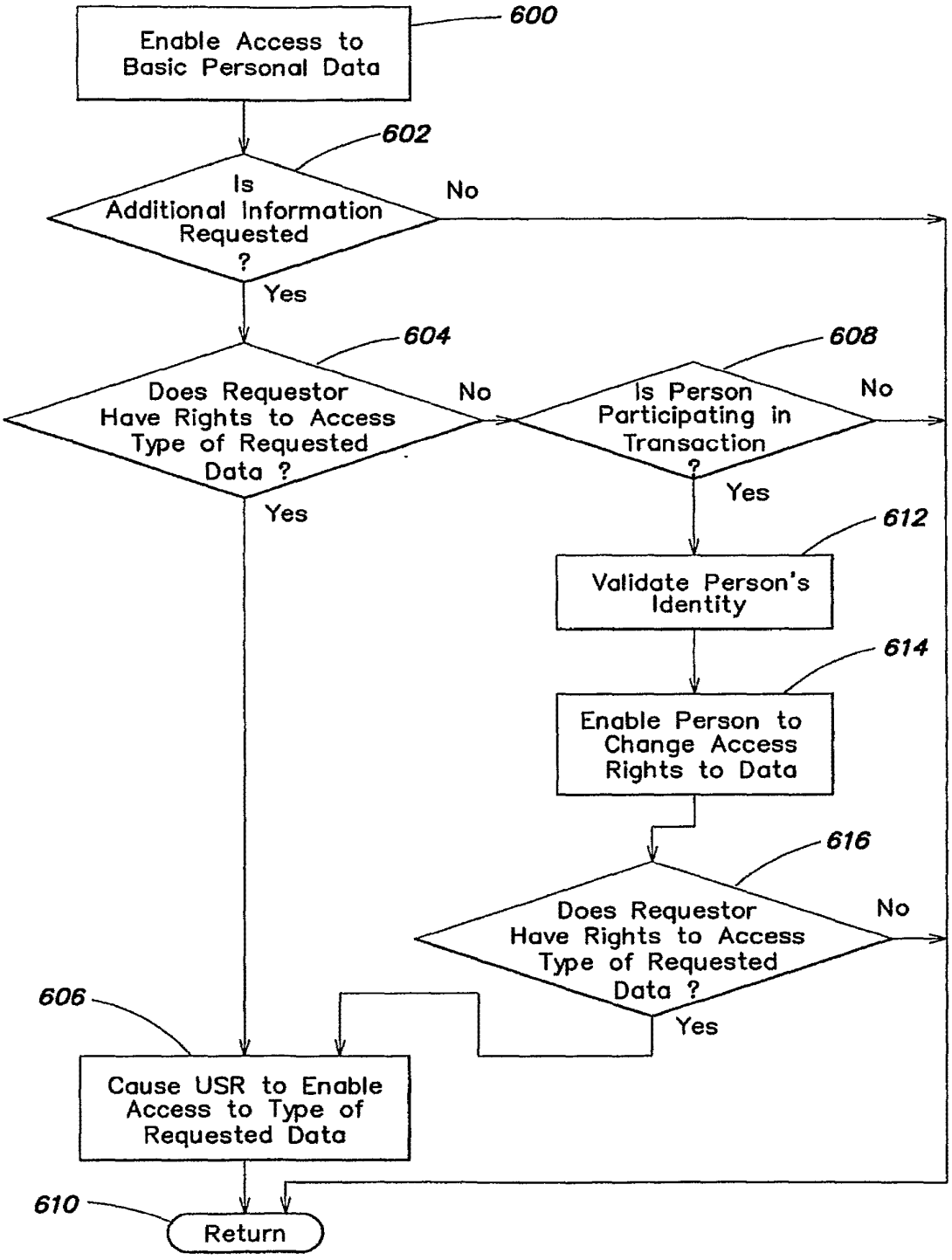


FIG. 6

IPR2025-01152
Apple EX1002 Page 1239

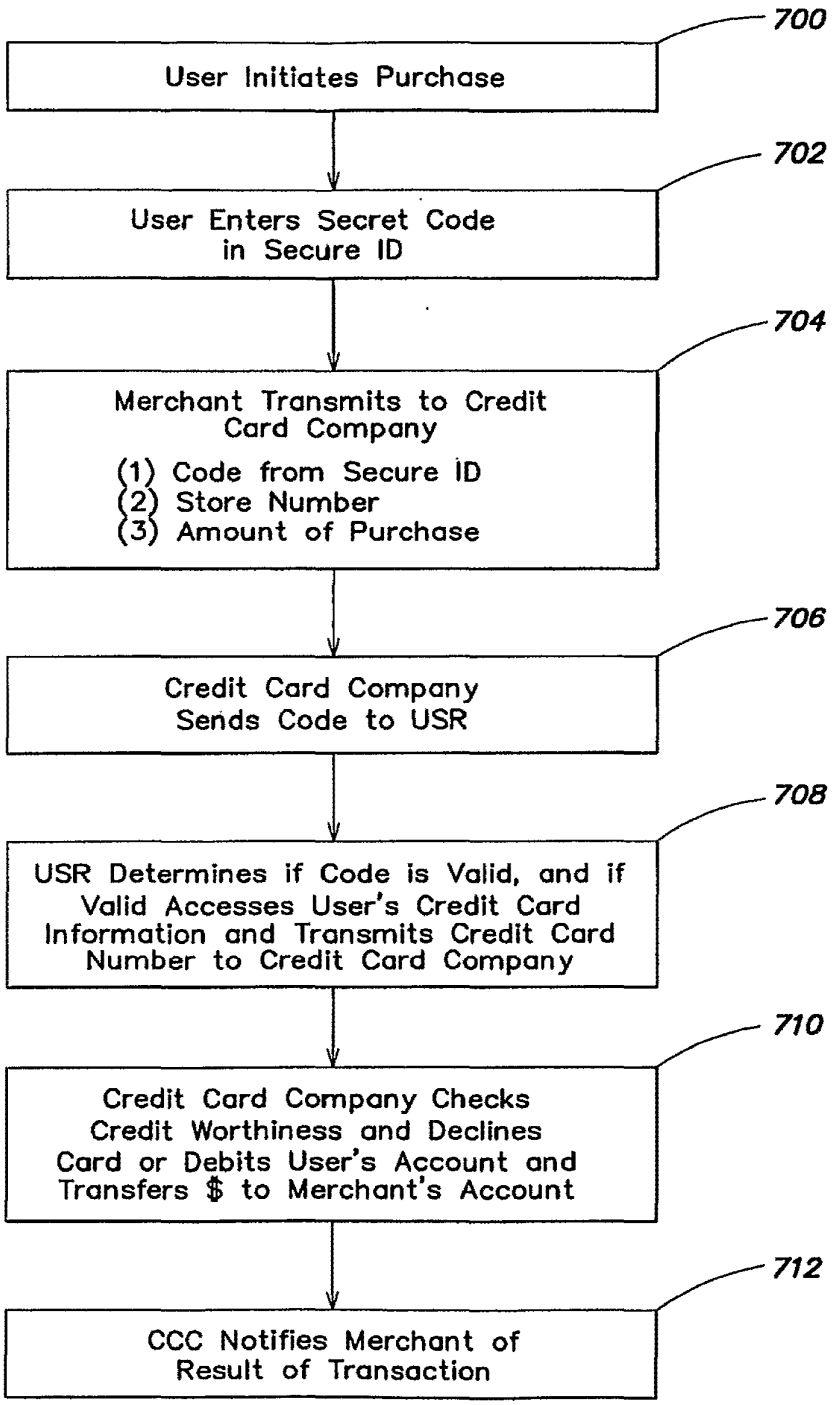


FIG. 7

IPR2025-01152
Apple EX1002 Page 1240

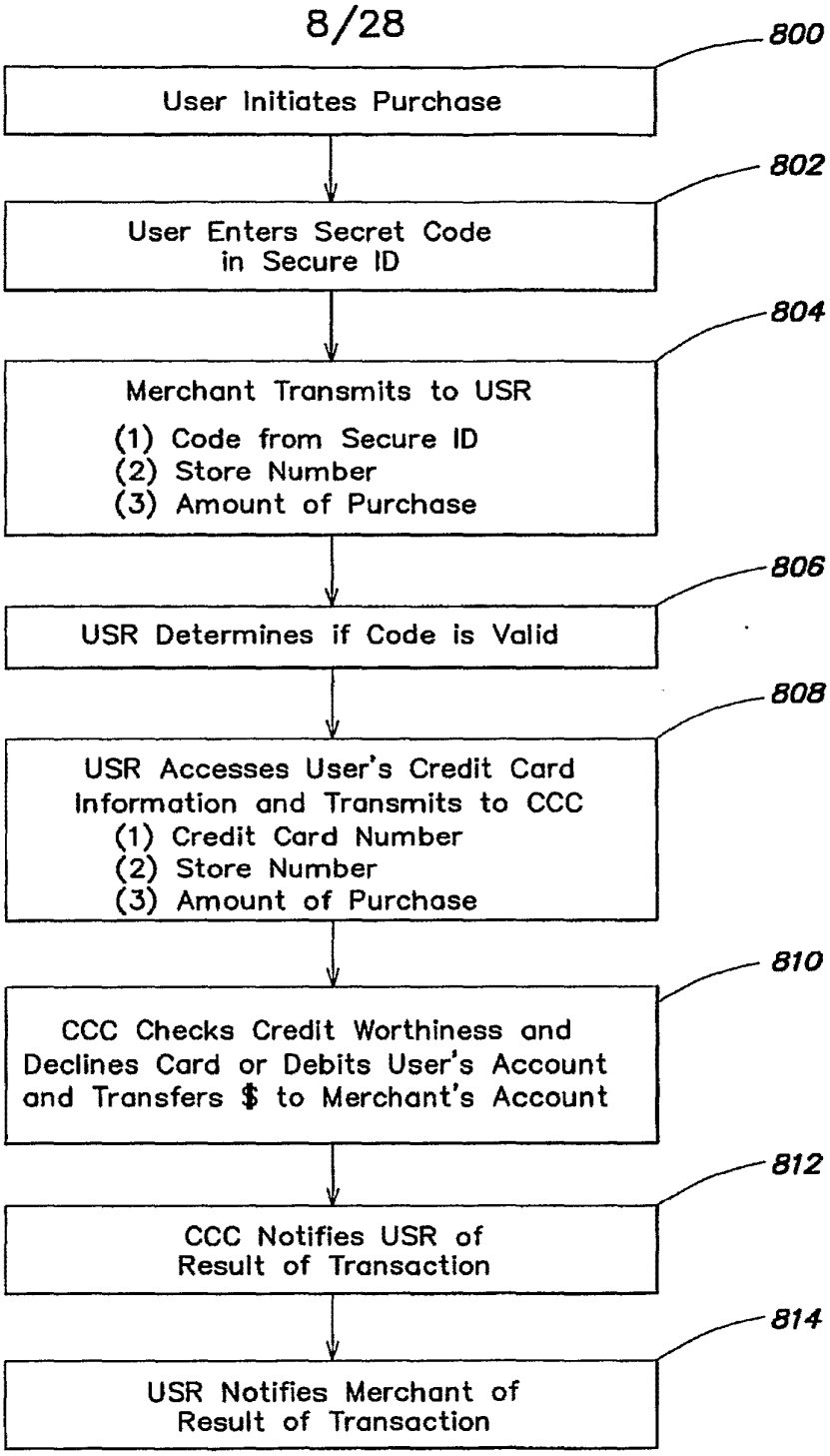


FIG. 8

IPR2025-01152
Apple EX1002 Page 1241

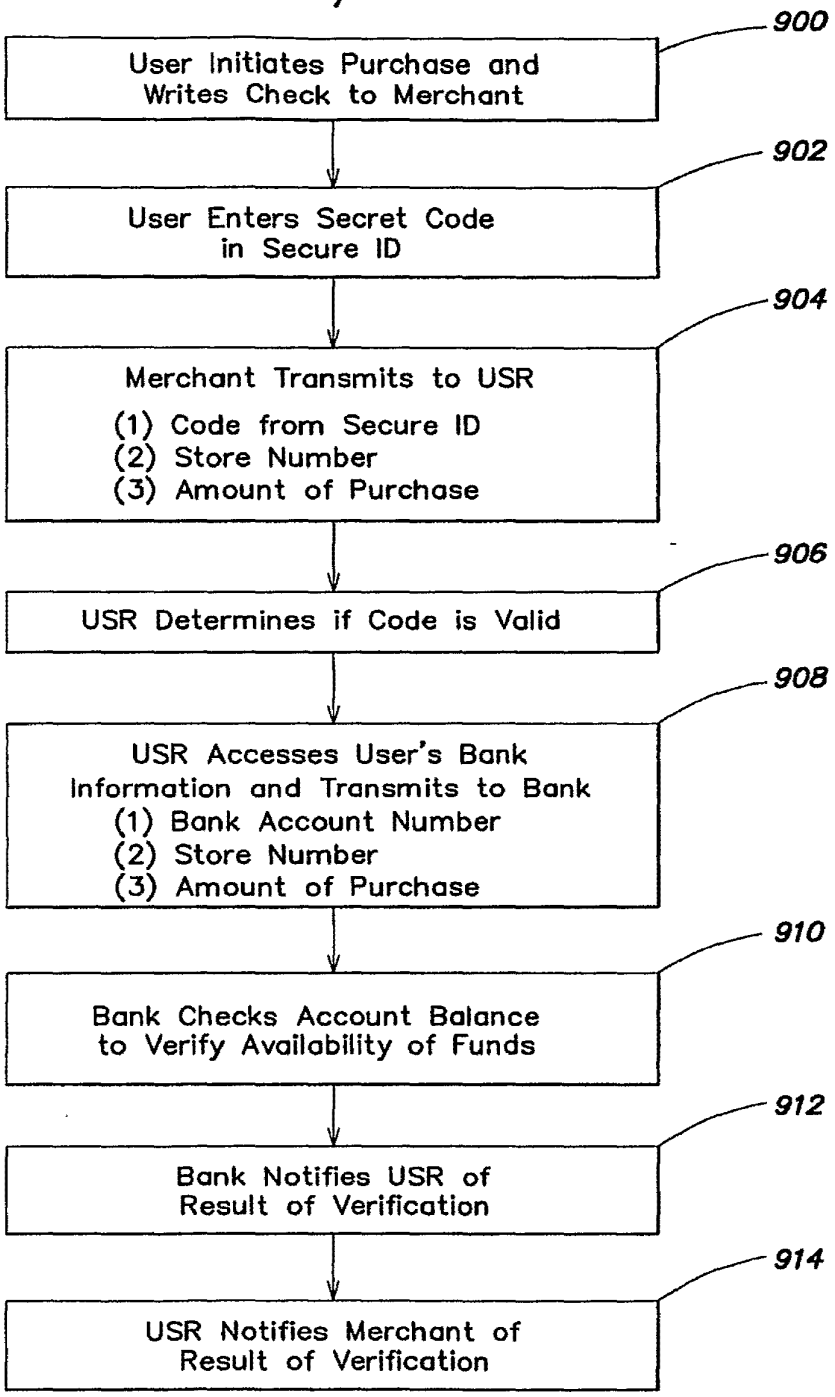


FIG. 9

IPR2025-01152
Apple EX1002 Page 1242

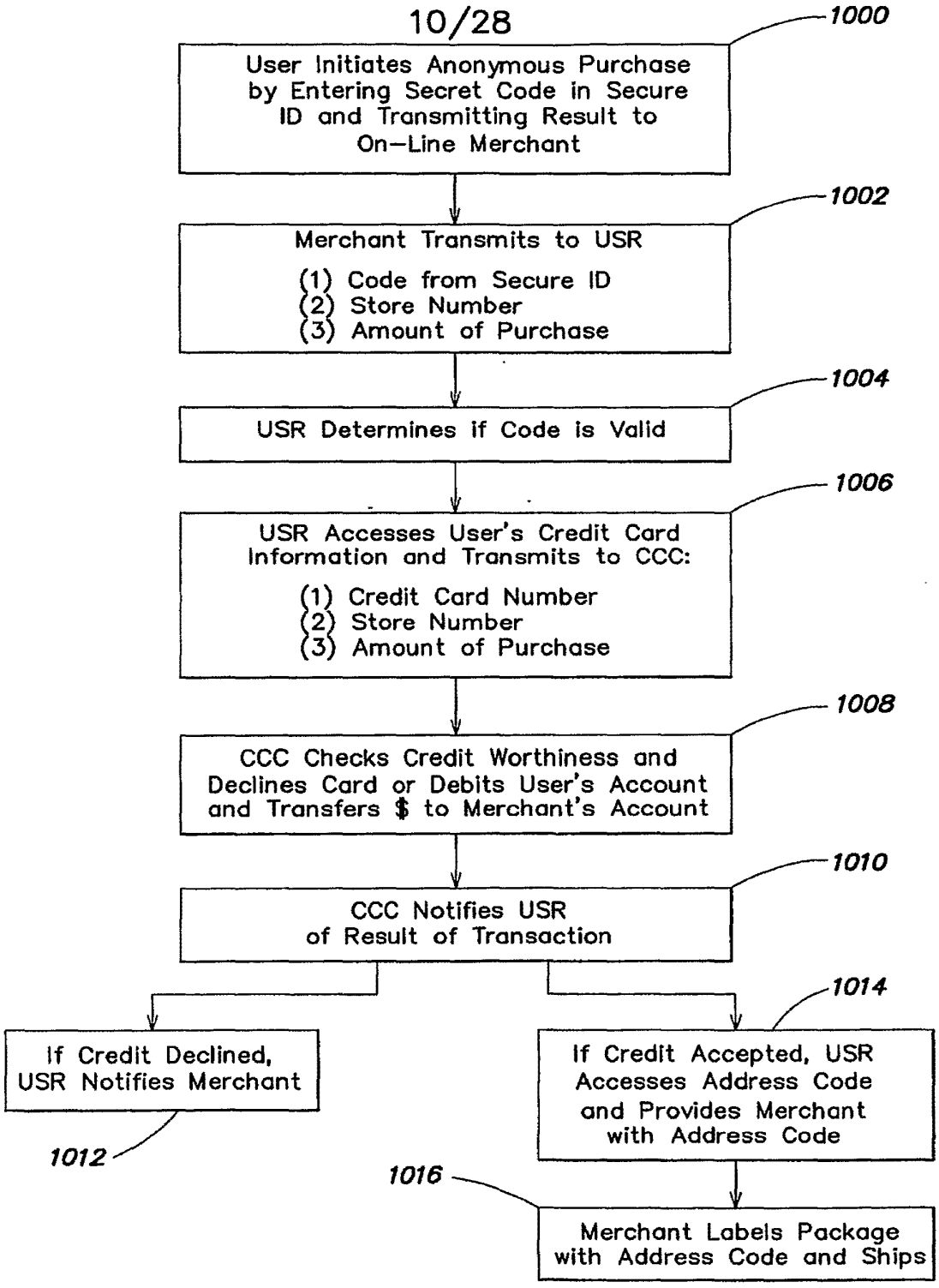


FIG. 10

IPR2025-01152
Apple EX1002 Page 1243

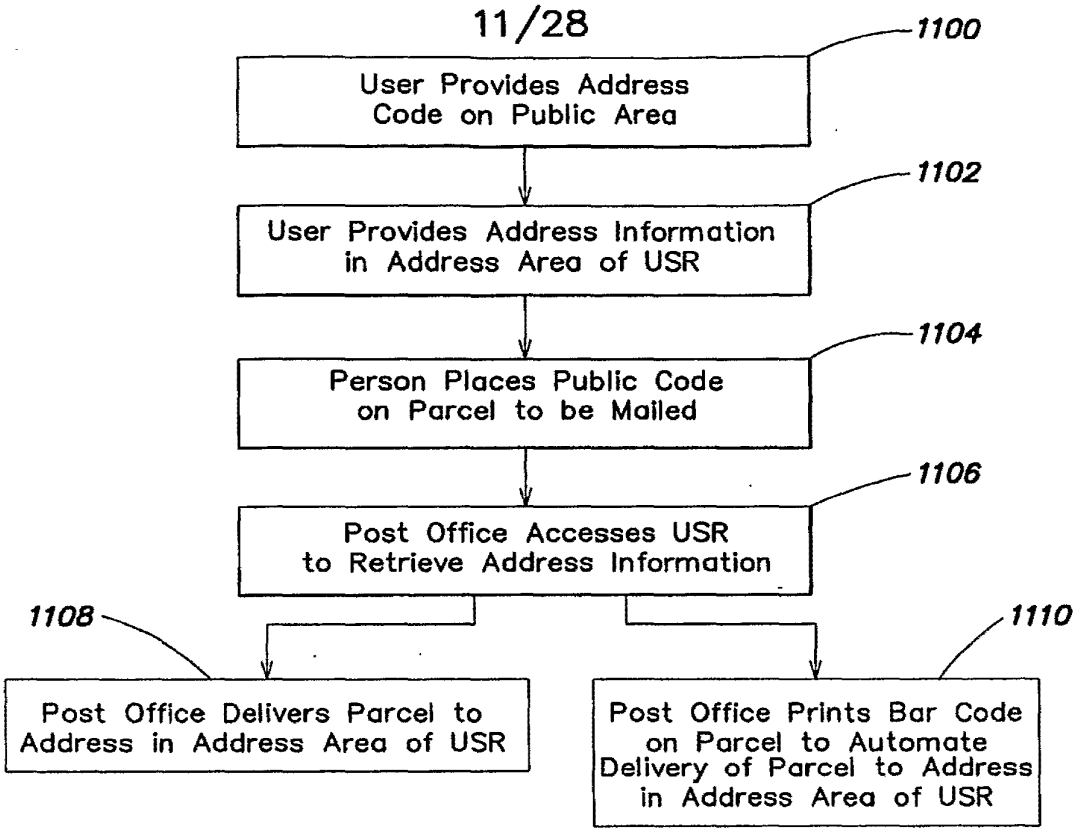


FIG. 11

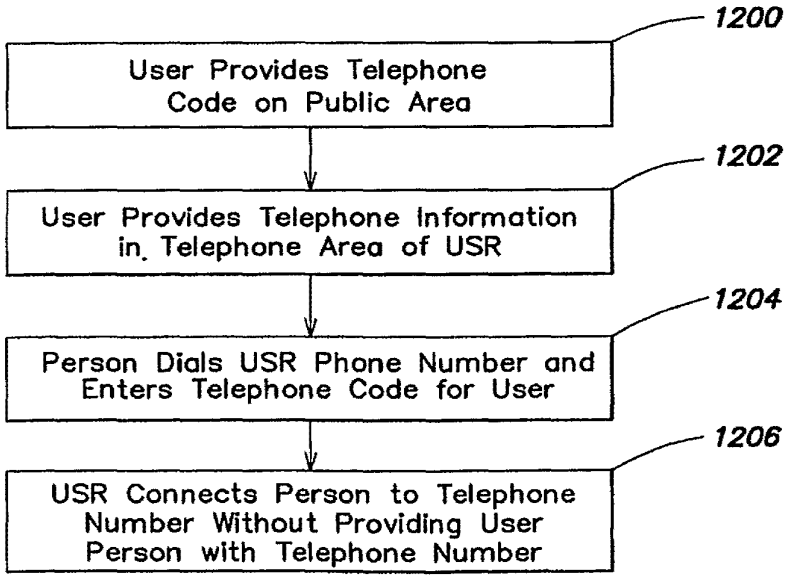


FIG. 12

IPR2025-01152
Apple EX1002 Page 1244

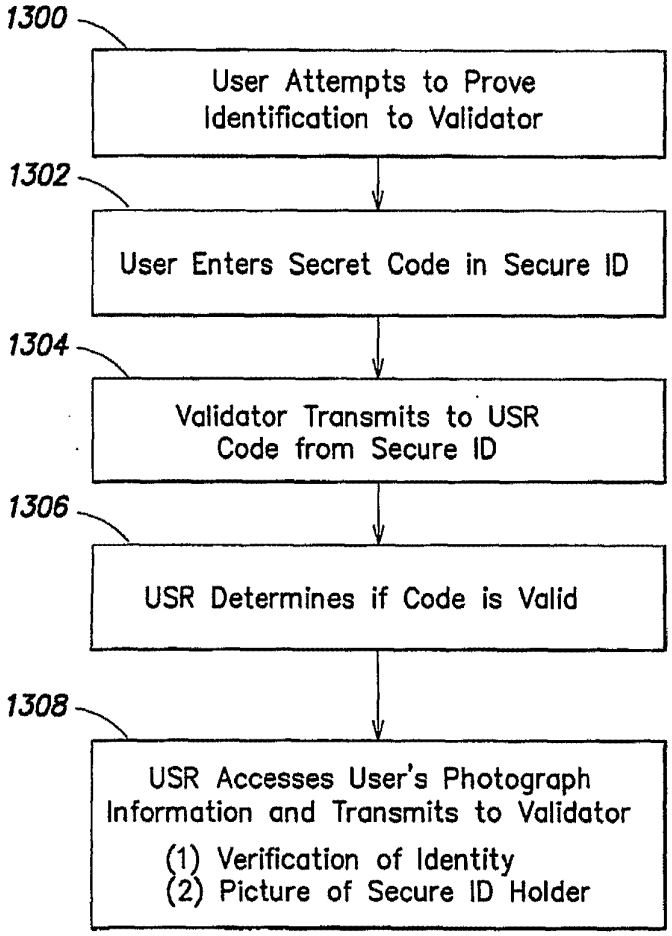


FIG. 13

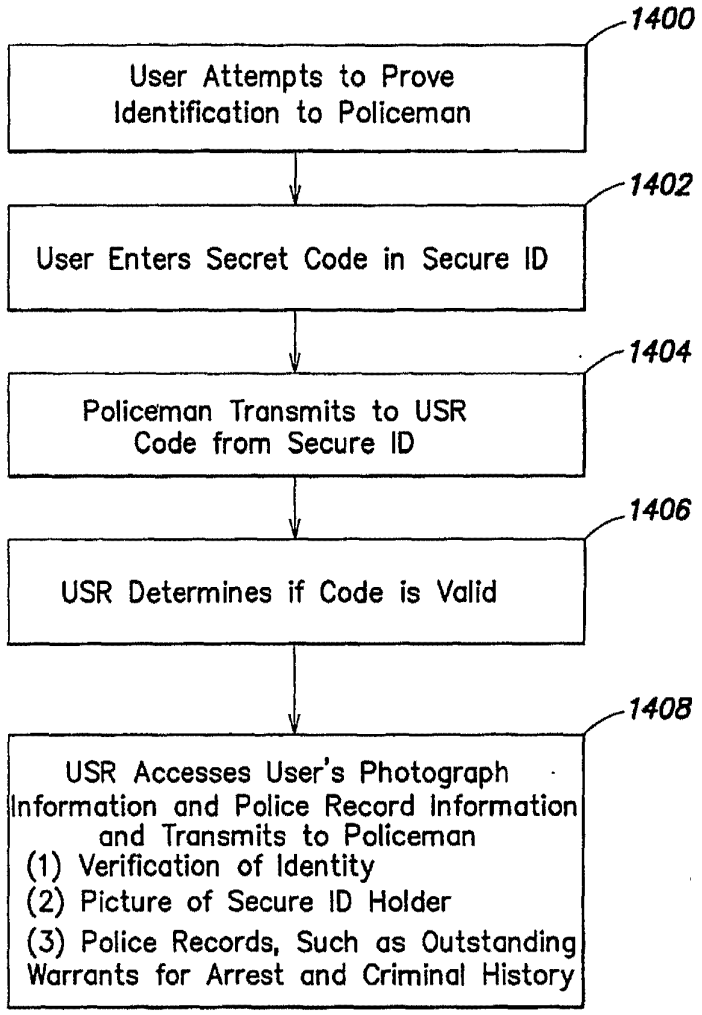


FIG. 14

IPR2025-01152
Apple EX1002 Page 1245

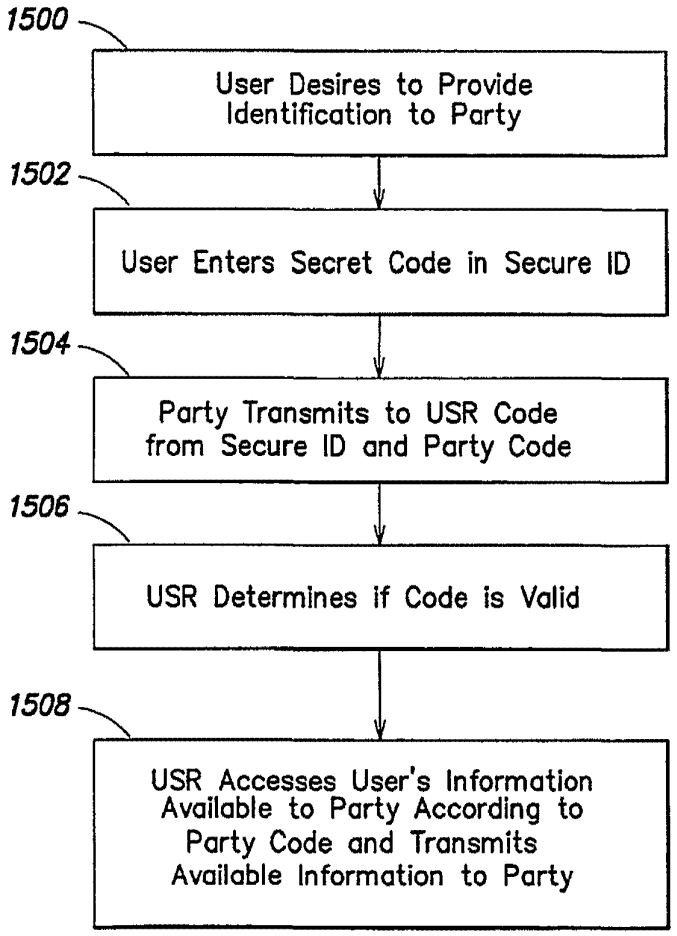


FIG. 15

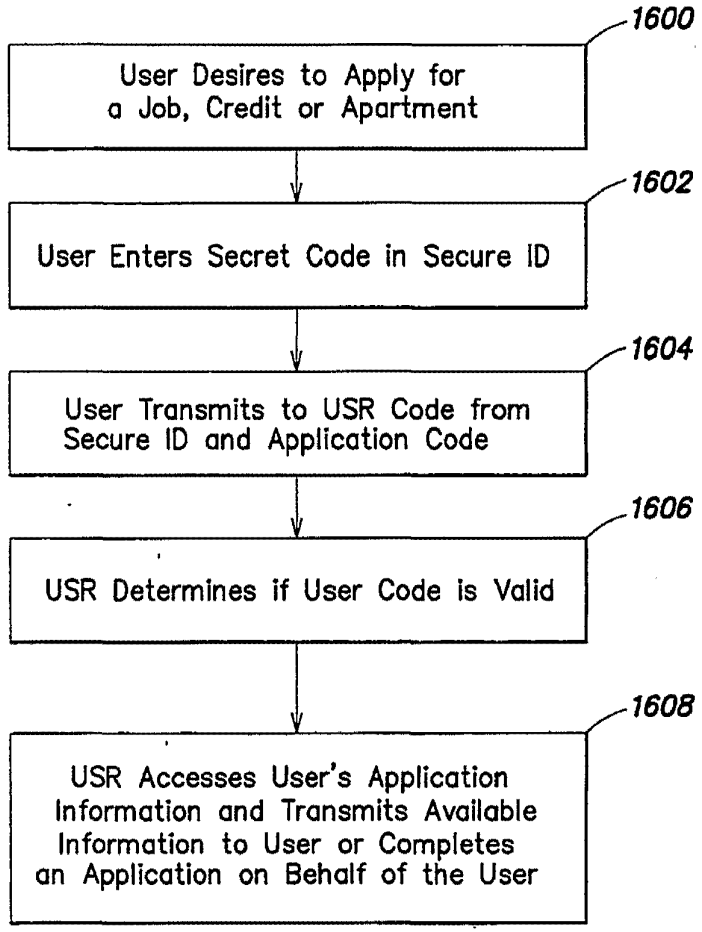


FIG. 16

IPR2025-01152
Apple EX1002 Page 1246

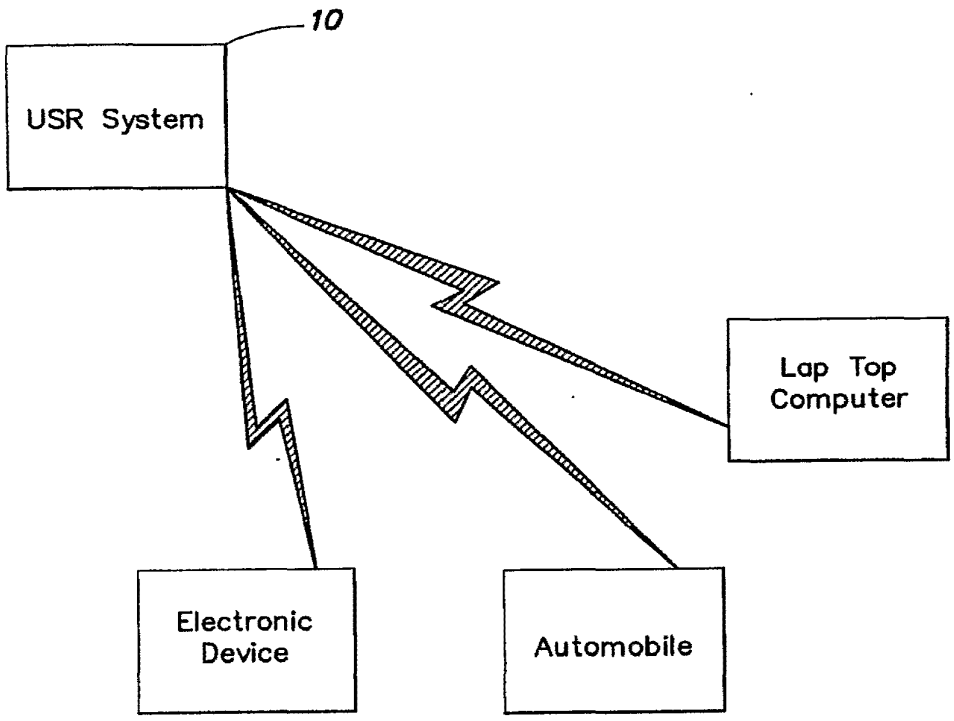


FIG. 17

IPR2025-01152
Apple EX1002 Page 1247

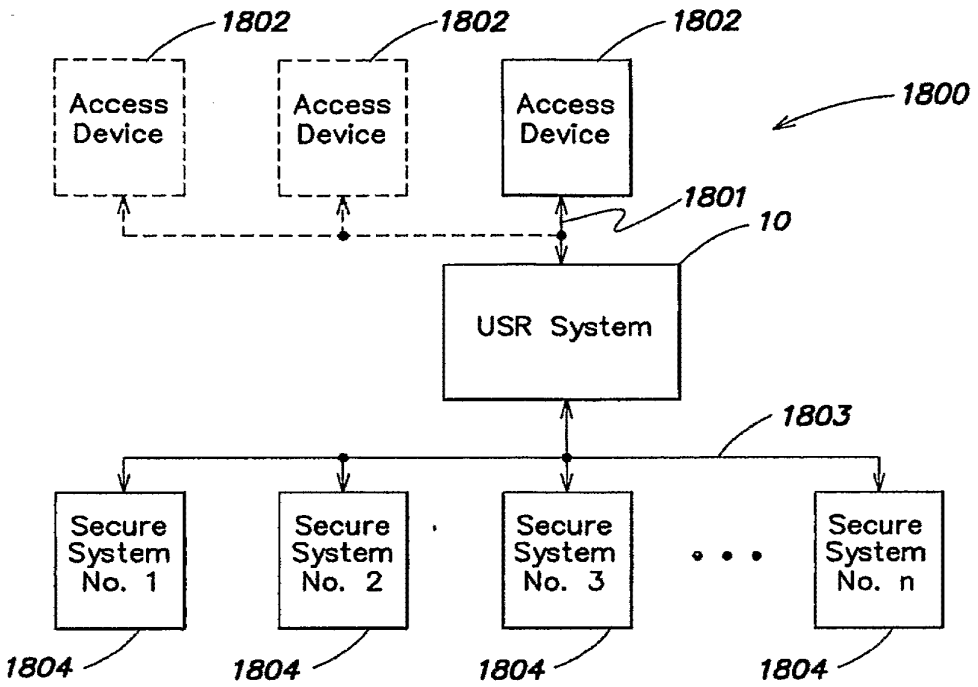


FIG. 18A

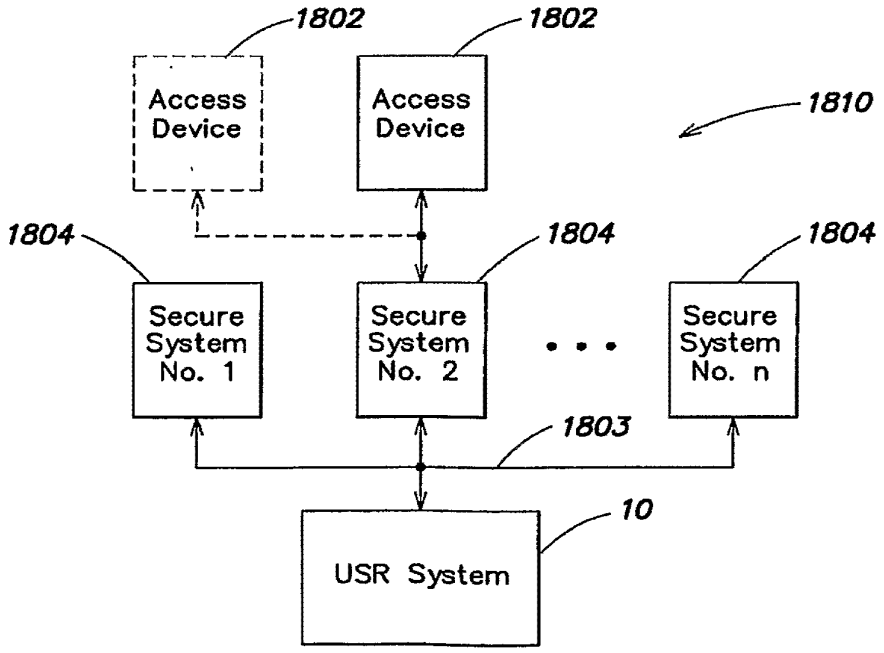


FIG. 18B

IPR2025-01152
Apple EX1002 Page 1248

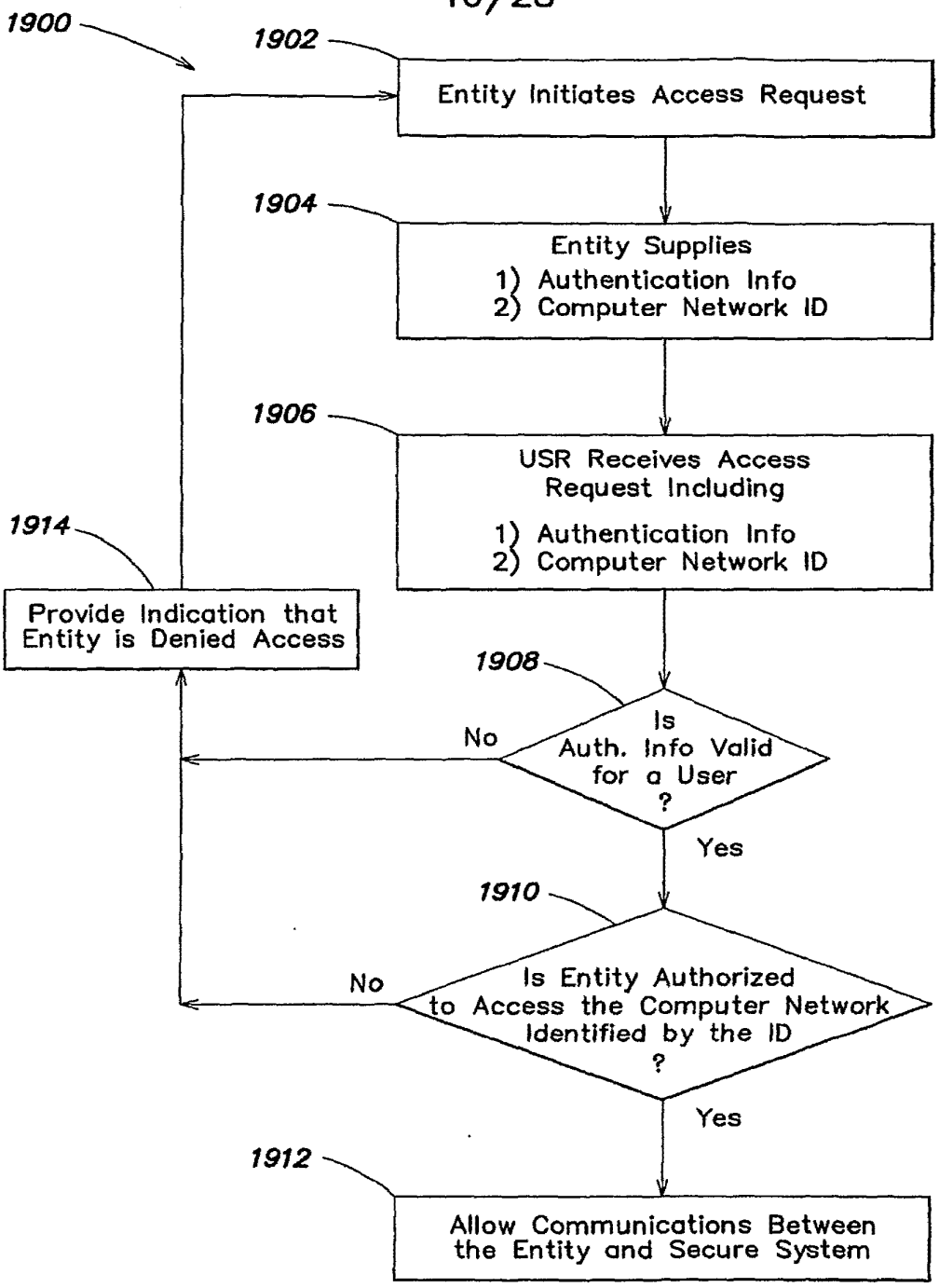


FIG. 19

IPR2025-01152
Apple EX1002 Page 1249

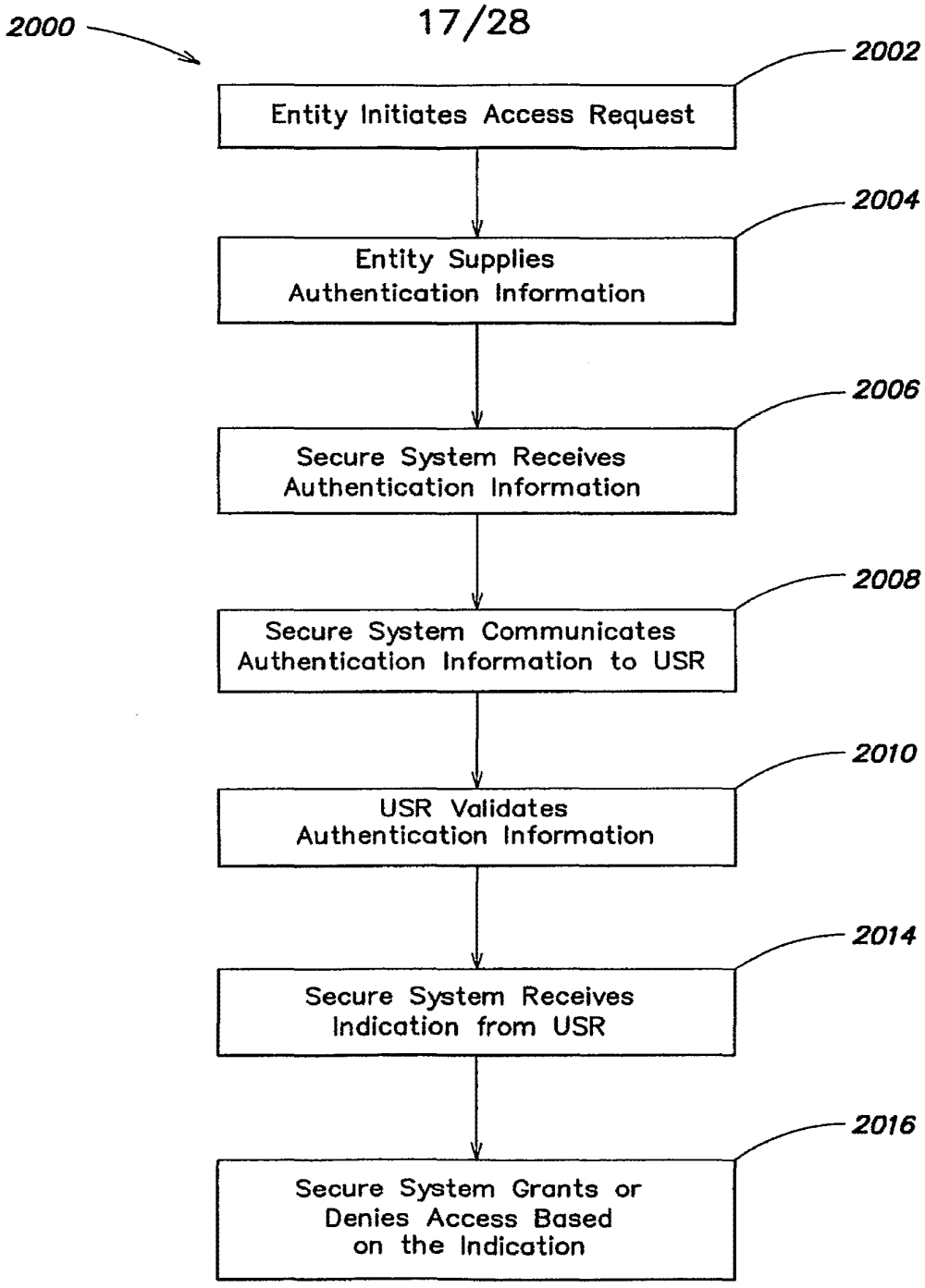


FIG. 20

IPR2025-01152
Apple EX1002 Page 1250

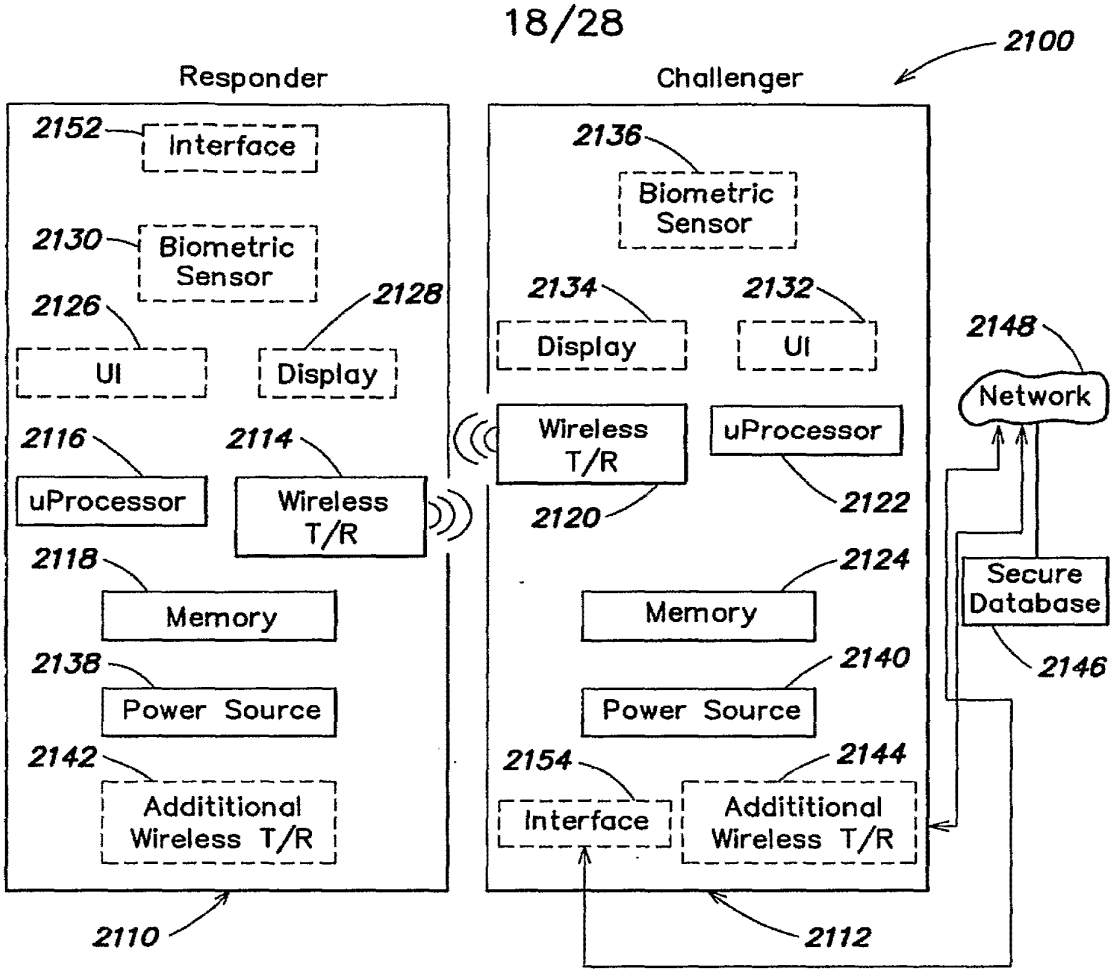


FIG. 21

IPR2025-01152
Apple EX1002 Page 1251

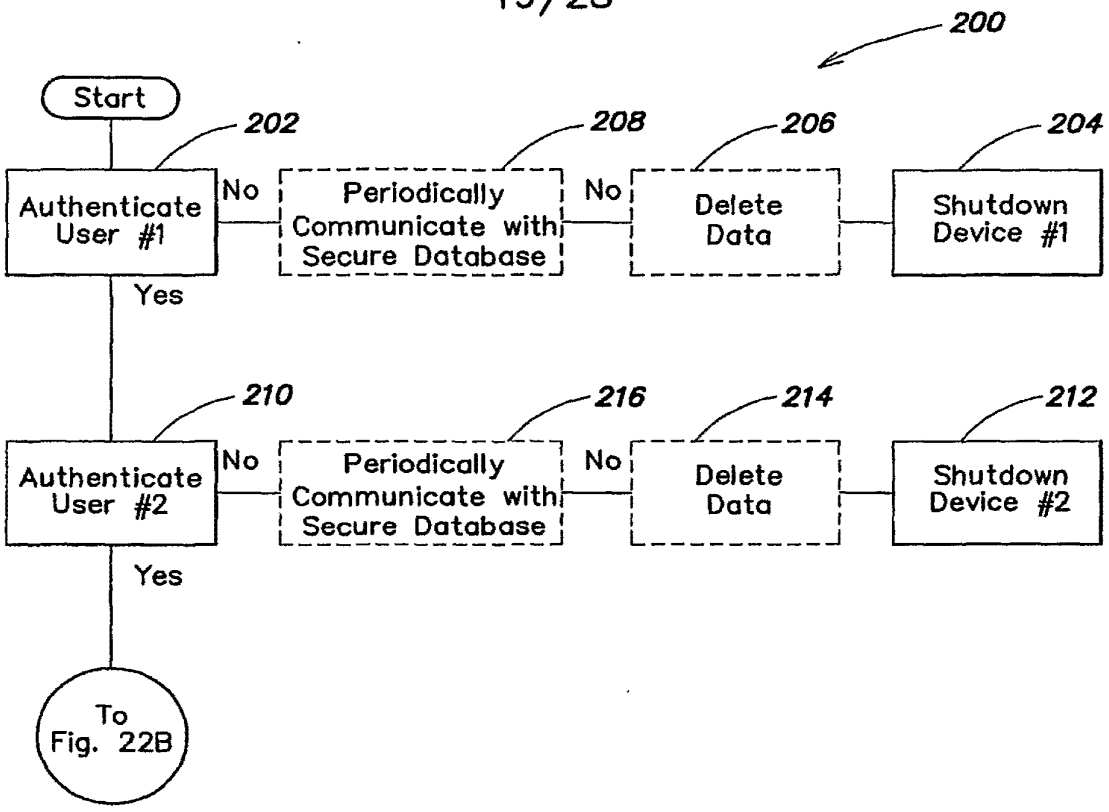


FIG. 22A

IPR2025-01152
Apple EX1002 Page 1252

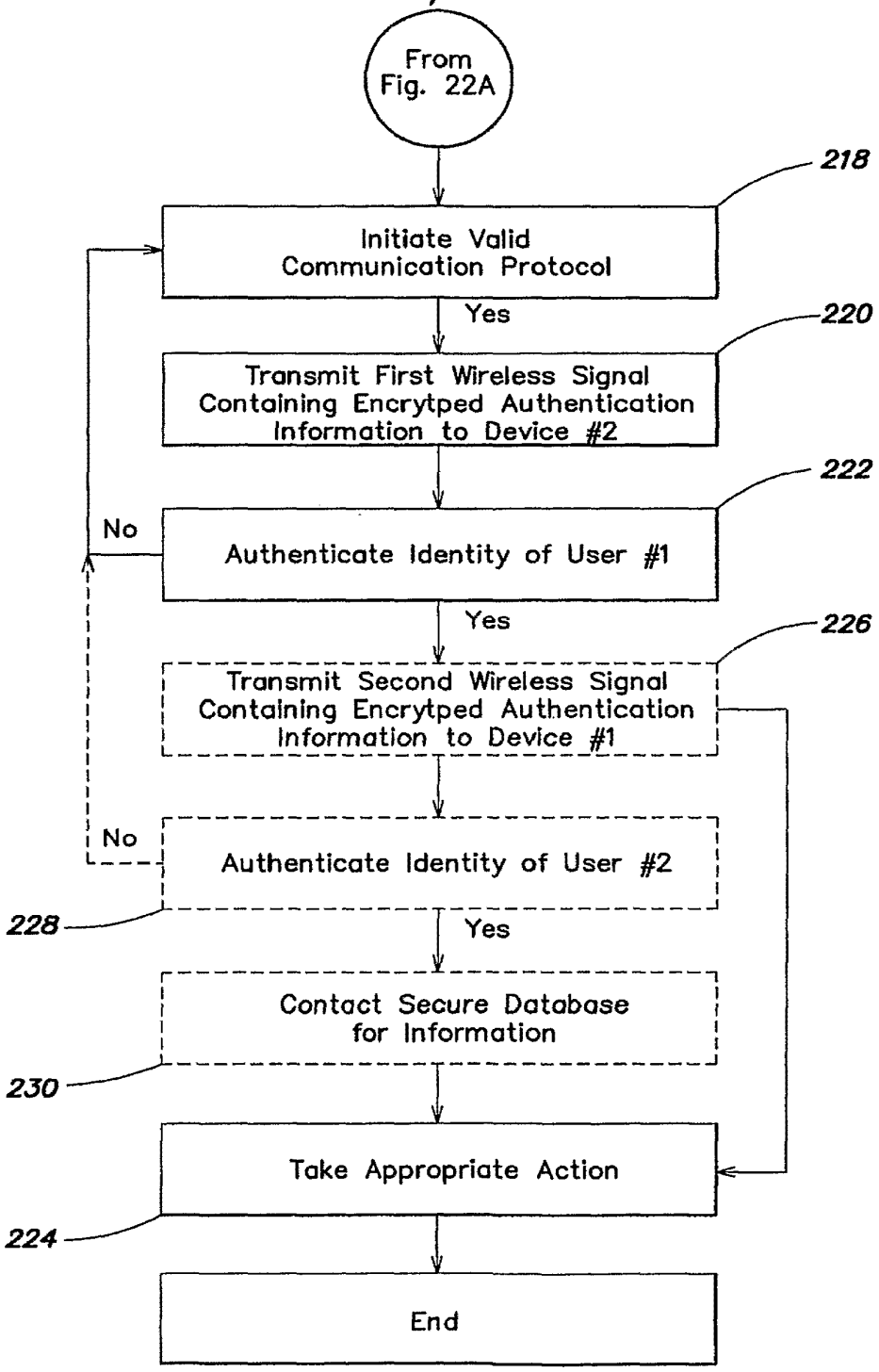


FIG. 22B

IPR2025-01152
Apple EX1002 Page 1253

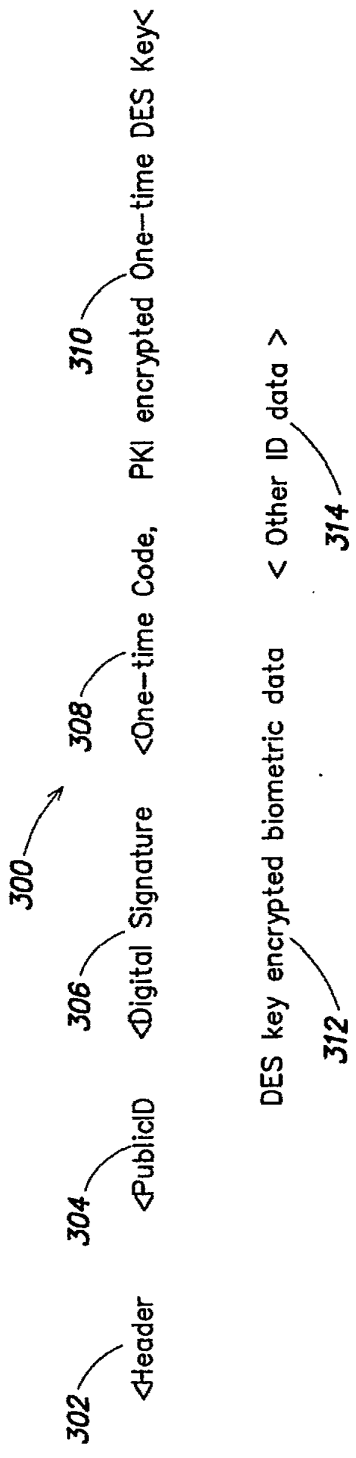


FIG. 23

IPR2025-01152
Apple EX1002 Page 1254

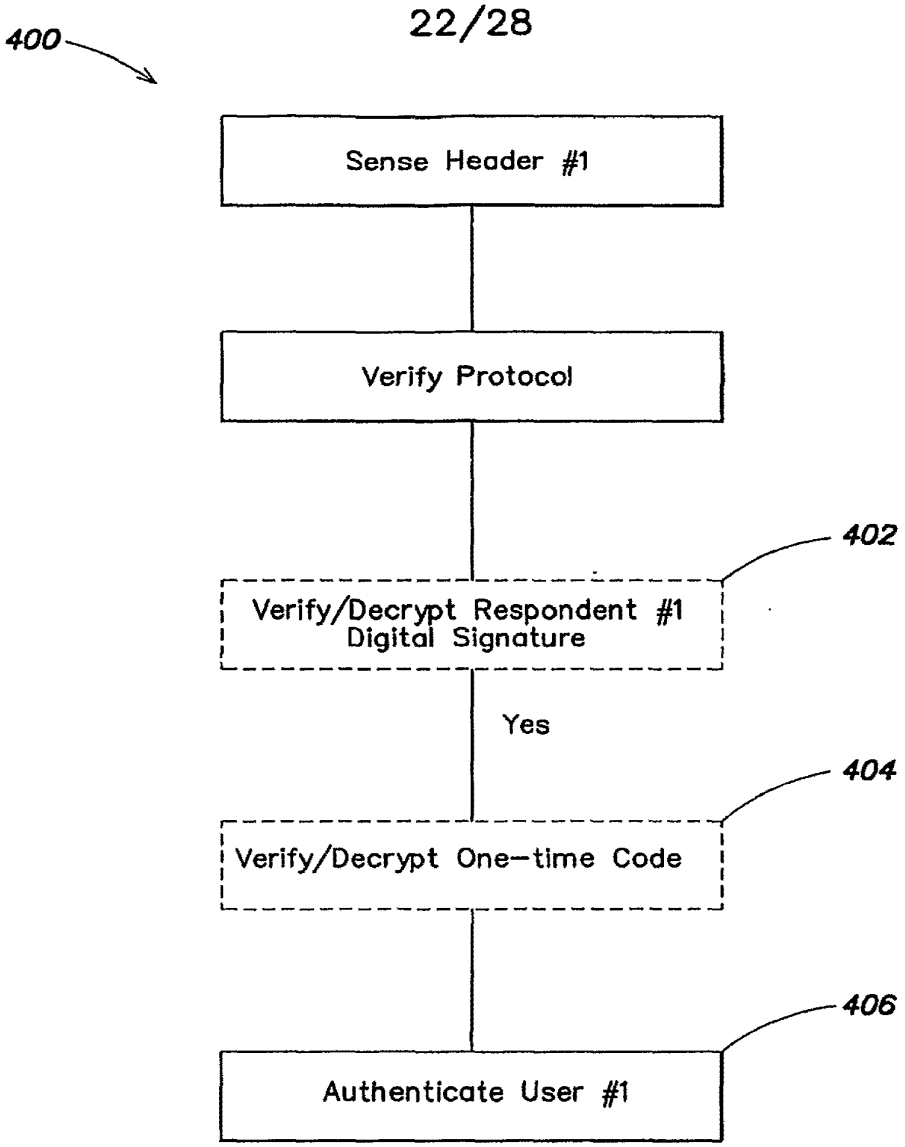


FIG. 24

IPR2025-01152
Apple EX1002 Page 1255

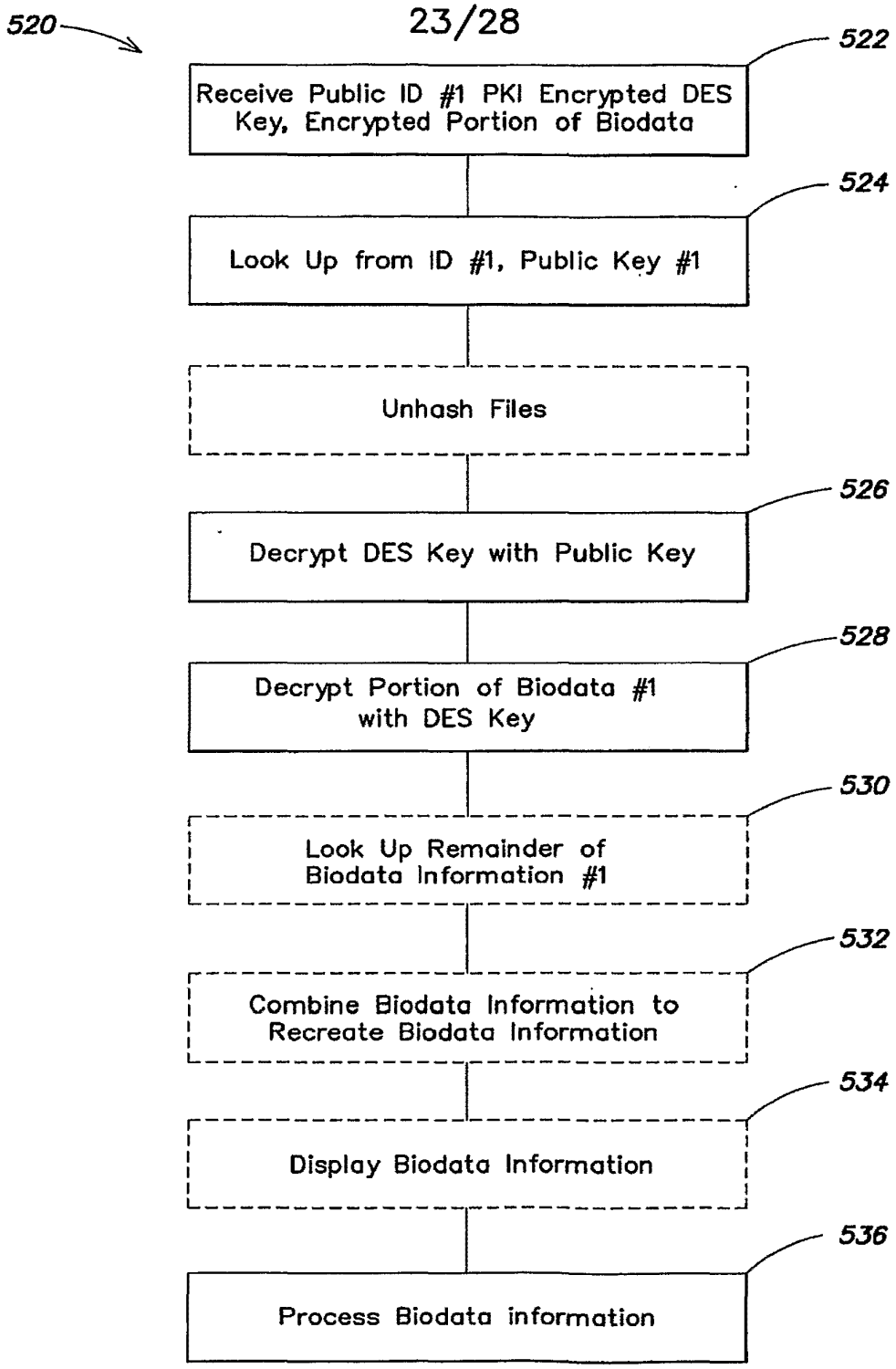


FIG. 25

IPR2025-01152
Apple EX1002 Page 1256

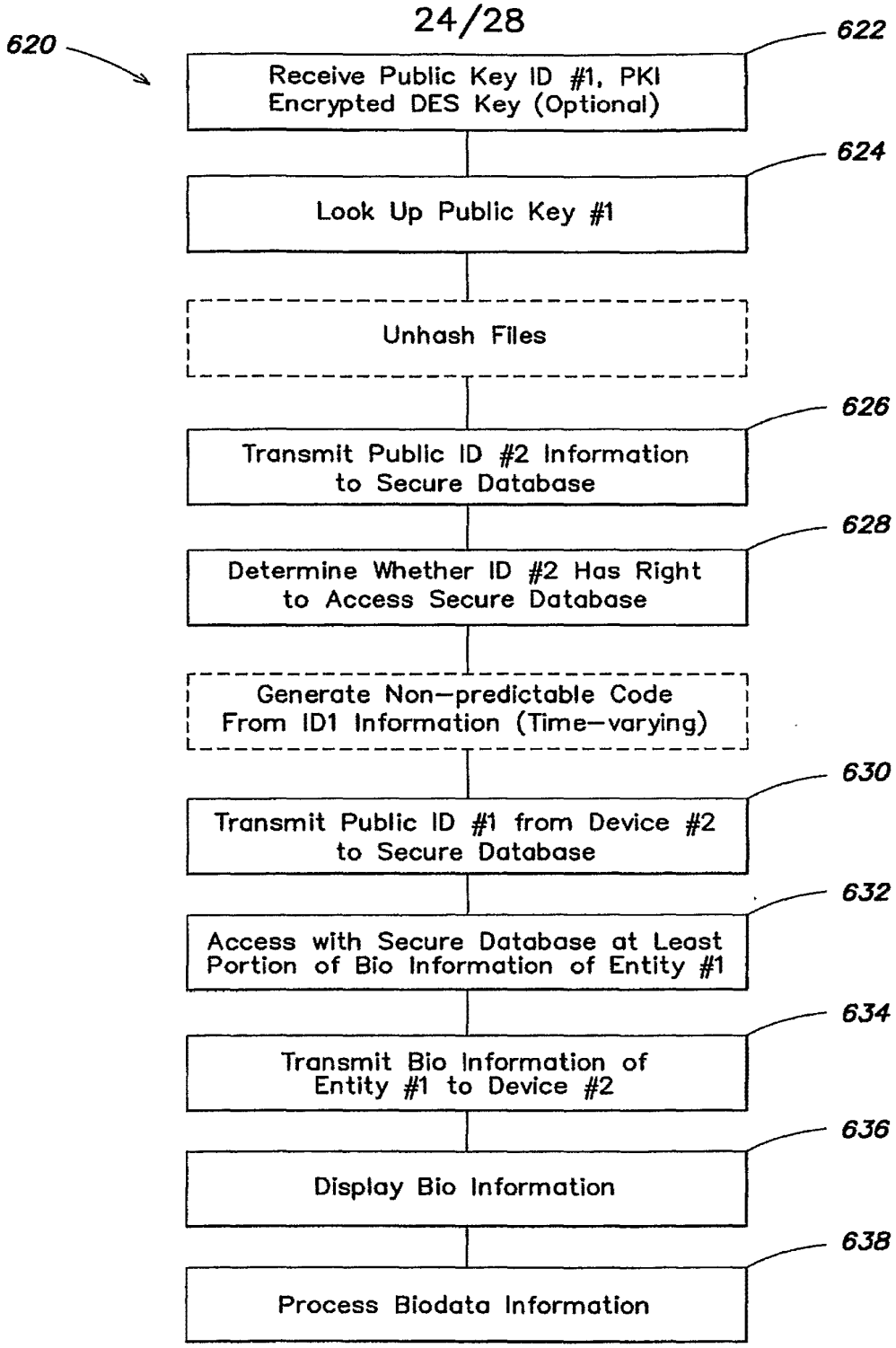


FIG. 26

IPR2025-01152
Apple EX1002 Page 1257

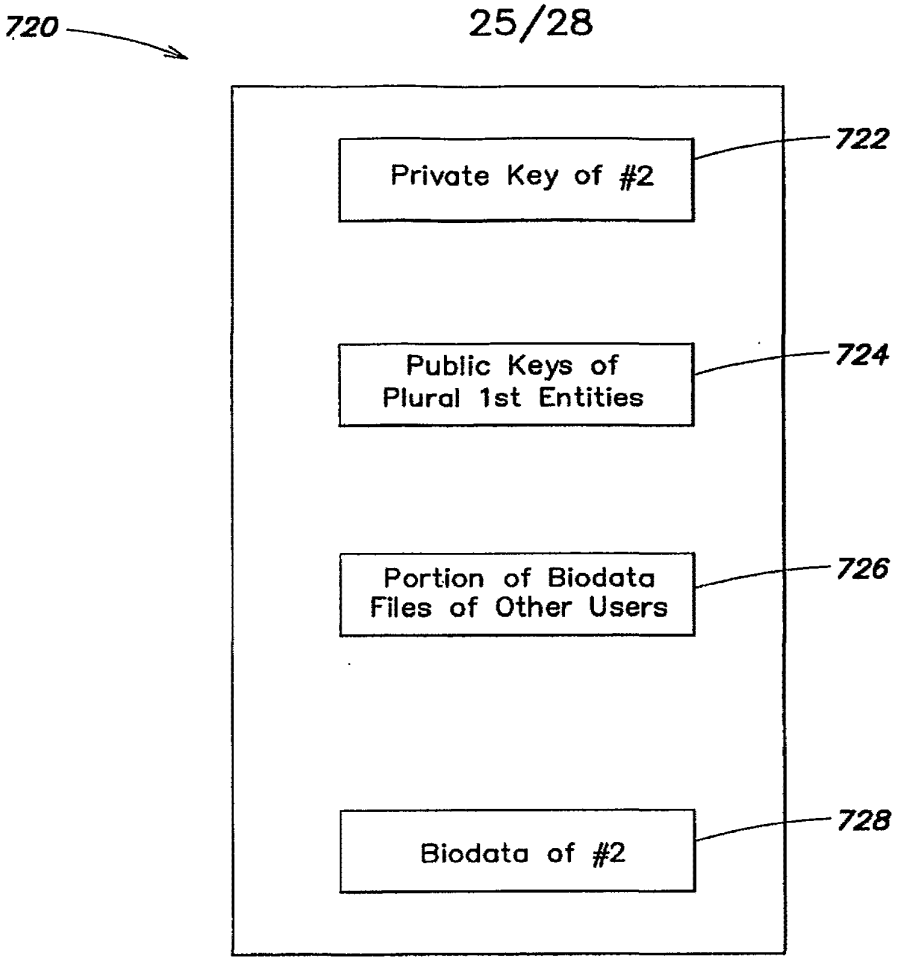


FIG. 27

IPR2025-01152
Apple EX1002 Page 1258

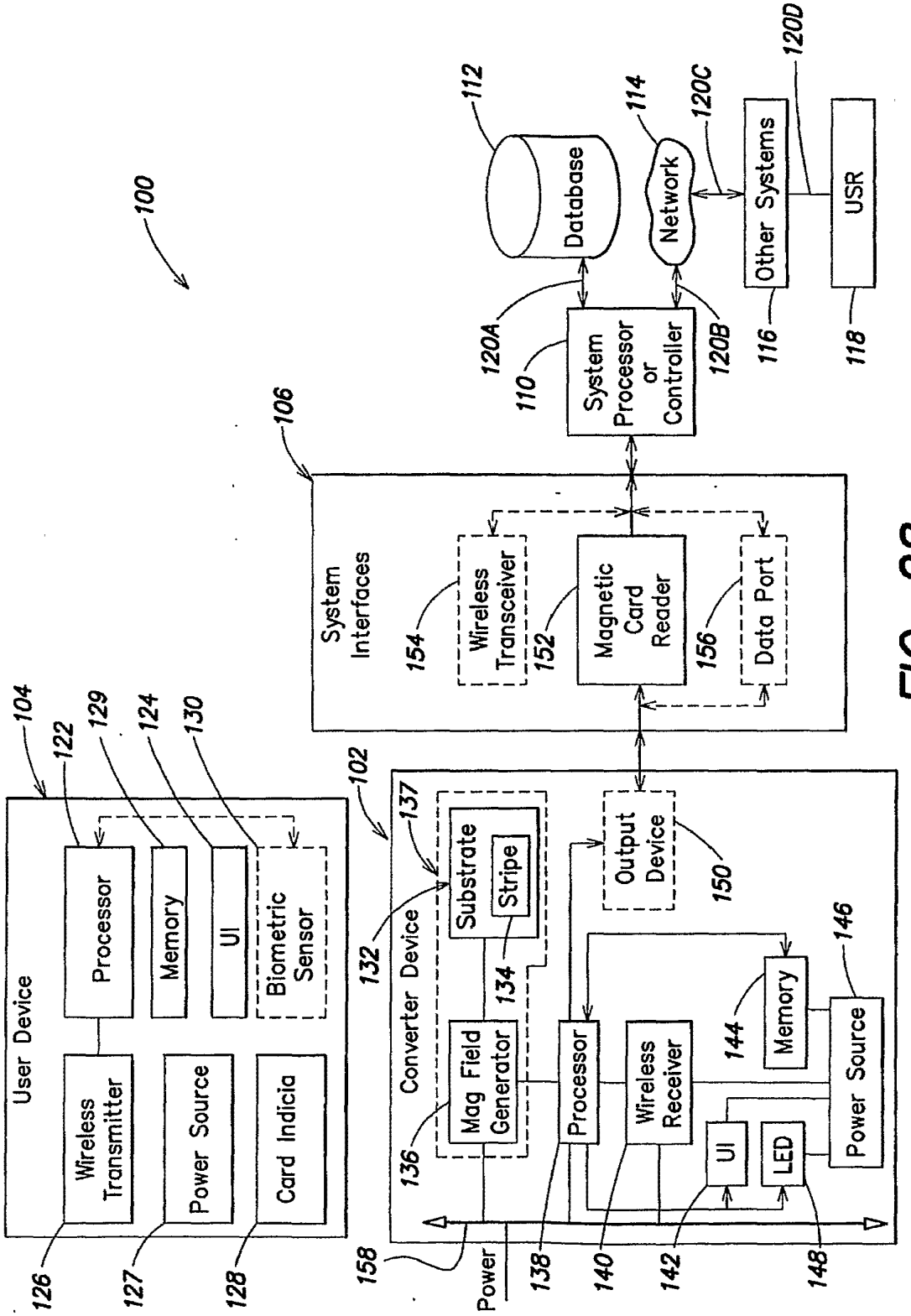


FIG. 28

IPR2025-01152
Apple EX1002 Page 1259

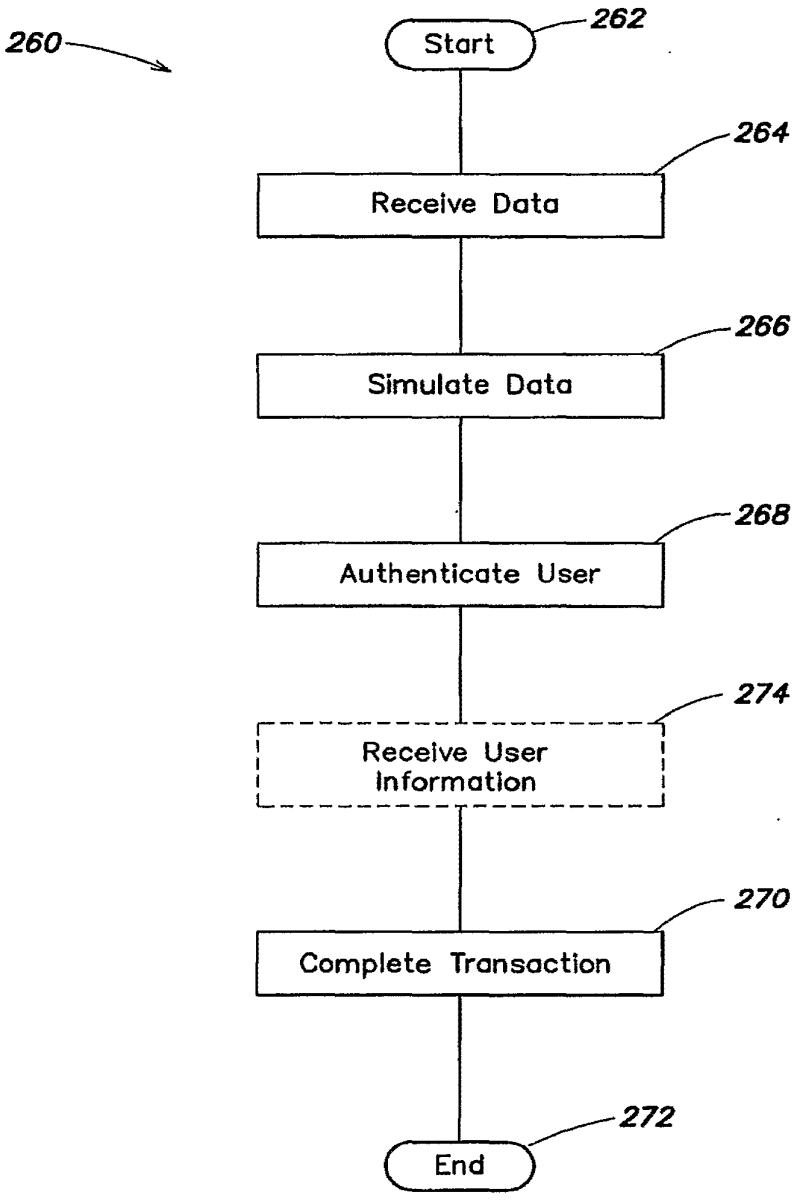


FIG. 29

IPR2025-01152
Apple EX1002 Page 1260

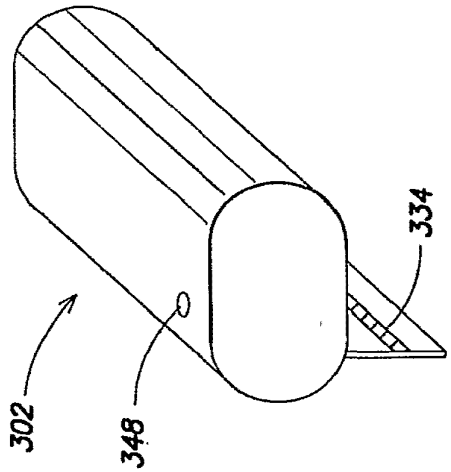


FIG. 30B

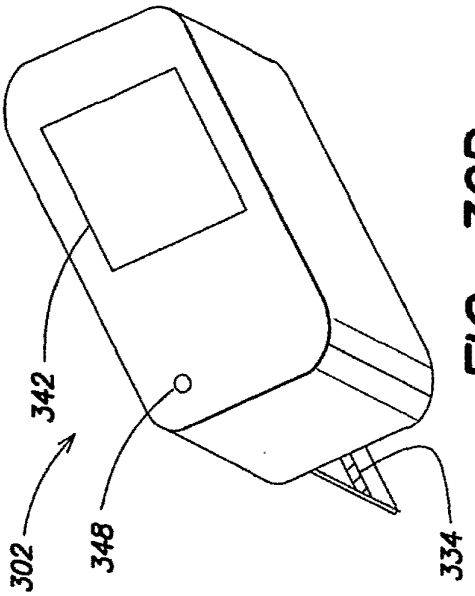


FIG. 30D

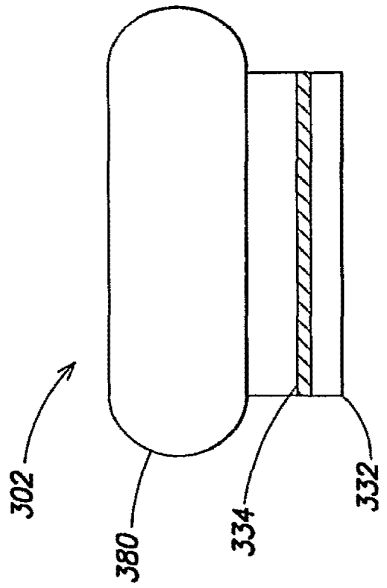


FIG. 30A

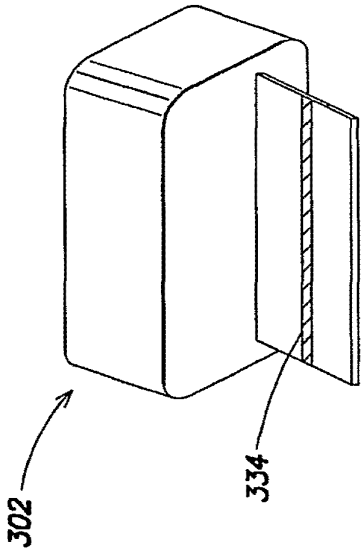


FIG. 30C

IPR2025-01152
Apple EX1002 Page 1261

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.

IPR2025-01152
Apple EX1002 Page 1263

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	

IPR2025-01152
Apple EX1002 Page 1266

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).

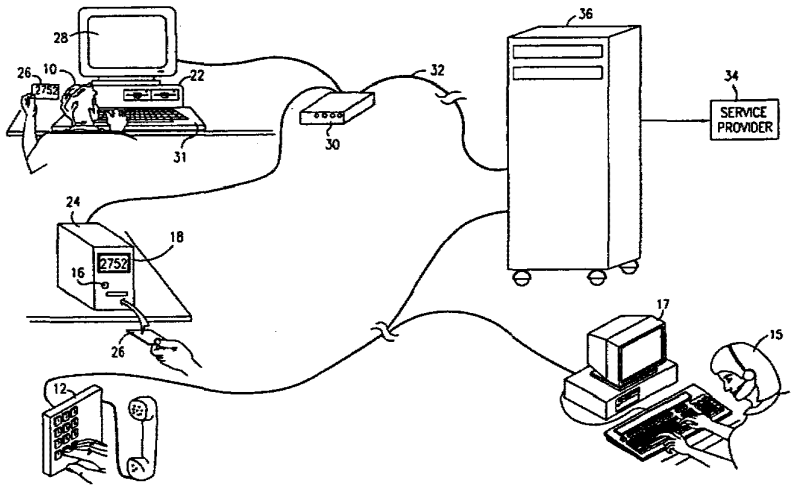
(81) Designated States: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, 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.

IPR2025-01152
Apple EX1002 Page 1267

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

IPR2025-01152
Apple EX1002 Page 1284

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.

IPR2025-01152
Apple EX1002 Page 1289

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:

IPR2025-01152
Apple EX1002 Page 1291

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

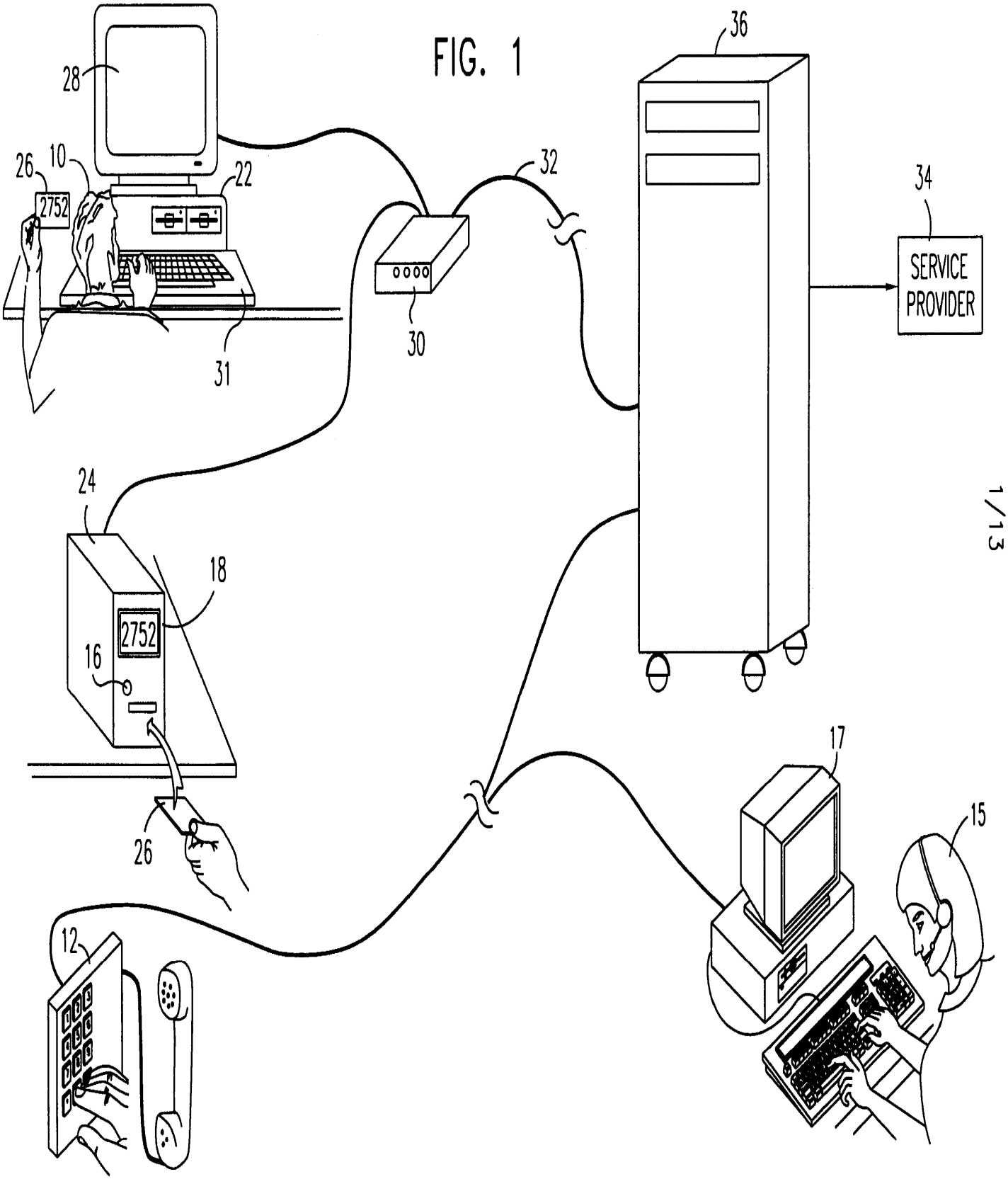

28
36
26
10
22
32
34
2752
SERVICE PROVIDER
30
31
24
18
2752
16
17
26
15
12

FIG. 2

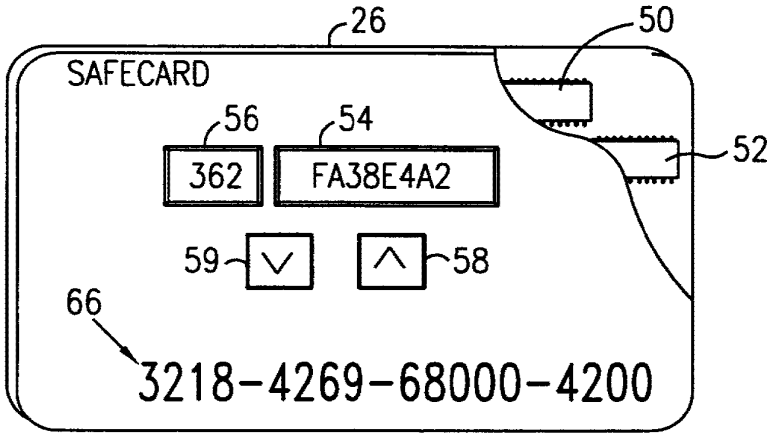

26
50
SAFECARD
56
54
362
FA38E4A2
52
59
58
66
3218-4269-68000-4200

FIG. 3

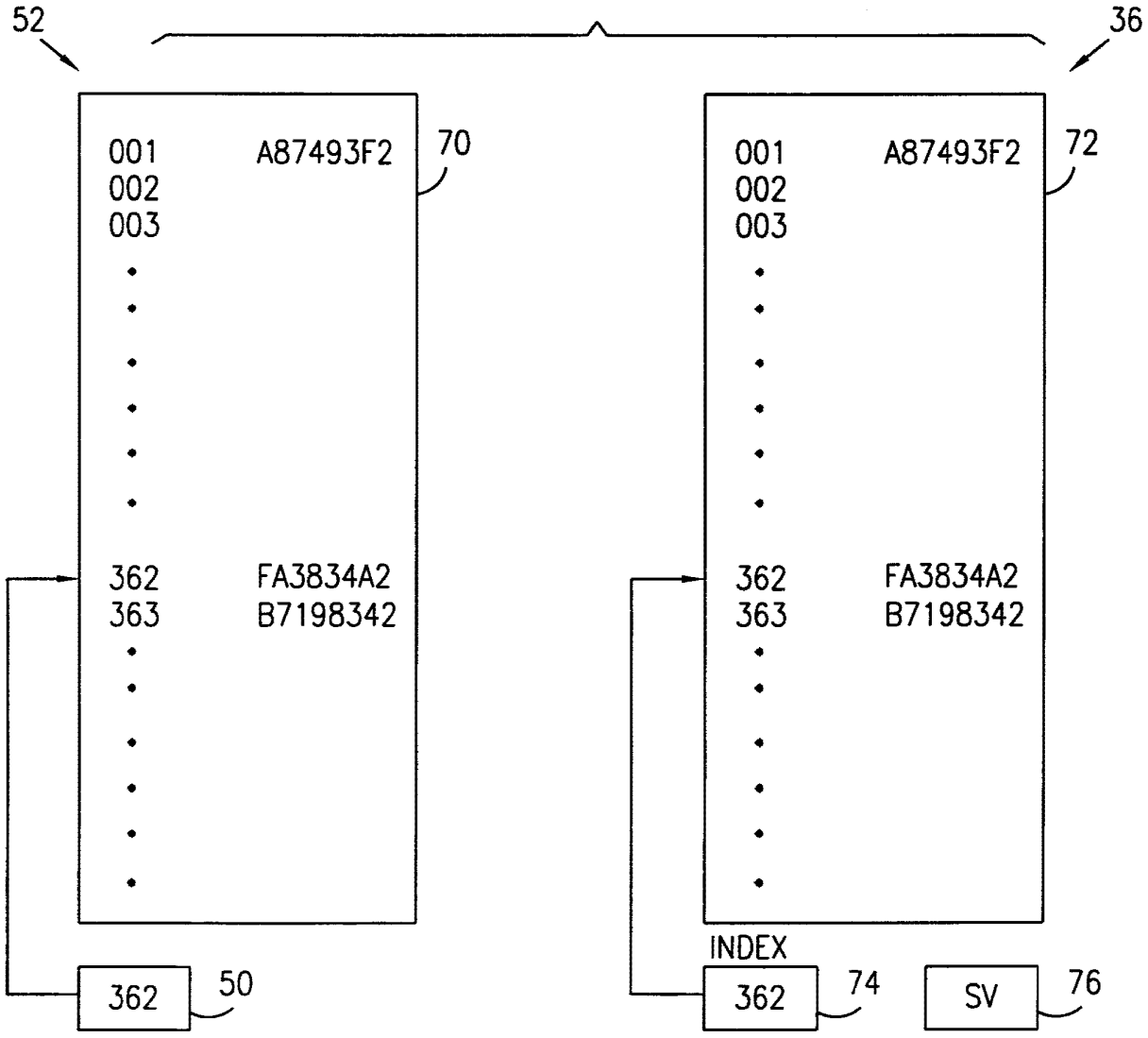

52
36
001 A87493F2
002
003
70
362 FA3834A2
363 B7198342
362
50
001 A87493F2
002
003
72
362 FA3834A2
363 B7198342
INDEX
362
74
SV
76

FIG. 4

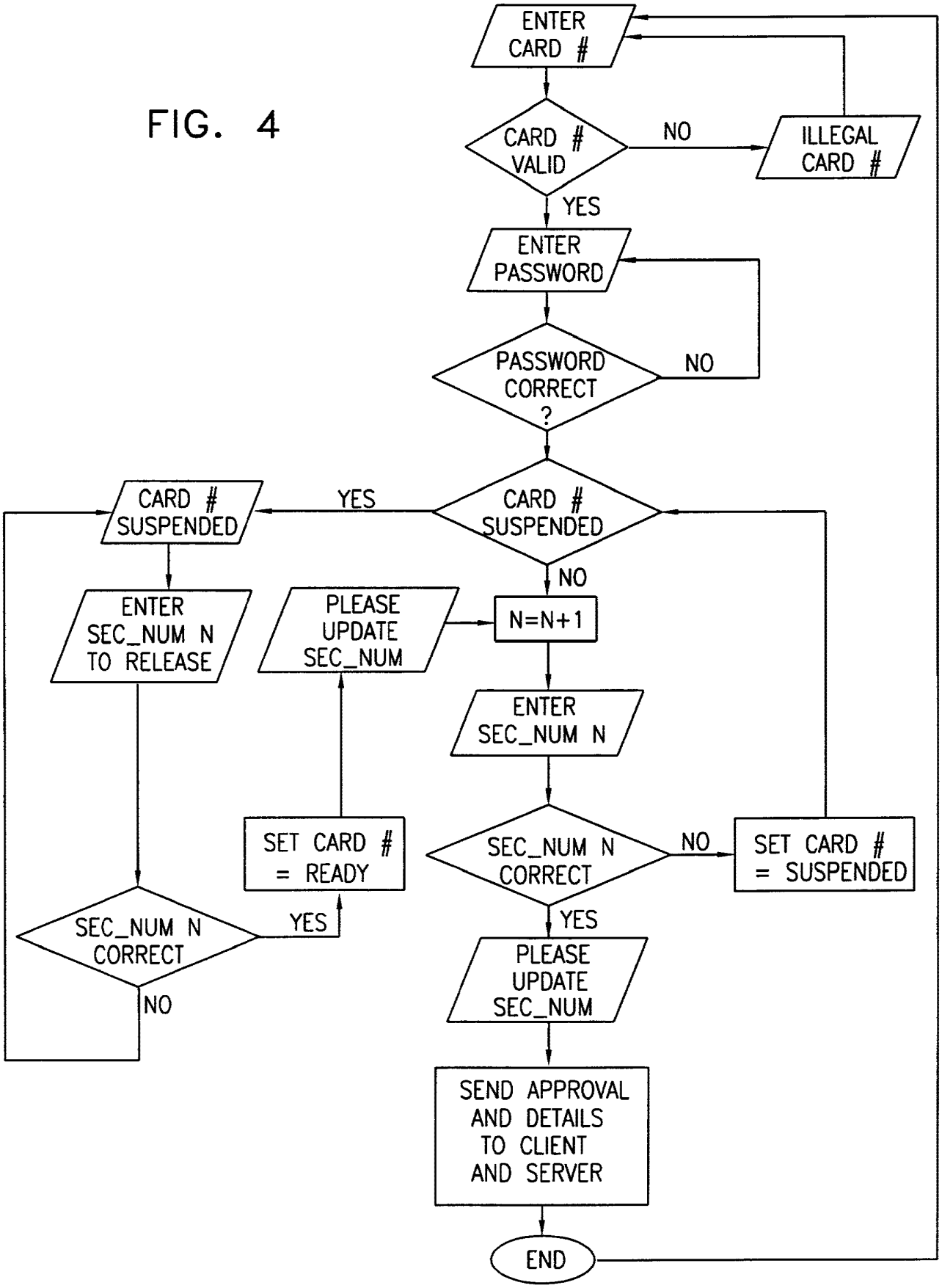

ENTER CARD #
CARD # VALID
NO
ILLEGAL CARD #
YES
ENTER PASSWORD
PASSWORD CORRECT ?
NO
CARD # SUSPENDED
YES
CARD # SUSPENDED
NO
ENTER SEC_NUM N TO RELEASE
PLEASE UPDATE SEC_NUM
N=N+1
ENTER SEC_NUM N
SET CARD # = READY
SEC_NUM N CORRECT
NO
SET CARD # = SUSPENDED
YES
SEC_NUM N CORRECT
YES
NO
PLEASE UPDATE SEC_NUM
SEND APPROVAL AND DETAILS TO CLIENT AND SERVER
END

FIG. 5

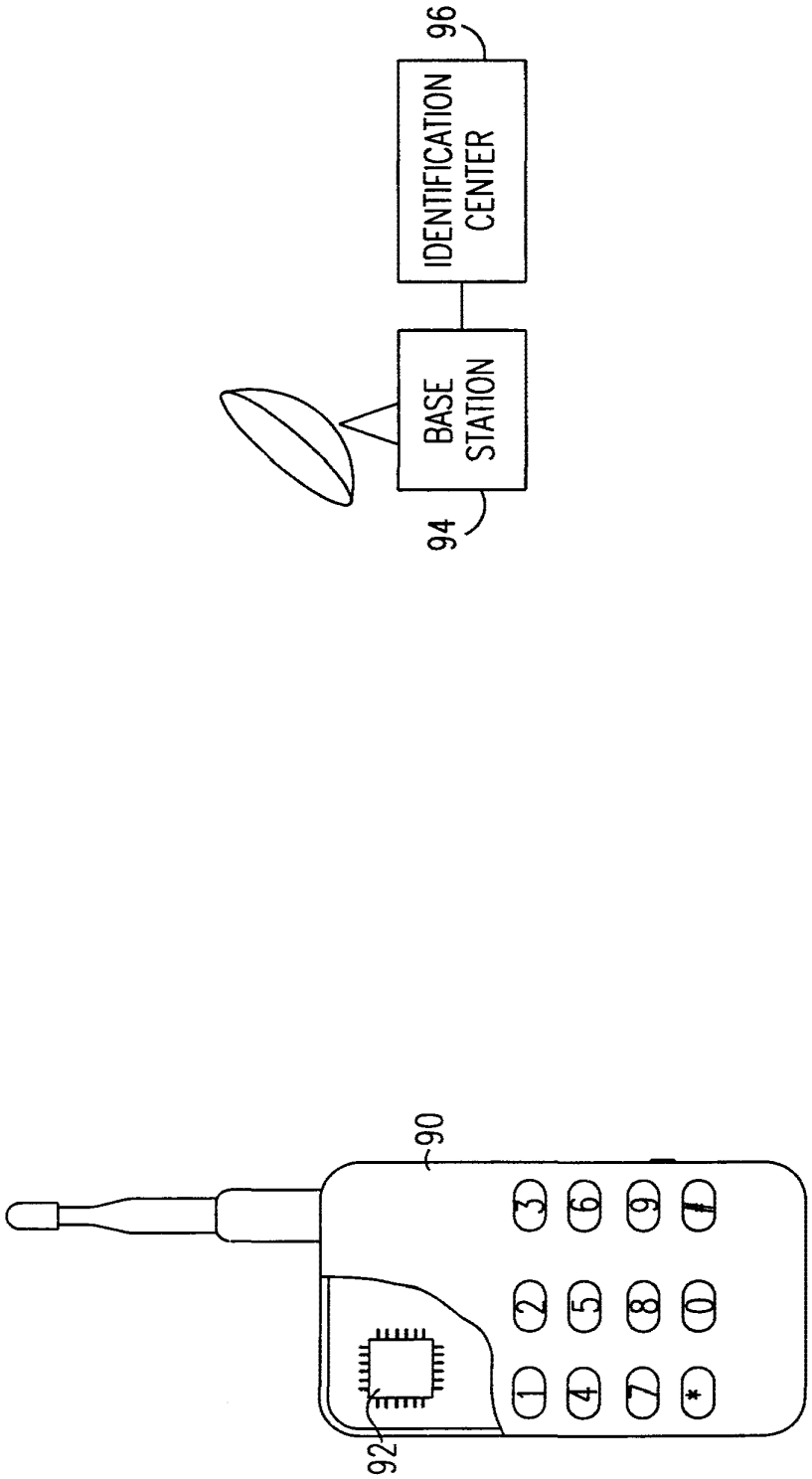


FIG. 6

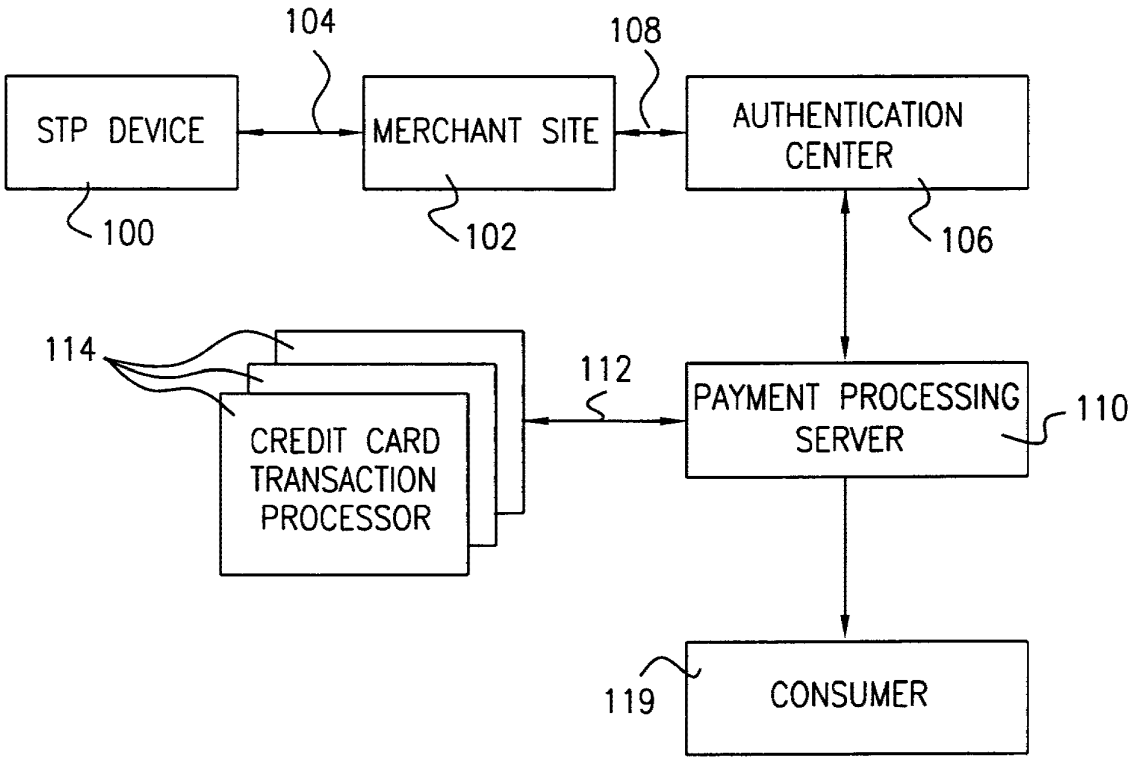

104
108
STP DEVICE
MERCHANT SITE
AUTHENTICATION CENTER
100
102
106
114
112
CREDIT CARD TRANSACTION PROCESSOR
PAYMENT PROCESSING SERVER
110
119
CONSUMER

FIG. 7

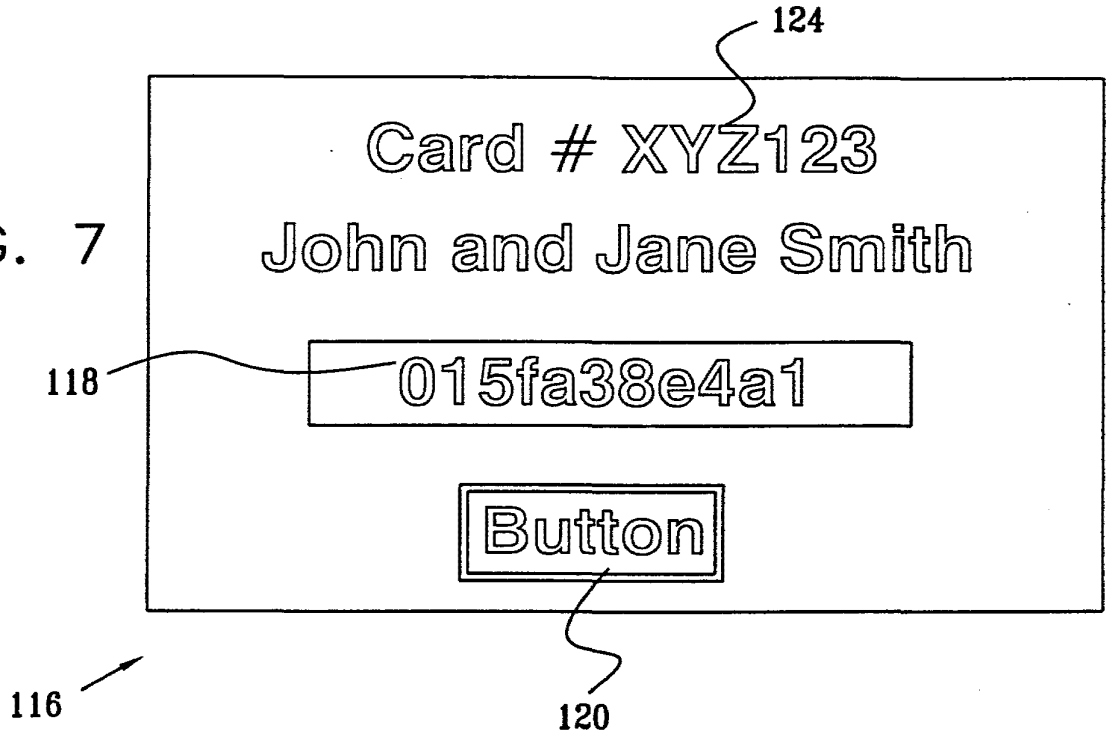


FIG. 8

ROM	001 rt237yu5 ... 015 fa38e4a1 016 xy568AD9 017 k6a7FI8

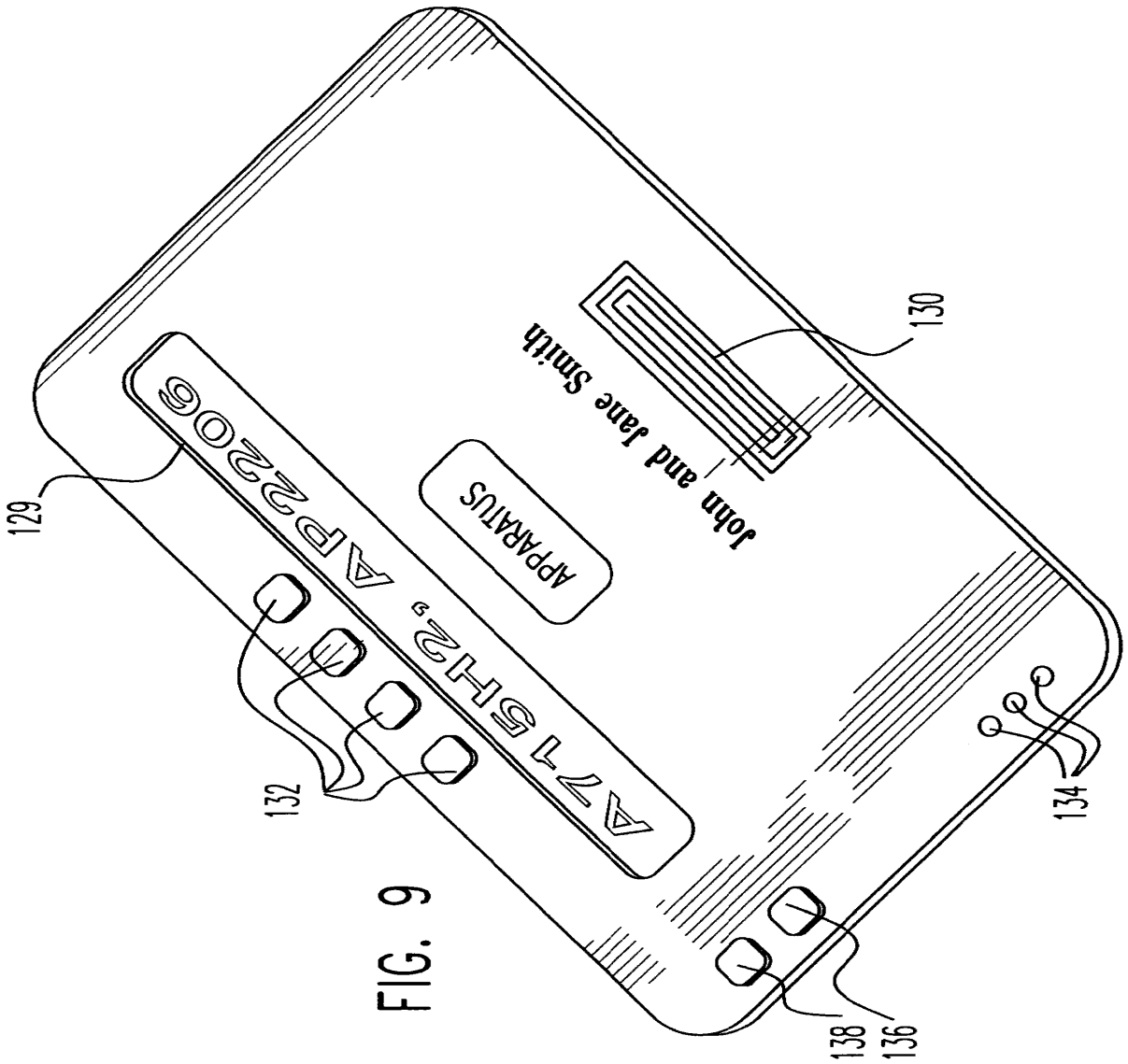


FIG. 9

IPR2025-01152
Apple EX1002 Page 1307

FIG. 10

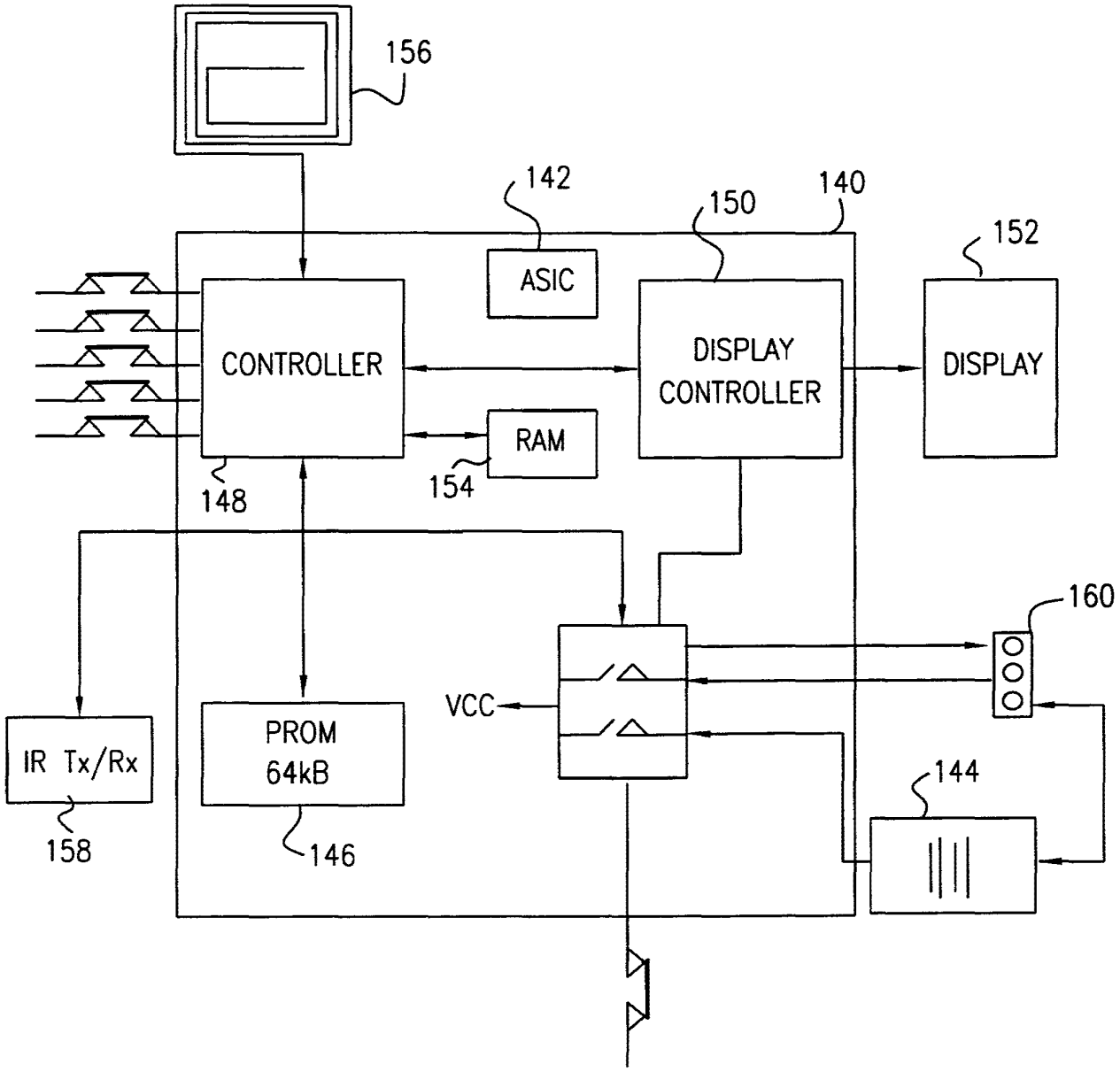

156
142
150
140
152
ASIC
CONTROLLER
DISPLAY CONTROLLER
DISPLAY
RAM
148
154
160
VCC
IR Tx/Rx
PROM 64kB
144
158
146

FIG. 11

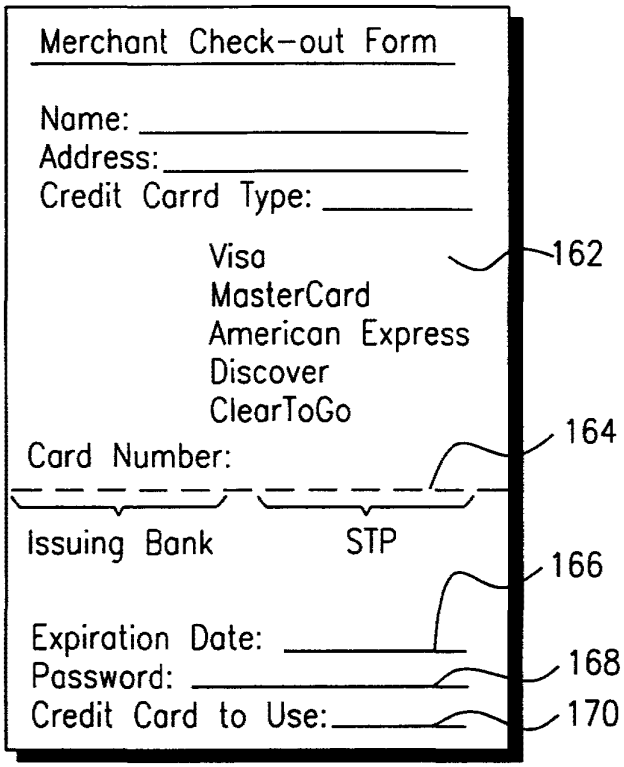


FIG. 12

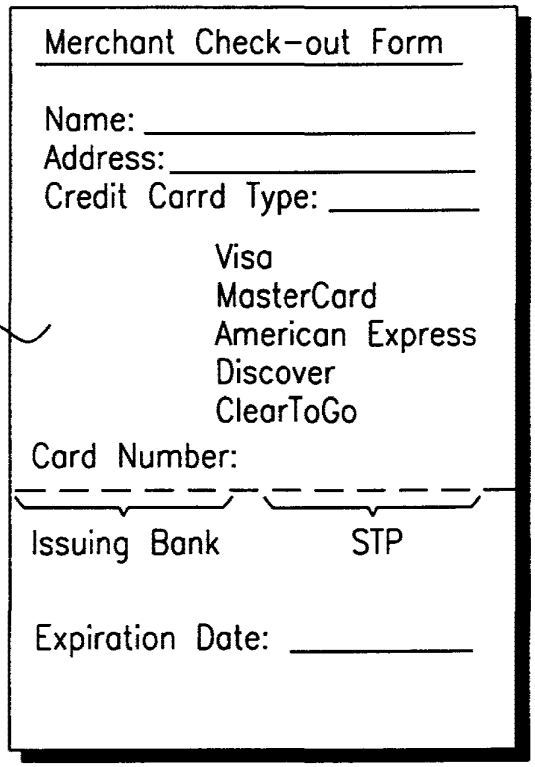
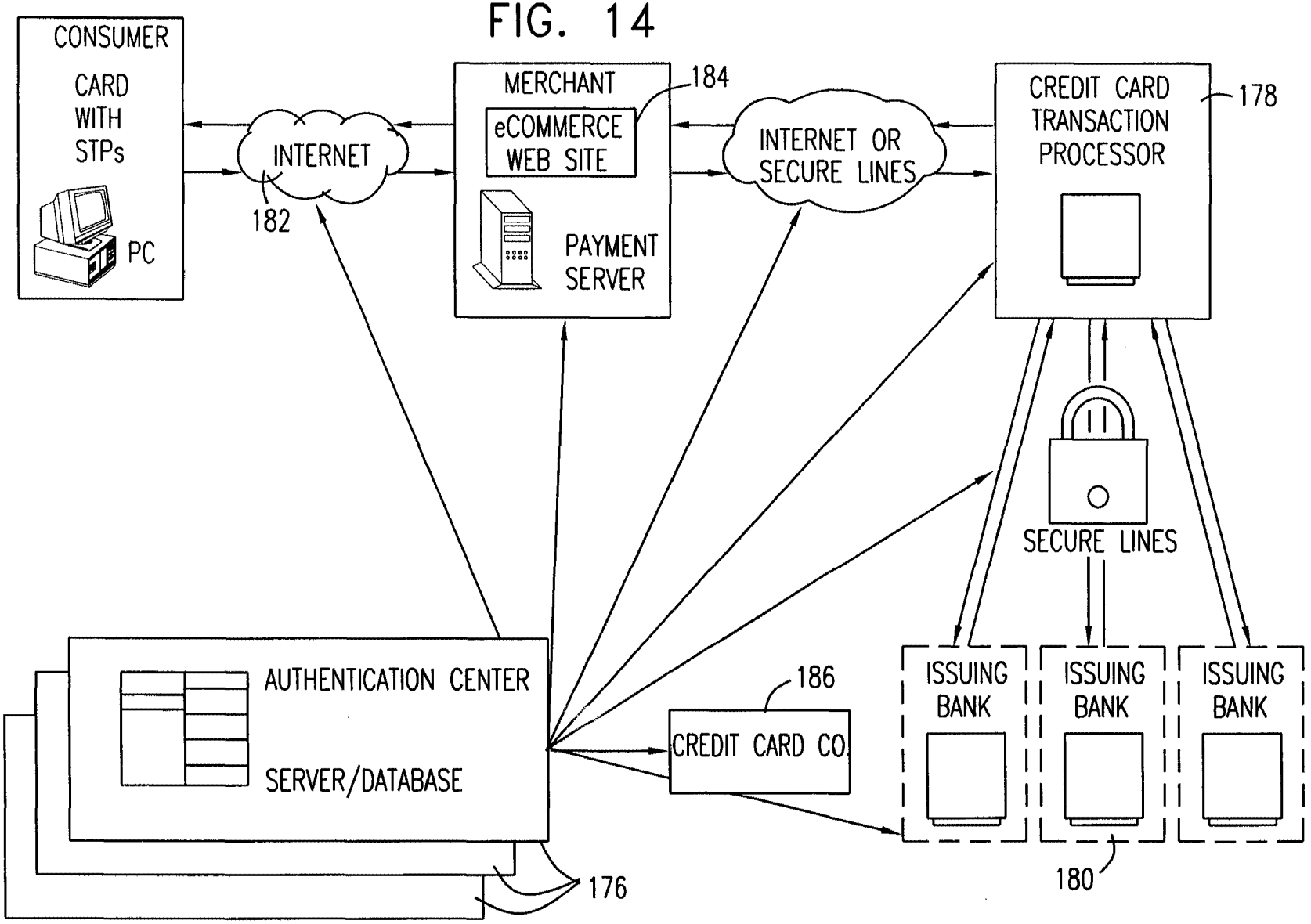


FIG. 13

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



IPR2025-01152
Apple EX1002 Page 1310

FIG. 15

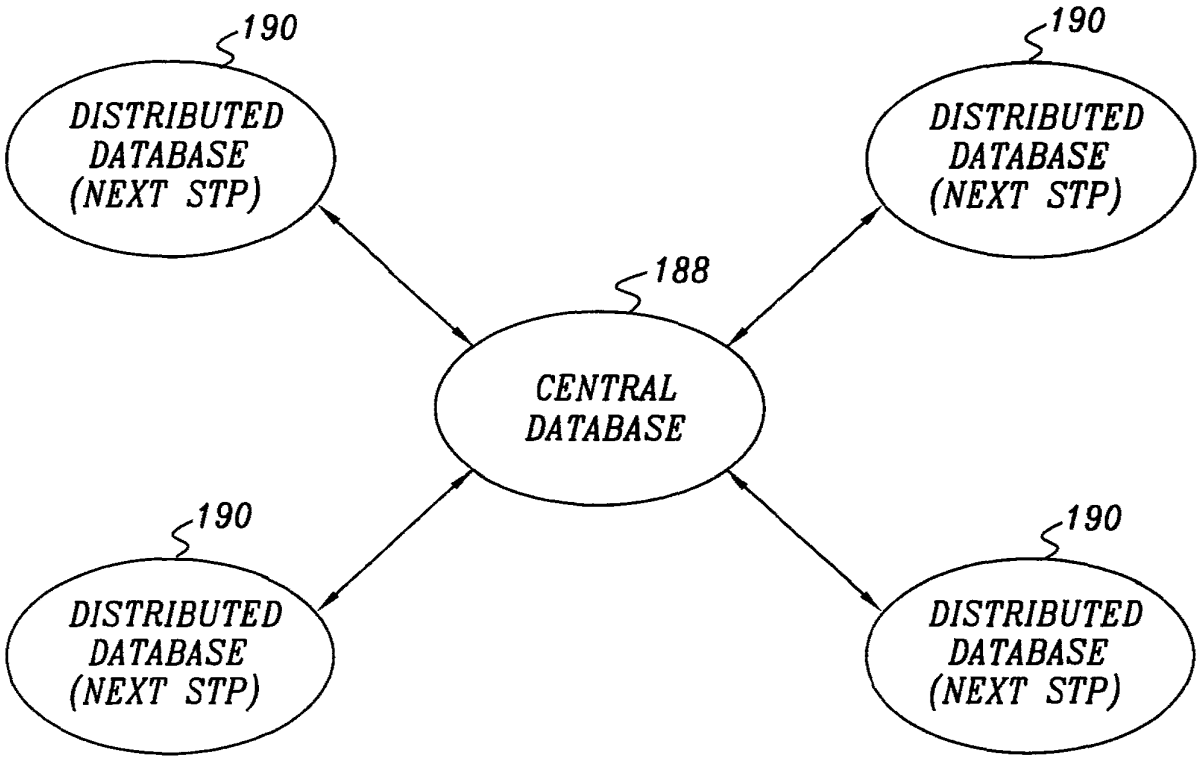

190
DISTRIBUTED DATABASE (NEXT STP)
190
DISTRIBUTED DATABASE (NEXT STP)
188
CENTRAL DATABASE
190
DISTRIBUTED DATABASE (NEXT STP)
190
DISTRIBUTED DATABASE (NEXT STP)

FIG. 16

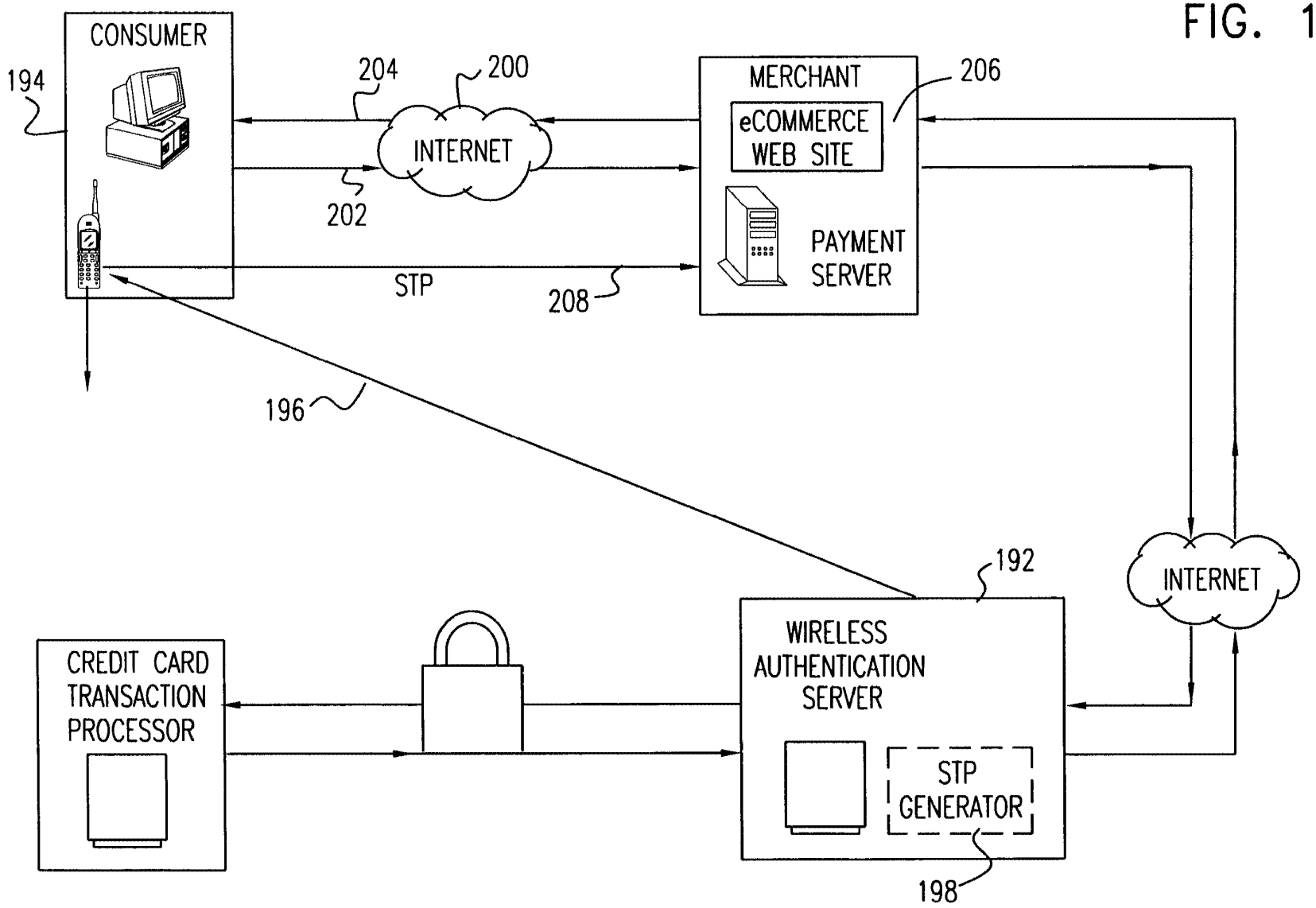
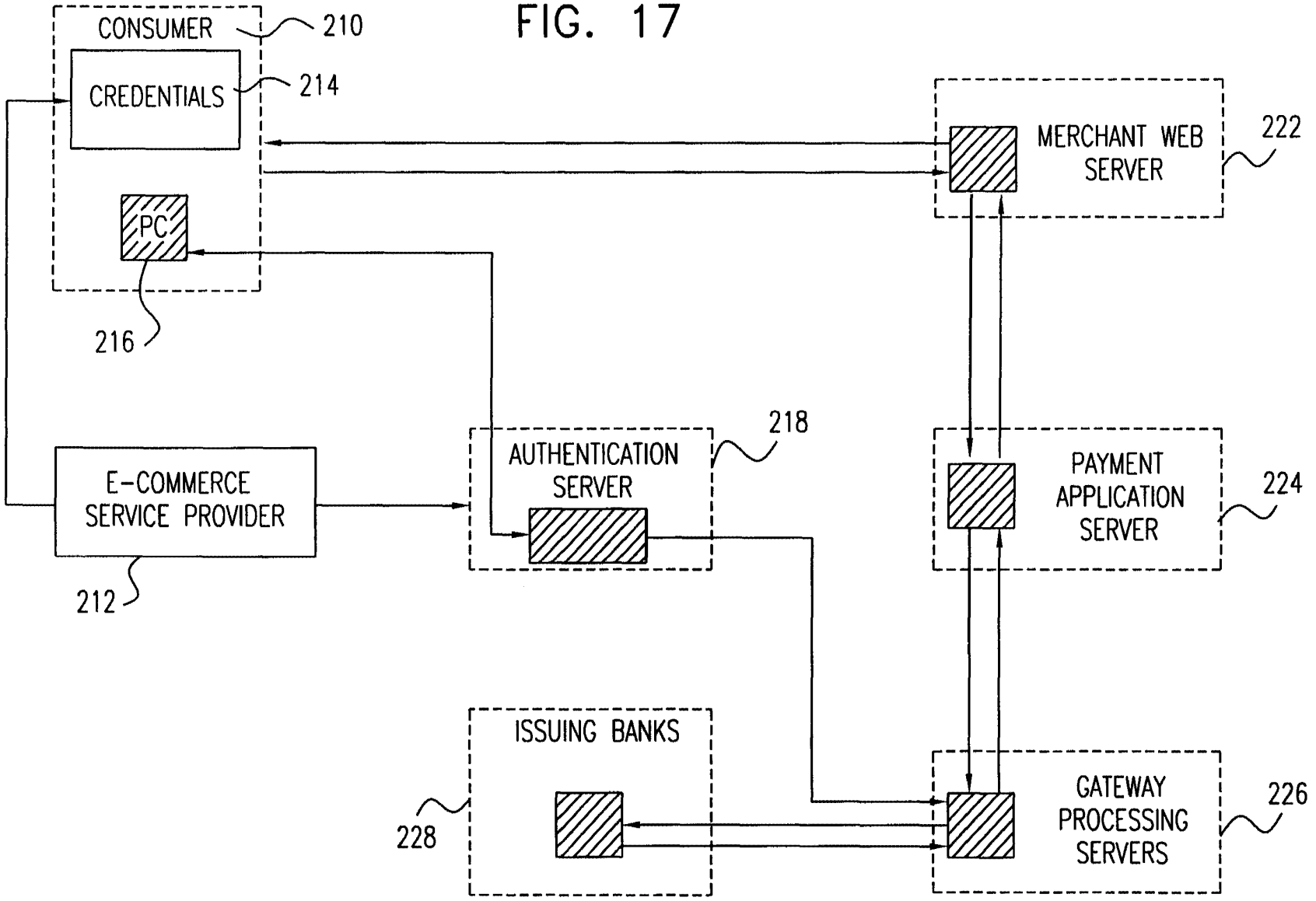

CONSUMER
194
204
200
INTERNET
202
MERCHANT
206
eCOMMERCE
WEB SITE
PAYMENT
SERVER
STP
208
196
192
INTERNET
WIRELESS
AUTHENTICATION
SERVER
CREDIT CARD
TRANSACTION
PROCESSOR
STP
GENERATOR
198

FIG. 17



IPR2025-01152
Apple EX1002 Page 1313

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL00/00211

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :G06F 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)★

IPR2025-01152
Apple EX1002 Page 1314

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

IPR2025-01152
Apple EX1002 Page 1315

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

IPR2025-01152
Apple EX1002 Page 1316

PTO/SB/08a (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.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17528073
Filing Date	2021-11-16
First Named Inventor	David WYATT
Art Unit	2876
Examiner Name	LEE, SEUNG H.
Attorney Docket Number	WYAT-0002-13C12US

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	1	Susan Pandy, "Securing Payments: Payments Tokenization in Primetime," Federal Reserve Bank of Boston Payments Symposium, January 20, 2016, pp. 1-20.	
	2	'SUMMARY OF ANS X9.119-Part 2 USE OF TOKENS TO PROTECT SENSITIVE CARD DATA," September 2017, pp.1-2.	
	3	Marianne Crowe et al., "Is Payment Tokenization Ready for Primetime?," June 11, 2015, pp. 1-51.	
	4	Terence Spies et al., "ANSI X9.119 Part 2: Using Tokenization Methods," 2013, pp. 1-20.	
	5	ASSORA et al., "A web transaction security scheme based on disposable credit card numbers," Int. J. Electronic Security and Digital Forensics, 2007, Vol. 1, No. 2, Inderscience Enterprises Ltd., pp. 146-155.	
	6	BOYD, "A pragmatic approach to temporary payment cards numbers," Int. J. Electronic Security and Digital Forensics, 2009, Vol. 2, No. 3, pp. 253-268.	
	7	BUCCAFURRI et al., "Implementing disposable credit card numbers by mobile phones," Electronic Commerce Research, Feb. 23, 2011, Vol. 11, Springer Publishing, pp. 271-296.	
	8	JAVANI et al., "A new credit card payment system based on 3D-Secure using one-time-use transaction numbers," Information Assurance and Security Letters, 2010, Vol. 1, Dynamic Publishers, Inc., USA, pp. 060-065.	
	9	KILLORAN et al., "A New Secure Wireless Financial Transaction Architecture," EUROCON 2005, November 22-24, 2005, IEEE, pp. 1060-1063.	
	10	LI et al., "A security-enhanced one-time payment scheme for credit card," Mar. 28-29, 2004, IEEE, pp. 1-11.	
	11	MJØLSNES et al., "On-Line E-Wallet System with Decentralized Credential Keepers," Mobile Networks and Applications, 2003, Vol. 8, Kluwer Academic Publishers, The Netherlands, pp. 87–99.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	12	NARAYANASWAMI et al., "What Would You Do with a Hundred MIPS on Your Wrist?," RC 22057 (98634) January 22, 2001, IBM Research, pp. 1-10.	
	13	QASIM et al., "Interactive Shopping with Mobile Wallet," World Congress on Sustainable Technologies, 2012, IEEE, pp. 32-36.	
	14	HONIG, "A Week with Google Wallet," Endgadget, September 19, 2011, pp. 1-49.	
	15	KADAMBI et al.,"Near-Field Communication-Based Secure Mobile Payment Service," ICEC'09, August 12–15, 2009, pp. 1-11.	
	16	"A closer look at Google Pay and tokenization," Rambus Press, February 23, 2016, pp. 1-2.	
	17	GHAG et al., "A Comprehensive Study of Google Wallet as an NFC Application," International Journal of Computer Applications, November 2012, Vol. 58, No.16, pp. 37-42.	
	18	"Add any credit or debit card," Google Wallet Help (archive.org), 2012, page 1.	
	19	"Add any credit or signature debit card," Wallet Help, Google Wallet, September 20, 2012, page 1.	
	20	"Allynis Mobile NFC," Gemalto, September 2007, pp. 1-4.	
	21	"Allynis TSM for Transport," Gemalto, October 2009, pp. 1-2.	
	22	ADAMS, "Amex Plays a Major Role in Revamped Isis Mobile Wallet," Payments Source, November 15, 2013, Vol. 1, No. 1, SourceMedia LLC d/b/a Arizent, pp. 1-2.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	23	PEREZ, "Android Pay, Google's Apple Pay Rival, Arrives Today," DigitalOcean, September 10, 2015, pp. 1-8.	
	24	HEISLER, "Apple Pay: An in-depth look at what's behind the secure payment system," Engadget, October 2, 2014, pp. 1-7.	
	25	FEHR, "Apple Pay: How different is it from other Pay solutions, what role does tokenisation play, and to what degree can Card not Present payment benefit from Apple Pay in future," Technical Report RHUL–ISG–2018–3, April 3, 2018, Egham, Surrey, UK, pp. 1-79.	
	26	'ATMIA publishes contactless ATM best practices," ATM Marketplace, September 27, 2012, pp. 1-2.	
	27	POPPER, "Banks Did It Apple's Way in Payments by Mobile," New York Times, September 11, 2014, pp. 1-2.	
	28	'Bell ID Simplifies EMV Smart Card and NFC Application Management with Versatile New Platform," eBanking & Payment News, May 5, 2011, page 1.	
	29	'BofA pursuing contactless ATM patent," Mobilepaymentstoday.com News, September 20, 2012, Newstex LLC, pp. 1-2.	
	30	'Chip Advisory #20, Visa Recommended Practices for EMV Chip Implementation in the U.S," July 11, 2012, pp. 1-10.	
	31	'Commbank, Mastercard and Samsung collaborate to launch NFC payment service," MarketLine NewsWire (Formerly Datamonitor), December 13, 2013, pp. 1-2.	
	32	'Contactless Payment: Secure Enough?," Card Technology, September 1, 2005, SourceMedia, Inc., Section: SPECIAL ISSUE: CONTACTLESS TECHNOLOGY, Vol. 10, No. 8, page 36.	
	33	'Eligible Devices," Google Wallet Help (archive.org), November 18, 2012, page 1.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	34	MOTT, "EMV and Mobile Payments, Questions abound, answers divide," Payments Summit Workshop, February 4, 2013, pp. 1-22.	
	35	"EMV Integrated Circuit Card Specifications for Payment Systems Book 2 Security and Key Management Version 4.1," May 2004, pp. 1-187.	
	36	"EMV Integrated Circuit Card Specifications for Payment Systems. Book 2, Security and Key Management, Version 4.3," November 2011, pp. 1-174.	
	37	"EMV Integrated Circuit Card Specifications for Payment Systems, Book 3, Application Specification, Version 4.3," November 2011, pp. 1-230.	

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17528073
Filing Date	2021-11-16
First Named Inventor	David WYATT
Art Unit	2876
Examiner Name	LEE, SEUNG H.
Attorney Docket Number	WYAT-0002-13C12US

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Jose S. Garcia/	Date (YYYY-MM-DD)	2023-01-12
Name/Print	Jose S. Garcia	Registration Number	43,628

This collection of information is required by 37 CFR 1.97 and 1.98. 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 1.14. This collection is estimated to take 1 hour 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. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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 record s.

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.

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 01:27:56 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 #	61424604	FILING DATE	11/16/2021
CUSTOMER #	136197	FIRST NAMED INVENTOR	David WYATT
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	-

Documents

TOTAL DOCUMENTS: 51

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
WYAT-0002-13C12US_IDS_transmittal_form_1.pdf	7	Information Disclosure Statement (IDS) Form (SB08)	1236 KB
BOYD.pdf	16	Non Patent Literature	1484 KB
BUCCAFURRI.pdf	26	Non Patent Literature	18760 KB
Card_Technology.pdf	2	Non Patent Literature	1400 KB
Chip_Advisory.pdf	10	Non Patent Literature	4354 KB
Commbank.pdf	2	Non Patent Literature	915 KB

ADAMS.pdf	2	Non Patent Literature	1268 KB
Allynis.pdf	4	Non Patent Literature	2218 KB
Allynis_TSM.pdf	2	Non Patent Literature	1429 KB
ASSORA.pdf	10	Non Patent Literature	525 KB
ATMIA.pdf	2	Non Patent Literature	829 KB
Bell.pdf	1	Non Patent Literature	50 KB
BofA.pdf	2	Non Patent Literature	972 KB
EMV_Version4_1_5_of_5.pdf	35	Non Patent Literature	21890 KB
EMV_Version4_3_1_of_6.pdf	44	Non Patent Literature	18367 KB
EMV_Version4_3_2_of_6.pdf	22	Non Patent Literature	10609 KB
Eligible_Devices.pdf	1	Non Patent Literature	359 KB
EMV_Version4_1_1_of_5.pdf	38	Non Patent Literature	16276 KB
EMV_Version4_1_2_of_5.pdf	38	Non Patent Literature	20147 KB
EMV_Version4_1_3_of_5.pdf	38	Non Patent Literature	20660 KB
EMV_Version4_1_4_of_5.pdf	38	Non Patent Literature	21751 KB
EMV_Version4_3_Book_3_2_of_4.pdf	58	Non Patent Literature	17652 KB
EMV_Version4_3_Book_3_3_of_4.pdf	58	Non Patent Literature	19875 KB
EMV_Version4_3_Book_3_4_of_4.pdf	56	Non Patent Literature	17117 KB

EMV_Version4_3_3_of_6.pdf	22	Non Patent Literature	14463 KB
EMV_Version4_3_4_of_6.pdf	22	Non Patent Literature	12252 KB
EMV_Version4_3_5_of_6.pdf	22	Non Patent Literature	12697 KB
EMV_Version4_3_6_of_6.pdf	42	Non Patent Literature	22311 KB
EMV_Version4_3_Book_3_1_of_4.pdf	58	Non Patent Literature	14723 KB
MJØLSNES.pdf	13	Non Patent Literature	1222 KB
MOTT.pdf	22	Non Patent Literature	12395 KB
NARAYANASWAMI.pdf	10	Non Patent Literature	2820 KB
PEREZ.pdf	8	Non Patent Literature	3975 KB
FEHR_1_of_2.pdf	40	Non Patent Literature	16209 KB
FEHR_2_of_2.pdf	39	Non Patent Literature	12433 KB
GHAG.pdf	6	Non Patent Literature	1711 KB
Google_Wallet.pdf	1	Non Patent Literature	595 KB
HEISLER.pdf	7	Non Patent Literature	4135 KB
HONIG.pdf	49	Non Patent Literature	6061 KB
JAVANI.pdf	6	Non Patent Literature	4074 KB
KADAMBI.pdf	11	Non Patent Literature	6408 KB
KILLORAN.pdf	4	Non Patent Literature	3277 KB
LI.pdf	11	Non Patent Literature	2268 KB

Summary_of_X9_119_Part2.pdf	2	Non Patent Literature	79 KB
tokenization_prime_time.pdf	51	Non Patent Literature	930 KB
Wallet_Help.pdf	1	Non Patent Literature	588 KB
X9_Tokenization_Webinar.pdf	20	Non Patent Literature	572 KB
POPPER.pdf	2	Non Patent Literature	992 KB
QASIM.pdf	5	Non Patent Literature	2677 KB
Rambus_Press.pdf	2	Non Patent Literature	994 KB
Securing_Payments_Payments_Tokenization_in_Primetime_Susan_Pandy.pdf	20	Non Patent Literature	1814 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
WYAT-0002-13C12US_IDS_transmittal_form_1.pdf	4F0C61245B9B943C8CDD1980604C62915688BD2FB91ED153113BB7F505135EE0E56F14A31D9412F4C8E6A7FB5F0611AEB88CB24D3652D38E0338895D9253C4F4
BOYD.pdf	D39B5EA68D301627A34756AD9BD1B06CA843EED22AB642B4A876FB74C8AB1DEC0F5AE064DE5007D5DAEC8E15F8B120FA8419966594726C29DD2741D4A08B84A7
BUCCAFURRI.pdf	0A03D387FF0B573B3D44288C20DA995EA07BBB7131D4966B500AE4E9936C64E407DCE7B3D23A7179B9206733F06FF9524E9712AD50CE3D1B91F1AC9870CE2AA4
Card_Technology.pdf	0809D4A22C921A988D89D6F68E953187CCF21D33A66525F04C26A70249ECA367A7C5931BDD42838D1F6D842A4033F05BFD

	BC3F5A0250F2E0D99E4CCAEB277E50
Chip_Advisory.pdf	3BF42C638C86E4CCE628BAE2FEB50602C48DDB1A618BDE703DC8AA70C22FF86566165328116OFC4A31EA6F335BF789B897473CD2017CF095ED8FDB11117499BF
Commbank.pdf	3F783425E0CD95911F2620801664B942C6052C062D6BBB0A7D166DD2BEA9B0909ACADA35C1E4F6427EEBA1B11C1A987D3C06E5407AC2339F5656D210AA8DE8A5
ADAMS.pdf	5538A8606D81EDB46E767776C89CBC10DBE56E87CE7D75DBCA999C1E6B0C145FBF2497EC3CF335E8B558F3BD00F9A9B004038120791D8D10F3C6EED942CED267
Allynis.pdf	AE1ED03818B28EFA0A821437DFB702B2F12B64199C77B38993CFCC0E24812B6D8D73D57D72085004133C2D27B4B303F09097F666A043E93743532AF53FFB8589
Allynis_TSM.pdf	B59AE47468827AF15EA3731015D7531260D0614D26D57E5E2FD965DCAD55541EE8B1126BF5D50BD6467B5EF8D79A9D7A937121155068BB19D0CC665034BE897D
ASSORA.pdf	72152DD9C6DA5F3F4B76822DC8EAA9E9EEAF01D772804D70796B7A58EA7619D48E9103E844F97839729D3B2785B3E61E0106CAA97D4E32AEA14639AEF5780D8C
ATMIA.pdf	0211530F0CB6627EE4E37AE62337AC066512E89EF5B4ECE51627B15ADCA344A6B92C2D1578095A5CBA79B3986E3DDCD49FC7955A75437465B8DE32517DC6FDCF
Bell.pdf	8064F8F28BF156C8D715B4E3DD393729D85784F6826A8EC6A93BEF703B8275D6F92F259B048FB26BC2A4FC46ED9F3D52C32BCB6068ADB5F7315F5A08BA610ED2
BofA.pdf	B9C51D87CBD3E127E48A4FC323A5C9A4F879C8829F33908A47F584F3F722F35C4C5BC77994C3838382FC2F59C938CD35579B740E8E5986CBC26A31C13EA68335
EMV_Version4_1_5_of_5.pdf	09E8648272DD8B8A94C796DB06AB8A089115D2C23723F66468923A63872D3BF86953A6BEB638D487AC9D6295D2513B469C7

	D845452DDD783BB4DDC0A7ED73B7A
EMV_Version4_3_1_of_6.pdf	6A683BE6E45691E5B837EEC4F73905520507606ACA25EE9871EA1BB6A7F3A3E38CCA80B795821BD1106D35C761259B02099F3AFEF6D15211F86EFEF896CDEFE5
EMV_Version4_3_2_of_6.pdf	6AFB6443D402596DB9B44C3420A4E016E52B510D9B4447859712CF58A231D11AE27A0432B0A8118E2C163C55DBC4C3D97FB6615542E972A3F532FE37BF0D3C3A
Eligible_Devices.pdf	E7485117B1C2B03C3E57978C24C80F344996A0BF6557E4F3E90F451A3C500BFC4BFE9CA24FA7752FF1B0E9F0250E9C30564140A1AF528334590AB968FED09A03
EMV_Version4_1_1_of_5.pdf	C881DF5451E974C752DA52A2E2A562AB265F57EBAE2774E9E53E331226548481C121353F6139084E7919DDCF580273AC0187351A32511E68D9A1EBD240BFDB87
EMV_Version4_1_2_of_5.pdf	8DBABA99D5CD6B530FDFDCF28D2317C470922190A30F560E03FB89A8342B16D587AB65D0FD63354872D176E5095531EFE144E00779A6FE26B62C19EFB699C731
EMV_Version4_1_3_of_5.pdf	91E406A620A19206E31ACAC834F41A166493704F2D57E20CC50D535C8C4C40EBEBB3D94097A92C35CF6EA82A099FAFC491D329C676BC6F77E0ECF8A32434E936
EMV_Version4_1_4_of_5.pdf	95675B681FDF86E36D4A8B0344D06DAF1E0F2C5D3937C02520F842A987462F85EE8C5B31F299EFDF5DD7431C745535605633C3E8C756EA1FB14A8DA22175A2F8
EMV_Version4_3_Book_3_2_of_4.pdf	BB2AD512AEDF46C95CFA42BE7C6277998D6184EF60B52539CD4E5EDE27E506D90FC11BB3A2CE12291E04E208B3DEF94B078F3A357A3C5DD7ED96AB765576D512
EMV_Version4_3_Book_3_3_of_4.pdf	BAEA77F15EB89EF675EBF883C1F5F32AF04A38EE434A47301928684B540883BFEB6240205DD7B31DCC25D35B4AC6448D479A32D69D120026DC4364E11E90734F
EMV_Version4_3_Book_3_4_of_4.pdf	877FF29B90A238E12574539C7D37CDFE609378ADEEA723394B7DEB6010C5101B7484D0BFD2AA59F29C88753D20E91BB4BF

	DEF8EE81F26673F046C013CFCE1DA9
EMV_Version4_3_3_of_6.pdf	DD5243F6F4744D9BF7E4150AF33414BC0A1F63296836B91141 7F792DB28AC797ED52EEA5258B861462FCB1B63E1DC193E8F 7EB9328B91A4D79773FAF762FB7B5
EMV_Version4_3_4_of_6.pdf	A0CBF5DE048BB65A28342200AA90D2DB67518FB008402A154 9FE93C35D25646C3EA8893A36EBA38637123047B15F01ADE0 F40C9F6CACEC52F6D8365B96E1AF5A
EMV_Version4_3_5_of_6.pdf	EFDDAF48C250F6B032202793A25FDCCA391B321E4DAFF8D0 C4996D16C4224F3C80C3F5B7D6E06DE65F26040D8D0F9DC97 A21180AFA4F3F7A3806E1F8EA2C25D0
EMV_Version4_3_6_of_6.pdf	CCB68CAA90AB233F7A81EB8F0FADE2E709869436A22CEB6A 193D5EF1B88FB0BA25925173DF9C63741D99525CB8C895E50 1944A012E4A57891934C4ED15938229
EMV_Version4_3_Book_3_1_of _4.pdf	6930BDEDACE65535E0B1CE174B42C865A1A3C89352C0C9AB 7F76AFBC4E156DFFBDBFE45F4012A00BF2CB17EC782ECB8A 0FF9EC4169CB4432769374BF89F91488
MJØLSNES.pdf	09D5809D62DD012C6ADEE666A17D3182F18B22AF9B8DDFB7 F7398D10FB60242B48F30404B8F6B0DE4D33990511D03F310C 0547287EC3FCE7A7EFCE19769D5AE0
MOTT.pdf	F5787F4B247AE378139D1974886D273B671EFCA194DC5FF1E D6B1042123433DA4645B7FEC6D27414D143831D29ABCC930F 9006D5FE9C3057465965562E9D566
NARAYANASWAMI.pdf	1F01E07A411880966 4E0D9CC83FC20A6B960A9AFF640C1752F 7F5CD80BF49CF293A8B00AC0140898CE6CAAB2FF8CA551AF 0DADA899EFB9B74F6368245E993795
PEREZ.pdf	338F26C8F06091EA9D3BBC34096CF77DF4E11F23D432D66CB 5775D98DE781A68804BA5E436D31C561B8B643B1171C22B4D 0C93FC5F1E5B3DA12DA5B535C922FC
FEHR_1_of_2.pdf	85FFB2B011773749EDC984747130C968BDA51C0260966D1FE0 44F389270F548C01A44ECCC5BAFC2FEE2DE83A022EFBF057

	B7F2EDA4D651C8DAB11F066B049B5A
FEHR_2_of_2.pdf	7900EC82C6BE4655B37103766DE66F86E5F6E5C12D3BFD8C05BE0547E53E684DE6D10C38D4362E0C399194C2BE5CD3CB148F05ABE3653DA24D73E5014BEC0DBB
GHAG.pdf	954672BA13D15FA8ABC894A85FA1FDAA59C8D856E871460C1C5B95DB127B63B415127F3F04315362904D3C35C02CCF82696EC8A7C706337175A277A404356253
Google_Wallet.pdf	8DE6568D7B8A287E65F9A5F38DAFE05157D68838BECF7D5C9A39077B87AA9C2603AFFBB7D5D8089105BE7C8E50A44CB11ABF434A46703A917F25857DB21F9336
HEISLER.pdf	0E16D814795430518BA5A076A2E7E9B9BD3FE9634A06F6244938DE72238F52193449D709F2AB1038F861D111C47136E1EB04707564ED39AF1BA37EB4A8E34E7C
HONIG.pdf	A2884CD2EC73B871CA75F215B7BCBAA9499D4BC858336EAE80AD7D60DB03890910554D16C790E802FEBF3B7CFD4329056557D99134401E90100FBF42214068E8
JAVANI.pdf	C1C1C6016E392BE5703EE23C81F44301C270112C39F70E46BF154EC418C795EB1D58752408E78114556D07AB4F625631BB93AD09897016178230 2BE80FF9E7FC
KADAMBI.pdf	55DDD4E83880ADE76EAC158D99CFF5CBA4F5F19788B43599DD9F25CCCAEFB4A47D3EE87763CF0DE37BBE0D29A60E14AF6EE32AB836EB0793194BC576334A21E9
KILLORAN.pdf	31D22C0393C99C2464F7E79D35CD518E2D8BE96574C00C6E052BAA2FE4658D25DE3E026CF660C67217EDAA58C43431136600996FAA4D959D210B95488FEBA2B3
LI.pdf	A5D9430B1149889FAE605EE6A9BCF8F3ACA84E058B1ECE680EF9F5BB967BB48862D1C09ADC185AFCA1442C77FA356C82B37FC19D6ECAB8027A5ECC285E0646C8
Summary_of_X9_119_Part2.pdf	869F6F2AFA594E838EF6B0589B11819DE452077F807B36F28C5C961E0CD26E9ACD6B6603C18F908D5194429A78A419349889

	ED7018FD23D8B59D629A223C34BA
tokenization_prime_time.pdf	B8AE3162E55ED2C8A3466534174D192DF3C5CD0D92CA3C6A FE7D55A6214EA2C66EC8137D326C3AB62BD50B10D0B918EE B2423781024213532A1BB6C33B8FACCC
Wallet_Help.pdf	093CF9F287C81267050436 8F67CCAEE14CCA99404536 5B28126FD67E0852A79FC2B32E4C24D202DEA6E271A07A5ED194BD 7ABE31317FC62F107F13373A0E60BA
X9_Tokenization_Webinar.pdf	0AF132928B9667E9A7A146D1990C6E6C3A1A7D667A170C3D6 036A151B1244C339D26937084A01AAA44A1876E5A08DB9BAF4 6B6FF1F70CD8883DAD2DEE005B8B3
POPPER.pdf	14723D8F1788F840B6227D379A0D6D637AF2BEFC5B0456B12 D6215F3753F9226E3C13654E41514804952720 5B68F19D410E7 566A8542FEC22F09FFB4B0E6C7BE
QASIM.pdf	412CA0030F07729AE1E0C74E6A24C962E33CF30397E768FF63 D3ADEE0EA94F20BCC39E2051F29F663F877639D52BF20A4A3 1376E0B78EC5DD4495927C1382178
Rambus_Press.pdf	333A954C9E71DC993BCDD386494DAB6D5F1C92FD923D4E38 06843911D2A9F98CD7CAD0CA34DB71FE25444833F221BE3F1 325D49EF2A1F72F8C64A42A061D6B67
Securing_Payments_Payments_Tokenization_in_Primetime_Susan_Pandy.pdf	875973E804A5800330E6FFCB7D5FC3E9BB11D2BC66F10838C 7342F8E4E48BA0FC2762F20E1408C6DC2931DFBD824D1A11C 6799593DAECD4DCB09435D707AA4A5

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.

PTO/SB/08a (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.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17528073
Filing Date	2021-11-16
First Named Inventor	David WYATT
Art Unit	2876
Examiner Name	LEE, SEUNG H.
Attorney Docket Number	WYAT-0002-13C12US

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	1	"EMVCO Publishes Technical Framework for its Payment Tokenisation Specification," EMVCO, March 11, 2014, pp. 1-2.	
	2	"Encryption and Tokenization: Which is best for your business?," Townsend Security, 2010, pp. 1-4.	
	3	MOLEN, "Engadget Primed: What is NFC, and why do we care?," Engadget, June 10, 2011, pp. 1-11.	
	4	"Exploring Google Wallet using the secure element interface," nelenkov.blogspot.com, August 27, 2012, pp. 1-11.	
	5	"Financial Cryptography," 5th International Conference, FC 2001 Proceedings, Grand Cayman, British West Indies, February 19-22, 2001, Paul F. Syverson (Editor), pp. 1-57.	
	6	"Gemalto to Provide Isis Mobile Commerce Platform with Trusted Service Manager (TSM) Solution," Business Wire, December 12, 2011, pp. 1-3.	
	7	"Google Checkout checks out, replaced by Google Wallet," Android Community, November 17, 2011, page 1.	
	8	"Google Checkout HTML API Short Attribute Reference," Google Checkout, Google Code (archive.org), March 27, 2012, pp. 1-4.	
	9	"Google Commerce: Building one wallet: Google Checkout is transitioning to Google Wallet," commerce.googleblog.com, November 16, 2011, pp. 1-2.	
	10	"Google Prepaid Cards," Wallet Help, Google (archive.org), October 3, 2012, page 1.	
	11	CLARK, "Google Unveils first Android NFC phone - but Nexus S is limited to tag reading only for now," NFC World, December 7, 2010, pp. 1-4.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	12	"Google Wallet launches officially on Nexus S 4G," Android Community, September 19, 2011, pp. 1-2.	
	13	GARSIDE, "Google Wallet mobile payments system launched to public," The Guardian, September 19, 2011, page 1.	
	14	BOULTON, "Google Wallet Mobile Payments Coming to New York, Francisco; Google Wallet will launch this summer to enable consumers to pay for goods by tapping their Samsung Nexus 2 4G Android phones at NFC-fitted sales terminals at Subway, Macy's and other retailers," eWeek.com, May 26, 2011, pp. 1-2.	
	15	FINGAS, "Google Wallet reaches the web, reminds most of us that it exists," Engadget, October 4, 2012, pp. 1-6.	
	16	RAPHAEL, "Google's Eric Schmidt spills clues about Android Gingerbread," ComputerWorld, November 15, 2010, pp. 1-3.	
	17	"Handset makers line up behind Isis NFC payment platform," Old GigaOm, September 27, 2011, pp. 1-2.	
	18	"How it Works," Wallet Help, Google (archive.org), March 12, 2013, page 1.	
	19	"How to find out IMEI number on Google Nexus S phone," Tech Notes Desk, January 10, 2013, page 1.	
	20	"La Caixa," Annual Report, 2010, Barcelona, Spain, pp. 1-190.	
	21	"INSIDE Contactless to Equip KTFMobile Payment Project Mobile Phones; Korean Manufacturer Confirms INSIDE's NFC Maturity by Embedding MicroRead into LG Electronics and Samsung Electronics Mobile Phones for its Mobile Payment Project," Business Wire, July 16, 2007, pp. 1-2.	
	22	CLUCKEY, "Is a contactless ATM inevitable? Bank of America seems to think so; the FI has filed a patent application for a 'Contactless Automated Teller Machine,'" ATM Marketplace, September 20, 2012, pp. 1-3.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	23	"Isis™ Launches in Austin and Salt Lake City; As Many as 20 Isis Ready™ Handsets to Be Available by Year End," Business Wire, October 22, 2012, page 1.	
	24	PEREZ, "Isis Revealed: Carrier-Led Mobile Payments Venture Shows Off Its New App, Announces Banking Partners," TechCrunch, February 27, 2012, pp. 1-6.	
	25	SADEWO, "Isis to officially launch on Oct 22, more supported devices announced," androidauthority.com, October 18, 2012, pp. 1-2.	
	26	"MasterCard Approves NFC Phones from HTC, Intel, LG Electronics, Nokia, RIM, Samsung Electronics and Sony," Professional Services Close-Up, May 10, 2012, Close-Up Media, Inc., pp. 1-2.	
	27	"MASTERCARD INC, FORM 10-K (Annual Report)," Filed February 28, 2007, for the Period Ending December 31, 2006, pp. 1-204.	
	28	"MasterCard, Visa and American Express Propose New Global Standard to Make Online and Mobile Shopping Simpler and Safer," Global Hub, Engagement Bureau, Press Release, October 1, 2013, pp. 1-2.	
	29	"Fact Sheet: Mobile Commerce: A New Way to Pay: MasterCard Mobile Commerce," May 26, 2011, pp. 1-4.	
	30	"McDonald's testing e-payment system," USA Today, May 29, 2001, pp. 1-3.	
	31	"Mobile Contactless Payments Trialled Live at Mobile World Congress 2010; GSMA, Samsung, Telefónica and Visa, with Giesecke & Devrient, Ingenico, ITN International and La Caixa, collaborate across industries to give Congress attendees an opportunity to experience NFC," Business Wire, February 15, 2010, pp. 1-3.	
	32	"Mobile Payment Bringing value to payments on mobile," Gemalto, November 2011, pp. 1-4.	
	33	WOO, "Mobile PayPass Meets Cloud in Google Wallet," Global Hub, August 1, 2012, pp. 1-2.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	34	HEUN, "Mobile Wallet Consortium Strives Cautiously In 2012; The telco joint effort proceeded more slowly than expected, but its leaders maintain that the mobile wallet business is big enough for lots of players," Section: MOBILE: ISIS, January 1, 2013, Page 47, Vol. 2, No. 1, SouceMedia LLC d/b/a Arizent, pp. 1-3.
	35	BELL, "Mobile's Gains Prompt More Banks To Move Beyond Cards For ATM Access," Payments Source, Section: DEBIT: Vol. 1, No. 1, May 12, 2011, pp. 1-4.

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Jose S. Garcia/	Date (YYYY-MM-DD)	2023-01-12
Name/Print	Jose S. Garcia	Registration Number	43,628

This collection of information is required by 37 CFR 1.97 and 1.98. 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 1.14. This collection is estimated to take 1 hour 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. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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 record s.

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.

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 01:46:45 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 #	61424625	FILING DATE	11/16/2021
CUSTOMER #	136197	FIRST NAMED INVENTOR	David WYATT
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	-

Documents

TOTAL DOCUMENTS: 50

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
WYAT-0002-13C12US_IDS_transmittal_form_2.pdf	7	Information Disclosure Statement (IDS) Form (SB08)	1237 KB
Global_Hub_Engagement_Bureau.pdf	2	Non Patent Literature	1475 KB
Google Prepaid.pdf	1	Non Patent Literature	376 KB
Google_Checkout.pdf	4	Non Patent Literature	3470 KB
Google_Commerce.pdf	2	Non Patent Literature	732 KB
HEUN.pdf	3	Non Patent Literature	1732 KB

How_it_Works.pdf	1	Non Patent Literature	451 KB
INSIDE.pdf	2	Non Patent Literature	916 KB
Isis.pdf	1	Non Patent Literature	757 KB
Android_Community.pdf	1	Non Patent Literature	467 KB
BELL.pdf	4	Non Patent Literature	1164 KB
BOULTON.pdf	2	Non Patent Literature	906 KB
CLARK.pdf	4	Non Patent Literature	2713 KB
CLUCKEY.pdf	3	Non Patent Literature	1441 KB
EMVCO.pdf	2	Non Patent Literature	1685 KB
Financial_Cryptography.pdf	57	Non Patent Literature	3150 KB
FINGAS.pdf	6	Non Patent Literature	3940 KB
GARSIDE.pdf	1	Non Patent Literature	884 KB
Gemalto.pdf	3	Non Patent Literature	878 KB
GigaOm.pdf	2	Non Patent Literature	1035 KB
La_Caixa_6_of_6.pdf	30	Non Patent Literature	17444 KB
La_Caixa_1_of_6.pdf	32	Non Patent Literature	21513 KB
La_Caixa_2_of_6.pdf	32	Non Patent Literature	22815 KB
La_Caixa_3_of_6.pdf	32	Non Patent Literature	23969 KB
La_Caixa_4_of_6.pdf	32	Non Patent Literature	23751 KB
La_Caixa_5_of_6.pdf	32	Non Patent Literature	22026 KB

MASTERCARD_6_of_10.pdf	23	Non Patent Literature	17955 KB
MASTERCARD_7_of_10.pdf	11	Non Patent Literature	9661 KB
MASTERCARD_8_of_10.pdf	23	Non Patent Literature	22363 KB
MASTERCARD_9_of_10.pdf	11	Non Patent Literature	5409 KB
MASTERCARD_10_of_10.pdf	68	Non Patent Literature	2896 KB
MASTERCARD_1_of_10.pdf	16	Non Patent Literature	15168 KB
MASTERCARD_2_of_10.pdf	18	Non Patent Literature	20531 KB
MASTERCARD_3_of_10.pdf	17	Non Patent Literature	17524 KB
MASTERCARD_4_of_10.pdf	9	Non Patent Literature	8309 KB
MASTERCARD_5_of_10.pdf	8	Non Patent Literature	5521 KB
Nexus.pdf	2	Non Patent Literature	571 KB
Professional_Services.pdf	2	Non Patent Literature	862 KB
RAPHAEL.pdf	3	Non Patent Literature	2247 KB
SADEWO.pdf	2	Non Patent Literature	534 KB
Tech_Notes_Desk.pdf	1	Non Patent Literature	404 KB
TechCrunch.pdf	6	Non Patent Literature	2920 KB
Townsend_Security.pdf	4	Non Patent Literature	3446 KB
WOO.pdf	2	Non Patent Literature	991 KB
McDonald.pdf	3	Non Patent Literature	1042 KB

Mobile_Commerce.pdf	4	Non Patent Literature	934 KB
Mobile_Contactless.pdf	3	Non Patent Literature	1066 KB
Mobile_Payment_Bringing.pdf	4	Non Patent Literature	2643 KB
MOLEN.pdf	11	Non Patent Literature	6042 KB
nelenkov.pdf	11	Non Patent Literature	7576 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
WYAT-0002-13C12US_IDS_transmittal_form_2.pdf	BA5830495ECB05C97C396842A418096913A6E649F75664D3958C60D9CB72FBCD84283D12C381C98A5D1F8300B27A2E65DFB0144E59DDF6C3BEC22FC610CC32E7
Global_Hub_Engagement_Bureau.pdf	1B2860549A9F1865136D4CE3E063C0FE6E3A4FAF018910007863734D65E5C569F0CFECF996FA01A0019C2B9A76CB689B9DEB760C764B665434789199C46603D7
Google Prepaid.pdf	8B959C8B9FF29691DA36109A27CA0546D1E5ED86E05C7C2D718BF7233732E5971CA4EC9838E68135651FD99EE59DFE227D3C1E4BB8953AD92156FEF958C1D03D
Google_Checkout.pdf	DE1F2BCF81860AE1700F454C78CB662CB8F2012C4BF435FBF9386171224F5A2374259149A295785CD3CB53F7CED26AEE8CD6E79BF92FDDC6D0778EABF6EFE3CD
Google_Commerce.pdf	D6A206586977D368963108F750504B9C64DF513A0277AA7DF4443390E8082E29D3CAB008CF227C7954E187BD02E65015A25FF3085AF9872EAE071C681F4D067D
HEUN.pdf	4518A78961CBC9DD99CC0245FA7782798E5599CE9D9FF2C40943E617400FADFB527A60B372B9839BC2CAC96FCD3ED7893CFCBAEB9685E874459A29FAB1558E25

How_it_Works.pdf	6A1075DBE81FC8DFFA36D02EC494923AF1949AF433B4C1ED6C2BDC0F74ED79F0D2D34B51A9E6B84EFC136F91DFD756E1865AE2C1E5BBD6661859ED884D80649B
INSIDE.pdf	06D31CC4E819EDF91CFB310231189A1DA08355775DFCDDF4EE9E253F98B94CEA1756F1296F3400EB146B0C24C3C6B3B87A862FF81C3B98A70D9130AE4190F406
Isis.pdf	0B1F28A30106AC28361C50B4C69409BE601C7A4FFE4A6DA75867F09CC2FC8062DFB32A49C3488C2218D96BBEABA26CCC7631994B1A1E8AB6E97C09378C65514C
Android_Community.pdf	C3BC9C2062C05D56BA3660C9F2D60486B0BEB99D18E73A594875AECC931B2634A7544F3FB23E57F1710789F76019F9AC8DC71F618DF2D18F6D854682C51537EE
BELL.pdf	315832184105E00308AAD8A29B95A000D6749F8CB7C65041F9566C441DD3162D1FC7A19009D00668D356569BBC482284FFFEDCEA7F1CFEE4F075B0AB357DA480
BOULTON.pdf	E6D39974975D00C9AB39E25494338B6DC0EEDB4F1D0D4DF00AB2B703A05F8FCD8D56657CDD2A7A603C4438CBAAFFF69ED36231A0A0679374E351C8B3927C19BA
CLARK.pdf	384376E17AF5B596674C2AC229D494E0F5ACC90454A41EC94C18184774A65C56ECAB0F4172F969E862E0B1544FB152BE402516752757C829747A0E56C46631F2
CLUCKEY.pdf	81DE99B649A5FAB49D3418750A508E9F1F6DF25034531987F96B6D18987D1AF0DEFCF0B7C5ABAC710815DBC8783FDF0530C0D2263CBC4E0E2C172D80D6170DD1
EMVCO.pdf	E49043EA9DE6EAB06874594838EFBF040F38176620AAD582C2EAA7AF1CC9ED9F5EC83021DEF43C8067A779F52D900B042896438A6C9AD9A50226F411ACD7095E
Financial_Cryptography.pdf	8AD5653B2E0B3E6D48A3A006BCDA86D880D9DC1DDDBE9CB2DFCA329662729C3497F2744875FF09CCF031E72EC1116C7F5A4425C24EAA7099CFBEFD6C4B4E0449

FINGAS.pdf	F5F5A38053FDCD7C45275A7CC8F5B1DF3178E0F710A9B443C0367EE949B9D01CF79A1F9440DB7D9444F744C68037ACD0D46841CE792929FD5B6FB364CF179E90
GARSIDE.pdf	CF87ECE84BC9B4ABA95B312829C5F63D0B681E82700761A0D2C40116CEC37B7EAAA27EEDD13D40A2FE6DD20AECD59AF4480F423F9FD46A2C3E1ABAC5E9F6E6F0
Gemalto.pdf	3D6D9B0AB8B7880DC398814B53D29D703969763EA27B3FC1857D3F7751313A5620E42EF0480F18B4B5BA4FBDC76B8CBFE833E9D80C5A11262D0A57D2FBD385A5
GigaOm.pdf	1350964A54E57749A04DF79088AE54D805D398FAD47C2196517DCC1FEB5398916789DE59319492D14578F7DDE32AF54C6931F60D26758A39B5DA607ACEEF0A53
La_Caixa_6_of_6.pdf	B985241C5F6784FC20C29002A7A7AF3D8F612BD40ED122824A6C1F5F6AC598952B6A997280F03FE5C8D815141A6270DF94913BE22320F63B77BC7FE47AAAA789
La_Caixa_1_of_6.pdf	6067EC177712DA341ACE17FCDFC84CC30E24FF87E635F26BF2F96FE9CB3B82FEADD90C94FE02CD9AB91CE35BF932C01D45B0B485DE6D04EB49A3E9CEC1D67FE7
La_Caixa_2_of_6.pdf	EF8BE7810751C2D53CDB859E9D4177268EAD1B4A05C8CD5D559846A1CDF5162D4E3DA4D3124BA3414196118AE05D3532573B91831742F2FDE10A4CCF3F107263
La_Caixa_3_of_6.pdf	9F15E16381D20F1AE4DD17CCCDB4D1B0CF9DA6D7ECB795527A97FA3BA6F4CD299F577DFBB9464B2DE61B074DFDA093258FA720376A3D187AD6D0B71CD55528FE
La_Caixa_4_of_6.pdf	A7403E4E11CFCB0348C4A5E248246A9DC0BCB87466201A2C4DC8EBBDC6335F360E9849235295B6C977A8E636FDE5D13F1E9D18924F010975EB5A01D1FE6CB78B
La_Caixa_5_of_6.pdf	B70D3D3DA9361727698707DD052C2F4379DD4A752D79B0B06737CDC44052618EAB10253E4B9D3D2B03D10ACC61665E930613D1F7A867D924DDE413B1B339A008

MASTERCARD_6_of_10.pdf	FDA16A567C7AD537B8F913F79E9F710BD2FA86F0F28DC3CE5A21546F31B02D24D8A9FD529A74E71006F1346F7726E9BF657A6445606D9BFE87E9A3FAF807DBCC
MASTERCARD_7_of_10.pdf	69B212D15BAC37F3163786A6F720DD1686351F62076E47FA201CD90F441173DBBFDE18B7B5765AD9D3325CCCFBEFD3754A830FFF06CE34C488BE5AB5A9DB0628
MASTERCARD_8_of_10.pdf	F7228FEFE4EB74FA3DB9A137027494961B592F3860A0682849CA771838EDDD45A034B8C008C571D26F5E5DAB54B9A2E93358BC639D9B05F955A5CB28A87BB5EB
MASTERCARD_9_of_10.pdf	C065FE1371A60E2A6C7407E5D8BB6D0394195A54796C70D1FF25CB3CCC99D8BC6B31EABDC6E1B17FCB01FFC11CE432A6BADEBDD85D5CE286C3915394FFCEB0BB
MASTERCARD_10_of_10.pdf	86C8EBC3B75FDCC84C2FE3E2AB2ABEC0DAA1CBF8391C0574D363AFDE5F889CF4149609E0BEE685EA21FC1B965C72417AE78A282C998D6A27C150DC8C267D190B
MASTERCARD_1_of_10.pdf	7AE810B5E952B26E945BED3DFF552935360682F39E99CA6989D99CC20921CB9ABD2D3DC2D9FB80450034F260D9E8E6C1B899847612B9FE06143BA36ACB225013
MASTERCARD_2_of_10.pdf	0E8A605D28CBE07995AE1652D69FCE321DEB5C1307576C42735560DFDF0ED540FCE9B8F637C963C95E9D9782D623A29033DE9FD7C2A9B0BFA6F34FCCEEBC6B69
MASTERCARD_3_of_10.pdf	F5B7FD326B1E4A5C7725ADC75EC7D614C0388311A63F82349A0AB673B98B08AF2C7984649EB4F722A12AC6A611E52615BAF9F34D7A7A8B5604494E4E4E5621B1
MASTERCARD_4_of_10.pdf	24406E095B1C7D490FFE0CB8C1258C03E8752468EDDC38680815988BC9CDCF625828C5E5E6F9AB5846122D9AF6FB82AE3345A24F41EEBF5F336D9EDA1A84950D
MASTERCARD_5_of_10.pdf	4CA7B532789C799CA62C239737A7586FFD2A4DD8AD9999DD8910E659D80CB5E30F37A6C504C810A34E222C893C160913C5713FC996A06605B6FE18816B7EEE94

Nexus.pdf	CD282E7EB93402841F3598C1ABF9323875831FC28BC5C38869538B099FF1ADF3251DCBC6944C57CC9DC480032807212CA8A8F1B1A79CA3D20F46D69235B1E282
Professional_Services.pdf	8CF1A963590524130C097DB5B2B4B5890D7A04FC91400CF1D026B4B94C3129C7EE6DFAFA8172F846E40B276760D3EBB7F766E6DD68CF1B40D8990831 4E08E74F
RAPHAEL.pdf	233867F75F5A66CC2E307DDB2F9454BDDA5CF6276DC1038A2D4CD3750E2CF0E5F746B7801AC979F5D9FAD49C0CE2C638CA5A6D915D2DE75ADA795F4ADC025BA6
SADEWO.pdf	81450CBFEE8BC606808F7CCF9CF2E91DCAC75A91F44CE662E2DFFF88FD5EA7CE429CD3225C048A8A6BBD1689CC3DF3B8AEB788B54F41424C03A4FFA67B926D9A
Tech_Notes_Desk.pdf	6983DE0BBC7E54384E3180638091F493CCB954E76A4CB98A20F4F4D2EF379CCCAB748D6FE86BDBEB4E83A50C2110265A2F6D6BF55F0EE95D3B278A2C479F6266
TechCrunch.pdf	6F15C32BC38897983129699DDBA3B8F066B911CF4174D4FCB6DF3D7687D639EDAA4F0AFFA409AFF581AB1ACDAEB42BD27209ABA831831B36FBAB9A54C9EB1473
Townsend_Security.pdf	0FFA78E14FD633D718F240117AD1CDD22780404495877A3F83841834AA4A81C3238E580C9267DF46433445C610657AE1127DAFD4CDDA10B5C46FF1829E99A62C
WOO.pdf	5515199EAF19479E8EB34185F3050DE852A2DABE1D7515C140AD39FA93034B77A9EA3A23A8D1D2B7FD4528CBE2F52CD0F82D8A02ADA1516A5B7CF209B6BF6B50
McDonald.pdf	FF3C99784A6AC857ACEE5F64B2ACB7940FCF7DA7F752A38CFC60EB7773FEFEEC63F34106FC94BF8B5830919C173C73A95A7F2487B673065028807C05C07C09CC
Mobile_Commerce.pdf	0C444481F5FAF77E1A024752C687615FEF5B3540D496D12BBE8F7D9738C6E541B472EC16FC621FF600423C138BA7E5AEBE59185E6BCB6C5891C0D475FDE5809B

Mobile_Contactless.pdf	449F08C62980BE2BE60DA53B29F7A0C80EFC4C85C63A4C595A12836E103D1329E8F0C7B5BEC56DC54634861E264463B535EF6A08A939E4789D74679F9F40DB78
Mobile_Payment_Bringing.pdf	848523007D735C5E54C5F4B4DB6664458D511C4F7F5F803DB695C7B27BD373C155FA94D594FE6B9698B6F40F254D6D3453DB4C64BA64B88A1F91C7D9BBC76A8C
MOLEN.pdf	2DC48712A930C9EEED6A6AE3DF301005B13B3F9A539FFC0B681DFC9D4D613B745FC0FC1D07CA00BCA7CCCC1C731568892D309F5D3154206D8D93CEFB4CB8775E
nelenkov.pdf	F808120F02058F894E7E039FA3136A5EFD52AD3AB88AEA3DD05314D11F36FB64AD149608CB9C76129FE688CF82606CD781000AD235E837E496556926D7A5F43A

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.

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (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.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17528073
Filing Date	2021-11-16
First Named Inventor	David WYATT
Art Unit	2876
Examiner Name	LEE, SEUNG H.
Attorney Docket Number	WYAT-0002-13C12US

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	1	Motorola MotoACTV Smartwatch, http://www.manualplanet.com/pdf/watches/motorola/motorola-motoactv-gpsfitness-tracker-quick-start-guide.pdf, 2012, pp. 1-2.	
	2	PEREZ, "New NFC-Enabled Phones to Hit Europe," ReadWriteWeb, February 18, 2011, pp. 1-3.	
	3	WESTER, "New Samsung Galaxy S4 phone includes NFC, innovative barcode technology; New Samsung smartphone adds a number of features that may spur mobile payment adoption," Mobile Payments Today, March 15, 2013, Networld Media Group, pp. 1-2.	
	4	"NFC Focus: Which Smartphones Have NFC?," International Business Times News, August 9, 2012, pp. 1-3	
	5	"NFC for mobile operators; Maximizing opportunities in the mobile NFC marketplace," Gemalto, November 2009, pp. 1-2.	
	6	CATHELINAIS, "Nice, the first city to switch to contactless payment," 01net.com, May 21, 2010, pp. 1-6.	
	7	CLARK, "Orange to offer Samsung Wave 578 NFC across Europe - but not in the UK," NFC World, February 14, 2011, pp. 1-4.	
	8	CLARK, "Orange to roll out NFC services across Europe in 2011," NFC World, December 16, 2010, pp. 1-3.	
	9	"PayPal Credit Card Tokenization Extension - Magento Connect," Magento Extension Marketplace, http://www.magentocommerce.com/magentoconnect/catalog/product/view/id/18715/s/paypal-credit-card-tokenization-extension-4490/, October 5, 2013, page 1.	
	10	Nanninga, "PayPal Credit Card Tokenization in Magento," SitePoint, September 30, 2013, pp. 1-11.	
	11	"Payment Card Industry (PCI), Data Security Standard, PCI DSS Applicability in an EMV Environment, A Guidance Document, Version 1," PCI Security Standards Council, October 5, 2010, pp. 1-12.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	12	"Standard: PCI PIN Transaction Security Point of Interaction Security Requirements (PCI PTS POI), Version: 1.0, Information Supplement: ATM Security Guidelines," PCI Security Standards Council, January 2013, pp. 1-44.	
	13	"PayPal NVP API Developer Reference Enterprise Edition - eBay," August 28, 2012, pp. 1-382.	
	14	"Rambus' Bell ID to support Android Pay," Rambus, February 18, 2016, page 1.	
	15	"RIM implements Bell ID's Token Manager software for mobile payments," WMI Company News, January 23, 2013, World Market Intelligence Private Ltd., page 1.	
	16	LAI, "Samsung and Visa join forces to enable NFC mobile payment at 2012 Olympics," Engadget, April 1, 2011, pp. 1-6.	
	17	"Samsung and Visa Showcase Mobile Payments at the London 2012 Olympic and Paralympic Games," Business Wire, May 9, 2012, pp. 1-4.	
	18	WARREN, "Samsung and Visa Take NFC Mobile Payments Global," Mashable.com, February 25, 2013, pp. 1-2.	
	19	HASELTON, "Samsung and Visa team up for NFC mobile payments at London 2012 Olympics," Boy Genius Report, March 31, 2011, pp. 1-3.	
	20	"Samsung and Visa to Showcase Mobile Payments @ the London Olympics," Samsung Global Newsroom, May 9, 2012, pp. 1-3.	
	21	"Samsung Announces Launch Dates for Groundbreaking Mobile Payment Service: Samsung Pay," Samsung Global Newsroom, August 14, 2015, pp. 1-2.	
	22	GROTTA, "Samsung Begins to Phase Out Support of MST for Samsung Pay," PaymentsJournal, February 22, 2021, pp. 1-3.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	23	MURPH, "Samsung cooks up its own NFC module, destined for the Nexus S?," Engadget, December 1, 2010, pp. 1-2.	
	24	MOLEN, "Samsung Galaxy S III for Verizon Wireless review," Engadget, July 9, 2012, pp. 1-10.	
	25	TRENHOLM, "Samsung Galaxy S3 is Olympic phone for no-touch payments," CNET, May 9, 2012, pp. 1-2.	
	26	"Samsung Google Nexus S - Full Phone Specifications, Reviews: Royal droid," GSMArena.com (archive.org), November 2010, pp. 1-2.	
	27	"Samsung Google Nexus S review: Royal droid," GSMArena.com (archive.org), February 11, 2011, pp. 1-2.	
	28	"Samsung partners with FeliCa for Japanese NFC solutions, unveils 2012 Olympics' mobile payment app with Visa," Engadget, February 24, 2012, pp. 1-3.	
	29	CLARK, "Samsung picks NXP for S3," NFCW, May 14, 2012, pp. 1-2.	
	30	"SAMSUNG to Acquire LoopPay, Transformative Digital Wallet Platform," Samsung US Newsroom, February 18, 2015, pp. 1-2.	
	31	HEUN, "Samsung to Unveil NFC Smartwatch - Has Wrist-Payments' Time Come?," Payments Source, September 2, 2013, SourceMedia LLC d/b/a Arizent, pp. 1-2.	
	32	"Samsung's New Secu-NFC Chip Enables Secure Mobile Payment by Enhancing NFC with Security Features," Plus NEWS, November 30, 2011, pp. 1-2.	
	33	NANNINGA, "Save Credit Cards in Magento with Our New Paypal Extension," Classy Llama, August 15, 2013, pp. 1-4.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	34	'Shift4 Releases New Technology to Insure the Security of Its Merchants' and Partners' Payment Processing," Hotel Online (archive.org), October 5, 2005, pp. 1-2.
	35	'S-Pay: What is MST?," Samsung Levant, September 22, 2020, pp. 1-2.

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Jose S. Garcia/	Date (YYYY-MM-DD)	2023-01-12
Name/Print	Jose S. Garcia	Registration Number	43,628

This collection of information is required by 37 CFR 1.97 and 1.98. 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 1.14. This collection is estimated to take 1 hour 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. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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 record s.

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.

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 02:09:45 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 #	61424648	FILING DATE	11/16/2021
CUSTOMER #	136197	FIRST NAMED INVENTOR	David WYATT
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	-

Documents

TOTAL DOCUMENTS: 49

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
WYAT-0002-13C12US_IDS_transmittal_form_3.pdf	7	Information Disclosure Statement (IDS) Form (SB08)	1236 KB
MURPH.pdf	2	Non Patent Literature	1799 KB
Nanninga.pdf	11	Non Patent Literature	5410 KB
NFC_for_mobile_operators.pdf	2	Non Patent Literature	1832 KB
NFC_Smartwatch.pdf	2	Non Patent Literature	729 KB
NFC_World.pdf	3	Non Patent Literature	1717 KB

NFCW.pdf	2	Non Patent Literature	642 KB
Payment_Card_Industry.pdf	12	Non Patent Literature	7876 KB
Business_Wire.pdf	4	Non Patent Literature	1109 KB
CATHELINAIS.pdf	6	Non Patent Literature	2624 KB
CLARK.pdf	4	Non Patent Literature	2212 KB
Classy_Llama.pdf	4	Non Patent Literature	1389 KB
FeliCa.pdf	3	Non Patent Literature	1019 KB
GROTTA.pdf	3	Non Patent Literature	983 KB
GSMArena.pdf	2	Non Patent Literature	1073 KB
HASELTON.pdf	3	Non Patent Literature	1674 KB
International_Business_Times.pdf	3	Non Patent Literature	970 KB
LAI.pdf	6	Non Patent Literature	1345 KB
LoopPay.pdf	2	Non Patent Literature	561 KB
Magento.pdf	1	Non Patent Literature	388 KB
Mashable.pdf	2	Non Patent Literature	748 KB
PayPal_5_of_13.pdf	30	Non Patent Literature	16398 KB
PayPal_6_of_13.pdf	30	Non Patent Literature	19630 KB
PayPal_7_of_13.pdf	30	Non Patent Literature	12785 KB
PayPal_8_of_13.pdf	30	Non Patent Literature	5647 KB

PayPal_1_of_13.pdf	30	Non Patent Literature	15334 KB
PayPal_2_of_13.pdf	30	Non Patent Literature	17236 KB
PayPal_3_of_13.pdf	30	Non Patent Literature	22001 KB
PayPal_4_of_13.pdf	30	Non Patent Literature	22603 KB
PayPal_11_of_13.pdf	30	Non Patent Literature	16996 KB
PayPal_12_of_13.pdf	30	Non Patent Literature	11931 KB
PayPal_13_of_13.pdf	22	Non Patent Literature	15402 KB
PCI_PTS_POI_1_of_2.pdf	30	Non Patent Literature	18011 KB
PCI_PTS_POI_2_of_2.pdf	14	Non Patent Literature	8792 KB
PayPal_9_of_13.pdf	30	Non Patent Literature	17093 KB
PayPal_10_of_13.pdf	30	Non Patent Literature	16828 KB
Samsung_Pay.pdf	2	Non Patent Literature	964 KB
Shift4.pdf	2	Non Patent Literature	1706 KB
TRENHOLM.pdf	2	Non Patent Literature	1139 KB
WESTER.pdf	2	Non Patent Literature	890 KB
Plus_NEWS.pdf	2	Non Patent Literature	880 KB
Rambus.pdf	1	Non Patent Literature	715 KB
ReadWriteWeb.pdf	3	Non Patent Literature	1647 KB
RIM.pdf	1	Non Patent Literature	563 KB
Samsung_Galaxy.pdf	10	Non Patent Literature	5158 KB

Samsung_Global_Newsroom.pdf	3	Non Patent Literature	1692 KB
Samsung_Google.pdf	2	Non Patent Literature	892 KB
Samsung_Levant.pdf	2	Non Patent Literature	36 KB
Motorola.pdf	2	Non Patent Literature	946 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
WYAT-0002-13C12US_IDS_transmittal_form_3.pdf	E8F9662C840C33CF74178A92BD1829C7645747EB26A802ED12E1CDF6307F71904B95419B294EB20E078BEE49209BD45CE9EDF460301F3A713431337AAB1E019F
MURPH.pdf	3343EC02813F63AA251B29CCB759F410E7DA034EB61509565ACE5C9EFB123AEAF72763AA84F7C49FF21BD23F3C363C889D16EBBF249264F22730C98757B8C2BC
Nanninga.pdf	958C75487F5B101A3DF678BB33ECD2362EC70D1BB1E99FABF60F92FBB86C5E32EBE2ACB431B21C0FC3B99596EE2F29AED38D7D10FDA0D03AB4A851A1998F02A5
NFC_for_mobile_operators.pdf	68894F1EA5E57AFB428276AACEB67DCD87754F069DC06BE8C468402382602E46A6EF22F9B1E56929DAFD6071B57D0DD37C4C736D5ACECEE2C42DBCE88F2A0DFC
NFC_Smartwatch.pdf	7216E6FB9A7DBFA2E8C65E91A93623E3B7768ACBECBA0D1C5ECF5D6AF20D0A3CE3B46805B3AD220580186DA805E4FEA388EBCC888906FB1FF79261D1B2207285
NFC_World.pdf	9990DB3A91B2A162BE8A7131186E480FD515164903DC41D44B691329A44DA8A0148088C7102DFAE24355D1D5DF6C29BDC46067C259515B0A34AE3BCB543F3554
NFCW.pdf	0748C68CB295C0077BE7B8928744DED92BEB79BFA2E6D774

	E908A2AEEF7A4A9D6748A838206FB16F1E5C4295E044E61F2D3048568546686CD73C29BBE8D2FA4
Payment_Card_Industry.pdf	D548536D5AE1478E7351E8AAE2493CF8D203FF8D012F486EF1088DDCF885FBA6E70F5A8836711E8AC61B025E2D344E21F5171B54F1D8EEB7471FB13D2454F217
Business_Wire.pdf	9BBA328F64D067B28C7B507554458C1F8724977B81EA513E7E3BF45B90A68A1589DADA1C06AAFC4548A17BEACD5C3F2FAC9E180D40C6597C5805F8A53473C28F
CATHELINAIS.pdf	6E916ABFEE7615F6351CA0EE2774D195CAA14EABDC8DA1886EC415FC838AFFFFC9E5820F181094913BB9DA254A8E88B27DAB125AA0CB6F79BA313B36AAC3BCC1
CLARK.pdf	5542D017F144811C16CF888D6BBB7BF937D52EE45BAAC79445947646EF2CFEF1E289CE92E82BE16B6D177545AC495DF4B77FF43AF8A77FD40551ED6BB0F2376C
Classy_Llama.pdf	72B58E9ADC9D64B80D65D35E68476DE49AED4236C00680BC8AAC8D9849A6FEB3AFF61528270AAE548588993359408C15EA4DF7E053370311F3A4F8F59FB0CAB6
FeliCa.pdf	670F486FEC047C6C1A05C06ECEE07B5DB59E59999ED5D6F0D07CB42A663BDE44D62BA8124C00805BCCA25D2281511FE9DE077A1B5AE25FFC8BBCAEA458D2BAC7
GROTTA.pdf	FD48510D7BB56CA1A742C865728E869091FC6F2FC95539459F62C2CC299DFE18CFDA1E3CA4CBEBAF9948085D53DD91BEC83E1C4359ED9785F382C4A5EB235D68
GSMArena.pdf	F8AB00D2266A2F0638BF0DEEE9661533D41B7F3F1E02757A19C1E45523B10D894F323DAD77D3898BD9A68647F3614ECD542A905BABC187E19A0C0BC57479A3C7
HASELTON.pdf	3B7D85DE2D57659655D30DCA596E3C15B939FA21061DD1ABAC3031695BF7E0327E2979EE882A950F0C040D0D755A87E015047BF0E8E7FBBE6732B05F1DBFAD4C
International_Business_Times.p	591C8296C7326A16249AA877F4DF77F5FA1222CA14F49ECD1

df	3EEE469437C0869529539DA8E74FC2414298BF01CE7948FEC E28D4747812821499D614FDFE2FA81
LAI.pdf	3059934B176978C6E78F0C0FFC9F3B1CA3369EA0AE1291B518 0D3C009793D862B8B926ACEE4D027671DF0A4DDB46103914F 983126613D4694BAF81337131FFB1
LoopPay.pdf	7039BEEFF390C4B80E8AFFED67475DCDCBE0ECE48239F5B6 9CFEC0AF61457CA3E0CB46D8F2F52FF1B561BF840F17692D6 2D5FE6CB64B830BCD62791A79669F22
Magento.pdf	44AF16EA96332713F7D66853873ABB9F41D01E8CA30EB17FC C35C5F266C03B15DCB10425C21F0B7CDF1A57498136A6B343 677237284932 2EB77B87F793066A9B
Mashable.pdf	3F0BA00846A5FCA74ECFF125CD4BC670652E67CBB6B4B1EA 4002C91634BBB681D6F408569CE24691BD2877D28667C30B22 6E67D782C07744F978BF9F5B3C2B34
PayPal_5_of_13.pdf	9CACF4F33E2096E277465D5963E5EE84B05C3BD88269101A5 80428F5463D0FC56D7281BEA8A6E6CE2F51BBD4F41317BD6E D333E0071F114AB9F74EBC8CE4C20A
PayPal_6_of_13.pdf	F7914E8F14A46A69FAE5D1B04F73DCD42BD7ECB560AE8C43 5D086A5F3B028D95D65C5151A476EEFD4C42822F609E91AF8 F3EE98A04E830DA6CE21368B5FDB108
PayPal_7_of_13.pdf	7CCBDDA691AB8E566F8B5119FDFE4528C0EE48A5A635BBE2 35EC5D2206E614F17F39EFFC674C7533BEA9F6A4840FFC537 422782BC1C94FD57C17C86E3BF121FC
PayPal_8_of_13.pdf	E27C2390D887B918E317E516BB462556ACFE0EA45F6DCAB50 5CC41F2A33BD16B0B3BD9B1131686908AAE8A7B97F336A92C 1712E183078ADFFF59D583AD575A95
PayPal_1_of_13.pdf	AC0FD0DE7855150CFFD10C179950A71811A00F4DFDDA72C4 1268C12A674B42E3CF9A01DD762BFB289E3678D3F005553396 CE3976FD1DC15982011 9642FC2E25E
PayPal_2_of_13.pdf	2C310F42691C9572B6CAF696A6AF5ED68CA7BD527685E7337

	58D9116A0DE0018A61402251695C2E458B629EE6367D254EE49ECB5BC8612CB9D9BCFE901D97760
PayPal_3_of_13.pdf	12B535B15206D4E8717E56AA41962AC82240A71075EFE1ADBC603E98753A52884D086476D3D285FEE6219107D844B60C55E1789953D65A10359A436CA290E475
PayPal_4_of_13.pdf	78315A5E792007E6F6142B05ECF1299D45B146C547EBBC14E7D7D841B7B3D298E3F0CE55D092B15951A5391E273194FD7964F6B4C5DE2E976D85BD2E038ECD19
PayPal_11_of_13.pdf	C6AFC974D2D88BF92CA5BBCC165E892141BC05DE02B95B0A327DFA058534261A4D206BCDB03AA724526433D425E4D0F36EC8E40C7B298A9D132BA89781F4FFCF
PayPal_12_of_13.pdf	05F22582C380EF3B605D38128FD1C8F5462123C46CC8227C71CA8C17D2012B87B4BAC78AB07E00A750ACB802CE14C3877CB2F057517D6F0F18745FE6277A86E9
PayPal_13_of_13.pdf	8CF0AB1E777DE8E0816A59757D3642EEC5E42929AF052936E7121818B3FE3868CE959249BE905466FFE8F6EE5F582BE06C83597CBA0BD788D31682B7CB2C4F2B
PCI_PTS_POI_1_of_2.pdf	C0B91A6103A6C07B88004B990A7D414E5913C9396630FC2CC244058EB58000E5B9A37F620883E47023FC67AA34E225EDCD7425793AA2DBD85187DC2BF20A9DA1
PCI_PTS_POI_2_of_2.pdf	FAF8888E206D4EE6F49A7FAC6C9853B5AA76FB6529797A8A98F86EEF5631E8927E3891AD31235B4F5EAC2EA329912C758F0ED8FDA450FAB62F885B76541A64FA
PayPal_9_of_13.pdf	58C0C122AD3BAF6747D0767190E7028CDF21432DDFC39D833FF603B3C868B37CF3E7C004E3EFA57396C5166256AB166F96F1572C029970825F6791858BAC587D
PayPal_10_of_13.pdf	26F5F95BEAB1B6A09781805A16344D399C7651F3CA87790583D7063930B5EE49EC8CD44389E0574DB9A19A1ADE2807D1BD71604358AE2F0787F7F22D4709A05E
Samsung_Pay.pdf	581D5F13A8CB2E23FEA45F0B826823C3CD9E92A8BB5CF3096

	C014191C7A99AD0CB2F7E15E58EAC39408DECC78B6E3D7EEDB91E85A10F146CC74353CAFD864C4A
Shift4.pdf	42F5EDB83F5B6F24A615A65FAA3075905F49A4E2CA85638BEBB17D75868E3B1431834668DEFD91F71A7AF3394C40A12C75A04DE24C27E8217B073ADEDEFA4D4D
TRENHOLM.pdf	D6E3A1ADDE798B4BE7AE403A39FC5C7FDF4E03AC0CDE0D564D8C1D31FE2204D57836A1DF056739A1AACEAC059539143E7DED32B80660A7DC0144182671042702
WESTER.pdf	206B8E60D15719ADCA9F5EE9A29F7FD7D5C64D261EDE01D91036A255713C93E7E58156E33D49199DFC5D10CE47D1C7D093F572495EE34CBE8CDBF25B6766AD0F
Plus_NEWS.pdf	C94575650FD55ECAE244F014B254DF475D23BECAE1F2BD7201DD5358D224239783AE873112734242B4B9FA6EB44FAEA9D5E4068F24AD36B2CBB106F7703F3506
Rambus.pdf	78310B3329B37D36B4842F7D1393C7792615E1676AB316E49CC95BA4498BDBF7AAFF2ED5D462DFB49AD57F02BF15F0EA0F83FF118C7C581FCFD6B474A501E2C6
ReadWriteWeb.pdf	A2A332300AED6C2E9517C2F7F5FF19ABCBA8C1BAFB15E9FC1A272377B938A7AE9BDBA49CFE1947A74C3543F6BB3647E33D5CC9D9A54876BE2177FA1F63D3CAA9
RIM.pdf	868BF8BE96D1E79F931C1BFC246DE2D6D91525D0962B3945D8D58FF12365DCF695B4F65C4B56B11066F01AB0ACD9CE3BE84C6A4AF7EDFCB3851F16D4487C6E32
Samsung_Galaxy.pdf	4257D3887702AD8610308A665E48511CEA9DE418B3FF3C956C08DFEBDC1B99A9B035708B201F5A369A762319C39CC13C3D713A3E2CB28CC5185386BED95A11C9
Samsung_Global_Newsroom.pdf	02507BBFF5B3F9948C806E2FC305B342085B008CC9A96227F0D10A9F69E401974C2197ADFE9933EC2246B9D92F761C29B101939C3DFA96A873CC7490588EE3C0
Samsung_Google.pdf	22BF35D2C3D91795D664F6742893B3DEB9C280C5297F36CFC

	C913CB022DC48F424F60BB78F13EDF7CAF283E94E1E8B2717780B92E52466261E9D42C1D39ACF0A
Samsung_Levant.pdf	F40563239657AFE4F2C1C636507E74190BE388D0246553B0159F720A82F6EA3F81635B3376E734E25CDEB73C9CC2DD0E0C83FD9F43F663BA811445C01676EFDA
Motorola.pdf	5A43B41EDECA9FCF0F787DA9B737A6E146C77E7B96386C1660EF71BF5BC8BB4F7276BB1055F0D4805B870AEE7DD55E523AFE932BD07E43F54E30407517B9763

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.

PTO/SB/08a (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.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17528073
Filing Date	2021-11-16
First Named Inventor	David WYATT
Art Unit	2876
Examiner Name	LEE, SEUNG H.
Attorney Docket Number	WYAT-0002-13C12US

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	1	"Standing Document (SD1): WG8 Projects: ISO/IEC 14443, Proximity Cards (PICCS)," ISO/IEC JTC1/SC17/WG8 (archive.org), October 25, 2010, pp. 1-6.	
	2	"Telefonica O2 Czech Republic prepares NFC payments," DmEurope, March 25, 2011, page 1.	
	3	MARKKANEN, "Telefonica, Samsung to Pilot SIM-Based NFC Payment Solution in Spain," IHS Global Insight, February 15, 2010, pp. 1-2.	
	4	"The Mobile Payments and NFC Landscape: A U.S. Perspective," Smart Card Alliance, September 2011, pp. 1-53.	
	5	"Tokenization Guidance: How to reduce PCI compliance costs, Version 1.0," Securosis, December 10, 2011, pp. 1-31.	
	6	"Tokenization: What's Next After PCI," RSA, 2012, pp. 1-8.	
	7	SEIFERT, "Verizon won't offer Google Wallet for the Galaxy Nexus because it uses a 'secure element'," The Verge, December 10, 2012, pp. 1-2.	
	8	"Visa and Google Sign Licensing Deal to Boost Mobile Payment Adoption," Visa, September 19, 2011, pp. 1-2.	
	9	"Visa Best Practices for Tokenization Version 1.0," Visa, July 14, 2010, pp. 1-4.	
	10	CROSMAN, "Visa Certifies BlackBerry, Samsung And LG Phones For PayWave NFC Payments," Payments Source, January 10, 2012, pp. 1-2.	
	11	"Visa Completes Acquisition of Rambus Payments Portfolio," Business Wire, October 22, 2019, page 1.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	12	"Convenience for customers. Profits for you," Visa PayWave (archive.org), January 2013, pp. 1-2.	
	13	"Verizon User Manual: Samsung Galaxy SIII," Verizon, January 2012, pp. 1-204.	
	14	"World leader in proven and efficient cards for EMV deployment," Gemalto, February 2010, pp. 1-2.	
	15	BECKER, "29C3: A Rambling Walk Through an EMV Transaction (EN)," YouTube, https://www.youtube.com/watch?v=VdNm9JJmCzg, December 30, 2012, pp. 1-2.	
	16	"ARQC and ARPC Generation and Validation," YouTube, https://www.youtube.com/watch?v=I1XTn175FFk, Paragon Application Systems, July 25, 2012, pp. 1-3.	
	17	"CardVault by 3Delta Systems - Securing Credit Card Payments for B2B and B2G through Tokenization," YouTube, https://www.youtube.com/watch?v=h3zuiLiF51k, February 1, 2010, pp. 1-3.	
	18	"CardVault by 3Delta Systems - Securing Credit Card Payments for B2B and B2G through Tokenization," Transcript of YouTube, https://www.youtube.com/watch?v=h3zuiLiF51k, February 1, 2010, pp. 1-3.	
	19	"Credit Card Processing with EPX BuyerWall Tokenization," YouTube, https://www.youtube.com/watch?v=_7E5hj9li4g, December 21, 2010, pp. 1-3.	
	20	"Credit Card Processing with EPX BuyerWall Tokenization," Transcript of YouTube, https://www.youtube.com/watch?v=_7E5hj9li4g, December 21, 2010, pp. 1-7.	
	21	"Find out how PayPal works," YouTube, https://www.youtube.com/watch?v=dn42Y-2uFQM, March 14, 2012, pp. 1-2.	
	22	"Google checkout," YouTube, https://www.youtube.com/watch?v=-UeYkxePW2c, June 29, 2006, pp. 1-2.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	23	'See Google I/O 2011: Google Checkout: A Foundation For Payments," YouTube, https://www.youtube.com/watch?v=7ts7Lkykn0E, May 13, 2011, pp. 1-2.	
	24	'See Google I/O 2011: Google Checkout: A Foundation For Payments," Transcript of YouTube, https://www.youtube.com/watch?v=7ts7Lkykn0E, May 13, 2011, pp. 1-64.	
	25	'Google I/O 2011: How to NFC," YouTube, https://www.youtube.com/watch?v=49L7z3rxz4Q, May 10, 2011, pp. 1-2.	
	26	'Google I/O 2011: How to NFC," Transcript of YouTube, https://www.youtube.com/watch?v=49L7z3rxz4Q, May 10, 2011, pp. 1-62.	
	27	'Google I/O 2012: Introducing Google Wallet Cloud APIs," YouTube, https://www.youtube.com/watch?v=tpEGuSwv1fY, June 29, 2012, pp. 1-3.	
	28	'Google I/O 2012: Introducing Google Wallet Cloud APIs," Transcript of YouTube, https://www.youtube.com/watch?v=tpEGuSwv1fY, June 29, 2012, pp. 1-40.	
	29	'Google Nexus S by Samsung at CES 2011," YouTube, https://www.youtube.com/watch?v=5ZjtXH9S9KM, January 11, 2011, pp. 1-2.	
	30	'Google Nexus S by Samsung at CES 2011," Transcript of YouTube, https://www.youtube.com/watch?v=5ZjtXH9S9KM, January 11, 2011, pp. 1-2.	
	31	'Google Payments Live - Google Wallet updates," YouTube, https://www.youtube.com/watch?v=1pxkQ1mFjNA, August 23, 2012, pp. 1-2.	
	32	'Google Payments Live - Google Wallet updates," Transcript of YouTube, https://www.youtube.com/watch?v=1pxkQ1mFjNA, August 23, 2012, pp. 1-40.	
	33	'Google Wallet Demonstration," YouTube, https://www.youtube.com/watch?v=6tBAB5ls5vM, May 26, 2011, pp. 1-2.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	34	"Google Wallet Demonstration," Transcript of YouTube, https://www.youtube.com/watch?v=6tBAB5ls5vM, May 26, 2011, pp. 1-2.	
	35	"Google Wallet Hands-On - Engadget," YouTube, https://www.youtube.com/watch?v=5s9wYEkRAgs, May 26, 2011, pp. 1-3.	
	36	"Google Wallet - How to Setup and Use this Exciting NFC Technology," YouTube, https://www.youtube.com/watch?v=_ay1FfLCsHs, July 26, 2012, pp. 1-3.	
	37	"Google Wallet - How to Setup and Use this Exciting NFC Technology," Transcript of YouTube, https://www.youtube.com/watch?v=_ay1FfLCsHs, July 26, 2012, pp. 1-7.	
	38	"Google Wallet Make Your Phone Your Wallet by Google," YouTube, https://www.youtube.com/watch?v=qRVQTQlJV0g, February 18, 2013, pp. 1-2.	
	39	"Google Wallet Make Your Phone Your Wallet by Google," Transcript of YouTube, https://www.youtube.com/watch?v=qRVQTQlJV0g, February 18, 2013, page 1.	
	40	"Google Wallet Product Launch," YouTube, https://www.youtube.com/watch?v=am8t6iZ7up0, May 27, 2011, pp. 1-3.	
	41	"Google Wallet Product Launch," Transcript of YouTube, https://www.youtube.com/watch?v=am8t6iZ7up0, May 27, 2011, pp. 1-56.	
	42	"Google Wallet Walkthrough," YouTube, https://www.youtube.com/watch?v=xmbRSXYdFFs, February 13, 2012, pp. 1-2.	
	43	"How does Google Wallet work? Really well!," YouTube, https://www.youtube.com/watch?v=jY2p-pNkjHA, December 7, 2011, pp. 1-2.	
	44	"How does Google Wallet work? Really well!," Transcript of YouTube, https://www.youtube.com/watch?v=jY2p-pNkjHA, December 7, 2011, pp. 1-2.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	45	"How Does PayPal Work?," YouTube, https://www.youtube.com/watch?v=MdrPOCCFQ2k, July 24, 2012, pp. 1-2.	
	46	"How To Use Google Wallet On Android," YouTube, https://www.youtube.com/watch?v=6DeiEVBIBcs, October 28, 2011, pp. 1-2.	
	47	"How To Use Google Wallet On Verizon Galaxy Nexus - Pocketnow," YouTube, https://www.youtube.com/watch?v=AZ8t757ZfUs, April 20, 2012, pp. 1-2.	

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Jose S. Garcia/	Date (YYYY-MM-DD)	2023-01-12
Name/Print	Jose S. Garcia	Registration Number	43,628

This collection of information is required by 37 CFR 1.97 and 1.98. 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 1.14. This collection is estimated to take 1 hour 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. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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 record s.

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.

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 02:28:24 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 #	61424667	FILING DATE	11/16/2021
CUSTOMER #	136197	FIRST NAMED INVENTOR	David WYATT
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	-

Documents

TOTAL DOCUMENTS: 50

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
WYAT-0002-13C12US_IDS_transmittal_form_4.pdf	8	Information Disclosure Statement (IDS) Form (SB08)	1236 KB
Google_Wallet_Cloud.pdf	3	Non Patent Literature	1396 KB
Google_Wallet_Demonstration.pdf	2	Non Patent Literature	775 KB
Google_Wallet_Hands.pdf	3	Non Patent Literature	1438 KB
Google_Wallet_updates.pdf	2	Non Patent Literature	807 KB
Google_Wallet_work.pdf	2	Non Patent Literature	22 KB

How_PayPal_Work.pdf	2	Non Patent Literature	789 KB
How_to_NFC.pdf	2	Non Patent Literature	764 KB
MARKKANEN.pdf	2	Non Patent Literature	772 KB
NFC_Technology.pdf	7	Non Patent Literature	124 KB
Paragon.pdf	3	Non Patent Literature	1278 KB
PayPal_works.pdf	2	Non Patent Literature	776 KB
Pocketnow.pdf	2	Non Patent Literature	820 KB
RSA.pdf	8	Non Patent Literature	5143 KB
3Delta.pdf	3	Non Patent Literature	47 KB
BECKER.pdf	2	Non Patent Literature	810 KB
BuyerWall.pdf	7	Non Patent Literature	112 KB
CardVault.pdf	3	Non Patent Literature	1472 KB
CROSMAN.pdf	2	Non Patent Literature	729 KB
DmEurope.pdf	1	Non Patent Literature	515 KB
EPX.pdf	3	Non Patent Literature	1305 KB
Exciting_NFC_Technology.pdf	3	Non Patent Literature	1298 KB
Foundation_For_Payments.pdf	2	Non Patent Literature	810 KB
Google_API.pdf	40	Non Patent Literature	746 KB
Google_checkout.pdf	2	Non Patent Literature	795 KB

Google_Checkout_Foundation.pdf	64	Non Patent Literature	1183 KB
Google_NFC.pdf	62	Non Patent Literature	1150 KB
Google_Payments_Live.pdf	40	Non Patent Literature	751 KB
Wallet work.pdf	2	Non Patent Literature	823 KB
Wallet_by_Google.pdf	1	Non Patent Literature	15 KB
Wallet_Demonstration.pdf	2	Non Patent Literature	28 KB
Wallet_Google.pdf	2	Non Patent Literature	849 KB
Wallet_Launch.pdf	56	Non Patent Literature	1025 KB
Wallet_On_Android.pdf	2	Non Patent Literature	784 KB
Wallet_Product_Launch.pdf	3	Non Patent Literature	1312 KB
Wallet_Walkthrough.pdf	2	Non Patent Literature	754 KB
WG8_Projects.pdf	6	Non Patent Literature	4118 KB
World_leader.pdf	2	Non Patent Literature	1906 KB
Samsung_CES.pdf	2	Non Patent Literature	22 KB
Samsung_CES_2011.pdf	2	Non Patent Literature	823 KB
Securosis.pdf	31	Non Patent Literature	9201 KB
SEIFERT.pdf	2	Non Patent Literature	779 KB
Smart_Card_Alliance.pdf	53	Non Patent Literature	22963 KB
Verizon_1_of_3.pdf	70	Non Patent Literature	15740 KB

Verizon_2_of_3.pdf	70	Non Patent Literature	16395 KB
Verizon_3_of_3.pdf	64	Non Patent Literature	14961 KB
Visa_and_Google.pdf	2	Non Patent Literature	1100 KB
Visa_Best.pdf	4	Non Patent Literature	870 KB
Visa_Completes.pdf	1	Non Patent Literature	709 KB
Visa_PayWave.pdf	2	Non Patent Literature	811 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
WYAT-0002-13C12US_IDS_transmittal_form_4.pdf	5E70D693D28972B92B219403B10E9073E2D866E13075ECCDDC5CD34275B1DF17B0D0E4D22E47620EF11388E751E3BFD6208192E93AD9693CCE61F632BE057297
Google_Wallet_Cloud.pdf	B6F206DBCC53DD0CC7972D397A54DFE1452E43EEED4B4D18CF22D3F5A86D62931990CE2617FA530A9377EE221D5B2D5727435A83D23E2C868EFA1AEC502381A5
Google_Wallet_Demonstration.pdf	CDF5E3E39689FDFF4505A68CE3500BD63A443ACB80E22691EF26505C4ABA564306AF35D24ED429545F39CE392010A9CEB4E87CF3E41BAE1FEE4C0507FFBBAC0B
Google_Wallet_Hands.pdf	F46B216F42A7A7BFBB67B6BCC5DCADFFF3D3F14C9BA313C7089CCAB9627894E56F4A5C9CF32737F1E37D1D5BA899DF765D5109F2228C5955C4749D63150BCEA7
Google_Wallet_updates.pdf	49BA06569961F8F3EB65593933B07CA67589DEEF5D1675BA6BE5DAC44C89C31868B99266E16B789C4966026D2E5B4DEBBA6A30F298BEE6C5D44F206120D19050
Google_Wallet_work.pdf	828A4D631937EBF37AC47EF3141F381AACAD491A908FC6102DE3C565AA3F811538344B6DC29EBAF87A95A8DD18ED5162D

	A0826DB678EBE3029D62A48884D3083
How_PayPal_Work.pdf	035B5005566DB198EC1EDFA5FEFEF19E6DD3E30A3FCB92A1 6305E364F8108AE86EA3670F7ADDD3C4D429D3027CAAE1449 68335248BF3C0D5F80EECD1C1748684
How_to_NFC.pdf	397A3713D95403C73A600EB29202AD7AFF64DAF1F332CAA76 2CFC3042519D9FDED5276A2272107ABB8B3CC1E5BC7C5AC5 564B99E31654C56EC94DEBBB26D40E8
MARKKANEN.pdf	96E9C15ECE817D004BE536A2DBFA538018C936C0232A69C7F 457E555B786240770AF10B69765AF3EE55F436FF16D247759B5 383EA6B935B443F655059407579E
NFC_Technology.pdf	21BDC2275F639A45771600E656F9737AA6B12CF3AE477D4336 FD3CCD80FD8C57D4280900FCE4A4627F6041828B83233105D E5683693D7763CACAB085B5C310B9
Paragon.pdf	0B87C16EFD6DBF194FABA3861A3C19195825F83A5B69DB480 402C8D634F45F38190EF6FB67B133EAF424C5F4892B8D0135A 5386719AD5BB6152DD11189545417
PayPal_works.pdf	A69C192BAE071C5A253C1BE11BC964161F1F67AF1FDD14927 A3B850BF1004FC0871C5E11729E3B4D076B706DDD7B5441CA 1846AD075772412A7C1CF15CAC6618
Pocketnow.pdf	B7010092212F97F7209D641CDE35B9EFBFD4A592CE2AFA9EB A24390B3DDBE059697D4E1C6C8375542DAB76FA247F215D7D B1887DDA59E43B933D1C4AEC8DD3AA
RSA.pdf	7DE349EF70CBE408BD36C605E88072A7640DCFD802E6AF264 B602DA955A58362223E553FB13CE7370DFAC2DC77DEFFA507 71662E378012E3CE2402C0C343AC7A
3Delta.pdf	5F58BF76E0A65E05FC7A09B1DDD2A3C23B2954248DB941337 FC8E7F700F8EC601B7CB134D1774C0A0D1F949B43ADB8282C 809CC9A8C336691BBB15AAB2FA44B5
BECKER.pdf	7AE3168987BC803BF6021F4321284813FB5D5E65C14977C0B5 A6A3CBC5963F29337C1BC0F0DA67626497ECA363C8F97E1F4

	8531217F359EF9BB5EAF0681C1050
BuyerWall.pdf	176A7116AFC2B862606470EE7E266B280E2BD452E21658D1A CB7FA65FBE9B086C8B26C07FB053984CF4D5C65B16F1A0A2 C3C387C43FEF85DBA58F220A87D3B64
CardVault.pdf	3EBC0558D09B9D98E4BB26775641CD309F394C5ACC8C14074 B7FC477E5A544F9463EED1A2AD7C82C3A488AAD6FD5CBCD 0BC039FC5CE6366AE7CDFF1D8E91691D
CROSMAN.pdf	79CE5973DB99844D147A1E6A600283347F9F28F1F464906FA0 CA9251E8B95BE3A12608C11DB3C45970C78C620CCCBC8C88 79CF1DFADFC0339B0991B420277445
DmEurope.pdf	D0193DFD7FF6542DBFD4542CA950AA08BD85C7F7473622E6B 7C3B2CB0A184E12AF18FBA4552611FD51243CFCC04F4484D8 9E1C3C5C1130AD38FACA3684DEEEF2
EPX.pdf	FC2AD534B54D2DD40ADAEDD7EBDA2A9E1DBBC5A8241E2E2 FFAC139EBD828E6C0E282E78C708F322A07AD018E398C49C7 AC2A4C07D8D9848B6A10C2D12E3781DB
Exciting_NFC_Technology.pdf	685F9940825018B8E2341557224608CAF6AA32041B5F13DC6C 26F856E8C64C4C782D5F69FB3654FA417CEC2BD00B156D0E3 1255849B9AEECFFA5C015CB67BFCD
Foundation_For_Payments.pdf	797359B1EF874B7BB1C6C21F0AFE7D10E1C52D3544EF8779B 080A6D9C3EE57F53A484B9741A0568ABC97D23D97D616B084 768B2B6B9D2706EFC600CD3BC3EA4D
Google_API.pdf	D62D83D2418C28439D5D885D267180506669A59785B882A87B 5EA250F2BD43AAA9AD7C764D846A49A9773F57B3754ED8657 A03A38A3B9A68C63C6602F5CEE728
Google_checkout.pdf	8E87C7C4A286876577F861B84EDE72639133271E5DCEB2B4E B2C88EC293024EF2DD27F53137BCE5F1E2CB52FE089AEB45 E8872F6C2160B95E5032F01847A5C7C
Google_Checkout_Foundation.pdf	19C9D87386B08AA4FD0077E52123F86675A593B42E5E287742 C9E431F2B52AD74C21F7BB992AB012AA6D026F79B56225E75

	3302143EA60D805E77492386F4E37
Google_NFC.pdf	0499C68DAD4A7F65FE610E9786FAEF18B8689DCD17EA0012E7BCE20D30283CFC1CC58E1F6A60715EE0E0A2D10ACD5D6EAF30A4F3C708B2CA4CD5BFAC7AA07D99
Google_Payments_Live.pdf	3194CC69D59F5CAF93E304819107E7DAC26C20685EC1E9CF05E8CF2F7C076CA53FB0A94A06FB38725E1FF42F6917C18A13D6C7211968E6360438AB63E625A5A3
Wallet work.pdf	0371B369633DDCA25DD348EEFF0F93A4721B33787F5A8C7C7EBD3892774950A2A7C56DEEE310503210FC532638958FB3A7A696F2E52A3E8D80CE0C31648F6986
Wallet_by_Google.pdf	847808F7887C8445CC3E7158CCB4BCF0D0C9E4C0AB3F2567025FA20A9DB7033C73D436A3A804BD0132C4C302FA12193E1ACCA290B6340122BF4C03DE53DE24FF
Wallet_Demonstration.pdf	D74DAA4ADDEFAC9E0E2564BCF70DB5D481F036DA823B07190D9A03372B6AE1D251DA2ACC98820453A3B9C4C827EF145DE1613B466764D2D9F92529521A6A3C70
Wallet_Google.pdf	8B79366116A8C3BBC5869EAF1BFE11981BE0DC9DE7C1095C6BCDD35F1B9A69199439A4710F8C2DDFF1FE95B45955A7563B31B1AD5C08CC018A8C68F79636D189
Wallet_Launch.pdf	02083F93DCFB96309CDE6CA1B2343DAAF2D8A2699D47128D4BDA695EACCED01A38782BBFDB6F66EA905BCE240CA596B958D91CFDB0969E26D475486A19449CF9
Wallet_On_Android.pdf	A353DAE20A3767618C03E997A9F5084B775D4FBD3542C83F966A54D655497448A153389B80FF51F3ACB42DD44FD8EB5679A2D5AFBE6652CE0AC65C72DB396B37
Wallet_Product_Launch.pdf	0F61528E884E682744497C155ACCEB542CC9682F9925647683ADF074611828D8A4BA9138E448F059B94BD2454FE96A2EDC6AD65EE291B9C674B38E661A5E437F
Wallet_Walkthrough.pdf	1153C63A606DCB1BC1EBB86C186F5BFE931A6045E00FF3679141B38F9722C2E080746CD2104FEB73F9C269B35A3D380EDF

	DC4BF2DE9729EB675347973D74E4B7
WG8_Projects.pdf	27A492D99A1D0A9086D45D113773E32CDC2BFF721FE98090B3A96A4E32AB61C3AD54782DCD3FE57385E4BC8CA25123C762B2BCF8E6FF82E1D6E3CECA7152ECD8
World_leader.pdf	3D8EB2B23D0F0E8B878986CCB252317CD30F08B9FAA1CC8534DDE7576CD0097EAC59F88FF194DB6B8CF029DC6EA54122FB946BE1BC442A950A17C5CCA0C04CDF
Samsung_CES.pdf	9B9BFD06BD02652E9C098E0B2BAB3AFE53E4FC406E080E2D9C8220383F1EF8784469BD3008C631E129D2E2EE4397C1DA0716E0608EC81E8C894B2339DB86F85F
Samsung_CES_2011.pdf	05BB81954FDB00527DE4D9304A420559ADB891292F2D631FEE6823691998D267072B02FC55B38CD1A7F43763E175586F975C298E22A124DC75B86AE099917667
Securosis.pdf	F270B900A99253A6269E7C36147DB4F6698CBBD29D3EB51BC06E65493EFE4FDB88A6560C77C38036A26A250EC012814A28D4AD20942C4D1140F05260054BB409
SEIFERT.pdf	737CE3D851358447FC0F73A90A454BAED0409CCD60E9FED1E39C2774550B3719D50B2B37A382A33257F5F9FB28E0DD9027EE61ADB12AA08F502923C541D1C053
Smart_Card_Alliance.pdf	98AB0621D0AF0B237C70DA5B48A493B54DE0055FC58CB4EDDCECD53AE2EC17349A36B20E47B33BD367EDDAFF9755346382ABEB2330DAEB44D12D61B56A9A903D
Verizon_1_of_3.pdf	2908F01FEA2A8F32FB71FB9409C7C165767ABD9B2F7743A08E45DABE28530F2E1A991FFA0CE93DA15A123D964B3DD8254345373A954E63D22DE7C21F423958A0
Verizon_2_of_3.pdf	0429CC0F0DBE0B76A1A17BFE6B6A2CAF856FCD71D601B446F3CFD5F2959D51686F0C38A2D452901018E74FF75B0618821A913374D1554C04541930FD7722292A
Verizon_3_of_3.pdf	7EFB00955B6DF940179F345523499EB22385BFC14A53012B223D62ABE4885406AE41F5982E6D8E5AD2C660C3B555CACF383

	6561AF2AEA10A49AD30D2A4CF07D4
Visa_and_Google.pdf	F4F4F8A0FE2734FE22127DBB67A34F8A87CCB77CF25946AF2770B72DC9E6475ABC4FDA422F2989B52BC16D2B359E7009473071B9A1EE3692870EE84615A29AAA
Visa_Best.pdf	092C0EAF5A90E7AFFA4E90C6B979317A42E71C9384C640D736CE76896B6578E186A45089FD790AC5871E2DE152C8B8AA3AB9A071DCDE2E094AAB5730AEAF83B7
Visa_Completes.pdf	61707E6231D3C5DA19A0E989AD084F71611C9DE5E02CCD0B8FAC82E1B056DDE2A63D509D6D0AE27F8791098FD61BE610C1E2F14364EEFA2500C053E9A4EDA94E
Visa_PayWave.pdf	C0FE1C7C3C50168EBCE5C979A38365CEAF943B4C822874DCB0E4248DD2AAABD78E15340ACE90EA1E9C078DDE4EC67E2AFD49CE6FE34C5490BAC0F9C56C4C2844

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.

PTO/SB/08a (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.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17528073
Filing Date	2021-11-16
First Named Inventor	David WYATT
Art Unit	2876
Examiner Name	LEE, SEUNG H.
Attorney Docket Number	WYAT-0002-13C12US

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	1	"Isis NFC-payment from SXSW 2012," YouTube, https://www.youtube.com/watch?v=Z2MOAtUhR7k, March 10, 2012, pp. 1- 2.	
	2	"Isis NFC-payment from SXSW 2012," Transcript of YouTube, https://www.youtube.com/watch?v=Z2MOAtUhR7k, March 10, 2012, pp. 1- 3.	
	3	"NFC - Google Wallet and More - EE Times - Mobile World Congress," YouTube, https://www.youtube.com/watch?v=AgSk7L6HhVw, March 6, 2012, pp. 1-3.	
	4	"NFC - Google Wallet and More - EE Times - Mobile World Congress," Transcript of YouTube, https://www.youtube.com/watch?v=AgSk7L6HhVw, March 6, 2012, pp. 1-8.	
	5	"Paying With Google Wallet," YouTube, https://www.youtube.com/watch?v=jTeilSIzBPQ, February 6, 2012, pp. 1-2.	
	6	"Seinfeld - Google Wallet," YouTube, https://www.youtube.com/watch?v=baaCvgTRYsU, June 14, 2013, pp. 1-2.	
	7	"Technology: Google Wallet - The New York Times," YouTube, https://www.youtube.com/watch?v=I8JOT6ban7o, September 23, 2011, pp. 1-2.	
	8	"Using Google Wallet in McDonald's!," YouTube, https://www.youtube.com/watch?v= 1p6co4YIvbA, September 14, 2012, pp. 1-2.	
	9	"Virtual terminal- #1 storing credit card data with tokenization," YouTube, https://www.youtube.com/watch?v=eSXIIGbACew, February 28, 2011, pp. 1-3.	
	10	"What is Google Wallet?," YouTube, https://www.youtube.com/watch?v=iuvyN4iZiP8, August 9, 2011, pp. 1-3.	
	11	"What is Tokenization?," YouTube, https://www.youtube.com/watch?v=ypm5FFfEN34, January 17, 2011, pp. 1-3.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	12	"How Credit Card Number Tokenization can Reduce PCI Compliance Stress - File 1 of 3," YouTube, https://www.youtube.com/watch?v=FHD5XzAIKDI, Jul 28, 2009, pp. 1-3.	
	13	"How Credit Card Number Tokenization can Reduce PCI Compliance Stress - File 1 of 3," Transcript of YouTube, https://www.youtube.com/watch?v=FHD5XzAIKDI, Jul 28, 2009, pp. 1-12.	
	14	"HOW CREDIT CARD NUMBER "TOKENIZATION" CAN REDUCE PCI COMPLIANCE STRESS - File 2 of 3," YouTube, https://www.youtube.com/watch?v=t-fWpcLdb3o, Jul 28, 2009, pp. 1-3.	
	15	"HOW CREDIT CARD NUMBER "TOKENIZATION" CAN REDUCE PCI COMPLIANCE STRESS - File 2 of 3," Transcript of YouTube, https://www.youtube.com/watch?v=t-fWpcLdb3o, Jul 28, 2009, pp. 1-12.	
	16	"HOW CREDIT CARD NUMBER "TOKENIZATION" CAN REDUCE PCI COMPLIANCE STRESS- File 3 of 3," YouTube, https://www.youtube.com/watch?v=_CdoKEuEB9s, Jul 28, 2009, pp. 1-3.	
	17	"HOW CREDIT CARD NUMBER "TOKENIZATION" CAN REDUCE PCI COMPLIANCE STRESS- File 3 of 3," Transcript of YouTube, https://www.youtube.com/watch?v=_CdoKEuEB9s, Jul 28, 2009, pp. 1-8.	
	18	"Caixer contactless lacaixa," YouTube, https://www.youtube.com/watch?v=It2CpMcxQC4, April 4, 2011, pp. 1-2.	
	19	"Understanding Proximity Sensors - T-Mobile," YouTube, https://www.youtube.com/watch?v=npD48agt0xY, January 2010, pp. 1-2.	
	20	"Understanding Proximity Sensors - T-Mobile," YouTube, https://www.youtube.com/watch?v=npD48agt0xY, January 2010, page 1.	
	21	"Understanding Proximity Sensors - T-Mobile," Transcript of YouTube, https://www.youtube.com/watch?v=npD48agt0xY, January 2010, pp. 1-2.	
	22	"Google I/O 2012 - The Sensitive Side of Android," YouTube, https://www.youtube.com/watch?v=Q0V_Id7iNw4, June 29, 2012, pp. 1-2.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	23	"Google Wallet Overview," YouTube, https://www.youtube.com/watch?v=VuFVsaFCzsw, August 1, 2012, page 1.	
	24	"Google Wallet Overview," Transcript of YouTube, https://www.youtube.com/watch?v=VuFVsaFCzsw, August 1, 2012, pp. 1-2.	
	25	"Android 4.0 APIs | Android Developers," mit.edu, https://stuff.mit.edu/afs/sipb/project/android/docs/about/versions/android-4.0.html, 2011, pp. 1-23.	
	26	"EMV Integrated Circuit Card Specifications for Payment Systems, Book 2, Security and Key Management, Version 4.3," EMVCo, November 2011, pp. 1-174.	
	27	"Exploring Google Wallet using the secure element interface," nelenkov.blogspot.com, August 27, 2012, pp. 1-20.	
	28	GARSIDE, "Google Wallet mobile payments system launched to public," The Guardian, https://www.theguardian.com/technology/2011/sep/19/google-wallet-available-public, September 19, 2011, pp. 1-5.	
	29	PURDY, "How to grab a screenshot from iPhone, Android, and nearly any other smartphone," Computer World, April 20, 2012, pp. 1-6.	
	30	"Maximum failed passcode attempts in restrictions - what happens?," Apple Community, https://discussions.apple.com/thread/3690633, January 2012, pp. 1-3.	
	31	"Simplify, Organize & Pay with Loop by Will Graylin & George Wallner," Kickstarter, March 2019, pp. 1-13.	
	32	"Hands-on with ISIS Mobile Wallet," YouTube, https://www.youtube.com/watch?v=eOMqvGVKjmM, March 10, 2012, page 1.	
	33	"EMV Solutions," Paragon Application Systems, https://web.archive.org/web/20120818221214/http://www.paragonedge.com/solutions/emv-solutions.html, August 18, 2012, page 1.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	34	SULLIVAN, "The Changing Nature of U.S. Card Payment Fraud: Industry and Public Policy Options," Economic Review, Federal Reserve Bank of Kansas City, Second Quarter 2010, ProQuest Information and Learning, Vol. 95, No. 2, pp 101-133.	
	35	"EMV Integrated Circuit Card Specifications for Payment Systems, Book 1, Application Independent ICC to Terminal Interface Requirements, Version 4.3," EMVCo, November 2011, pp. 1-189.	
	36	"EMV Contactless Specifications for Payment Systems, Book B, Entry Point Specification, Version 2.1," EMVCo, March 2011, pp. 1-50.	
	37	ETHERINGTON, "Android Pay Is Real, And Will Give Developers The Reins As An API," TechCrunch, https://techcrunch.com/2015/03/02/android-pay-is-real-and-will-give-developers-the-reins-as-an-api, March 2, 2015, pp. 1-7.	
	38	"PCI DSS Version 2.0 Information Supplement: PCI DSS Tokenization Guidelines," PCI Security Standards Council, pcisecuritystandards.org, https://listings.pcisecuritystandards.org/documents/Tokenization_Guidelines_Info_Supplement.pdf., v 2.0, August 2011, pp. 1-23.	
	39	"EMVCo Updates Payment Tokenisation Specification to Introduce 'Payment Account Reference,'" www.emvco.com, March 29, 2016, pp. 1-2.	

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Jose S. Garcia/	Date (YYYY-MM-DD)	2023-01-12
Name/Print	Jose S. Garcia	Registration Number	43,628

This collection of information is required by 37 CFR 1.97 and 1.98. 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 1.14. This collection is estimated to take 1 hour 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. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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 record s.

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.

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 02:47:58 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 #	61424685	FILING DATE	11/16/2021
CUSTOMER #	136197	FIRST NAMED INVENTOR	David WYATT
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	-

Documents

TOTAL DOCUMENTS: 44

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
WYAT-0002-13C12US_IDS_transmittal_form_5.pdf	7	Information Disclosure Statement (IDS) Form (SB08)	1236 KB
Paragon_Application_Systems_EMV.pdf	1	Non Patent Literature	159 KB
passcode_attempts.pdf	3	Non Patent Literature	1011 KB
Paying_Google.pdf	2	Non Patent Literature	746 KB
PCI_Compliance.pdf	3	Non Patent Literature	1345 KB
PCI_Compliance_Stress.pdf	12	Non Patent Literature	204 KB

PCI_Tokenization_Guidelines_Info_Supplement.pdf	23	Non Patent Literature	638 KB
Proximity_Sensors.pdf	2	Non Patent Literature	629 KB
REDUCE_PCI.pdf	3	Non Patent Literature	1473 KB
REDUCE_PCI_STRESS.pdf	12	Non Patent Literature	206 KB
screenshot.pdf	6	Non Patent Literature	1897 KB
Android_API.pdf	23	Non Patent Literature	18175 KB
Android_Pay_Is_Real_TechCrunch.pdf	7	Non Patent Literature	5242 KB
B_Entry_Point_Specification_v2_1_March2011.pdf	50	Non Patent Literature	328 KB
CARD_NUMBER.pdf	3	Non Patent Literature	1439 KB
Changing_Nature_of_US_Card_Payment_Fraud_Industry_and_Public_Policy_Options.pdf	33	Non Patent Literature	446 KB
contactless_lacaixa.pdf	2	Non Patent Literature	634 KB
CREDIT_CARD_NUMBER.pdf	8	Non Patent Literature	135 KB
EMV_v4.3_Book_1_ICC_to_Terminal_Interface.pdf	189	Non Patent Literature	1027 KB
EMVCo_Updates_Payment_Tokenisation_Specification.pdf	2	Non Patent Literature	127 KB
Exploring_Google_Wallet.pdf	20	Non Patent Literature	12200 KB

Google_Wallet_Overview.pdf	1	Non Patent Literature	300 KB
Hands_on_with_ISIS_Mobile_Wallet.pdf	1	Non Patent Literature	205 KB
Isis_NFC.pdf	2	Non Patent Literature	753 KB
Isis_SXSW.pdf	3	Non Patent Literature	42 KB
Mobile_World.pdf	3	Non Patent Literature	1511 KB
Mobile_World_Congress.pdf	8	Non Patent Literature	137 KB
New_York_Times.pdf	2	Non Patent Literature	779 KB
Using_Google_Wallet.pdf	2	Non Patent Literature	782 KB
Virtual_terminal.pdf	3	Non Patent Literature	1469 KB
Wallet_mobile_payments.pdf	5	Non Patent Literature	2498 KB
Wallet_Overview.pdf	2	Non Patent Literature	21 KB
What_Google_Wallet.pdf	3	Non Patent Literature	1334 KB
Will_Graylin.pdf	13	Non Patent Literature	4632 KB
Security_Key_Management_1_of_5.pdf	35	Non Patent Literature	12146 KB
Security_Key_Management_2_of_5.pdf	35	Non Patent Literature	14749 KB
Security_Key_Management_3_of_5.pdf	35	Non Patent Literature	17761 KB
Security_Key_Management_4_of_5.pdf	35	Non Patent Literature	17097 KB

Security_Key_Management_5_of_5.pdf	34	Non Patent Literature	16191 KB
Seinfeld.pdf	2	Non Patent Literature	705 KB
Sensitive_Side.pdf	2	Non Patent Literature	655 KB
T_MOBILE.pdf	1	Non Patent Literature	277 KB
Tokenization.pdf	3	Non Patent Literature	1541 KB
Understanding_Proximity_Sensors.pdf	2	Non Patent Literature	291 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
WYAT-0002-13C12US_IDS_transmittal_form_5.pdf	EB152BE38E8F14A1D1022A1EB20CAAB1E1AFA37556F759B0A9584EC443492165FA65C6C54BB3370D61F79B7C133F06B957104961BE509658FD8D89DD8C146F07
Paragon_Application_Systems_EMV.pdf	AF376E74FC80C73DC8BAEE41F09ECE67605F12E71111098FE1770819CD12E6AE7F3D3FAD34743C6B1D626EFFAB87C3E83C80EA79FB0B00327FCD066DE9DC145A
passcode_attempts.pdf	C9E4FC3CF7D261392F9A86402A2431190D534FB0BC622679C3778154B567459FC03B8D1C85FBB7A3996D61706FD5B413DB69508FABF58BFDD6D6823583D7F483
Paying_Google.pdf	601BCF273175710BE405124C4DA9B46C6B0F2DB06F9739012A31A50FD6B05D4B596410C4DDB111CE7617C7DD681149E95F7A88A60366046E77F0EE18BB7B9643
PCI_Compliance.pdf	3B8B4A36EB201D0FCF1C2CD9CB59D580AD571310E765CB535C92F0B3C2F4ABE94B483FD7C4415735C1EE9C019769056E7D63C98F690B40020D21BF09FA89B196

PCI_Compliance_Stress.pdf	0EF6F246F86CB5B7CAF15CAF7932B0ABDD4E150C8E12D5D158D5F5EA31F0DCD8053D77E85F7B02B59D2F7EF8609BFBAE93CB151CBE115E7A4840E3CA00003FE0
PCI_Tokenization_Guidelines_Info_Supplement.pdf	5FE7C5562730405694C5554CCC5F9926E15C0DFF68F6BB882657326C379CC845C2BD4AEE52DB72E8EF2054D1C3147A934C8F9A1477560D5F6CCEBA9F14B30581
Proximity_Sensors.pdf	8A40C7A3B9DCE6F7446FD7BFA67FF5501E9F023312A4BF6A31FC55C5B4D4BA2C31BB8E29A9A7475FB7016DBA680C459EEAB7FA4D24C5089C003836D525002388
REDUCE_PCI.pdf	4C35268DC06DF30510C90BFF65CB19013F131F06A0B13355B36CF3909DFAF67783EC798BBB6067567EB151467D79D26C37240D9A58CC2F6239B924C3AAE3D471
REDUCE_PCI_STRESS.pdf	A556B8E60973E1948D21AA39563968AF4EA5EAC790150BCE437DC0B84E09E6AB49D4A64D1EFBFB1D1B9816B8BF04E0CB89149B084204A68DC2BCCC067F160113
screenshot.pdf	51EFBD790AF43DBEDF9BD006BD9C8C4D5A30F7F8D54074C173C8AB65E59885C3856E71F2ECE9686E85C792D947408DEBA603B7B9DEE9FD463CF4BE9F7840EE4D
Android_API.pdf	D299177B4ED333463CAB066AA0D24F59369B3E220270A6D3875193983396969C84E68671D3E31574AD90AB6921335A9A265935D8DC368AEB2D1A10277A41CDE0
Android_Pay_Is_Real_TechCrunch.pdf	C4F0DDC061BA696B63644BAADAE8FB6143DEB310A308A251662AB19E27A5D6290BFDC5CCE15140336F3A2CD78F4C5A38FD1167F363C69CBDDC3050ADA5600F00
B_Entry_Point_Specification_v2_1_March2011.pdf	7FEEA416D0E066BECAE398697FDD86EF827441D98F6BFA2089D5A42CB022BA6D0A453CE64DF76899FE54DC01DA10A910829F0657C4D987210B68356098C6EF7D
CARD_NUMBER.pdf	71812AF5700B57C1AB25A8FC556E185FBA6A7C1D79F08A4084821B3BFD3AA958A69D4A1030F0565E8DAB842BDD7215F071E0C7D29B7308A8FAEFB9B20874CFC9

Changing_Nature_of_US_Card_Payment_Fraud_Industry_and_Public_Policy_Options.pdf	327509AF153AD3CB176379B5848415B7119BE7D946D01C4B4C71FD7A1DB0FFA12BB6C383A09297C453AB16193A8C2DEEF43618A3D4BCCA2BCB0CCBDC287F1EE
contactless_lacaixa.pdf	E3B844123B8982BB27C07443F3C9021F2F8DD0271B149B18AB4C1F6F2004281DD7C38BC9002E832E836FF11F20FEB7244753A44CA7C947F3069F1E9251A8B278
CREDIT_CARD_NUMBER.pdf	AEA238B431E2F4108021379775865281863 9BF4DFA2D427A12C39615B250E7C463ED4B0F45B2DD2EF94391D6CBC12DAB7B0C644FDF40910B4E4A347188875ECC
EMV_v4.3_Book_1_ICC_to_Terminal_Interface.pdf	1E687B6A1F33CC017C0C90CE52A3F6D23FFA457B3F58380110635FA9F6901D5295DB5870A7BF949983BD920124FB518B86CC0E53BE978BA8839E7EEBDA0CE20F
EMVCo_Updates_Payment_Tokenisation_Specification.pdf	D15DB971C91EEE5A17D8FBB971D1DDDF748A532293769A462048C1035C798DE0050C186BC230531E097A7B198781AEC0F4BC227CA57A8E88A0D9CBA0C089CB82
Exploring_Google_Wallet.pdf	DF6C87563AFAE759ADE235C519F75F41EF468B3C4296C3FD379529107BBE25B28BAD5D776292C15873110DF15660240FA2D5847DBE5E63C3F036CF898FD99AD3
Google_Wallet_Overview.pdf	6410185709EEBDCCB8059DD7640EFC309FB0569B8EC76EA526E3B05F5EB155133D2D499F820C7A4C6FCA1F41B0BE37849D5EA12831775175ECEC92D07A0F4B8C
Hands_on_with_ISIS_Mobile_Wallet.pdf	F415943E01EFB6E850FBBF782B5A5F1EF50C90105D21552F02F5A9A6AEBC742F2BA54F8C4AE936A10524B4278666B11FA9438499B65E494111E352E7F3F835FA
Isis_NFC.pdf	3AC49AD9FDEF91F9B1200F424AFF6861D51FBB616FCD40D9D1745F7CC702A99311F52D95B575C9FB21046963AE18B3ACCAC1AD832822450828EA37AE753F5E97
Isis_SXSW.pdf	868CC0AECD79D60F8ECCC5DD916C9DC1915F9445B683694A63E3DE618C5EFC7FE56EA44FF6B16F2EE52A18A3966E5AAD340F0D7D759F13D6C2FDC6CAC994C19D

Mobile_World.pdf	74C72C18BD46A49569BDC41192294347FDD95BFEDB7923944CB86A1C2B1FDAC51F1D0FDD122221B2DEFAC0A4D3B3A3969D789A3500CA21BF5D98C2818CDFE558
Mobile_World_Congress.pdf	F0C2B759CB7755B651703DD68FB6460021D1D6518006FB887B5E9C0CFE3E4285C04C16CC18215CBE07A87B1F2998E2A08582DD57756BF54415480802059 70B0C
New_York_Times.pdf	72CE5D91AAD01B131EF53C98BBEC955CD2EBD1AF7297C1F595E9AB46BA36AE475011E0C45841BAC6B0F5F09E3FA526F7A39316402ED1D900C88857F0688339AB
Using_Google_Wallet.pdf	8A4A36DEBDE2D6AC68F5FCA96FD931ED22B2C88244AA20F0D83C4A8BB241BBB02E977D2835BC2A263FCF69DBE6E3B8412C74EBE57FA3EF23BAC2F18981163878
Virtual_terminal.pdf	EA989A5B6BC6A95F36CDA7702AED719D7A246F43D5A584695DB2E844A1DDE5D59E62D67C51BB8D7BBE1823C8A553B862B122F903BE689E9EFC581DD07061D084
Wallet_mobile_payments.pdf	5F86AB0325A6918D7A6BD31D32522099DCC56A90BC7BB6F69BC76E5EB668715CE41BB1BA800C92AFBA9D72DB5B90EF19B3217458650BA447917A02A0D18642E0
Wallet_Overview.pdf	5B74F1AD54B320354499D3E23D8A8C71299C630C78F3BA7F1D075900E338F2C4FFDF0D2A767A9D80D5DD9BD38ADC8B40D2A96FD3E9274FC8636E7E0630B7AA1A
What_Google_Wallet.pdf	ACE563AB3E52C0C2AA5F4DA3E9CA63A28734AEDB88E18B8E61672D5CAA7042BEBDCB6C1C5C42A20904610A1FFDAFEDD02F0F3E9B0522E33C4CAE5E4A8063246F
Will_Graylin.pdf	694DBBA98709129E04A695B85CCE8114D8949DAB0FC559A1DBABE15892053B0C85E5DB7B6306291BA2FD8971082ED5956E2CE41124606BB4B18809FDB04A8AB8
Security_Key_Management_1_of_5.pdf	2B5BE6BB0C5FC5C2AC07582D4C3763E66357010D8BE537D2FF1FC44183A9DCDFCDF962DF5EF39F4E59765AEB8CD6DCA6006620E8DE772057EB655EDD24BFC2CD

Security_Key_Management_2_of_5.pdf	1EE397678DB5A81A51358ADAF5FDE8849D93FE2C91FBB713362BFF56BD8AC5AE7799513A45D6E65C111B2D6E9242C121A953D1B3745DFEF1FDBEBC4CBB8AB89F
Security_Key_Management_3_of_5.pdf	A0733EDB9871753DED2B125B7FEC211EBCBFB1F1DB13A80BE5176A40FB40FF3FFDCB421D495D2178CD30B0BCC98BFA7A385B0D0714527B9869A7D40BB741F58E
Security_Key_Management_4_of_5.pdf	73D99B8583AABAC48C73B6FBAC0770B26FACAE3ACB0A60A48490C27C561BFB0968BD65BF18BA03827C9C67F7B336CC52D173E8C0F01F1D50AE59B2541BA63DE4
Security_Key_Management_5_of_5.pdf	BEEF6C4A4E316E20A91B761441763C8745BDB09D148E846E3F3FCCA69B825B9BD7DF8DC0C843142A2491310C610FEAFC024CAD2ADA84CA3AB6CC1086FD7F7C2D
Seinfeld.pdf	9F449A18E85956D7C28BFCD0CA63FDF6C1D4D5A30DA3DED18069FEAB4EA176ADE7D2BEE52924B3D91D5737F645329B5BF9629FC8617146E3FB53C52B4BC7C516
Sensitive_Side.pdf	317C4948BB4B63F43AEF2357780EDCB4233E3C2998F3A2EC2C57B232D4CCB72B89A04C37A873C83E7FDC20BDA6A8385DFD88A7620169D6D7144D38CB69CD8DC2
T_MOBILE.pdf	BB1994F921DD7982A6B3161056B45A3745BB61B535A92DA705DEEAA25D1C23EB61877914B2EBD91130B8BC525CE1D204E8536E7A0EA034EDC35A027658829317
Tokenization.pdf	7AE63B12CEB14F98A85D4139682F2DCCF49DBBC4AFCDE7AB961760D721D0AF4DA50D5FF7FFAD9A5F088D7A1D2B4E260D005E17DC8A9A9A19B8ABD2C0BC302F0D
Understanding_Proximity_Sensors.pdf	2E181A79CCCF26BD11387AE9D3A466722679EA7119AAEF64560195EC48FC5661D9C9A2F8A2E67DDF24F832EE8C62FDFB4A18B3F388371DA0B6DE3CFF312A7FEB

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

Corrected Application Data Sheet

17528073 : MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

~~Strike through~~ indicates removal of data from existing record Underline indicates new data being added to the application If no data is shown, no data has been corrected

Inventor Information

Data of record	Updated Data

No data change in this section

Application Information

Title of Invention	MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE	
Attorney Docket Number	~~WYAT-0002.USD1C1C1C1C1C~~	WYAT-0002-13C12US
Entity Status	Small	

Domestic Benefit/National Stage Information

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c), 386(c), or indicate National Stage entry from a PCT application. Providing benefit claim information in the Application Data Sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78(a)(2) or CFR 1.78(a)(4), and need not otherwise be made part of the specification.

	Updated Data

Data of record

No data change in this section

Foreign Priority Information

This section allows for the applicant to claim benefit of foreign priority and to identify any prior foreign application for which priority is not claimed. Providing this information in the Application Data Sheet constitutes the claim for priority as required by 35 U.S.C. 119 (b) and 37 CFR 1.55. When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX) the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(i)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

Data of record	Updated Data

No data change in this section

Applicant Information

The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46.

Data of record	Updated Data
CARDWARE, INC --- --- ~~San Jose, CA 95130~~ UNITED STATES Phone : --- Email : --- Fax : --- Organization Applicant type : Assignee	111 Congress Ave Suite 500 Austin, TX 78701

Assignee Information including Non-Applicant Assignee Information

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Data of record	Updated Data
No data change in this section	

Signature

NOTE:

This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b).

This Application Data Sheet **must** be signed by a patent practitioner if one or more of the applicants is a **juristic entity** (e.g., corporation or association). If the applicant is two or more joint inventors, this form must be signed by a patent practitioner, **all** joint inventors who are the applicant, or one or more joint inventor-applicants who have been given power of attorney (e.g., see USPTO Form PTO/AIA/81) on behalf of **all** joint inventor-applicants.

See CFR 1.4(d) for the manner of making signatures and certifications.

Signature	First name	Last name	Registration #	Date
/Jose S. Garcia/	Jose	Garcia	43628	02/09/2023

Doc Code: R46C.REQ
Document Description: Request under 37 CFR 1.46(c) to correct, update or change the applicant.

PTO/AIA/41 (04-15)
Approved for use through 11/30/2020. 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 displays a valid OMB control number.

REQUEST TO CORRECT OR UPDATE THE NAME OF THE APPLICANT UNDER 37 CFR 1.46(c)(1), OR CHANGE THE APPLICANT UNDER 37 CFR 1.46(c)(2)

(FOR USE ONLY IN APPLICATIONS FILED ON OR AFTER SEPTEMBER 16, 2012)

Application Number	17/528,073
Filing Date	11-16-2021
First Named Inventor	David WYATT
Art Unit	2876
Examiner Name	LEE, SEUNG H.
Practitioner Docket Number	WYAT-0002-13C12US

To: Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Applicant hereby **requests that the name of the applicant be corrected or updated under 37 CFR 1.46(c)(1), or that the applicant be changed under 37 CFR 1.46(c)(2),** in the above-identified application. **Requests under 37 CFR 1.46(c)(1) or (c)(2) cannot be submitted after payment of the issue fee or if the application has been patented.**

Please check the applicable box(es) below.

☐ 1. This request is to **correct or update the name of the applicant** (**under 37 CFR 1.46(c)(1)**) and includes:

☐ An application data sheet (ADS) in accordance with 37 CFR 1.76(c) with the corrected or updated information shown with markings (*e.g.*, underlining for insertions, strikethrough for deletions). A Corrected Web-based ADS may be used.

Note: Requests under 37 CFR 1.46(c)(1) may be filed to correct typographical errors in the name of the § 1.46 applicant, or for updating the name of the § 1.46 applicant (*i.e.*, where there is no change in the applicant itself but just in the applicant's name). See the Manual of Patent Examining Procedure (MPEP) section 605.01.

■ 2. This request is to **change the applicant** (**under 37 CFR 1.46(c)(2)**) and includes:

■ An application data sheet (ADS) in accordance with 37 CFR 1.76(c) that identifies the changes with proper markings (underlining for insertions and strikethrough for deletions). A Corrected Web-based ADS may be used.

■ A Statement Under 37 CFR 3.73(c) (Form PTO/AIA/96 or equivalent). See MPEP 325.

I am the

☐ applicant* ■ attorney or agent of record Registration number 43628 ☐ attorney or agent acting under 37 CFR 1.34 Registration number _____

Signature /Jose S. Garcia/

Typed or printed name Jose S. Garcia

Date 02/09/2023

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. *Juristic entities must be represented by a patent practitioner (See 37 CFR 1.31, applicable to any paper filed on or after September 16, 2012 that is presented on behalf of a juristic entity, regardless of application filing date). Submit multiple forms if more than one signature is required, see below**.

☐ ** Total of _____ forms are submitted.

This collection of information is required by 37 CFR 1.36. 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. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, 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 disclosure of these records is required by the Freedom of Information Act.
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 inspection 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.

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	**02/09/2023 10:30:58 PM 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 #	61576205	FILING DATE	11/16/2021
CUSTOMER #	136197	FIRST NAMED INVENTOR	David WYATT
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	-

Documents

TOTAL DOCUMENTS: 3

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
CorrectedADS.pdf	3	Application Data Sheet to update/correct info	71 KB
WYAT-0002-13C12US_aia0041_Request_to_Change_Applicant.pdf	2	Request for Corrected Filing Receipt	235 KB
WYAT-0002-13C12US_aia0096_Statement_under_3_73c.pdf	3	Assignee showing of ownership per 37 CFR 3.73	206 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
CorrectedADS.pdf	1A33C7267A8D023270FD6E2B020D686A5E58F264598F8F5E74485D8388015307249FE1B9D933E1F4A18A864CCCFA682C67C20D59C58BDDC8AE90A1E377648660
WYAT-0002-13C12US_aia0041_Request_to_Change_Applicant.pdf	DDA42D25A1D83DD80DF20D7E4B149C92DD0ECA78949770726B66E1E62C74B42A9BB8AFAB8FB65A6FAF5950AFB55D26501FD947FAF166618D74641441540DE717
WYAT-0002-13C12US_aia0096_Statement_under_3_73c.pdf	ECAA0CB00E24AE36313253321C3465010A67EF77A7BA014A633FF497C86088A2F88E3BB6AFBBBD582D7EFF487B6F41777D07628194C5DFAC8E4AC2366FD3C4E3

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.

PTO/AIA/96 (08-12)
Approved for use through 11/30/2020. 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 displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

Applicant/Patent Owner: CARDWARE, INC.

Application No./Patent No.: 17/528,073 Filed/Issue Date: 11-16-2021

Titled: MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

CARDWARE, INC., a corporation

(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that, for the patent application/patent identified above, it is (choose **one** of options 1, 2, 3 or 4 below):

1. ☑ The assignee of the entire right, title, and interest.

2. ☐ An assignee of less than the entire right, title, and interest (check applicable box):

   ☐ The extent (by percentage) of its ownership interest is _____%. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.

   ☐ There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

3. ☐ The assignee of an undivided interest in the entirety (a complete assignment from one of the joint inventors was made). The other parties, including inventors, who together own the entire right, title, and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

4. ☐ The recipient, via a court proceeding or the like (*e.g.*, bankruptcy, probate), of an undivided interest in the entirety (a complete transfer of ownership interest was made). The certified document(s) showing the transfer is attached.

The interest identified in option 1, 2 or 3 above (not option 4) is evidenced by either (choose **one** of options A or B below):

A. ☐ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.

B. ☑ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: David WYATT To: CARDWARE, INC.

   The document was recorded in the United States Patent and Trademark Office at
   Reel 058892, Frame 0036, or for which a copy thereof is attached.

2. From: CARDWARE, INC. To: CARDWARE, INC.

   The document was recorded in the United States Patent and Trademark Office at
   Reel 062030, Frame 0299, or for which a copy thereof is attached.

This collection of information is required by 37 CFR 3.73(b). 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. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, 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.

PTO/AIA/96 (08-12)
Approved for use through 11/30/2020. 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 displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

3. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

4. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

5. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

6. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☑ As required by 37 CFR 3.73(c)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/Jose S. Garcia/	02/09/2023
Signature	Date
Jose S. Garcia	attorney for CARDWARE, INC.
Printed or Typed Name	Title or Registration Number

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 disclosure of these records is required by the Freedom of Information Act.
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 inspection 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.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
17/528,073	11/16/2021	2876	3750	WYAT-0002.USD1C1C1C1C1C	14	2

CONFIRMATION NO. 4809

CORRECTED FILING RECEIPT

136197
David Wyatt c/o Murabito, Hao & Barnes
111 North Market Street
Suite 700
San Jose, CA 95113

OC000000136862754

Date Mailed: 11/17/2022

Receipt is acknowledged of this non-provisional utility patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF FIRST INVENTOR, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection.

Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a corrected Filing Receipt, including a properly marked-up ADS showing the changes with strike-through for deletions and underlining for additions. If you received a "Notice to File Missing Parts" or other Notice requiring a response for this application, please submit any request for correction to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections provided that the request is grantable.

Inventor(s)

David WYATT, Austin, TX; ~~San Jose, CA~~;

Applicant(s)

CARDWARE, INC, San Jose, CA;

Power of Attorney: The patent practitioners associated with Customer Number 136197

Domestic Priority data as claimed by applicant

This application is a CON of 17/075,637 10/20/2020 PAT 11176538
which is a CON of 16/459,150 07/01/2019 PAT 10810579
which is a CON of 15/701,261 09/11/2017 PAT 10339520
which is a CON of 14/981,757 12/28/2015 PAT 9760884
which is a CON of 14/680,979 04/07/2015 PAT 9224083
which is a DIV of 14/217,261 03/17/2014 PAT 9022286
which claims benefit of 61/794,891 03/15/2013

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

IPR2025-01152
Apple EX1002 Page 1409

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 11/30/2021
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 17/528,073**
Projected Publication Date: Not Applicable
Non-Publication Request: No
Early Publication Request: No
**** SMALL ENTITY ****
Title

MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

Preliminary Class

235

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative,

IPR2025-01152
Apple EX1002 Page 1410

this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop

IPR2025-01152
Apple EX1002 Page 1411

technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

IPR2025-01152
Apple EX1002 Page 1412

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	**02/09/2023 11:19:57 PM 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 #	61576291	FILING DATE	11/16/2021
CUSTOMER #	136197	FIRST NAMED INVENTOR	David WYATT
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	-

Documents

TOTAL DOCUMENTS: 2

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
CorrectedADS.pdf	3	Application Data Sheet to update/correct info	70 KB
WYAT-0002-13C12US_Filing_Receipt_Correction.pdf	4	Request for Corrected Filing Receipt	223 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
CorrectedADS.pdf	1B1B34F3B58961AC151A192A146DCB79F1A229C64E171B8698

	63815BCF5E35D68BF7CD747614283FF95034DECCF6FB68366387FFA25A515FACF5A877FA45A29F
WYAT-0002-13C12US_Filing_Receipt_Correction.pdf	4889C75A123B8BA21E4F1CBA3970685B1D3408B25CA12FEEDF9F944657CC26C88CFC0A2D3C0D795E5C25AAECE2DD3CE5632070A46296BCDE6BDEA8AA4A515102

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

Corrected Application Data Sheet

17528073 : MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

~~Strike through~~ indicates removal of data from existing record Underline indicates new data being added to the application If no data is shown, no data has been corrected

Inventor Information

Data of record	Updated Data
David WYATT	
Residence Information US Residency San Jose, CA UNITED STATES	
Mailing Address ~~1314 Vanna Ct~~ ~~---~~ ~~San Jose, CA 95131~~ UNITED STATES	**Mailing Address** 1306 Norwalk Ln Apt 303 Austin, TX 78703

Application Information

Title of Invention	MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE	
Attorney Docket Number	WYAT-0002.USD1C1C1C1C1C	
Entity Status	~~Small~~	Regular Undiscounted

Domestic Benefit/National Stage Information

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c), 386(c), or indicate National Stage entry from a PCT application. Providing benefit claim information in the Application Data Sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78(a)(2) or CFR 1.78(a)(4), and need not otherwise be made part of the specification.

Data of record	Updated Data
No data change in this section	

Foreign Priority Information

This section allows for the applicant to claim benefit of foreign priority and to identify any prior foreign application for which priority is not claimed. Providing this information in the Application Data Sheet constitutes the claim for priority as required by 35 U.S.C. 119 (b) and 37 CFR 1.55. When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX) the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(i)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

Data of record	Updated Data
No data change in this section	

Applicant Information

The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46.

Data of record	Updated Data
No data change in this section	

Assignee Information including Non-Applicant Assignee Information

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Data of record	Updated Data
No data change in this section	

Signature

NOTE:

This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b).

This Application Data Sheet must be signed by a patent practitioner if one or more of the applicants is a **juristic entity** (e.g., corporation or association). If the applicant is two or more joint inventors, this form must be signed by a patent practitioner, all joint inventors who are the applicant, or one or more joint inventor-applicants who have been given power of attorney (e.g., see USPTO Form PTO/AIA/81) on behalf of all joint inventor-applicants.

See CFR 1.4(d) for the manner of making signatures and certifications.

Signature	First name	Last name	Registration #	Date
/Jose S. Garcia/	Jose	Garcia	43628	02/09/2023

Document Description: Application Data Sheet to update/correct info
Doc Code: ADS.CORR

CORRECTED ADS FORM

Application Number	17528073
Title of Invention	MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

Inventor Information

****If no data is shown, no data has been corrected****

	Data of Record	Updated Data
Order Number	1	
Name	David WYATT	
Residence Information		
Residency	us-residency	
City	~~San Jose~~	Austin
State	~~CA~~	TX
Country of Residence	US	
Mailing Address of Inventor		
Address 1	~~1314 Vanna Ct~~	1306 Norwalk Ln
Address 2		Apt 303
City,State/Province, Postal Code	~~San Jose CA 95131~~	Austin TX 78703
Country	US	

IPR2025-01152
Apple EX1002 Page 1418

Document Description: Application Data Sheet to update/correct info
Doc Code: ADS.CORR

Application Information

	Data of Record	Updated Data
Title of Invention	MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE	
Attorney Docket Number	WYAT-0002.USD1C1C1C1C1C	
Entity Type	Small	

Domestic Benefit/National Stage Information

****If no data is shown, no data has been corrected****

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121,365(c), or 386(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S. C. 119(e) or 120, and 37 CFR 1.78(a).

		Data of Record	Updated Data
	Prior Application Status		
	Application Number		
	Continuity Type		
	Prior Application Number		
	Filing Date (YYYY-MM-DD)		
	Patent Number		
	Issue Date (YYYY-MM-DD)		

Foreign Priority Information

IPR2025-01152
Apple EX1002 Page 1419

Document Description: Application Data Sheet to update/correct info
Doc Code: ADS.CORR

****If no data is shown, no data has been corrected****

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55. When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX) the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(i)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

		Data of Record	Updated Data
	Application Number		
	Country		
	Filing Date		
	Access Code		

Applicant Information

****If no data is shown, no data has been corrected****
Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

	Data of Record	Updated Data
Applicant Type		
If applicant is the legal representative, indicate the authority to file the patent application, the inventor is		
Name of the Deceased or Legally Incapacitated Inventor		
Applicant is an Organization		
Name		
Organization Name		
Address 1		
Address 2		

City,State/Province,Postal Code		
Country		
Phone Number		
Fax Number		
Email Address		

Assignee Information including Non-Applicant Assignee Information

****If no data is shown, no data has been corrected****
Providing this information in the application data sheet does not substitute for compliance with any requirement of part 3 of Title 37 of the CFR to have an assignment recorded in the Office

	Data of Record	Updated Data
Order		
Applicant is an Organization		
Name		
Organization Name		

Mailing Address

Address 1		
Address 2		
City,State/Province,Postal Code		
Country		
Phone Number		
Fax Number		
Email Address		

Signature

NOTE: This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b).

This Application Data Sheet **must** be signed by a patent practitioner if one or more of the applicants is a **juristic entity** (e.g., corporation or association). If the applicant is two or more joint inventors, this form must be signed by a patent practitioner, **all** joint inventors who are the applicant, or one or more joint inventor-applicants who have been given power of attorney (e.g., see USPTO Form PTO/AIA/81) on behalf of **all** joint inventor-applicants.

See 37 CFR 1.4(d) for the manner of making signatures and certifications.

Signature	/Jose S. Garcia/	Registration Number	43628
First Name	Jose	Last Name	Garcia

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
17/528,073	11/16/2021	2876	3750	WYAT-0002.USD1C1C1C1C1C	14	2

CONFIRMATION NO. 4809
CORRECTED FILING RECEIPT

136197
David Wyatt c/o Murabito, Hao & Barnes
111 North Market Street
Suite 700
San Jose, CA 95113

OC000000136862754

Date Mailed: 11/17/2022

Receipt is acknowledged of this non-provisional utility patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF FIRST INVENTOR, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection.

Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a corrected Filing Receipt, including a properly marked-up ADS showing the changes with strike-through for deletions and underlining for additions. If you received a "Notice to File Missing Parts" or other Notice requiring a response for this application, please submit any request for correction to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections provided that the request is grantable.

Inventor(s)

David WYATT, Austin, TX; ~~San Jose, CA~~;

Applicant(s)

CARDWARE, INC, San Jose, CA;

Power of Attorney: The patent practitioners associated with Customer Number 136197

Domestic Priority data as claimed by applicant

This application is a CON of 17/075,637 10/20/2020 PAT 11176538
which is a CON of 16/459,150 07/01/2019 PAT 10810579
which is a CON of 15/701,261 09/11/2017 PAT 10339520
which is a CON of 14/981,757 12/28/2015 PAT 9760884
which is a CON of 14/680,979 04/07/2015 PAT 9224083
which is a DIV of 14/217,261 03/17/2014 PAT 9022286
which claims benefit of 61/794,891 03/15/2013

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

IPR2025-01152
Apple EX1002 Page 1423

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 11/30/2021
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 17/528,073**
Projected Publication Date: Not Applicable
Non-Publication Request: No
Early Publication Request: No
**** SMALL ENTITY ****
Title

MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

Preliminary Class

235

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative,

IPR2025-01152
Apple EX1002 Page 1424

this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop

IPR2025-01152
Apple EX1002 Page 1425

technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

IPR2025-01152
Apple EX1002 Page 1426

Electronic Acknowledgement Receipt

EFS ID:	47512106
Application Number:	17528073
International Application Number:	
Confirmation Number:	4809
Title of Invention:	MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE
First Named Inventor/Applicant Name:	David WYATT
Customer Number:	136197
Filer:	Jose S. Garcia
Filer Authorized By:	
Attorney Docket Number:	WYAT-0002.USD1C1C1C1C1C
Receipt Date:	10-FEB-2023
Filing Date:	16-NOV-2021
Time Stamp:	00:42:50
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Application Data Sheet to update/ correct info	CorrectedADS.pdf	102555 87a8012224df8c08385be2eddb0830e64a3b53bd	no	5

Warnings:

IPR2025-01152
Apple EX1002 Page 1427

Information:					
2	Request for Corrected Filing Receipt	WYAT-0002-13C12US_Filing_Receipt_Correction.pdf	227895 35b0059b8c0e1e5d2d8c0318ee672669d4e8e09d	no	4
Warnings:					
Information:					
			Total Files Size (in bytes):	330450	

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 a 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

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

136197 7590 02/13/2023

David Wyatt c/o Murabito, Hao & Barnes
111 North Market Street
Suite 700
San Jose, CA 95113

EXAMINER
LEE, SEUNG H

ART UNIT	PAPER NUMBER
2876	

DATE MAILED: 02/13/2023

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/528,073	11/16/2021	David WYATT	WYAT-0002.USD1C1C1C1C1C	4809

TITLE OF INVENTION: MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0.00	$0.00	$480	05/15/2023

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 40% the amount of undiscounted fees, and micro entity fees are 20% the amount of undiscounted fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

IPR2025-01152
Apple EX1002 Page 1429

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

136197 7590 02/13/2023
David Wyatt c/o Murabito, Hao & Barnes
111 North Market Street
Suite 700
San Jose, CA 95113

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/528,073	11/16/2021	David WYATT	WYAT-0002.USD1C1C1C1C1C	4809

TITLE OF INVENTION: MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0.00	$0.00	$480	05/15/2023

EXAMINER	ART UNIT	CLASS-SUBCLASS
LEE, SEUNG H	2876	235-380000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

❑ Change of correspondence address (or Change of Correspondence Address form PTO/AIA/122 or PTO/SB/122) attached.

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/AIA/47 or PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. Fees submitted: ❑ Issue Fee ❑ Publication Fee (if required) ❑ Advance Order - # of Copies _____

4b. Method of Payment: *(Please first reapply any previously paid fee shown above)*

❑ Electronic Payment via EFS-Web ❑ Enclosed check ❑ Non-electronic payment by credit card (Attach form PTO-2038)

❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. _____

5. **Change in Entity Status** (from status indicated above)

❑ Applicant certifying micro entity status. See 37 CFR 1.29

❑ Applicant asserting small entity status. See 37 CFR 1.27

❑ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

IPR2025-01152
Apple EX1002 Page 1430

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/528,073	11/16/2021	David WYATT	WYAT-0002.USD1C1C1C1C1C	4809

136197 7590 02/13/2023

David Wyatt c/o Murabito, Hao & Barnes
111 North Market Street
Suite 700
San Jose, CA 95113

EXAMINER	
LEE, SEUNG H	
ART UNIT	PAPER NUMBER
2876	

DATE MAILED: 02/13/2023

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

IPR2025-01152
Apple EX1002 Page 1431

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. 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 1.14. This collection is estimated to take 30 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, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

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 disclosure of these records is required by the Freedom of Information Act.
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 inspection 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.

IPR2025-01152
Apple EX1002 Page 1432

Notice of Allowability	Application No. 17/528,073	Applicant(s) WYATT, David	
	Examiner SEUNG H LEE	Art Unit 2876	AIA (FITF) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☑ This communication is responsive to 1/12/2023.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☑ The allowed claim(s) is/are 15-86 . As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see **http://www.uspto.gov/patents/init_events/pph/index.jsp** or send an inquiry to **PPHfeedback@uspto.gov.**

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some* c) ☐ None of the:

   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____ .

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____ .

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☑ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 6 IDSs filed on 1/12/2023.
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____.
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date. _____.
5. ☐ Examiner's Amendment/Comment
6. ☑ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/SEUNG H LEE/
Primary Examiner, Art Unit 2876

IPR2025-01152
Apple EX1002 Page 1433

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application is being examined under the pre-AIA first to invent provisions.

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on January 12, 2023 has been entered.

Allowable Subject Matter

3. Claims 15-86 are allowed.

4. The following is an examiner's statement of reasons for allowance:

None of prior art teaches a method of generating and using limited-use payment information for performing a payment transaction, the method comprising: receiving an input at an electronic device, wherein the input comprises a priming operation, and, wherein the electronic device comprises: a processor; a touch-screen display coupled to the processor; and a near field communications (NFC) interface coupled to the processor; responsive to said priming operation, readying said device to perform a payment transaction by an identified user; receiving a payment request for the payment transaction at said electronic device; displaying, on the touch-screen display, information reflecting the payment request, and an image representing a selected

issued payment account; dynamically generating, by the processor, limited-use payment information; wherein said limited-use payment information is dynamically generated based on a per-transaction sequential parameter originating from the electronic device; using said limited-use payment information in connection with the payment transaction in place of issued payment information associated with said selected issued payment account; transmitting said limited-use payment information from said electronic device via said NFC interface for receipt by an NFC recipient.; responsive to the transmitting the limited-use payment information, receiving via the NFC interface information reflecting a status of said payment transaction; and displaying the status of said payment transaction via said touch-screen display, and a system of the same as set forth in the claims.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to SEUNG H LEE whose telephone number is (571)272-2401. The examiner can normally be reached 7-4:00PM.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an

interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Steven Paik can be reached on 571-272-2404. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of published or unpublished applications may be obtained from Patent Center. Unpublished application information in Patent Center is available to registered users. To file and manage patent submissions in Patent Center, visit: https://patentcenter.uspto.gov. Visit https://www.uspto.gov/patents/apply/patent-center for more information about Patent Center and https://www.uspto.gov/patents/docx for information about filing in DOCX format. For additional questions, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/SEUNG H LEE/
Primary Examiner, Art Unit 2876

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/528,073	WYATT, David
	Examiner	Art Unit
	SEUNG H LEE	2876

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☑ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	11/05/2022	01/28/2023							
1	15	=	=							
2	16	=	=							
7	17	=	=							
8	18	=	=							
9	19	=	=							
10	20	=	=							
11	21	=	=							
12	22	=	=							
13	23	=	=							
14	24	=	=							
15	25	=	=							
16	26	=	=							
17	27	=	=							
23	28	=	=							
24	29	=	=							
25	30	=	=							
26	31	=	=							
3	32	=	=							
18	33	=	=							
4	34	=	=							
27	35	=	=							
28	36	=	=							
21	37	=	=							
22	38	=	=							
5	39	=	=							
6	40	=	=							
19	41	=	=							
20	42	=	=							
29	43	=	=							
30	44	=	=							
31	45	=	=							
32	46	=	=							
33	47	=	=							
34	48	=	=							
35	49	=	=							
36	50	=	=							
38	51	=	=							
37	52	=	=							
39	53	=	=							
40	54	=	=							
41	55	=	=							
44	56	=	=							

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/528,073	WYATT, David
	Examiner	**Art Unit**
	SEUNG H LEE	2876

CLAIM		DATE								
Final	Original	11/05/2022	01/28/2023							
42	57	=	=							
43	58	=	=							
45	59	=	=							
46	60	=	=							
47	61	=	=							
48	62	=	=							
49	63	=	=							
50	64	=	=							
51	65	=	=							
52	66	=	=							
53	67	=	=							
54	68	=	=							
55	69	=	=							
56	70	=	=							
57	71	=	=							
60	72	=	=							
61	73	=	=							
58	74	=	=							
59	75	=	=							
62	76	=	=							
63	77	=	=							
64	78	=	=							
65	79	=	=							
66	80	=	=							
67	81	=	=							
68	82	=	=							
69	83	=	=							
70	84	=	=							
71	85	=	=							
72	86	=	=							

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/528,073	WYATT, David
	Examiner	Art Unit
	SEUNG H LEE	2876

CPC - Searched*		
Symbol	Date	Examiner
G06Q20/341 or G06K19/06206 or G06K19/0716 or G06K19/07749 or G06Q20/06 or G06Q20/065 or G06Q20/223 or G06Q20/24 or G06Q20/346 or G06Q20/347 or G06Q20/352 or G06Q20/3827 or G06Q20/385 or G06Q20/4012 or G06Q20/409 or G07F7/0873 or G07F19/00	01/28/2023	sl

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
PE2E	01/28/2023	sl
14/680979,14/981757,15/701261,16/459150, 17/075637 (parent cases)	01/28/2023	sl
NPL	11/05/2022	sl

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner
	same as above	01/28/2023	sl

IPR2025-01152
Apple EX1002 Page 1439

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/528,073	WYATT, David
	Examiner	Art Unit
	SEUNG H LEE	2876

IPR2025-01152
Apple EX1002 Page 1440

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/528,073	WYATT, David
	Examiner	**Art Unit**
	SEUNG H LEE	2876

CPC						
Symbol					**Type**	**Version**
G06Q	/	20	/	341	F	2013-01-01
G07F	/	19	/	00	I	2013-01-01
G06Q	/	20	/	06	I	2013-01-01
G06Q	/	20	/	223	I	2013-01-01
G06Q	/	20	/	347	I	2013-01-01
G06Q	/	20	/	385	I	2013-01-01
G07F	/	7	/	0873	I	2013-01-01
G06K	/	19	/	06206	I	2013-01-01
G06K	/	19	/	0716	I	2013-01-01
G06K	/	19	/	07749	I	2013-01-01
G06Q	/	20	/	24	I	2013-01-01
G06Q	/	20	/	352	I	2013-01-01
G06Q	/	20	/	409	I	2013-01-01
G06Q	/	20	/	065	I	2013-01-01
G06Q	/	20	/	346	I	2013-01-01
G06Q	/	20	/	3827	I	2013-01-01
G06Q	/	20	/	4012	I	2013-01-01

CPC Combination Sets							
Symbol					**Type**	**Set**	**Ranking**	**Version**
	/		/					

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	72	
/SEUNG H LEE/ Primary Examiner, Art Unit 2876	28 January 2023	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

U.S. Patent and Trademark Office

Part of Paper No.: 20230126

IPR2025-01152
Apple EX1002 Page 1441

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/528,073	WYATT, David
	Examiner	**Art Unit**
	SEUNG H LEE	2876

INTERNATIONAL CLASSIFICATION					
CLAIMED					
G06Q20/34	/	20	/	34	

NON-CLAIMED					
	/		/		

US ORIGINAL CLASSIFICATION	
CLASS	**SUBCLASS**

CROSS REFERENCES(S)						
CLASS	**SUBCLASS (ONE SUBCLASS PER BLOCK)**					

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	72	
/SEUNG H LEE/ Primary Examiner, Art Unit 2876	28 January 2023	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

U.S. Patent and Trademark Office

Part of Paper No.: 20230126

IPR2025-01152
Apple EX1002 Page 1442

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/528,073	WYATT, David
	Examiner	**Art Unit**
	SEUNG H LEE	2876

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☑ T.D. ☐ R.1.47

CLAIMS

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	15	14	24	18	33	20	42	38	51	46	60	55	69	64	78
2	16	15	25	4	34	29	43	37	52	47	61	56	70	65	79
7	17	16	26	27	35	30	44	39	53	48	62	57	71	66	80
8	18	17	27	28	36	31	45	40	54	49	63	60	72	67	81
9	19	23	28	21	37	32	46	41	55	50	64	61	73	68	82
10	20	24	29	22	38	33	47	44	56	51	65	58	74	69	83
11	21	25	30	5	39	34	48	42	57	52	66	59	75	70	84
12	22	26	31	6	40	35	49	43	58	53	67	62	76	71	85
13	23	3	32	19	41	36	50	45	59	54	68	63	77	72	86

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	72	
/SEUNG H LEE/ Primary Examiner, Art Unit 2876	28 January 2023	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

U.S. Patent and Trademark Office

Part of Paper No.: 20230126

IPR2025-01152
Apple EX1002 Page 1443

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (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.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17528073
Filing Date	2021-11-16
First Named Inventor	David WYATT
Art Unit	2876
Examiner Name	LEE, SEUNG H.
Attorney Docket Number	WYAT-0002-13C12US

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.H.L./

IPR2025-01152
Apple EX1002 Page 1444

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	1	"Isis NFC-payment from SXSW 2012," YouTube, https://www.youtube.com/watch?v=Z2MOAtUhR7k, March 10, 2012, pp. 1- 2.	
	2	"Isis NFC-payment from SXSW 2012," Transcript of YouTube, https://www.youtube.com/watch?v=Z2MOAtUhR7k, March 10, 2012, pp. 1- 3.	
	3	"NFC - Google Wallet and More - EE Times - Mobile World Congress," YouTube, https://www.youtube.com/watch?v=AgSk7L6HhVw, March 6, 2012, pp. 1-3.	
	4	"NFC - Google Wallet and More - EE Times - Mobile World Congress," Transcript of YouTube, https://www.youtube.com/watch?v=AgSk7L6HhVw, March 6, 2012, pp. 1-8.	
	5	"Paying With Google Wallet," YouTube, https://www.youtube.com/watch?v=jTeilSIzBPQ, February 6, 2012, pp. 1-2.	
	6	"Seinfeld - Google Wallet," YouTube, https://www.youtube.com/watch?v=baaCvgTRYsU, June 14, 2013, pp. 1-2.	
	7	"Technology: Google Wallet - The New York Times," YouTube, https://www.youtube.com/watch?v=I8JOT6ban7o, September 23, 2011, pp. 1-2.	
	8	"Using Google Wallet in McDonald's!," YouTube, https://www.youtube.com/watch?v= 1p6co4YIvbA, September 14, 2012, pp. 1-2.	
	9	"Virtual terminal- #1 storing credit card data with tokenization," YouTube, https://www.youtube.com/watch?v=eSXIIGbACew, February 28, 2011, pp. 1-3.	
	10	"What is Google Wallet?," YouTube, https://www.youtube.com/watch?v=iuvyN4iZiP8, August 9, 2011, pp. 1-3.	
	11	"What is Tokenization?," YouTube, https://www.youtube.com/watch?v=ypm5FFfEN34, January 17, 2011, pp. 1-3.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.H.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	17528073
Filing Date	2021-11-16
First Named Inventor	David WYATT
Art Unit	2876
Examiner Name	LEE, SEUNG H.
Attorney Docket Number	WYAT-0002-13C12US

	12	"How Credit Card Number Tokenization can Reduce PCI Compliance Stress - File 1 of 3," YouTube, https://www.youtube.com/watch?v=FHD5XzAIKDI, Jul 28, 2009, pp. 1-3.	
	13	"How Credit Card Number Tokenization can Reduce PCI Compliance Stress - File 1 of 3," Transcript of YouTube, https://www.youtube.com/watch?v=FHD5XzAIKDI, Jul 28, 2009, pp. 1-12.	
	14	"HOW CREDIT CARD NUMBER "TOKENIZATION" CAN REDUCE PCI COMPLIANCE STRESS - File 2 of 3," YouTube, https://www.youtube.com/watch?v=t-fWpcLdb3o, Jul 28, 2009, pp. 1-3.	
	15	"HOW CREDIT CARD NUMBER "TOKENIZATION" CAN REDUCE PCI COMPLIANCE STRESS - File 2 of 3," Transcript of YouTube, https://www.youtube.com/watch?v=t-fWpcLdb3o, Jul 28, 2009, pp. 1-12.	
	16	"HOW CREDIT CARD NUMBER "TOKENIZATION" CAN REDUCE PCI COMPLIANCE STRESS- File 3 of 3," YouTube, https://www.youtube.com/watch?v=_CdoKEuEB9s, Jul 28, 2009, pp. 1-3.	
	17	"HOW CREDIT CARD NUMBER "TOKENIZATION" CAN REDUCE PCI COMPLIANCE STRESS- File 3 of 3," Transcript of YouTube, https://www.youtube.com/watch?v=_CdoKEuEB9s, Jul 28, 2009, pp. 1-8.	
	18	"Caixer contactless lacaixa," YouTube, https://www.youtube.com/watch?v=It2CpMcxQC4, April 4, 2011, pp. 1-2.	
	19	"Understanding Proximity Sensors - T-Mobile," YouTube, https://www.youtube.com/watch?v=npD48agt0xY, January 2010, pp. 1-2.	
	20	"Understanding Proximity Sensors - T-Mobile," YouTube, https://www.youtube.com/watch?v=npD48agt0xY, January 2010, page 1.	
	21	"Understanding Proximity Sensors - T-Mobile," Transcript of YouTube, https://www.youtube.com/watch?v=npD48agt0xY, January 2010, pp. 1-2.	
	22	"Google I/O 2012 - The Sensitive Side of Android," YouTube, https://www.youtube.com/watch?v=Q0V_Id7iNw4, June 29, 2012, pp. 1-2.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.H.L./

IPR2025-01152
Apple EX1002 Page 1446

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	23	"Google Wallet Overview," YouTube, https://www.youtube.com/watch?v=VuFVsaFCzsw, August 1, 2012, page 1.	
	24	"Google Wallet Overview," Transcript of YouTube, https://www.youtube.com/watch?v=VuFVsaFCzsw, August 1, 2012, pp. 1-2.	
	25	"Android 4.0 APIs | Android Developers," mit.edu, https://stuff.mit.edu/afs/sipb/project/android/docs/about/versions/android-4.0.html, 2011, pp. 1-23.	
	26	"EMV Integrated Circuit Card Specifications for Payment Systems, Book 2, Security and Key Management, Version 4.3," EMVCo, November 2011, pp. 1-174.	
	27	"Exploring Google Wallet using the secure element interface," nelenkov.blogspot.com, August 27, 2012, pp. 1-20.	
	28	GARSIDE, "Google Wallet mobile payments system launched to public," The Guardian, https://www.theguardian.com/technology/2011/sep/19/google-wallet-available-public, September 19, 2011, pp. 1-5.	
	29	PURDY, "How to grab a screenshot from iPhone, Android, and nearly any other smartphone," Computer World, April 20, 2012, pp. 1-6.	
	30	"Maximum failed passcode attempts in restrictions - what happens?," Apple Community, https://discussions.apple.com/thread/3690633, January 2012, pp. 1-3.	
	31	"Simplify, Organize & Pay with Loop by Will Graylin & George Wallner," Kickstarter, March 2019, pp. 1-13.	
	32	"Hands-on with ISIS Mobile Wallet," YouTube, https://www.youtube.com/watch?v=eOMqvGVKjmM, March 10, 2012, page 1.	
	33	"EMV Solutions," Paragon Application Systems, https://web.archive.org/web/20120818221214/http://www.paragonedge.com/solutions/emv-solutions.html, August 18, 2012, page 1.	

IPR2025-01152
Apple EX1002 Page 1447

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	34	SULLIVAN, "The Changing Nature of U.S. Card Payment Fraud: Industry and Public Policy Options," Economic Review, Federal Reserve Bank of Kansas City, Second Quarter 2010, ProQuest Information and Learning, Vol. 95, No. 2, pp 101-133.
	35	"EMV Integrated Circuit Card Specifications for Payment Systems, Book 1, Application Independent ICC to Terminal Interface Requirements, Version 4.3," EMVCo, November 2011, pp. 1-189.
	36	"EMV Contactless Specifications for Payment Systems, Book B, Entry Point Specification, Version 2.1," EMVCo, March 2011, pp. 1-50.
	37	ETHERINGTON, "Android Pay Is Real, And Will Give Developers The Reins As An API," TechCrunch, https://techcrunch.com/2015/03/02/android-pay-is-real-and-will-give-developers-the-reins-as-an-api, March 2, 2015, pp. 1-7.
	38	"PCI DSS Version 2.0 Information Supplement: PCI DSS Tokenization Guidelines," PCI Security Standards Council, pcisecuritystandards.org, https://listings.pcisecuritystandards.org/documents/Tokenization_Guidelines_Info_Supplement.pdf., v 2.0, August 2011, pp. 1-23.
	39	"EMVCo Updates Payment Tokenisation Specification to Introduce 'Payment Account Reference,'" www.emvco.com, March 29, 2016, pp. 1-2.

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/SEUNG H LEE/	Date Considered	01/28/2023

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.H.L./

IPR2025-01152
Apple EX1002 Page 1448

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17528073
Filing Date	2021-11-16
First Named Inventor	David WYATT
Art Unit	2876
Examiner Name	LEE, SEUNG H.
Attorney Docket Number	WYAT-0002-13C12US

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Jose S. Garcia/	Date (YYYY-MM-DD)	2023-01-12
Name/Print	Jose S. Garcia	Registration Number	43,628

This collection of information is required by 37 CFR 1.97 and 1.98. 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 1.14. This collection is estimated to take 1 hour 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. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

IPR2025-01152
Apple EX1002 Page 1449

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 record s.

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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH.

IPR2025-01152
Apple EX1002 Page 1450

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (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.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17528073
Filing Date	2021-11-16
First Named Inventor	David WYATT
Art Unit	2876
Examiner Name	LEE, SEUNG H.
Attorney Docket Number	WYAT-0002-13C12US

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S. H. L./

IPR2025-01152
Apple EX1002 Page 1451

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	1	"EMVCO Publishes Technical Framework for its Payment Tokenisation Specification," EMVCO, March 11, 2014, pp. 1-2.	
	2	"Encryption and Tokenization: Which is best for your business?," Townsend Security, 2010, pp. 1-4.	
	3	MOLEN, "Engadget Primed: What is NFC, and why do we care?," Engadget, June 10, 2011, pp. 1-11.	
	4	"Exploring Google Wallet using the secure element interface," nelenkov.blogspot.com, August 27, 2012, pp. 1-11.	
	5	"Financial Cryptography," 5th International Conference, FC 2001 Proceedings, Grand Cayman, British West Indies, February 19-22, 2001, Paul F. Syverson (Editor), pp. 1-57.	
	6	"Gemalto to Provide Isis Mobile Commerce Platform with Trusted Service Manager (TSM) Solution," Business Wire, December 12, 2011, pp. 1-3.	
	7	"Google Checkout checks out, replaced by Google Wallet," Android Community, November 17, 2011, page 1.	
	8	"Google Checkout HTML API Short Attribute Reference," Google Checkout, Google Code (archive.org), March 27, 2012, pp. 1-4.	
	9	"Google Commerce: Building one wallet: Google Checkout is transitioning to Google Wallet," commerce.googleblog.com, November 16, 2011, pp. 1-2.	
	10	"Google Prepaid Cards," Wallet Help, Google (archive.org), October 3, 2012, page 1.	
	11	CLARK, "Google Unveils first Android NFC phone - but Nexus S is limited to tag reading only for now," NFC World, December 7, 2010, pp. 1-4.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S. L./

IPR2025-01152
Apple EX1002 Page 1452

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	12	"Google Wallet launches officially on Nexus S 4G," Android Community, September 19, 2011, pp. 1-2.	
	13	GARSIDE, "Google Wallet mobile payments system launched to public," The Guardian, September 19, 2011, page 1.	
	14	BOULTON, "Google Wallet Mobile Payments Coming to New York, Francisco; Google Wallet will launch this summer to enable consumers to pay for goods by tapping their Samsung Nexus 2 4G Android phones at NFC-fitted sales terminals at Subway, Macy's and other retailers," eWeek.com, May 26, 2011, pp. 1-2.	
	15	FINGAS, "Google Wallet reaches the web, reminds most of us that it exists," Engadget, October 4, 2012, pp. 1-6.	
	16	RAPHAEL, "Google's Eric Schmidt spills clues about Android Gingerbread," ComputerWorld, November 15, 2010, pp. 1-3.	
	17	"Handset makers line up behind Isis NFC payment platform," Old GigaOm, September 27, 2011, pp. 1-2.	
	18	"How it Works," Wallet Help, Google (archive.org), March 12, 2013, page 1.	
	19	"How to find out IMEI number on Google Nexus S phone," Tech Notes Desk, January 10, 2013, page 1.	
	20	"La Caixa," Annual Report, 2010, Barcelona, Spain, pp. 1-190.	
	21	"INSIDE Contactless to Equip KTFMobile Payment Project Mobile Phones; Korean Manufacturer Confirms INSIDE's NFC Maturity by Embedding MicroRead into LG Electronics and Samsung Electronics Mobile Phones for its Mobile Payment Project," Business Wire, July 16, 2007, pp. 1-2.	
	22	CLUCKEY, "Is a contactless ATM inevitable? Bank of America seems to think so; the FI has filed a patent application for a 'Contactless Automated Teller Machine,'" ATM Marketplace, September 20, 2012, pp. 1-3.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.H.L./

IPR2025-01152
Apple EX1002 Page 1453

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	23	"Isis™ Launches in Austin and Salt Lake City; As Many as 20 Isis Ready™ Handsets to Be Available by Year End," Business Wire, October 22, 2012, page 1.	
	24	PEREZ, "Isis Revealed: Carrier-Led Mobile Payments Venture Shows Off Its New App, Announces Banking Partners," TechCrunch, February 27, 2012, pp. 1-6.	
	25	SADEWO, "Isis to officially launch on Oct 22, more supported devices announced," androidauthority.com, October 18, 2012, pp. 1-2.	
	26	"MasterCard Approves NFC Phones from HTC, Intel, LG Electronics, Nokia, RIM, Samsung Electronics and Sony," Professional Services Close-Up, May 10, 2012, Close-Up Media, Inc., pp. 1-2.	
	27	"MASTERCARD INC, FORM 10-K (Annual Report)," Filed February 28, 2007, for the Period Ending December 31, 2006, pp. 1-204.	
	28	"MasterCard, Visa and American Express Propose New Global Standard to Make Online and Mobile Shopping Simpler and Safer," Global Hub, Engagement Bureau, Press Release, October 1, 2013, pp. 1-2.	
	29	"Fact Sheet: Mobile Commerce: A New Way to Pay: MasterCard Mobile Commerce," May 26, 2011, pp. 1-4.	
	30	"McDonald's testing e-payment system," USA Today, May 29, 2001, pp. 1-3.	
	31	"Mobile Contactless Payments Trialled Live at Mobile World Congress 2010; GSMA, Samsung, Telefónica and Visa, with Giesecke & Devrient, Ingenico, ITN International and La Caixa, collaborate across industries to give Congress attendees an opportunity to experience NFC," Business Wire, February 15, 2010, pp. 1-3.	
	32	"Mobile Payment Bringing value to payments on mobile," Gemalto, November 2011, pp. 1-4.	
	33	WOO, "Mobile PayPass Meets Cloud in Google Wallet," Global Hub, August 1, 2012, pp. 1-2.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINE THROUGH CITATION.

IPR2025-01152
Apple EX1002 Page 1454

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	34	HEUN, "Mobile Wallet Consortium Strives Cautiously In 2012; The telco joint effort proceeded more slowly than expected, but its leaders maintain that the mobile wallet business is big enough for lots of players," Section: MOBILE: ISIS, January 1, 2013, Page 47, Vol. 2, No. 1, SouceMedia LLC d/b/a Arizent, pp. 1-3.
	35	BELL, "Mobile's Gains Prompt More Banks To Move Beyond Cards For ATM Access," Payments Source, Section: DEBIT: Vol. 1, No. 1, May 12, 2011, pp. 1-4.

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/SEUNG H LEE/	Date Considered	01/28/2023

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17528073
Filing Date	2021-11-16
First Named Inventor	David WYATT
Art Unit	2876
Examiner Name	LEE, SEUNG H.
Attorney Docket Number	WYAT-0002-13C12US

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Jose S. Garcia/	Date (YYYY-MM-DD)	2023-01-12
Name/Print	Jose S. Garcia	Registration Number	43,628

This collection of information is required by 37 CFR 1.97 and 1.98. 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 1.14. This collection is estimated to take 1 hour 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. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

IPR2025-01152
Apple EX1002 Page 1456

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.S.G./

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 record s.

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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.T./

IPR2025-01152
Apple EX1002 Page 1457

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (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.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17528073
Filing Date	2021-11-16
First Named Inventor	David WYATT
Art Unit	2876
Examiner Name	LEE, SEUNG H.
Attorney Docket Number	WYAT-0002-13C12US

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.H.L./

IPR2025-01152
Apple EX1002 Page 1458

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	1	"Standing Document (SD1): WG8 Projects: ISO/IEC 14443, Proximity Cards (PICCS)," ISO/IEC JTC1/SC17/WG8 (archive.org), October 25, 2010, pp. 1-6.	
	2	"Telefonica O2 Czech Republic prepares NFC payments," DmEurope, March 25, 2011, page 1.	
	3	MARKKANEN, "Telefonica, Samsung to Pilot SIM-Based NFC Payment Solution in Spain," IHS Global Insight, February 15, 2010, pp. 1-2.	
	4	"The Mobile Payments and NFC Landscape: A U.S. Perspective," Smart Card Alliance, September 2011, pp. 1-53.	
	5	"Tokenization Guidance: How to reduce PCI compliance costs, Version 1.0," Securosis, December 10, 2011, pp. 1-31.	
	6	"Tokenization: What's Next After PCI," RSA, 2012, pp. 1-8.	
	7	SEIFERT, "Verizon won't offer Google Wallet for the Galaxy Nexus because it uses a 'secure element'," The Verge, December 10, 2012, pp. 1-2.	
	8	"Visa and Google Sign Licensing Deal to Boost Mobile Payment Adoption," Visa, September 19, 2011, pp. 1-2.	
	9	"Visa Best Practices for Tokenization Version 1.0," Visa, July 14, 2010, pp. 1-4.	
	10	CROSMAN, "Visa Certifies BlackBerry, Samsung And LG Phones For PayWave NFC Payments," Payments Source, January 10, 2012, pp. 1-2.	
	11	"Visa Completes Acquisition of Rambus Payments Portfolio," Business Wire, October 22, 2019, page 1.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.H.L./

IPR2025-01152
Apple EX1002 Page 1459

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	12	"Convenience for customers. Profits for you," Visa PayWave (archive.org), January 2013, pp. 1-2.	
	13	"Verizon User Manual: Samsung Galaxy SIII," Verizon, January 2012, pp. 1-204.	
	14	"World leader in proven and efficient cards for EMV deployment," Gemalto, February 2010, pp. 1-2.	
	15	BECKER, "29C3: A Rambling Walk Through an EMV Transaction (EN)," YouTube, https://www.youtube.com/watch?v=VdNm9JJmCzg, December 30, 2012, pp. 1-2.	
	16	"ARQC and ARPC Generation and Validation," YouTube, https://www.youtube.com/watch?v=I1XTn175FFk, Paragon Application Systems, July 25, 2012, pp. 1-3.	
	17	"CardVault by 3Delta Systems - Securing Credit Card Payments for B2B and B2G through Tokenization," YouTube, https://www.youtube.com/watch?v=h3zuiLiF51k, February 1, 2010, pp. 1-3.	
	18	"CardVault by 3Delta Systems - Securing Credit Card Payments for B2B and B2G through Tokenization," Transcript of YouTube, https://www.youtube.com/watch?v=h3zuiLiF51k, February 1, 2010, pp. 1-3.	
	19	"Credit Card Processing with EPX BuyerWall Tokenization," YouTube, https://www.youtube.com/watch?v=_7E5hj9li4g, December 21, 2010, pp. 1-3.	
	20	"Credit Card Processing with EPX BuyerWall Tokenization," Transcript of YouTube, https://www.youtube.com/watch?v=_7E5hj9li4g, December 21, 2010, pp. 1-7.	
	21	"Find out how PayPal works," YouTube, https://www.youtube.com/watch?v=dn42Y-2uFQM, March 14, 2012, pp. 1-2.	
	22	"Google checkout," YouTube, https://www.youtube.com/watch?v=-UeYkxePW2c, June 29, 2006, pp. 1-2.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S. L./

IPR2025-01152
Apple EX1002 Page 1460

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	23	"See Google I/O 2011: Google Checkout: A Foundation For Payments," YouTube, https://www.youtube.com/watch?v=7ts7Lkykn0E, May 13, 2011, pp. 1-2.	
	24	"See Google I/O 2011: Google Checkout: A Foundation For Payments," Transcript of YouTube, https://www.youtube.com/watch?v=7ts7Lkykn0E, May 13, 2011, pp. 1-64.	
	25	"Google I/O 2011: How to NFC," YouTube, https://www.youtube.com/watch?v=49L7z3rxz4Q, May 10, 2011, pp. 1-2.	
	26	"Google I/O 2011: How to NFC," Transcript of YouTube, https://www.youtube.com/watch?v=49L7z3rxz4Q, May 10, 2011, pp. 1-62.	
	27	"Google I/O 2012: Introducing Google Wallet Cloud APIs," YouTube, https://www.youtube.com/watch?v=tpEGuSwv1fY, June 29, 2012, pp. 1-3.	
	28	"Google I/O 2012: Introducing Google Wallet Cloud APIs," Transcript of YouTube, https://www.youtube.com/watch?v=tpEGuSwv1fY, June 29, 2012, pp. 1-40.	
	29	"Google Nexus S by Samsung at CES 2011," YouTube, https://www.youtube.com/watch?v=5ZjtXH9S9KM, January 11, 2011, pp. 1-2.	
	30	"Google Nexus S by Samsung at CES 2011," Transcript of YouTube, https://www.youtube.com/watch?v=5ZjtXH9S9KM, January 11, 2011, pp. 1-2.	
	31	"Google Payments Live - Google Wallet updates," YouTube, https://www.youtube.com/watch?v=1pxkQ1mFjNA, August 23, 2012, pp. 1-2.	
	32	"Google Payments Live - Google Wallet updates," Transcript of YouTube, https://www.youtube.com/watch?v=1pxkQ1mFjNA, August 23, 2012, pp. 1-40.	
	33	"Google Wallet Demonstration," YouTube, https://www.youtube.com/watch?v=6tBAB5ls5vM, May 26, 2011, pp. 1-2.	

IPR2025-01152
Apple EX1002 Page 1461

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.H.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	34	"Google Wallet Demonstration," Transcript of YouTube, https://www.youtube.com/watch?v=6tBAB5ls5vM, May 26, 2011, pp. 1-2.	
	35	"Google Wallet Hands-On - Engadget," YouTube, https://www.youtube.com/watch?v=5s9wYEkRAgs, May 26, 2011, pp. 1-3.	
	36	"Google Wallet - How to Setup and Use this Exciting NFC Technology," YouTube, https://www.youtube.com/watch?v=_ay1FfLCsHs, July 26, 2012, pp. 1-3.	
	37	"Google Wallet - How to Setup and Use this Exciting NFC Technology," Transcript of YouTube, https://www.youtube.com/watch?v=_ay1FfLCsHs, July 26, 2012, pp. 1-7.	
	38	"Google Wallet Make Your Phone Your Wallet by Google," YouTube, https://www.youtube.com/watch?v=qRVQTQlJV0g, February 18, 2013, pp. 1-2.	
	39	"Google Wallet Make Your Phone Your Wallet by Google," Transcript of YouTube, https://www.youtube.com/watch?v=qRVQTQlJV0g, February 18, 2013, page 1.	
	40	"Google Wallet Product Launch," YouTube, https://www.youtube.com/watch?v=am8t6iZ7up0, May 27, 2011, pp. 1-3.	
	41	"Google Wallet Product Launch," Transcript of YouTube, https://www.youtube.com/watch?v=am8t6iZ7up0, May 27, 2011, pp. 1-56.	
	42	"Google Wallet Walkthrough," YouTube, https://www.youtube.com/watch?v=xmbRSXYdFFs, February 13, 2012, pp. 1-2.	
	43	"How does Google Wallet work? Really well!," YouTube, https://www.youtube.com/watch?v=jY2p-pNkjHA, December 7, 2011, pp. 1-2.	
	44	"How does Google Wallet work? Really well!," Transcript of YouTube, https://www.youtube.com/watch?v=jY2p-pNkjHA, December 7, 2011, pp. 1-2.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S. L./

IPR2025-01152
Apple EX1002 Page 1462

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	45	"How Does PayPal Work?," YouTube, https://www.youtube.com/watch?v=MdrPOCCFQ2k, July 24, 2012, pp. 1-2.
	46	"How To Use Google Wallet On Android," YouTube, https://www.youtube.com/watch?v=6DeiEVBIBcs, October 28, 2011, pp. 1-2.
	47	"How To Use Google Wallet On Verizon Galaxy Nexus - Pocketnow," YouTube, https://www.youtube.com/watch?v=AZ8t757ZfUs, April 20, 2012, pp. 1-2.

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/SEUNG H LEE/	Date Considered	01/28/2023

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.H.L./

IPR2025-01152
Apple EX1002 Page 1463

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17528073
Filing Date	2021-11-16
First Named Inventor	David WYATT
Art Unit	2876
Examiner Name	LEE, SEUNG H.
Attorney Docket Number	WYAT-0002-13C12US

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Jose S. Garcia/	Date (YYYY-MM-DD)	2023-01-12
Name/Print	Jose S. Garcia	Registration Number	43,628

This collection of information is required by 37 CFR 1.97 and 1.98. 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 1.14. This collection is estimated to take 1 hour 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. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

IPR2025-01152
Apple EX1002 Page 1464

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.S.G./

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 record s.

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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH.

IPR2025-01152
Apple EX1002 Page 1465

PE2E SEARCH - Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
L1	30843	(G06Q20/341 or G06Q20/4012 or G06Q20/3827 or G06Q20/346 or G06Q20/065 or G06Q20/409 or G06Q20/352 or G06Q20/24 or G06K19/07749 or G06K19/0716 or G06K19/06206 or G07F7/0873 or G06Q20/385 or G06Q20/347 or G06Q20/223 or G06Q20/06 or G07F19/00).cpc.	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/04/27 12:21 PM
L2	1	nfc same transaction same payment same logo same limited same issuer	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/04/27 12:22 PM
L4	311	monitor$4 same master same node same wireless same sensor	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/01 12:55 PM
L5	18	L4.clm.	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/01 12:55 PM
L6	107	L4 same (slave peripheral)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/01 12:56 PM
L7	7	L6.clm.	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/01 12:56 PM
L8	17	("20030018927"|"9860688"|"20180165568"|"20150154531"|"9189226"|"20100082870"|"20170039666"|"20180046964"|"9824329"|"20080239282"|"9182231"|"20130107770"|"20070049291"|"6614392"|"20100299401"|"20160233927").PN.	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/01 12:58 PM
L9	9	L6 same (environment$4 temperature)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/01 01:00 PM
L10	9	("20130250357"|"20150324745"|"7177054"|"8292173"|"7048194"|"7299990"|"7540603"|"8072620"|"20100096181").PN.	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/01 01:04 PM

L11	39	("2015/0324745").URPN.	(USPAT)	OR	OFF	OFF	2020/05/02 08:57 AM
L12	35	label same wireless same master same (slave peripheral)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/02 09:00 AM
L13	39	"517508"	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/02 09:19 AM
L14	6	(("10339520") or ("9760884") or ("9224083") or ("9022286")).PN.	(US-PGPUB; USPAT; USOCR; EPO; JPO)	OR	OFF	OFF	2020/05/04 05:07 AM
L15	55	nfc same transaction same payment same limited same issuer	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/04 05:07 AM
L16	5	L15 same proximity	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/04 05:08 AM
L17	30909	(G06Q20/341 or G06Q20/4012 or G06Q20/3827 or G06Q20/346 or G06Q20/065 or G06Q20/409 or G06Q20/352 or G06Q20/24 or G06K19/07749 or G06K19/0716 or G06K19/06206 or G07F7/0873 or G06Q20/385 or G06Q20/347 or G06Q20/223 or G06Q20/06 or G07F19/00).cpc.	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/05 08:24 AM
L18	129	L17 and (nfc same select$4 same payment same limit$4)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/05 08:25 AM
L19	43	L17 and (nfc same select$4 same payment same limit$4 same display$4)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/05 08:26 AM
L20	6	(("10339520") or ("9760884") or ("9224083") or ("9022286")).PN.	(US-PGPUB; USPAT; USOCR; EPO; JPO)	OR	OFF	OFF	2020/05/05 08:33 AM
L21	0	L20 and (nfc same select$4 same payment same limit$4 same display$4)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/05 08:33 AM
L22	109	(nfc same select$4 same payment same limit$4 same display$4)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/05 08:33 AM
L23	94	L22 same (mobile portable)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/05 08:34 AM
L24	4186	dynamic same credit	(US-PGPUB; USPAT;	OR	OFF	OFF	2020/05/05

		same card	EPO; JPO)				08:35 AM
L25	7	L22 and L24	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/05 08:35 AM
L26	23	("20020073025" | "20030101137" | "20070278290" | "20100057553" | "20100082487" | "20110137748" | "20110302089" | "20120006891" | "20140052607" | "20140129422" | "20140143037" | "20140195324" | "20140249941" | "20140279474" | "20150058145" | "20160027005" | "20160086161" | "20160162857" | "20160162887" | "20160335619" | "6633223" | "9292849" | "9489671").PN.	(US-PGPUB; USPAT; USOCR)	OR	OFF	OFF	2020/05/05 08:38 AM
L27	6	("20040168067" | "20090276347" | "20110016047" | "20120173311" | "20130159186" | "6163771").PN.	(US-PGPUB; USPAT; USOCR)	OR	OFF	OFF	2020/05/05 08:39 AM
L28	4	(("10339520") or ("9760884") or ("9224083") or ("9022286")).PN.	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2020/05/05 09:39 AM
L29	1	L28 and (respons$4 same nfc same generat$4)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/05/05 09:40 AM
L30	31288	(G06Q20/341 or G06Q20/4012 or G06Q20/3827 or G06Q20/346 or G06Q20/065 or G06Q20/409 or G06Q20/352 or G06Q20/24 or G06K19/07749 or G06K19/0716 or G06K19/06206 or G07F7/0873 or G06Q20/385 or G06Q20/347 or G06Q20/223 or G06Q20/06 or G07F19/00).cpc.	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/06/21 02:19 PM
L31	135	L30 and (nfc same	(US-PGPUB; USPAT;	OR	OFF	OFF	2020/06/21

		select$4 same payment same limit$4)	EPO; JPO)				02:19 PM
L32	112	L30 and (nfc same payment same limit$4 same approv$4)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/06/21 02:20 PM
L33	7	L30 and (nfc same payment same limit$4 same approv$4 same interface)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/06/21 02:20 PM
L34	10	L30 and (nfc same select$4 same payment same limit$4 same approv$4)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/06/21 02:28 PM
L35	36	(nfc same select$4 same payment same limit$4 same approv$4)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2020/06/21 02:29 PM
L36	6	(("10339520") or ("9760884") or ("9224083") or ("9022286")).PN.	(US-PGPUB; USPAT; USOCR; EPO; JPO)	OR	OFF	OFF	2020/06/21 02:30 PM
L37	51	"075637"	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/28 10:02 PM
L38	1	"10810579".pn.	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/28 10:03 PM
L39	35569	(G06Q20/341 or G06K19/07749 or G06Q20/347 or G06Q20/06 or G06Q20/409 or G06Q20/4012 or G06Q20/346 or G06Q20/3827 or G06K19/0716 or G07F19/00 or G06Q20/223 or G06Q20/24 or G06Q20/385 or G07F7/0873 or G06K19/06206 or G06Q20/065 or G06Q20/352).cpc.	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 06:36 AM
L40	6275	payment same transaction same (limit$4 tempora$6) same generat$4	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 06:39 AM
L41	1592	L39 and L40	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 06:39 AM
L42	862	L40 same issuer same account	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 06:40 AM
L43	265	L39 and L42	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 06:40 AM
L44	30	L42 same wireless$4	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 06:42 AM

L45	2	("8851370"|"9646301").PN.	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 07:07 AM
L46	31	("10013693" | "20060032908" | "20080223937" | "20100260388" | "20110140841" | "20130048712" | "20130124292" | "20130297509" | "20140052632" | "20140279555" | "20180240106" | "6631849" | "6641050" | "7128274" | "7202825" | "7360688" | "7784692" | "7793851" | "7841539" | "8577813" | "8639629" | "8702007" | "8768838" | "8856539" | "9022286" | "9100826" | "9224083" | "9430765" | "9530137" | "9536238" | "9760884").PN.	(US-PGPUB; USPAT; USOCR)	OR	OFF	OFF	2021/09/29 07:08 AM
L47	229	("7128274").URPN.	(USPAT)	OR	OFF	OFF	2021/09/29 07:16 AM
L48	369	("7793851").URPN.	(USPAT)	OR	OFF	OFF	2021/09/29 07:22 AM
L49	77	L40 and L48	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 07:22 AM
L50	47	L39 and L49	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 07:22 AM
L51	130	("2013/0159186").URPN.	(USPAT)	OR	OFF	OFF	2021/09/29 07:36 AM
L52	41	(nfc same select$4 same payment same limit$4 same approv$4)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 07:48 AM
L53	1218	(select$4 same payment same limit$4 same approv$4)	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 07:48 AM
L54	267	L39 and L53	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 07:48 AM
L55	346	L53 same generat$4	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 07:49 AM
L56	2785621	L55 sane dynamic$6	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 07:49 AM
L57	48	L55 same dynamic$6	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 07:50 AM
L58	11	L55 same static$4	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 07:51 AM
L59	543	("10043164" | "10075437" | "10129648" |	(US-PGPUB; USPAT; USOCR)	OR	OFF	OFF	2021/09/29 08:20 AM

		"10133979" | "10217105" | "20010010723" | "20010029485" | "20010034702" | "20010054003" | "20020078345" | "20020093530" | "20020100808" | "20020120583" | "20020152116" | "20020153424" | "20020165827" | "20030023554" | "20030034873" | "20030055727" | "20030078882" | "20030167350" | "20030208449" | "20040015958" | "20040039919" | "20040127256" | "20040215674" | "20040230799" | "20050044367" | "20050075985" | "20050081038" | "20050138387" | "20050156026" | "20050160049" | "20050195975" | "20050247797" | "20060006230" | "20060040726" | "20060041402" | "20060044153" | "20060047954" | "20060085848" | "20060136334" | "20060173985" | "20060174331" | "20060242698" | "20060280338" | "20070033642" | "20070055630" | "20070061266" | "20070061487" | "20070116292" | "20070118745" | "20070197261" | "20070224969" | "20070241182" | "20070256134" | "20070258594" | "20070278291" | "20080008315" | "20080011831" | "20080014867" |				

		"20080035738" | "20080071681" | "20080072303" | "20080086767" | "20080103968" | "20080109309" | "20080110983" | "20080120711" | "20080156873" | "20080162312" | "20080164308" | "20080207307" | "20080209543" | "20080223918" | "20080285746" | "20080308641" | "20090048026" | "20090132417" | "20090143104" | "20090171682" | "20090210308" | "20090235339" | "20090249077" | "20090282264" | "20100023449" | "20100023455" | "20100029202" | "20100030549" | "20100033310" | "20100036769" | "20100078471" | "20100082491" | "20100094754").PN. OR ("20100095130" | "20100100480" | "20100114731" | "20100192230" | "20100207742" | "20100211797" | "20100240413" | "20100257357" | "20100312634" | "20100312635" | "20110035604" | "20110060631" | "20110084132" | "20110101093" | "20110113245" | "20110125638" | "20110131415" | "20110153437" | "20110153496" | "20110208658" | "20110208965" | "20110211219" | "20110218911" | "20110238564" | "20110246780"				

		"20110258452" | "20110280406" | "20110282785" | "20110294418" | "20110312271" | "20120009946" | "20120024947" | "20120030047" | "20120030121" | "20120047071" | "20120079281" | "20120109735" | "20120143754" | "20120150737" | "20120178366" | "20120196583" | "20120207305" | "20120209773" | "20120238206" | "20120239560" | "20120252350" | "20120254394" | "20120284194" | "20120290472" | "20120296818" | "20120316992" | "20120317035" | "20120317628" | "20130005245" | "20130008956" | "20130026229" | "20130054474" | "20130065564" | "20130080228" | "20130080229" | "20130099587" | "20130104251" | "20130106576" | "20130119130" | "20130130614" | "20130144793" | "20130171929" | "20130179351" | "20130185772" | "20130191279" | "20130200999" | "20130216108" | "20130226791" | "20130226796" | "20130232082" | "20130238894" | "20130282360" | "20130303085" | "20130304651" | "20130312082" | "20130314593" | "20130344857" | "20140002238" |				

		"20140019352" | "20140027506" | "20140032409" | "20140032410" | "20140040120" | "20140040139" | "20140040147" | "20140047235" | "20140067690" | "20140074637").PN. OR ("20140074655" | "20140081720" | "20140095227" | "20140138435" | "20140171034" | "20140171039" | "20140172700" | "20140180851" | "20140208112" | "20140214674" | "20140229375" | "20140245391" | "20140256251" | "20140258099" | "20140258113" | "20140258125" | "20140274179" | "20140279479" | "20140337235" | "20140339315" | "20140346860" | "20140365780" | "20140379361" | "20150012444" | "20150032635" | "20150071486" | "20150088757" | "20150089586" | "20150134452" | "20150140960" | "20150154595" | "20150170138" | "20150178724" | "20150186871" | "20150205379" | "20150235211" | "20150302409" | "20150317626" | "20150332266" | "20150339474" | "20150371234" | "20160012465" | "20160026997" | "20160048913" | "20160055480" | "20160057619" | "20160065370" | "20160087957"				

		"20160092696" | "20160148193" | "20160232523" | "20160239672" | "20160253651" | "20160255072" | "20160267486" | "20160277383" | "20160277388" | "20160307187" | "20160307189" | "20160314472" | "20160330027" | "20160335531" | "20160379217" | "20170004502" | "20170011395" | "20170011406" | "20170017957" | "20170017964" | "20170024716" | "20170039566" | "20170041759" | "20170068950" | "20170103388" | "20170104739" | "20170109509" | "20170109730" | "20170116447" | "20170124568" | "20170140379" | "20170154328" | "20170154333" | "20170180134" | "20170221047" | "20170230189" | "20170237301" | "20170289127" | "20170295013" | "20170316696" | "20170317834" | "20170330173" | "20170374070" | "20180034507" | "20180039986").PN. OR ("20180068316" | "20180129945" | "20180160255" | "20180191501" | "20180205712" | "20180240106" | "20180254909" | "20180268132" | "20180270214" | "20180294959" | "20180300716" | "20180302396" | "20180315050"				

		"20180316666" | "20180322486" | "20180359100" | "20190014107" | "20190019375" | "20190036678" | "20190238517" | "4683553"	"4827113" | "4910773"	"5036461" | "5363448"	"5377270" | "5533126"	"5592553" | "5616901"	"5666415" | "5764789"	"5768373" | "5778072"	"5796827" | "5832090"	"5883810" | "5901874"	"5929413" | "5960411"	"6021203" | "6049328"	"6058373" | "6061666"	"6105013" | "6199114"	"6199762" | "6216227"	"6227447" | "6282522"	"6324271" | "6342844"	"6367011" | "6402028"	"6438550" | "6501847"	"6631197" | "6641050"	"6655585" | "6662020"	"6721706" | "6731778"	"6779115" | "6792533"	"6829711" | "6834271"	"6834795" | "6852031"	"6865547" | "6873260"	"6877656" | "6889198"	"6905411" | "6910627"	"6971031" | "6990588"	"7006986" | "7085931"	"7127605" | "7128274"	"7140550" | "7152045"	"7165727" | "7175076"	"7202773" | "7206806"	"7232073" | "7246752"	"7254569" | "7263507"	"7270276" | "7278025"	"7287692" | "7290709"	"7306143" | "7319986"	"7325132" | "7373515"	"7374099" | "7375616"	"7380710" | "7424977"	"7453439" | "7472829"	"7487357" | "7568631"	"7584153" | "7597250"	"7628322" | "7652578"	"7689832" | "7703142"	"7748609" | "7748617"	"7748636" | "7762457"	"7789302" | "7793851" | "7796013").PN. OR ("7801799"	"7801829"					

		| "7805755" | "7809643" | "7827115" | "7828214" | "7848746" | "7882553" | "7900048" | "7908216" | "7922082" | "7933589" | "7949559" | "7954716" | "7954723" | "7962369" | "7993197" | "8005426" | "8010405" | "8041954" | "8060012" | "8074877" | "8082450" | "8095113" | "8099332" | "8103249" | "8108687" | "8127143" | "8135648" | "8140010" | "8141136" | "8150321" | "8150767" | "8186602" | "8196131" | "8215563" | "8224753" | "8232879" | "8233841" | "8245292" | "8249654" | "8266451" | "8285329" | "8302872" | "8312519" | "8316237" | "8332272" | "8365988" | "8369960" | "8371501" | "8381307" | "8391719" | "8417231" | "8439271" | "8475367" | "8489112" | "8511542" | "8559872" | "8566916" | "8567670" | "8572386" | "8577810" | "8583454" | "8589335" | "8594730" | "8615468" | "8620218" | "8667285" | "8723941" | "8726405" | "8740073" | "8750514" | "8752189" | "8794509" | "8799668" | "8806592" | "8807440" | "8811892" | "8814039" | "8814052" | "8818867" | "8850538" | "8861733" | "8880027" | "8888002" | "8898088" | "8934837" | "8977569" | "8994498" | "9004365" | "9038894" | "9042814" | "9047531" | "9069976" | "9081948" | "9104853" | "9118663" | "9122964" | "9129280" | "9152832" | "9203800" | "9209867" | "9251330" | "9251518" | "9258715" | "9270337" | "9306626" | "9306942" | "9324066" | "9324067" | "9332587" | "9338622" | "9373141" | "9379841" | "9413430" | "9413768" | "9420496" | "9426132"				

		| "9432339" | "9455968" | "9473509" | "9491626" | "9553637" | "9619952" | "9635000").PN. OR ("9665858" | "9674705" | "9679286" | "9680942" | "9710804" | "9740342" | "9740988" | "9763097" | "9767329" | "9769662" | "9773151" | "9780953" | "9891823" | "9940571" | "9953323" | "9961194" | "9965756" | "9965911" | "9978058" | "RE42762").PN.					
L60	84	L40 same dynamic$6 same static$4	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 08:34 AM
L61	3	L60.clm.	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 08:34 AM
L62	417	("7580898").URPN.	(USPAT)	OR	OFF	OFF	2021/09/29 08:37 AM
L63	233	L39 and L62	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 08:38 AM
L64	87	L63 and nfc	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 08:39 AM
L65	160	L63 and online	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 08:39 AM
L66	62	L64 and L65	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2021/09/29 08:39 AM
L67	43	(Artificial Intelligence) Similar to: 17/528,073 with 0 CPC Selections and 0 Text Selections Text: (US-20210304187-A1 OR US-11176538-B2 OR US-20220207517-A1 OR US-20190325428-A1 OR US-10810579-B2 OR US-20220270077-A1 OR US-20210027276-A1 OR US-11328286-B2 OR US-10339520-B2 OR US-10628820-B2 OR US-20220318784-A1 OR US-20160148190-A1 OR US-20170132616-A1 OR US-9430765-B2 OR US-9760884-B2 OR US-10013693-B2 OR US-20190197520-A1 OR US-20150213351-	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN))	OR	ON	ON	2022/11/05 01:38 PM

		A1 OR US-20140263627-A1 OR US-20150213437-A1 OR US-9022286-B2 OR US-20180247300-A1 OR US-9224083-B2 OR US-10332101-B2 OR KR-102395069-B1 OR US-11341470-B1 OR US-20110240745-A1 OR US-10248949-B2 OR WO-2008035174-A3 OR US-20190188687-A1 OR US-5564486-A OR US-20210272091-A1 OR NL-2004464-B1 OR NL-2004464-A OR TW-200705350-A OR US-7328840-B2 OR US-10528941-B2 OR US-9830598-B2 OR WO-2006134545-A3 OR US-10984407-B2 OR US-20170109738-A1 OR US-20180005226-A1 OR US-8998096-B2 OR US-9183480-B1 OR US-20150186877-A1 OR GB-1446170-A OR WO-2018011630-A1 OR EP-3482366-A1 OR CN-111899412-A OR NL-2002671-C2).did.					
L68	35	"528073"	(US-PGPUB; USPAT; EPO; JPO)	OR	ON	ON	2022/11/05 01:45 PM
L69	39353	(G06Q20/341 OR G06K19/06206 OR G06K19/0716 OR G06K19/07749 OR G06Q20/06 OR G06Q20/065 OR G06Q20/223 OR G06Q20/24 OR G06Q20/346 OR G06Q20/347 OR G06Q20/352 OR G06Q20/3827 OR G06Q20/385 OR G06Q20/4012 OR G06Q20/409 OR G07F7/0873 OR G07F19/00).cpc.	(US-PGPUB; USPAT; EPO; JPO)	OR	ON	ON	2022/11/05 02:30 PM
L70	336	69 AND dynamic$6 SAME generat$4 SAME nfc	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2022/11/05 03:37 PM
L71	161	card SAME issu$4	(US-PGPUB; USPAT;	OR	OFF	OFF	2022/11/05

		SAME dynamic$6 SAME generat$4 SAME nfc	EPO; JPO)				03:38 PM
L72	66	69 AND 71	(US-PGPUB; USPAT; EPO; JPO)	OR	OFF	OFF	2022/11/05 03:38 PM
L73	38	(US-0044510-$ | US-0269005-$ | US-0275761-$ | US-0402811-$ | US-0423942-$ | US-0454728-$ | US-0460314-$ | US-0505277-$ | US-0516208-$ | US-0540647-$ | US-0546291-$ | US-0592893-$ | US-0680322-$ | US-0699266-$ | US-0713646-$ | US-0796299-$ | US-0803452-$ | US-0862718-$ | US-0902390-$ | US-0929851-$ | US-0990954-$ | US-0990959-$ | US-0998620-$ | US-1004075-$ | US-1017399-$ | US-1042855-$ | US-1061698-$ | US-10736322-$ | US-1074581-$ | US-1100431-$ | US-1107047-$ | US-1127010-$ | US-1129018-$ | US-11967211-$ | US-1227278-$ | US-1232339-$ | US-1321701-$ | US-17528073-$ | US-7528073-$ | US-9846866-$).DID.	(US-PGPUB; USPAT; EPO; JPO)	OR	ON	ON	2023/01/28 04:09 PM

PE2E SEARCH - Search History (Interference)

There are no Interference searches to show.

PE2E SEARCH - Search History (Similarity Search)

Ref #	Application Number	Text Selections	CPC Selections
L67	17/528,073	No selections	No selections

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (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.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	17528073
Filing Date	2021-11-16
First Named Inventor	David WYATT
Art Unit	2876
Examiner Name	LEE, SEUNG H.
Attorney Docket Number	WYAT-0002-13C12US

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	9600808		2017-03-21	Gomez, Sr.; William et al.	
	2	9098846		2015-08-04	Gill; Sara et al.	
	3	7690580		2010-04-06	Shoemaker; Austin William	
	4	8499334		2013-07-30	Doughty; Ralph O. et al.	
	5	11100431		2021-08-24	Mullen; Jeffrey D. et al.	
	6	8255323		2012-08-28	Casey; Brandon J et al.	
	7	8423462		2013-04-16	Amacker; Matthew W. et al.	
	8	10460314		2019-10-29	Hird; Geoffrey R. et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S. L./

IPR2025-01152
Apple EX1002 Page 1481

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	9	9846866		2017-12-19	Royyuru; Vijay	
	10	6736322		2004-05-18	Gobburu; Venkata T. et al.	
	11	7967211		2011-06-28	Challa; Nagesh et al.	
	12	8628012		2014-01-14	Wallner; George	
	13	8690059		2014-04-08	Wallner; George	
	14	8814046		2014-08-26	Wallner; George	
	15	9361613		2016-06-07	Wallner; George	
	16	9454679		2016-09-27	Wallner; George	
	17	9652642		2017-05-16	Wallner; George	
	18	9864994		2018-01-09	Huang; Enyang et al.	
	19	10044510		2018-08-07	Kwon; Eun Young et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S. L./

IPR2025-01152
Apple EX1002 Page 1482

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	17528073
Filing Date	2021-11-16
First Named Inventor	David WYATT
Art Unit	2876
Examiner Name	LEE, SEUNG H.
Attorney Docket Number	WYAT-0002-13C12US

	20	10269005		2019-04-23	Lee; Woo-Sup et al.	
	21	10275761		2019-04-30	Lee; Woo-Sup et al.	
	22	10402811		2019-09-03	Park; Yong Man et al.	
	23	10423942		2019-09-24	Lee; Woosup et al.	
	24	10454728		2019-10-22	Huang; Enyang	
	25	10505277		2019-12-10	Lee; Woosup et al.	
	26	10516208		2019-12-24	Lee; Woo-Sup et al.	
	27	10540647		2020-01-21	Park; Yong Man et al.	
	28	10546291		2020-01-28	Kim; Eun Jik et al.	
	29	10592893		2020-03-17	Lee; Hee-Dong et al.	
	30	10680322		2020-06-09	Lee; Woosup et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S. L./

IPR2025-01152
Apple EX1002 Page 1483

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	17528073
Filing Date	2021-11-16
First Named Inventor	David WYATT
Art Unit	2876
Examiner Name	LEE, SEUNG H.
Attorney Docket Number	WYAT-0002-13C12US

	31	10699266		2020-06-30	Lee; Hee-Dong et al.	
	32	10713646		2020-07-14	Lee; Hee-Dong et al.	
	33	10796299		2020-10-06	Lee; Woo-Sup et al.	
	34	10803452		2020-10-13	Kim; Eun Jik et al.	
	35	10862718		2020-12-08	Huang; Enyang	
	36	10902390		2021-01-26	Lee; Woosup et al.	
	37	10929851		2021-02-23	Kang; Minkoo et al.	
	38	10990954		2021-04-27	Park; Yong Man et al.	
	39	10990959		2021-04-27	Lee; Woo-Sup et al.	
	40	10998620		2021-05-04	Lee; Woosup et al.	
	41	11004075		2021-05-11	Lee; Je Min et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S. L./

IPR2025-01152
Apple EX1002 Page 1484

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	42	11017399		2021-05-25	Park; Yong Seok et al.	
	43	11042855		2021-06-22	Kim; Yu Hwan et al.	
	44	11061698		2021-07-13	Rhee; Injong et al.	
	45	11074581		2021-07-27	Kim; In Ho et al.	
	46	11107047		2021-08-31	Kim; Kibong et al.	
	47	11127010		2021-09-21	Cho; Boo Hyun et al.	
	48	11129018		2021-09-21	Kim; Ki Bong et al.	
	49	11227278		2022-01-18	Choi; Hoon et al.	
	50	11232339		2022-01-25	Lee; Woosup et al.	
	51	11321701		2022-05-03	Lee; Hee-Dong et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S. L./

IPR2025-01152
Apple EX1002 Page 1485

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17528073
Filing Date	2021-11-16
First Named Inventor	David WYATT
Art Unit	2876
Examiner Name	LEE, SEUNG H.
Attorney Docket Number	WYAT-0002-13C12US

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20130124410		2013-05-16	KAY; Christopher Erin et al.	
	2	20080319905		2008-12-25	CARLSON; Mark	
	3	20100185545		2010-07-22	Royyuru; Vijay K. et al.	
	4	20130262305		2013-10-03	Jones; Andrew R. et al.	
	5	20060089171		2006-04-27	Yoo; Kyung-Min et al.	
	6	20090048971		2009-02-19	Hathaway; Matthew et al.	
	7	20130232083		2013-09-05	SMITH; Theresa L. et al.	
	8	20080126260		2008-05-29	Cox; Mark A. et al.	
	9	20080222047		2008-09-11	Boalt; Adam	
	10	20080172317		2008-07-17	Deibert; Doug et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S. L./

IPR2025-01152
Apple EX1002 Page 1486

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	17528073
Filing Date	2021-11-16
First Named Inventor	David WYATT
Art Unit	2876
Examiner Name	LEE, SEUNG H.
Attorney Docket Number	WYAT-0002-13C12US

	11	20090159701		2009-06-25	Mullen; Jeffrey D. et al.	
	12	20120317035		2012-12-13	Royyuru; Vijay K. et al.	
	13	20130166441		2013-06-27	Kobylkin; Egor et al.	
	14	20120310760		2012-12-06	Phillips; Simon et al.	
	15	20080302876		2008-12-11	Mullen; Jeffrey D.	
	16	20110186626		2011-08-04	Manessis; Thomas et al.	
	17	20150147065		2015-05-28	Civelli; Jay Pierre et al.	
	18	20140143785		2014-05-22	Mistry; Pranav et al.	
	19	20050043997		2005-02-24	Sahota, Jagdeep Singh et al.	
	20	20150178724		2015-06-25	Ngo; Hao et al.	
	21	20160132881		2016-05-12	LEE; Yang-Soo et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S. L./

IPR2025-01152
Apple EX1002 Page 1487

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	22	20160253652		2016-09-01	JE; Seong-Min et al.	
	23	20160253657		2016-09-01	SOHN; Se Chang et al.	
	24	20190026725		2019-01-24	PARK; Yong Seok et al.	
	25	20190172051		2019-06-06	LEE; Hui Jae et al.	
	26	20190173290		2019-06-06	HA; Min Cheol et al.	
	27	20210311752		2021-10-07	Rhee; Injong et al.	
	28	20220005046		2022-01-06	KIM; Inho et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	2478712	GB		2011-09-21	JACKSON, DAVID		
	2	2485442	GB		2012-05-16	CUBIC CORP		

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S. H. L./

IPR2025-01152
Apple EX1002 Page 1488

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	3	00/62214	WO		2000-10-19	CLEARTOGO.COM et al.		
	4	01/57620	WO		2001-08-09	COMSENSE TECHNOLOGIES LTD et al.		
	5	2007145687	WO		2007-12-21	WEISS, KENNETH P.		
	6	2010043974	WO		2010-04-22	RICHARD, CHRISTIAN		
	7	2012154915	WO		2012-11-15	DYNAMICS INC et al.		
	8	2005119607	WO		2005-12-15	TYFONE INC et al.		

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/SEUNG H LEE/	Date Considered	01/28/2023

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17528073
Filing Date	2021-11-16
First Named Inventor	David WYATT
Art Unit	2876
Examiner Name	LEE, SEUNG H.
Attorney Docket Number	WYAT-0002-13C12US

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

IPR2025-01152
Apple EX1002 Page 1490

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.H.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17528073
Filing Date	2021-11-16
First Named Inventor	David WYATT
Art Unit	2876
Examiner Name	LEE, SEUNG H.
Attorney Docket Number	WYAT-0002-13C12US

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Jose S. Garcia/	Date (YYYY-MM-DD)	2023-01-12
Name/Print	Jose S. Garcia	Registration Number	43,628

This collection of information is required by 37 CFR 1.97 and 1.98. 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 1.14. This collection is estimated to take 1 hour 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. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

IPR2025-01152
Apple EX1002 Page 1491

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.S.G./

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 record s.

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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.T./

IPR2025-01152
Apple EX1002 Page 1492

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (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.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17528073
Filing Date	2021-11-16
First Named Inventor	David WYATT
Art Unit	2876
Examiner Name	LEE, SEUNG H.
Attorney Docket Number	WYAT-0002-13C12US

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.H.L./

IPR2025-01152
Apple EX1002 Page 1493

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	1	Motorola MotoACTV Smartwatch, http://www.manualplanet.com/pdf/watches/motorola/motorola-motoactv-gpsfitness-tracker-quick-start-guide.pdf, 2012, pp. 1-2.	
	2	PEREZ, "New NFC-Enabled Phones to Hit Europe," ReadWriteWeb, February 18, 2011, pp. 1-3.	
	3	WESTER, "New Samsung Galaxy S4 phone includes NFC, innovative barcode technology; New Samsung smartphone adds a number of features that may spur mobile payment adoption," Mobile Payments Today, March 15, 2013, Networld Media Group, pp. 1-2.	
	4	"NFC Focus: Which Smartphones Have NFC?," International Business Times News, August 9, 2012, pp. 1-3	
	5	"NFC for mobile operators; Maximizing opportunities in the mobile NFC marketplace," Gemalto, November 2009, pp. 1-2.	
	6	CATHELINAIS, "Nice, the first city to switch to contactless payment," 01net.com, May 21, 2010, pp. 1-6.	
	7	CLARK, "Orange to offer Samsung Wave 578 NFC across Europe - but not in the UK," NFC World, February 14, 2011, pp. 1-4.	
	8	CLARK, "Orange to roll out NFC services across Europe in 2011," NFC World, December 16, 2010, pp. 1-3.	
	9	"PayPal Credit Card Tokenization Extension - Magento Connect," Magento Extension Marketplace, http://www.magentocommerce.com/magentoconnect/catalog/product/view/id/18715/s/paypal-credit-card-tokenization-extension-4490/, October 5, 2013, page 1.	
	10	Nanninga, "PayPal Credit Card Tokenization in Magento," SitePoint, September 30, 2013, pp. 1-11.	
	11	"Payment Card Industry (PCI), Data Security Standard, PCI DSS Applicability in an EMV Environment, A Guidance Document, Version 1," PCI Security Standards Council, October 5, 2010, pp. 1-12.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.H.L./

IPR2025-01152
Apple EX1002 Page 1494

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	12	"Standard: PCI PIN Transaction Security Point of Interaction Security Requirements (PCI PTS POI), Version: 1.0, Information Supplement: ATM Security Guidelines," PCI Security Standards Council, January 2013, pp. 1-44.	
	13	"PayPal NVP API Developer Reference Enterprise Edition - eBay," August 28, 2012, pp. 1-382.	
	14	"Rambus' Bell ID to support Android Pay," Rambus, February 18, 2016, page 1.	
	15	"RIM implements Bell ID's Token Manager software for mobile payments," WMI Company News, January 23, 2013, World Market Intelligence Private Ltd., page 1.	
	16	LAI, "Samsung and Visa join forces to enable NFC mobile payment at 2012 Olympics," Engadget, April 1, 2011, pp. 1-6.	
	17	"Samsung and Visa Showcase Mobile Payments at the London 2012 Olympic and Paralympic Games," Business Wire, May 9, 2012, pp. 1-4.	
	18	WARREN, "Samsung and Visa Take NFC Mobile Payments Global," Mashable.com, February 25, 2013, pp. 1-2.	
	19	HASELTON, "Samsung and Visa team up for NFC mobile payments at London 2012 Olympics," Boy Genius Report, March 31, 2011, pp. 1-3.	
	20	"Samsung and Visa to Showcase Mobile Payments @ the London Olympics," Samsung Global Newsroom, May 9, 2012, pp. 1-3.	
	21	"Samsung Announces Launch Dates for Groundbreaking Mobile Payment Service: Samsung Pay," Samsung Global Newsroom, August 14, 2015, pp. 1-2.	
	22	GROTTA, "Samsung Begins to Phase Out Support of MST for Samsung Pay," PaymentsJournal, February 22, 2021, pp. 1-3.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	23	MURPH, "Samsung cooks up its own NFC module, destined for the Nexus S?," Engadget, December 1, 2010, pp. 1-2.	
	24	MOLEN, "Samsung Galaxy S III for Verizon Wireless review," Engadget, July 9, 2012, pp. 1-10.	
	25	TRENHOLM, "Samsung Galaxy S3 is Olympic phone for no-touch payments," CNET, May 9, 2012, pp. 1-2.	
	26	"Samsung Google Nexus S - Full Phone Specifications, Reviews: Royal droid," GSMArena.com (archive.org), November 2010, pp. 1-2.	
	27	"Samsung Google Nexus S review: Royal droid," GSMArena.com (archive.org), February 11, 2011, pp. 1-2.	
	28	"Samsung partners with FeliCa for Japanese NFC solutions, unveils 2012 Olympics' mobile payment app with Visa," Engadget, February 24, 2012, pp. 1-3.	
	29	CLARK, "Samsung picks NXP for S3," NFCW, May 14, 2012, pp. 1-2.	
	30	"SAMSUNG to Acquire LoopPay, Transformative Digital Wallet Platform," Samsung US Newsroom, February 18, 2015, pp. 1-2.	
	31	HEUN, "Samsung to Unveil NFC Smartwatch - Has Wrist-Payments' Time Come?," Payments Source, September 2, 2013, SourceMedia LLC d/b/a Arizent, pp. 1-2.	
	32	"Samsung's New Secu-NFC Chip Enables Secure Mobile Payment by Enhancing NFC with Security Features," Plus NEWS, November 30, 2011, pp. 1-2.	
	33	NANNINGA, "Save Credit Cards in Magento with Our New Paypal Extension," Classy Llama, August 15, 2013, pp. 1-4.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S. L./

IPR2025-01152
Apple EX1002 Page 1496

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	34	"Shift4 Releases New Technology to Insure the Security of Its Merchants' and Partners' Payment Processing," Hotel Online (archive.org), October 5, 2005, pp. 1-2.
	35	"S-Pay: What is MST?," Samsung Levant, September 22, 2020, pp. 1-2.

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/SEUNG H LEE/	Date Considered	01/28/2023

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17528073
Filing Date	2021-11-16
First Named Inventor	David WYATT
Art Unit	2876
Examiner Name	LEE, SEUNG H.
Attorney Docket Number	WYAT-0002-13C12US

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Jose S. Garcia/	Date (YYYY-MM-DD)	2023-01-12
Name/Print	Jose S. Garcia	Registration Number	43,628

This collection of information is required by 37 CFR 1.97 and 1.98. 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 1.14. This collection is estimated to take 1 hour 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. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

IPR2025-01152
Apple EX1002 Page 1498

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.S.G./

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 record s.

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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH.

IPR2025-01152
Apple EX1002 Page 1499

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (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.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17528073
Filing Date	2021-11-16
First Named Inventor	David WYATT
Art Unit	2876
Examiner Name	LEE, SEUNG H.
Attorney Docket Number	WYAT-0002-13C12US

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.H.L./

IPR2025-01152
Apple EX1002 Page 1500

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	1	Susan Pandy, "Securing Payments: Payments Tokenization in Primetime," Federal Reserve Bank of Boston Payments Symposium, January 20, 2016, pp. 1-20.	
	2	"SUMMARY OF ANS X9.119-Part 2 USE OF TOKENS TO PROTECT SENSITIVE CARD DATA," September 2017, pp.1-2.	
	3	Marianne Crowe et al., "Is Payment Tokenization Ready for Primetime?," June 11, 2015, pp. 1-51.	
	4	Terence Spies et al., "ANSI X9.119 Part 2: Using Tokenization Methods," 2013, pp. 1-20.	
	5	ASSORA et al., "A web transaction security scheme based on disposable credit card numbers," Int. J. Electronic Security and Digital Forensics, 2007, Vol. 1, No. 2, Inderscience Enterprises Ltd., pp. 146-155.	
	6	BOYD, "A pragmatic approach to temporary payment cards numbers," Int. J. Electronic Security and Digital Forensics, 2009, Vol. 2, No. 3, pp. 253-268.	
	7	BUCCAFURRI et al., "Implementing disposable credit card numbers by mobile phones," Electronic Commerce Research, Feb. 23, 2011, Vol. 11, Springer Publishing, pp. 271-296.	
	8	JAVANI et al., "A new credit card payment system based on 3D-Secure using one-time-use transaction numbers," Information Assurance and Security Letters, 2010, Vol. 1, Dynamic Publishers, Inc., USA, pp. 060-065.	
	9	KILLORAN et al., "A New Secure Wireless Financial Transaction Architecture," EUROCON 2005, November 22-24, 2005, IEEE, pp. 1060-1063.	
	10	LI et al., "A security-enhanced one-time payment scheme for credit card," Mar. 28-29, 2004, IEEE, pp. 1-11.	
	11	MJØLSNES et al., "On-Line E-Wallet System with Decentralized Credential Keepers," Mobile Networks and Applications, 2003, Vol. 8, Kluwer Academic Publishers, The Netherlands, pp. 87–99.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S. L./

IPR2025-01152
Apple EX1002 Page 1501

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	12	NARAYANASWAMI et al., "What Would You Do with a Hundred MIPS on Your Wrist?," RC 22057 (98634) January 22, 2001, IBM Research, pp. 1-10.	
	13	QASIM et al., "Interactive Shopping with Mobile Wallet," World Congress on Sustainable Technologies, 2012, IEEE, pp. 32-36.	
	14	HONIG, "A Week with Google Wallet," Endgadget, September 19, 2011, pp. 1-49.	
	15	KADAMBI et al.,"Near-Field Communication-Based Secure Mobile Payment Service," ICEC'09, August 12–15, 2009, pp. 1-11.	
	16	"A closer look at Google Pay and tokenization," Rambus Press, February 23, 2016, pp. 1-2.	
	17	GHAG et al., "A Comprehensive Study of Google Wallet as an NFC Application," International Journal of Computer Applications, November 2012, Vol. 58, No.16, pp. 37-42.	
	18	"Add any credit or debit card," Google Wallet Help (archive.org), 2012, page 1.	
	19	"Add any credit or signature debit card," Wallet Help, Google Wallet, September 20, 2012, page 1.	
	20	"Allynis Mobile NFC," Gemalto, September 2007, pp. 1-4.	
	21	"Allynis TSM for Transport," Gemalto, October 2009, pp. 1-2.	
	22	ADAMS, "Amex Plays a Major Role in Revamped Isis Mobile Wallet," Payments Source, November 15, 2013, Vol. 1, No. 1, SourceMedia LLC d/b/a Arizent, pp. 1-2.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S. L./

IPR2025-01152
Apple EX1002 Page 1502

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	23	PEREZ, "Android Pay, Google's Apple Pay Rival, Arrives Today," DigitalOcean, September 10, 2015, pp. 1-8.	
	24	HEISLER, "Apple Pay: An in-depth look at what's behind the secure payment system," Engadget, October 2, 2014, pp. 1-7.	
	25	FEHR, "Apple Pay: How different is it from other Pay solutions, what role does tokenisation play, and to what degree can Card not Present payment benefit from Apple Pay in future," Technical Report RHUL–ISG–2018–3, April 3, 2018, Egham, Surrey, UK, pp. 1-79.	
	26	"ATMIA publishes contactless ATM best practices," ATM Marketplace, September 27, 2012, pp. 1-2.	
	27	POPPER, "Banks Did It Apple's Way in Payments by Mobile," New York Times, September 11, 2014, pp. 1-2.	
	28	"Bell ID Simplifies EMV Smart Card and NFC Application Management with Versatile New Platform," eBanking & Payment News, May 5, 2011, page 1.	
	29	"BofA pursuing contactless ATM patent," Mobilepaymentstoday.com News, September 20, 2012, Newstex LLC, pp. 1-2.	
	30	"Chip Advisory #20, Visa Recommended Practices for EMV Chip Implementation in the U.S," July 11, 2012, pp. 1-10.	
	31	"Commbank, Mastercard and Samsung collaborate to launch NFC payment service," MarketLine NewsWire (Formerly Datamonitor), December 13, 2013, pp. 1-2.	
	32	"Contactless Payment: Secure Enough?," Card Technology, September 1, 2005, SourceMedia, Inc., Section: SPECIAL ISSUE: CONTACTLESS TECHNOLOGY, Vol. 10, No. 8, page 36.	
	33	"Eligible Devices," Google Wallet Help (archive.org), November 18, 2012, page 1.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S. L./

IPR2025-01152
Apple EX1002 Page 1503

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17528073
	Filing Date	2021-11-16
	First Named Inventor	David WYATT
	Art Unit	2876
	Examiner Name	LEE, SEUNG H.
	Attorney Docket Number	WYAT-0002-13C12US

	34	MOTT, "EMV and Mobile Payments, Questions abound, answers divide," Payments Summit Workshop, February 4, 2013, pp. 1-22.	
	35	"EMV Integrated Circuit Card Specifications for Payment Systems Book 2 Security and Key Management Version 4.1," May 2004, pp. 1-187.	
	36	"EMV Integrated Circuit Card Specifications for Payment Systems. Book 2, Security and Key Management, Version 4.3," November 2011, pp. 1-174.	
	37	"EMV Integrated Circuit Card Specifications for Payment Systems, Book 3, Application Specification, Version 4.3," November 2011, pp. 1-230.	

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/SEUNG H LEE/	Date Considered	01/28/2023

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.H.L./

IPR2025-01152
Apple EX1002 Page 1504

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17528073
Filing Date	2021-11-16
First Named Inventor	David WYATT
Art Unit	2876
Examiner Name	LEE, SEUNG H.
Attorney Docket Number	WYAT-0002-13C12US

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Jose S. Garcia/	Date (YYYY-MM-DD)	2023-01-12
Name/Print	Jose S. Garcia	Registration Number	43,628

This collection of information is required by 37 CFR 1.97 and 1.98. 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 1.14. This collection is estimated to take 1 hour 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. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

IPR2025-01152
Apple EX1002 Page 1505

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.S.G./

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 record s.

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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH.

IPR2025-01152
Apple EX1002 Page 1506

UNITED STATES
PATENT AND TRADEMARK OFFICE

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

ACKNOWLEDGEMENT OF CHANGE TO SMALL ENTITY STATUS

APPLICATION #	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET #	REQUEST ID
17/528,073	11/16/2021	David WYATT	WYAT-0002-USD1C1C1C1C1C	64260

The entity status change request below filed through Patent Center on 02/13/2023 has been accepted.

Certifications

APPLICANT ASSERTING SMALL ENTITY STATUS. See 37CFR 1.27.

Signature

I certify, in accordance with 37 CFR 1.4(d)(4), that I am one of the signatories making the entity status change.

Signature	Name	Registration #
/Jose S. Garcia/	Jose Garcia	43628

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
17/528,073	11/16/2021	2876	3750	WYAT-0002-USD1C1C1C1C1C	14	2

CONFIRMATION NO. 4809

CORRECTED FILING RECEIPT

136197
David Wyatt c/o Murabito, Hao & Barnes
111 North Market Street
Suite 700
San Jose, CA 95113

OC000000137392572

Date Mailed: 02/14/2023

Receipt is acknowledged of this non-provisional utility patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF FIRST INVENTOR, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection.

Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a corrected Filing Receipt, including a properly marked-up ADS showing the changes with strike-through for deletions and underlining for additions. If you received a "Notice to File Missing Parts" or other Notice requiring a response for this application, please submit any request for correction to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections provided that the request is grantable.

Inventor(s)

David WYATT, Austin, TX;

Applicant(s)

CARDWARE, INC, Austin, TX;

Power of Attorney: The patent practitioners associated with Customer Number 136197

Domestic Priority data as claimed by applicant

This application is a CON of 17/075,637 10/20/2020 PAT 11176538
which is a CON of 16/459,150 07/01/2019 PAT 10810579
which is a CON of 15/701,261 09/11/2017 PAT 10339520
which is a CON of 14/981,757 12/28/2015 PAT 9760884
which is a CON of 14/680,979 04/07/2015 PAT 9224083
which is a DIV of 14/217,261 03/17/2014 PAT 9022286
which claims benefit of 61/794,891 03/15/2013

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

IPR2025-01152
Apple EX1002 Page 1508

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 11/30/2021
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 17/528,073**
Projected Publication Date: Not Applicable
Non-Publication Request: No
Early Publication Request: No
Title

MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

Preliminary Class

235

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific

IPR2025-01152
Apple EX1002 Page 1509

countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop

IPR2025-01152
Apple EX1002 Page 1510

technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

IPR2025-01152
Apple EX1002 Page 1511

PART B – FEE(S) TRANSMITTAL

Complete and send this form, together with the applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

By fax, send to: (571) 273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

David Wyatt c/o Murabito, Hao & Barnes LLP
111 North Market Steet
Suite 700
San Jose, CA 95113

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

Mina Oliveri	(Typed or printed name)
/Mina Oliveri/	(Signature)
2-14-2023	(Date)

APPLICATION NO	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO	CONFIRMATION NO
17/528,073	11/16/2021	David Wyatt	WYAT-0002.USD1C1C1C1C1C	4809

TITLE OF INVENTION: MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0.00	$0.00	$480	05/15/2023

EXAMINER	ART UNIT	CLASS-SUBCLASS

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363)

☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-09 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) The names of up to 3 registered patent attorneys or agents OR, alternatively, 1.

(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed. 2. 3.

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: CARDWARE, INC.

(B) RESIDENCE: (CITY and STATE or COUNTRY): AUSTIN, TEXAS

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☐ Corporation or other private group entity ☐ Government

4a. Fees Submitted: ☑ Issue Fee ☐ Publication Fee (if required) ☐ Advance Order - # of Copies _____

4b. Method of Payment (*Please first reapply any previously paid fee shown above*):

☑ Electronic Payment via EFS-Web ☐ Enclosed check ☐ Non-electronic payment by credit card (Attach form PTO-2038)

☑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. 504160

5. Change of Entity Status (from status indicated above)

☐ Applicant certifying micro entity status. See 37 CFR 1.29. NOTE: Absent a valid Certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

☐ Applicant asserting small entity status. See 37 CFR 1.27. NOTE: If the application was previously under micro entity status, checking this box will be taken as a notification of loss of entitlement to micro entity status.

☐ Applicant changing to regular undiscounted fee status. NOTE: Checking this box will be taken as a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature /Anthony C. Murabito/ Date 2-14-2023

Typed or printed name Anthony C. Murabito Registration No. 35,295

IPR2025-01152
Apple EX1002 Page 1512

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. 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 1.14. This collection is estimated to take 30 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, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

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 disclosure of these records is required by the Freedom of Information Act.
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 inspection 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.

Electronic Patent Application Fee Transmittal

Application Number:	17528073
Filing Date:	16-Nov-2021
Title of Invention:	MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE
First Named Inventor/Applicant Name:	David WYATT
Filer:	Anthony C. Murabito/Mina Oliveri
Attorney Docket Number:	WYAT-0002-13C12US

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
UTILITY APPL ISSUE FEE	2501	1	480	480

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**480**

Electronic Acknowledgement Receipt

EFS ID:	47531835
Application Number:	17528073
International Application Number:	
Confirmation Number:	4809
Title of Invention:	MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE
First Named Inventor/Applicant Name:	David WYATT
Customer Number:	136197
Filer:	Anthony C. Murabito/Mina Oliveri
Filer Authorized By:	Anthony C. Murabito
Attorney Docket Number:	WYAT-0002-13C12US
Receipt Date:	14-FEB-2023
Filing Date:	16-NOV-2021
Time Stamp:	15:28:05
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	EFT
Payment was successfully received in RAM	$480
RAM confirmation Number	E20232DF29188730
Deposit Account	504160
Authorized User	Mina Oliveri

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

37 CFR 1.17 (Patent application and reexamination processing fees)

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	WYAT-0002-USD1C1C1C1C1C_IssueFee_Tran_2-14-2023.pdf	296037 42f56887661a1a626d828d80618bf2d84b591e2e	no	2
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	38083 9be0bc43f8aeafb866a9db489893a13bcfeb6807	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	334120		

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 a 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

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/528,073	04/04/2023	11620634	WYAT-0002-13C12US	4809

136197 7590 03/15/2023

David Wyatt c/o Murabito, Hao & Barnes
111 North Market Street
Suite 700
San Jose, CA 95113

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 0 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Patents Stakeholder Experience (OPSE), Stakeholder Support Division (SSD) at (571)-272-4200.

INVENTOR(s) (Please see PAIR WEB site http://pair.uspto.gov for additional inventors):

David WYATT, Austin, TX;

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

CARDWARE, INC, Austin, TX;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

UNITED STATES
PATENT AND TRADEMARK OFFICE

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

ACKNOWLEDGEMENT OF LOSS OF ENTITLEMENT TO ENTITY STATUS DISCOUNT

APPLICATION #	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET #	REQUEST ID
17/528,073	11/16/2021	David WYATT	WYAT-0002-13C12US	267402

The entity status change request below filed through Patent Center on 08/29/2024 has been accepted.

Certifications

APPLICANT CHANGING TO REGULAR UNDISCOUNTED FEE STATUS

Signature

I certify, in accordance with 37 CFR 1.4(d)(4), that I am one of the signatories making the entity status change.

Signature	Name	Registration #
/Anthony C. Murabito/	Anthony Murabito	35295

AO 120 (Rev. 08/10)

TO:	Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas, Marshall Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:23-CV-00187	4/24/2023	Eastern District of Texas, Marshall Division

PLAINTIFF	DEFENDANT
CardWare Inc.	Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	11,620,634	4/4/2023	CARDWARE INC.
2			
3			
4			
5			

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director **Copy 3—Upon termination of action, mail this copy to Director**
Copy 2—Upon filing document adding patent(s), mail this copy to Director **Copy 4—Case file copy**

Print Save As...