Doc Code: TRACK1.REQ
Document Description: TrackOne Request

PTO/AIA/424 (03-14)

CERTIFICATION AND REQUEST FOR PRIORITIZED EXAMINATION UNDER 37 CFR 1.102(e) (Page 1 of 1)

First Named Inventor:	Dr. Paresh K. Patel	Nonprovisional Application Number (if known):	
Title of Invention:	METHOD AND SYSTEM FOR PERFORMING MOBILE DEVICE-TO-MACHINE PAYMENTS		

APPLICANT HEREBY CERTIFIES THE FOLLOWING AND REQUESTS PRIORITIZED EXAMINATION FOR THE ABOVE-IDENTIFIED APPLICATION.

1. The processing fee set forth in 37 CFR 1.17(i)(1), the prioritized examination fee set forth in 37 CFR 1.17(c), and if not already paid, the publication fee set forth in 37 CFR 1.18(d) have been filed with the request. The basic filing fee, search fee, and examination fee are filed with the request or have been already been paid. I understand that any required excess claims fees or application size fee must be paid for the application.

2. I understand that the application may not contain, or be amended to contain, more than four independent claims, more than thirty total claims, or any multiple dependent claims.

3. The applicable box is checked below:

I. ☑ Original Application (Track One) - Prioritized Examination under § 1.102(e)(1)

i. (a) The application is an original nonprovisional utility application filed under 35 U.S.C. 111(a). This certification and request is being filed with the utility application via EFS-Web.

---OR---

(b) The application is an original nonprovisional plant application filed under 35 U.S.C. 111(a). This certification and request is being filed with the plant application in paper.

ii. An executed inventor's oath or declaration under 37 CFR 1.63 or 37 CFR 1.64 for each inventor, **or** the application data sheet meeting the conditions specified in 37 CFR 1.53(f)(3)(i) is filed with the application.

II. ☐ Request for Continued Examination - Prioritized Examination under § 1.102(e)(2)

i. A request for continued examination has been filed with, or prior to, this form.
ii. If the application is a utility application, this certification and request is being filed via EFS-Web.
iii. The application is an original nonprovisional utility application filed under 35 U.S.C. 111(a), or is a national stage entry under 35 U.S.C. 371.
iv. This certification and request is being filed prior to the mailing of a first Office action responsive to the request for continued examination.
v. No prior request for continued examination has been granted prioritized examination status under 37 CFR 1.102(e)(2).

Signature	Date July 18, 2014
Name (Print/Typed) Douglas J. Crisman	Practitioner Registration Number 39,951

Note: *This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. Submit multiple forms if more than one signature is required.**

☑ *Total of _____ forms are submitted.

PayRange EXHIBIT - 2005 (Part 1)
KioSoft Technologies, LLC and Techtrex, Inc. v. PayRange Inc.
PGR2023-00045

METHOD AND SYSTEM FOR PERFORMING MOBILE DEVICE-TO-MACHINE PAYMENTS

PRIORITY CLAIM

[0001] The present application is a continuation of U.S. Patent Application Number 14/214,644, filed March 14, 2014, which claims priority to U.S. Provisional Patent Application Number 61/917,936, filed December 18, 2013, and is a continuation-in-part of U.S. Design Patent Application Number 29/477,025, filed December 18, 2013. The present application is based on and claims priority from these applications, the disclosures of which are hereby expressly incorporated herein by reference.

BACKGROUND OF THE INVENTION

[0002] Disclosed herein are mobile-device-to-machine payment systems and, more specifically, mobile-device-to-machine payment systems over a non-persistent network connection and featuring hands-free and manual modes.

[0003] Vending machines (or "automatic retailing" machines), in the broadest sense, have been around for thousands of years. The first simple mechanical coin operated vending machines were introduced in the 1880s. Modern vending machines stock many different types of products including, but not limited to drinks (e.g. water, juice, coffee, and soda) and edible food products/items (e.g. snacks, candy, fruit, and frozen meals), as well as a wide variety of non-food items. In this fast paced world, vending machines are ubiquitous.

[0004] Vending machines are one type of "payment accepting unit" (payment accepting units are also referred to herein generically as "machines"). A payment accepting unit (or machine) is equipment that requires payment for the dispensing of products and/or services. In addition to vending machines, payment accepting units can also be other machines that require payment for the dispensing of a product and/or services including, but not limited to parking meters, toll booths, laundromat washers and dryers, arcade games, kiosks, photo booths, toll booths, transit ticket dispensing machines, and other known or yet to be discovered payment accepting units.

[0005] In using a payment accepting unit, a user will (1) approach the payment accepting unit, (2) determine from the face of the payment accepting unit the product (or service) he desires, (3) insert payment (e.g. coins, bills, or payment cards), and (4) input his

selection into the payment accepting unit using a user interface (e.g. a series of buttons, a key pad, touch screen, or other input mechanism using, for example, the column and row at which a product is located). Based on the user's inputted selection, technology within the payment accepting unit provides the desired product (or service) to the user.

[0006] As the number of people with internet-connected mobile devices proliferates, so does the variety of uses for such devices. Mobile payment is a logical extension.

[0007] There is a large development effort around bringing mobile payment to the retail sector in an effort to not only provide options to the user, but also increased convenience.

[0008] In recent years, many improvements to modern vending machines have been suggested. Many of the innovations relate to means for communicating with the vending machine. Some of these communication innovations are detailed in U.S. Patent No. 6,584,309 to Whigham (the "Whigham reference"), U.S. Patent No. 7,085,556 to Offer (the "Offer reference"), U.S. Patent No. 7,127,236 to Khan et al. (the "Khan reference"), U.S. Patent No. 7,721,958 to Belfer et al. (the "Belfer reference"), U.S. Patent No. 8,396,589 to Katzenstein Garibaldi et al. (the "Garibaldi reference"), U.S. Patent No. 8,489,140 to Weiner et al. (the "Weiner reference"), and International Publication No. WO/2008/083025 to Carlson (the "Carlson reference").

[0009] The Whigham reference is directed to a system and method for purchasing a product from an automatic vending machine by means of a consumer's cellular telephone. The consumer requests a product available from the vending machine by dialing a specified telephone number that connects the consumer's cellular telephone to a server operated by a billing agency. The server recognizes the request for the product, creates a transaction record, and communicates a vend code to the consumer. Upon receiving the vend code from the server, the consumer transmits the vend code to the vending machine. The vend code may be an RF code, an audible tone code, or a manual code. Upon receipt of the vend code from the consumer, the vending machine dispenses the requested product.

[0010] The Offer reference is directed to a vending machine that is designed to communicate with a cellular phone such that it dispenses a product when it receives information indicating that the product has been selected. The Offer reference teaches permitting the cashless utilization of a vending machines via a communications service, such as a cellular telephone. A response to a signal from the cellular telephone from

[0011] the vending machine that indicates that a connection has been established between the vending machine and the cellular phone may be a visual indication that is displayed on the cellular telephone. The vending machine outputs the cost of the product and that cost is debited from an account to pay for the product.

[0012] The Khan reference describes a point of sale MicroAdapter device that enables payment transactions to be effected through a purchaser's personal trusted device (e.g. the user selecting the micropayment application on his personal trusted device and confirming or cancelling the purchase thereon) without relying upon tokens or prepayment cards. In one embodiment, the MicroAdapter includes a transceiver configured to receive a purchase signal from the personal trusted device including order and payment information. In response, the MicroAdapter communicates via wireless telephony with a transaction authorizer to receive authorization for effectuating the purchase transaction. The MicroAdapter can effectuate micropayment transactions authorized by a Billing On Behalf of Others program administered through a wireless carrier/ISP or third party.

[0013] The Belfer reference is directed to a system wherein a vending machine has an audio code collector and a code validator that is adapted to receive audio tones from a mobile device. The audio tones include authentication codes and dispense codes to control dispensing of product from the vending machine. To start the transaction, the consumer dials a unique set of symbols and digits to route the call to a verification server. The symbols and digits may correspond to a unique vending machine identification number and product identification numbers.

[0014] The Garibaldi reference is directed to an electronic device for the sale of intangible products through vending machines that include interfaces to communicate with external peripherals through the MDB protocol, the RS232 standard, and the DEX protocol, an interface to communicate with users, a communications system that enables it to act as part of a network and communicate with a central system, and a controller, that articulates the communication among the above-mentioned components, so as to enable a central system to perform diverse actions on a vending machine.

[0015] The Weiner reference is directed to a system and method for providing product or service with a cellular telephone. The problem identified in the Weiner reference is that mobile communication devices are long-range electronic devices designed to be used for long-range communications. Eschewing the use of near- field communication because it

requires special design or modification of the mobile station (e.g. the vending machine), the Weiner reference teaches a mobile communication device identifier, consisting of: a shielding defining a coverage area, the shielding arranged to reduce radio signals originating externally of the coverage area to be less than a pre-determined signal strength; an antenna associated within the defined coverage area; a transceiver coupled to the antenna, the transceiver communicating with a mobile station inserted within the defined coverage area utilizing a signal strength greater than the pre-determined signal strength; and a service control unit responsive to the transceiver, the service control unit responsive to the communication to output a signal indicative of an authorization to provide a product or service.

[0016] The Carlson reference is directed to a system and a method for using a portable consumer device such as a mobile phone for payments and the like. One embodiment of the Carlson system is directed to a method that includes the steps of receiving a payment request message (that includes a request to pay for a product from a vending machine) from a portable consumer device operated by a consumer, sending an authorization response message back to the vending machine wherein the vending machine subsequently prompts the consumer to enter a selection if the authorization response message indicates that the consumer is authorized to make a purchase, and receiving an acknowledgement message from the vending machine that the product was purchased. The step of "sending an authorization response message back to the vending machine" is performed by a remote payment server and would require a persistent network connection.

BRIEF SUMMARY OF THE INVENTION

[0017] Disclosed herein are mobile-device-to-machine payment systems and, more specifically, mobile-device-to-machine payment systems over a non-persistent network connection and featuring hands-free and manual modes.

[0018] Described herein is a mobile-device-to-machine payment system for facilitating a cashless transaction for purchase of at least one product or service by a user from a payment accepting unit that preferably has input mechanisms. The user has a mobile device that has both short-range communication technology and long-range communication technology. The payment accepting unit is capable of dispensing at least one product or service. The system includes an adapter module and a server. The adapter module is associated with the payment accepting unit and has short-range communication technology

for communicating with the short-range communication technology of the mobile device. The server has long-range communication technology for communicating with the long-range communication technology of the mobile device. The adapter module is for sending an authorization request for funds to the mobile device using short-range communication technology. The mobile device then forwards the authorization request for funds to the server using long-range communication technology. The server is for sending an authorization grant for funds to the mobile device using long-range communication technology. The mobile device the forwards the authorization grant for funds to the adapter module using short-range communication technology. The payment accepting unit dispenses the at least one product or service in response to receiving user input to the payment accepting unit input mechanism if the adapter module has received the authorization grant.

[0019] The adapter module may have security technology and the server may have security technology. The authorization request may be secured by the adapter module security technology to create a secured authorization request. The authorization grant may be secured by the server security technology to create a secured authorization grant. The secured authorization request and the secured authorization grant are preferably undecipherable to the mobile device.

[0020] The adapter module and the server may share a unique private key. The adapter module may have encryption/decryption technology and the server may have encryption/decryption technology. The authorization request may be encrypted by the adapter module encryption/decryption technology using the unique private key to create an encrypted authorization request. The encrypted authorization request may be decrypted by the server encryption/decryption technology using the unique private key. The authorization grant may be encrypted by the server encryption/decryption technology using the unique private key to create an encrypted authorization grant. The encrypted authorization grant may be decrypted by the adapter module encryption/decryption technology using the unique private key. The encrypted authorization request and the encrypted authorization grant are preferably undecipherable to the mobile device.

[0021] The adapter module is preferably surrounded by two zones, a payment zone and an authorization zone, wherein the payment zone is within the authorization zone. The adapter module sends the authorization request when the mobile device is within the authorization zone. The mobile device forwards the authorization grant for funds to the adapter module when the mobile device is within the payment zone. A third zone possible

zone is a communication zone, the authorization zone being within the communication zone. The mobile device preferably receives advertising broadcast signals from the adapter module within the communication zone.

[0022] The system may have a hands-free mode in which the payment accepting unit dispenses the at least one product or service without the user interacting with the mobile device. A display of the payment accepting unit may be used for displaying funds available based on information from the authorization grant. The input mechanisms of the payment accepting unit may be used for receiving user selection input when the user interacts with the input mechanisms to select the at least one product or service to be dispensed.

[0023] The adapter module may be an in-line dongle for in-line insertion within a multi-drop bus of the payment accepting unit. Further, the payment accepting unit may have a multi-drop bus to a payment receiving mechanism. The multi-drop bus may have a male adapter and a female adapter. The adapter module may have a male adapter and a female adapter. The adapter module is preferably insertable in serial with the multi-drop bus by connecting the male adapter of the adapter module to the female adapter of the multi-drop bus and by connecting the female adapter of the adapter module to the male adapter of the multi-drop bus.

[0024] Also described herein is a method for using a mobile-device-to-machine payment system for facilitating a cashless transaction for purchase of at least one product or service by a user from a payment accepting unit may have input mechanisms. The user may have a mobile device having both short-range communication technology and long-range communication technology. The payment accepting unit is preferably capable of dispensing at least one product or service. The method includes the steps of: (a) sending an authorization request for funds to the mobile device using short-range communication technology of an adapter module associated with the payment accepting unit; (b) receiving the authorization request for funds from the short-range communication technology of the adapter module at the short-range communication technology of the mobile device; (c) forwarding the authorization request for funds to a server using the long-range communication technology of the mobile device; (d) receiving the authorization request for funds from the long-range communication technology of the mobile device at long-range communication technology of the server; (e) sending an authorization grant for funds to the mobile device using the long-range communication technology of the server; (f) receiving the authorization grant for funds from long-range communication technology of the server at the

long-range communication technology of the mobile device; (g) forwarding the authorization grant for funds to the adapter module using the short-range communication technology of the mobile device; and (h) receiving the authorization grant for funds from the short-range communication technology of the mobile device at short-range communication technology of the adapter module. At least one product or service may then be dispensed from the payment accepting unit in response to receiving user input to the payment accepting unit input mechanism if the adapter module has received the authorization grant.

[0025] The method may include the steps of securing the authorization request using security technology associated with the adapter module to create a secured authorization request, securing the authorization grant using security technology associated with the server to create a secured authorization grant, and the secured authorization request and the secured authorization grant are preferably undecipherable to the mobile device.

[0026] The method may include the steps of (a) sharing a unique private key between the adapter module and the server, (b) encrypting using the unique private key the authorization request using encryption/decryption technology associated with the adapter module to create an encrypted authorization request, (c) decrypting using the unique private key the encrypted authorization request using encryption/decryption technology associated with the server, (d) encrypting using the unique private key the authorization grant using the encryption/decryption technology associated with the server to create an encrypted authorization grant, (e) decrypting using the unique private key the encrypted authorization grant using encryption/decryption technology associated with the adapter module, and (e) the encrypted authorization request and the encrypted authorization grant are preferably undecipherable to the mobile device.

[0027] The method may include the steps of (a) surrounding the adapter module with two zones, a payment zone and an authorization zone, wherein the payment zone is within the authorization zone, (b) the adapter module sending the authorization request when the mobile device is within the authorization zone; and (c) the mobile device forwarding the authorization grant for funds to the adapter module when the mobile device is within the payment zone. The adapter module may also include a third zone, a communication zone, wherein the authorization zone is within the communication zone. The mobile device receives advertising broadcast signals from the adapter module within the communication zone.

[0028] The method may have a hands-free mode in which the payment accepting unit dispenses the at least one product or service without the user interacting with the mobile device. The method may further include the steps of (a) displaying funds available on a display of the payment accepting unit, the funds available may be based on information from the authorization grant; and (b) receiving user selection input when the user interacts with input mechanisms of the payment accepting unit to select the at least one product or service to be dispensed.

[0029] The method may include the step of inserting the adapter module as an in-line dongle for in-line insertion within a multi-drop bus of the payment accepting unit. The method may include the step of inserting the adapter module in serial with the multi-drop bus by connecting a male adapter of the adapter module to a female adapter of the multi-drop bus and by connecting a female adapter of the adapter module to a male adapter of the multi-drop bus.

[0030] The subject matter described herein is particularly pointed out and distinctly claimed in the concluding portion of this specification. Objectives, features, combinations, and advantages described and implied herein will be more readily understood upon consideration of the following detailed description of the invention, taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

[0031] FIG. 1 is a schematic diagram that shows three zones: a first "communication zone" (e.g. "Bluetooth range"), a second "authorization zone," and a third "payment zone." The payment zone (that can't be zero) is smaller than or equal to (overlapping completely) the authorization zone.

[0032] FIG. 2 is a schematic diagram that shows the three zone of FIG. 1 with multiple users therein, the mobile-device-to-machine payment systems providing for managing and resolving multiple users.

[0033] FIG. 3 is a table that illustrates the hands-free credit or alert user principle.

[0034] FIG. 4 is a flow chart showing the logging RSSI at User Input.

[0035] FIG. 5 is a block schematic that shows elements of the system including, but not limited to, the adapter module, the machine, the mobile device, and exemplary servers, as well as communications therebetween.

[0036] FIG. 6 is a block schematic that shows there are three areas of encryption used (each is bi-directional) between the adapter module, the machine, the mobile device, and/or exemplary servers.

[0037] FIG. 7 is a block diagram that communications, messaging, vending sequence, and purchase flow between the adapter module, the mobile device, and a system management server.

[0038] FIG. 8A is a timing schematic diagram that shows additional elements and features of the system including, but not limited to, communications medium, messaging, vending sequence, and purchase flow, when the user enters the communication zone (Bluetooth Range).

[0039] FIG. 8B is a timing schematic diagram that shows additional elements and features of the system including, but not limited to, communications medium, messaging, vending sequence, and purchase flow, when the user enters the Authorization Zone.

[0040] FIG. 8C is a timing schematic diagram that shows additional elements and features of the system including, but not limited to, communications medium, messaging, vending sequence, and purchase flow, when the user enters the Payment Zone and, in particular, detailing the hands-free mode alternative and the swipe mode alternative.

[0041] FIG. 8D is a timing schematic diagram that shows additional elements and features of the system including, but not limited to, communications medium, messaging, vending sequence, and purchase flow, in a vending transaction including a loop for multiple transactions.

[0042] FIG. 8E is a timing schematic diagram that shows additional elements and features of the system including, but not limited to, communications medium, messaging, vending sequence, and purchase flow, in the Login mode.

[0043] FIG. 8F is a timing schematic diagram that shows additional elements and features of the system including, but not limited to, communications medium, messaging, vending sequence, and purchase flow, during Module bootup.

[0044] FIG. 8G is a timing schematic diagram that shows additional elements and features of the system including, but not limited to, communications medium, messaging, vending sequence, and purchase flow, during Account Check/Update.

[0045] FIGS. 9A - 9E are flow charts that show exemplary steps and features of the system including, but not limited to, communications, messaging, vending sequence, and purchase flow.

[0046] FIGS. 10A - 10D show an exemplary mobile device with a graphical representation of an exemplary mobile application shown thereon, the mobile application being used as part of the mobile-device-to-machine payment systems.

[0047] FIG. 11 is a perspective view of the exemplary first preferred in-line dongle adapter module.

[0048] FIG. 12 is a front plan view of the in-line dongle adapter module of FIG. 11.

[0049] FIG. 13 is a back plan view of the in-line dongle adapter module of FIG. 11.

[0050] FIG. 15 is a first end view of a connector receptacle of the in-line dongle adapter module of FIG. 11.

[0051] FIG. 16 is a second end view of a connector receptacle of the in-line dongle adapter module of FIG 11.

[0052] FIG. 17 is a perspective view taken from the first end of the in-line dongle adapter module of FIG. 11, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for environmental purposes.

[0053] FIG. 18 is a perspective view taken from the second end of the in-line dongle adapter module of FIG. 11, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for environmental purposes.

[0054] FIG. 19 is a perspective view of the in-line dongle adapter module of FIG. 11 within a vending machine.

[0055] FIG. 20 is a perspective view of the exemplary second preferred in-line dongle adapter module.

[0056] FIG. 21 is a front plan view of the in-line dongle adapter module of FIG. 20.

[0057] FIG. 22 is a back plan view of the in-line dongle adapter module of FIG. 20.

[0058] FIG. 23 is a first side view of the in-line dongle adapter module of FIG. 20, the second side being a mirror image of that shown.

[0059] FIG. 24 is a first end view of a connector receptacle of the in-line dongle adapter module of FIG. 20.

[0060] FIG. 25 is a second end view of a connector receptacle of the in-line dongle adapter module of FIG 20.

[0061] FIG. 26 is a perspective view taken from the first end of the in-line dongle adapter module of FIG. 20, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for environmental purposes.

[0062] FIG. 27 is a perspective view taken from the second end of the in-line dongle adapter module of FIG. 20, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for environmental purposes.

[0063] FIG. 28 is a perspective view of the in-line dongle adapter module of FIG. 20 within a vending machine.

[0064] FIG. 29 is a perspective view of the exemplary third preferred in-line dongle adapter module with a gap indicating the in-line dongle adapter module can be of any length.

[0065] FIG. 30 is a front plan view of the in-line dongle adapter module of FIG. 29.

[0066] FIG. 31 is a back plan view of the in-line dongle adapter module of FIG. 29.

[0067] FIG. 32 is a first side view of the in-line dongle adapter module of FIG. 29, the second side being a mirror image of that shown.

[0068] FIG. 33 is a first end view of a connector receptacle of the in-line dongle adapter module of FIG. 29.

[0069] FIG. 34 is a second end view of a connector receptacle of the in-line dongle adapter module of FIG. 29.

[0070] FIG. 35 is a perspective view taken from the first end of the in-line dongle adapter module of FIG. 29, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for environmental purposes.

[0071] FIG. 36 is a perspective view taken from the second end of the in-line dongle adapter module of FIG. 29, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for environmental purposes.

[0072] FIG. 37 is a perspective view of the in-line dongle adapter module of FIG. 29 within a vending machine.

[0073] FIG. 38 is a perspective view of the exemplary fourth preferred in-line dongle adapter module with two vertical gaps indicating the in-line dongle adapter module can be of any width.

[0074] FIG. 39 is a front plan view of the in-line dongle adapter module of FIG. 38.

[0075] FIG. 40 is a back plan view of the in-line dongle adapter module of FIG. 38.

[0076] FIG. 41 is a first side view of the in-line dongle adapter module of FIG. 38, the second side being a mirror image of that shown.

[0077] FIG. 42 is a first end view of a connector receptacle of the in-line dongle adapter module of FIG. 38.

[0078] FIG. 43 is a second end view of a connector receptacle of the in-line dongle adapter module of FIG 38.

[0079] FIG. 44 is a perspective view taken from the first end of the in-line dongle adapter module of FIG. 38, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for environmental purposes.

[0080] FIG. 45 is a perspective view taken from the second end of the in-line dongle adapter module of FIG. 38, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for environmental purposes.

[0081] FIG. 46 is a perspective view of the in-line dongle adapter module of FIG. 38 within a vending machine.

[0082] FIG. 47 is a perspective view of the exemplary fifth preferred in-line dongle adapter module and, specifically, the longitudinal center portion thereof, the dashed line depiction of the sides indicating the sides of the in-line dongle adapter module can be of any shape or curvature.

[0083] FIG. 48 is a front plan view of the in-line dongle adapter module of FIG. 47.

[0084] FIG. 49 is a back plan view of the in-line dongle adapter module of FIG. 47.

[0085] FIG. 51 is a first end view of a connector receptacle of the in-line dongle adapter module of FIG. 47.

[0086] FIG. 52 is a second end view of a connector receptacle of the in-line dongle adapter module of FIG 47.

[0087] FIG. 53 is a perspective view taken from the first end of the in-line dongle adapter module of FIG. 47, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for environmental purposes.

[0088] FIG. 54 is a perspective view taken from the second end of the in-line dongle adapter module of FIG. 47, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for environmental purposes.

[0089] FIG. 55 is a perspective view of the in-line dongle adapter module of FIG. 47 within a vending machine.

[0090] FIG. 56 is a block diagram of an exemplary adapter module.

[0091] FIG. 57 is a block diagram of an exemplary mobile device.

[0092] FIG. 58 is a block diagram of an exemplary server.

DETAILED DESCRIPTION OF THE INVENTION

[0093] Disclosed herein are mobile-device-to-machine payment systems and, more specifically, mobile-device-to-machine payment systems over a non-persistent network connection. The mobile-device-to-machine payment systems disclosed herein focus on the unattended retail space (e.g. a payment accepting unit 120 or machine 120). More specifically, mobile-device-to-machine payment systems disclosed herein allow a user (having a mobile device 150 with a mobile application 140 thereon) to make a cashless purchase from a payment accepting unit 120 (having an adapter module 100 associated therewith).

[0094] The mobile-device-to-machine payment systems described herein can be implemented with one or more of the following features: easy installation feature, a non-persistent network connection feature; a manual (swipe to pay) mode feature; a hands-free mode feature; and a multiple vending transactions (multi-vend) feature.

[0095] Easy Installation: Installation is very easy, requires no tools, requires no configuration, and takes as little as 30 seconds. This is accomplished by using an adapter module 100 such as an in-line dongle (a hardware device with software thereon) design for in-line insertion within a multi-drop bus (MDB) of a payment accepting unit (e.g. a vending machine). Installation is as simple as "powering down" (turning off) the machine 120, identifying the "wire" that connects with a payment receiving mechanism (e.g. the coin mechanism), disconnecting the wire (so that there are two loose ends, such as a male

connection end or adapter of an MDB and a female connection end or adapter of an MDB), plugging (inserting) the adapter module 100 in serial ("in-line") with the wire (for example, connecting the MDB female adapter to a male adapter of the adapter module 100 and connecting the MDB male adapter to a female adapter of the adapter module 100), tucking the wire and the installed adapter module 100 back into position, and "powering up" (turning on) the machine 120. Most vending machines made since 1995 have this industry standard MDB technology that would allow this easy 30-second installation. On machines without MDB technology, the adapter module 100 can be configured or designed to work with other serial protocols or activate a switch. In essence the adapter module 100 simulates establishing payment on payment accepting unit 120 in much the same manner as other alternative forms of payment (e.g. cash).

[0096] Non-persistent Network Connection: Although payment accepting units (or "machines") that accept only cash (e.g. paper currency and coins) may not require a connection (persistent or non-persistent) to a network, traditional payment accepting units that accept cashless payments (e.g. credit cards, debit cards, and alternative mobile device payment methods using, for example, smart phones) require a persistent connection to a network (wired or wireless) to facilitate the cashless payments. In other words, without a persistent (ongoing or accessible on demand) network connection, traditional payment accepting units cannot accept cashless payments. Most traditional payment accepting units that accept cashless payments include the technology to accomplish this persistent network connection that allows them to connect to a remote server. If the network connection to a traditional machine is temporarily interrupted, cashless payments will be temporarily unavailable. If the machine is located in a location where no signal is available, cashless payments will not be possible. The Whigham reference, the Offer reference, and the Belfer reference disclose alternative payment accepting units that accept cashless payments by using the user's cellular phone to allow the user to manually input coding to a remote server and, thereby act as an on-demand bridge network connection. These references, however, require significant user interaction with the cellular telephone to effectuate the transaction. In addition to using a mobile device 150 as an intermediary between the payment accepting units 120 and the server 130, mobile-device-to-machine payment systems described herein minimize (manual mode) or eliminate (hands-free mode) user interaction with the mobile device 150. Further, some mobile-device-to-machine payment systems described herein facilitate the acceptance of cashless payments without requiring any network connection near

the payment accepting unit 120. Mobile-device-to-machine payment systems described herein that are located in a remote location where no signal is available, therefore, can accept cashless payments.

[0097] Manual (Swipe to Pay) Mode: Using a "swipe to pay" feature (or just "swipe") refers to a user's action implemented on his mobile device 150 in which he quickly brushes his finger (or other pre-determined interaction) on the mobile device's touch screen 152 (or other input device associated with the mobile device 150). From the user's perspective, when the user is within range, a pre-installed mobile application 140 automatically connects to the payment accepting unit 120 (e.g. a vending machine). The mobile application 140 might display (on the touch screen 152) a prepaid balance that the user "swipes" to transfer payment to the payment accepting unit 120. The user could observe the transferred funds on the touch screen 152 of the mobile device 150 and/or on the display 122, 124 of the payment accepting unit 120. The transaction is completed just as if cash was inserted in the machine 120 with the user inputting his selection on the payment accepting unit 120 and the payment accepting unit 120 dispensing the product or service. After the selection is made, the change is returned to the mobile device 150 and this may be shown on the touch screen 152 of the mobile device 150.

[0098] Hands-Free Mode: A "hands-free pay" feature (or just "hands-free") would most likely be used with "favorite" payment accepting units 120 (e.g. a vending machine at work or school). From the user's perspective, he would approach the favorite payment accepting unit 120 and notice that the display 122, 124 of the payment accepting unit 120 showed funds available, he would select the product or service using the payment accepting unit's input mechanisms (e.g. buttons 126 or a touch screen display 124 shown in FIG. 19), and he would retrieve his dispensed services or products. It would be that simple. More specifically, when the user is within range, a pre-installed mobile application 140 automatically connects to the payment accepting unit 120 (e.g. a vending machine). The user may leave the mobile device 150 in a pocket, purse, briefcase, backpack, or other carrier. As the user approaches the payment accepting unit 120 and is in approximately "arms-length" distance (e.g. 3 to 5 feet), the user could observe the transferred funds on the display 122, 124 of the payment accepting unit 120. The transaction is completed just as if cash was inserted in the machine 120 with the user inputting his selection on the payment accepting unit 120 and the payment accepting unit 120 dispensing the product or service. After the selection is

made, the change is returned to the mobile device 150. FIG. 3 details when the hands-free mode would be available.

[0099] Multiple Vending Transactions (Multi-Vend): Both the "swipe to pay" feature and the "hands-free pay" feature could be used multiple times in sequence (implemented, for example, as a loop) so that a user may make multiple purchases. After making his first selection and receiving his product (or service), the user would observe that additional funds were available on the display 122, 124 on the payment accepting unit 120. He could make another selection (or multiple selections) and receive additional product(s) (or service(s)). More specifically, the display 122, 124 may reset as if the transaction is complete, but then, because the user is still standing in range, the mobile application 140 would send another credit to the payment accepting unit 120, allowing for a second purchase. When the walks away, the system clears (e.g. returns unused funds to the mobile application 140 on the mobile device 150.

[00100] The features described above, alone or in combination with other features described herein will revolutionize the hundred billion dollar automated retail industry. The exemplary hardware is very low cost and there are no reoccurring fees because no cellular connection is required on the machine 120. Using the mobile-device-to-machine payment systems described herein, operators can increase frequency of visits and items sold with each visit.

[00101] Mobile-device-to-machine payment systems described herein may be implemented as an apparatus and/or method for enabling payments to a machine 120 via a mobile device 150. Exemplary mobile-device-to-machine payment systems may be better understood with reference to the drawings, but the shown mobile-device-to-machine payment systems are not intended to be of a limiting nature.

Definitions

[00102] Before describing the mobile-device-to-machine payment systems and the figures, some of the terminology should be clarified. Please note that the terms and phrases may have additional definitions and/or examples throughout the specification. Where otherwise not specifically defined, words, phrases, and acronyms are given their ordinary meaning in the art. The following paragraphs provide some of the definitions for terms and phrases used herein.

- Adapter Module 100: As shown in FIGS. 1 and 2, the adapter module 100 is a physical device that is installed in a machine 120 (a payment accepting unit 120). The shown exemplary adapter module 100 is an in-line dongle (a hardware device with software thereon) device that may be inserted in-line within a multi-drop bus (MDB) of a machine 120. The adapter module 100 bridges the communication between the machine 120 and a mobile device 150. Although described as a unique component, it should be noted that the adapter module 100 could be implemented as a plurality of devices or integrated into other devices (e.g. components of a machine 120). In its unique component form, the adapter module 100 can be easily inserted into a machine 120 so that the machine 120 is able to perform new features with the assistance of the adapter module 100. FIG. 56 shows exemplary components associated with the adapter module 100. The shown example may be divided into multiple distinct components that are associated with each other or the example may be incorporated into or drawn from other technology (e.g. a computer or a payment accepting unit) as long as the components are associated with each other.

- Mobile Device 150 and Application 140 (also referred to as a "mobile application," "mobile app," or "app"): In general, a mobile device 150 may be a user's personal mobile device 150. The mobile device 150 (with a mobile application 140 thereon) acts as a communication bridge between the adapter module 100 (associated with a payment accepting unit 120) and the server 130. The mobile device 150 and application 140, however, are not "trusted" in that the communications (transmissions) it passes are encrypted. Encrypted (secured) communications are undecipherable (unencryptable, unreadable, and/or unuseable) by the mobile device 150. This keeps the passed communications secured and safe from hacking. Exemplary mobile devices include, but are not limited to smart phones, tablet or laptop computers, or personal digital assistants (PDAs), smart cards, or other technology (e.g. a hardware-software combination) known or yet to be discovered that has structure and/or capabilities similar to the mobile devices described herein. The mobile device 150 preferably has an application 140 (app 140) running on it. The term "app" is used broadly to include any software program(s) capable

of implementing the features described herein. FIGS. 10A-10D show exemplary mobile devices 150 with associated apps 140 associated therewith. It should be noted that the phrase "mobile device" can be assumed to include the relevant app unless specifically stated otherwise. Similarly, it should be noted that an "app" can be assumed to be running on an associated mobile device unless specifically stated otherwise. FIG. 57 shows exemplary components associated with the mobile device 150. The shown example may be divided into multiple distinct components that are associated with each other or the example may be incorporated into or drawn from other technology (e.g. the cell phone itself) as long as the components are associated with each other.

- Payment Accepting Unit 120 (or Machine 120): A payment accepting unit 120 (or machine 120) is equipment that requires payment for the dispensing of an product and/or service. Payment accepting units 120 may be vending machines, parking meters, toll booths, laundromat washers and dryers, arcade games, kiosks, photo booths, toll booths, transit ticket dispensing machines, and other known or yet to be discovered payment accepting units 120. Some payment accepting units 120 can accept cashless payments (payments other than cash (paper currency and coins)) by accepting payment from, for example, credit cards, debit cards, and mobile devices.
- Network Connections: For purposes of this discussion, a persistent network connection is a wired or wireless communications connection that is ongoing (e.g. a dedicated connection, a dedicated online connection, and/or a hardwired connection) or accessible on demand (e.g. the ability for the machine to make a temporary connection to a server or the ability for the user to contact a server from his mobile device). Typically the persistent network connection has been conducted over "long-range communication technology" (e.g. hardwired, telephone network technology, cellular technology, WiFi technology, wide area network (WAN), local area network (LAN), or any wired or wireless communication technology over the internet that is known or yet to be discovered). Traditionally, machines that accept payment other than cash require a persistent (ongoing or accessible on demand) connection to a network to facilitate payment. This is true for machines that accept, for

example, credit cards and debit cards. The payment accepting units 120 described herein do not require a traditional persistent network connection. The user's mobile device 150 acts as a communication bridge between the adapter module 100 and the server 130. Communications between user mobile devices 150 and the servers (e.g. a system management server 130 and/or a funding source server 160) take place using long-range communication technology. Communications between user mobile devices 150 and the adapter module 100 of the payment accepting unit 120 take place using "short-range communication technology" (e.g. Bluetooth (e.g. Bluetooth 4.0, Bluetooth Smart, Bluetooth LE (Low Energy), near-field communication, Ultra Wideband (UWB), RFID, infrared wireless, induction wireless, or any wired or wireless technology that could be used to communicate a small distance (e.g. approximately a hundred feet or closer) that is known or yet to be discovered). Neither the adapter module 100 nor the payment accepting unit 120, therefore require a traditional persistent long-range wireless network connection. The exemplary communications technology shown in the figures may be replaced with alternative like communications technology and, therefore, specific shown communications technologies are not meant to be limiting. For example WiFi technology could be replaced with another long-range communication technology.

- Server: A server is the host processing server that may be operated by the company running the system. For each user, the server 130 preferably maintains at least one "virtual wallet" having at least one "balance" (which can be $0) of designated funds for which the server 130 keeps an accounting. The balance may represent, for example, "cash" or it may be a "promotional value" that represents funds that may be spent under certain circumstances. If these funds begin to be depleted, the user may be notified (e.g. via the application 140 on the mobile device 150) that additional funds need to be designated and/or transferred. Alternatively, funds from other sources (e.g. the funding source server 160) may be automatically transferred to restore a predetermined balance. The balance may also be increased based on a promotion (e.g. points earned or coupons). As shown in FIG. 58, the server includes appropriate processors 950, memory 960 (which would keep an

accounting of the user's balance in a manner similar to a gift card), and communication systems 970. As shown, the communications unit 970 of the server 130 includes long-range communication technology (e.g. cellular technology and WiFi mechanisms). The server 130 also includes a security unit 955 for encrypting and decrypting messages. The server 130 receives an AuthRequest from the adapter module 100 (via a mobile device 150) and, if funds are available, returns the AuthGrant for funds. FIG. 58 shows exemplary components associated with the server 130. The shown example may be divided into multiple distinct components that are associated with each other or the example may be incorporated into or drawn from other technology (e.g. a computer or a main frame) as long as the components are associated with each other.

- Advertise Presence: Each adapter module 100 advertises its presence by broadcasting signals (advertising broadcast signals) to mobile devices in the zones 102, 104, 016. Each adapter module 100 can listen to other adapter modules' advertisements
- Received Signal Strength Indicator (RSSI): The adapter module 100 may have a self-calibrating signal strength to determine zone thresholds (e.g. a payment zone threshold). At the time the user selects an item (product or service) from the payment accepting unit 120, the Received Signal Strength Indicator (RSSI) is logged. At this moment, it is presumed the user is within "arms-length" (which may be a predetermined length approximating the distance of a user standing in front of a machine for the purpose of making a purchase) from the payment accepting unit 120. Mathematical computation (In-Range Heuristics) is conducted to derive the optimal RSSI threshold at which point payment should be triggered by an application 140 on a mobile device 150. The threshold may be payment accepting unit specific and can vary over a period of time. This optimal zone threshold is preferably reported to the mobile device 150 during an initial handshake.
- In-Range Heuristics: Mathematical computation that determines the RSSI threshold to determine when a user is in the authorization zone 104 and/or payment zone 102. This computation can take into consideration numerous historical data points as well as transaction specific information such as which

mobile device 150 is being used, payment accepting unit type, among other factors. Preferably the RSSI is logged while the user is making his selection (this is the one time in the entire process that the user definitely will be "in range" (e.g. they will be arm's length from the machine 120 because they are physically interacting with the machine 120). The type of user mobile device 150, accelerometer data (e.g. is the user moving or stationary), and/or other information may also be logged while the user is making his selection. The adapter module 100 can give a reference RSSI for the payment zone 102 for the machine 120, and the application 140 can make a +/- adjustment based on the specific mobile device 150 on which it is installed. Over a period of time, the system continues to improve itself based on additional data points.

- Authorization Request (AuthRequest): When a user enters the authorization zone 104, the mobile device 150 notifies the adapter module 100 and the adapter module 100 sends the secured authorization request (e.g. the encrypted authorization request) as a "message" (also referred to as a communication or transmissions) to the server 130 via the mobile device 150. Encryption may be performed by a security unit 755 (security technology that may be associated with the processing unit 750 and/or the memory 760). Significantly, the AuthRequest is a request for authorization of funds, not a request for authorization of a transaction. The purpose of the funds is irrelevant to the server 30.

- Authorization Grant Token (AuthGrant): This is a "message" (also referred to as a communication or transmissions) encrypted by the security unit 955 (security technology) of the server 130 with the unique private key for the adapter module 100. The secured authorization grant (e.g. the encrypted authorization grant) is passed from the server 130 (via the mobile device 150) to the adapter module 100 in the form of a message. The mobile device 150, however, is not able to decrypt and read the message. The authorization grant is in response to the authorization request. The amount of the funds granted by the AuthGrant may be determined by factors including, but not limited to, the amount of funds available (or, if funds are not available, a mini-loan could be granted), a pre-authorized amount (e.g. set by the server, set by the user during set-up, set by the funding source, or a standard amount), limited by

time (e.g. only a certain amount per hour, or a predetermined amount at specific times of the day), limited to the maximum amount of an item on the machine (or enough for two or three items in the machine), or one or more of these and other factors. Significantly, the AuthGrant makes the funds available, but does not authorize a transaction. The AuthGrant may have an associated expiration period in that it may expire if it is not used in a pre-determined time period. The length of time before the AuthGrant expires may be determined by factors including, but not limited to, the trustworthiness of the user (e.g. the user has a long history with the system or some known provider (e.g. credit card provider, bank, or credit union), the user has a good credit rating, or the user has a large wallet balance), a pre-authorized time period (e.g. set by the server, set by the user during set-up, set by the funding source, or a standard time period), limited by time (e.g. predetermined time periods at specific times of the day such as longer times during breakfast, lunch, and dinner), limited by the machine or the products or services sold in the machine, limited by the number of other users near the machine (e.g. if it is a crowded machine, the AuthGrant may expire faster), or one or more of these and other factors. The AuthGrant remains valid until it expires or some other event occurs to end its validity (e.g. the user cancels it). This means that under normal circumstances the mobile device 150 will hold the AuthGrant authorizing use of funds for a pre-determined time period that will allow the user sufficient time to make a purchase. The authorized amount may be considered to be the "wallet balance" that is held in a virtual "wallet."

- Synchronization: Time may be synchronized to the adapter module 100 from the server 130. The server 130 sends time information with encrypted messages and the adapter module 100 uses the time encoded in the messages for synchronization.

- The mobile-device-to-machine payment systems and components thereof may have associated hardware, software, and/or firmware (a variation, subset, or hybrid of hardware and/or software). The term "hardware" includes at least one "processing unit," "processor," "computer," "programmable apparatus," and/or other known or yet to be discovered technology capable of executing instructions or steps (shown as processing unit 750 in FIG. 56, processing unit

850 in FIG. 57, and processing unit 950 in FIG. 58). The term "software" includes at least one "program," "subprogram," "series of instructions," or other known or yet to be discovered hardware instructions or hardware-readable program code. Software may be loaded onto hardware (or firmware) to produce a "machine," such that the software executes on the hardware to create structures for implementing the functions described herein. Further, the software may be loaded onto the hardware (or firmware) so as to direct the mobile-device-to-machine payment systems (and components thereof) to function in a particular manner described herein or to perform a series of operational steps as described herein. "Hardware" such as the adapter module 100, mobile device 150, and payment accepting unit 120 may have software (e.g. programs and apps) loaded thereon. The phrase "loaded onto the hardware" also includes being loaded into memory (shown as memory 760 in FIG. 56, memory 860 in FIG. 57, and memory 960 in FIG. 58) associated with or accessible by the hardware. The term "memory" is defined to include any type of hardware (or other technology) -readable media (also referred to as computer-readable storage medium) including, but not limited to, attached storage media (e.g. hard disk drives, network disk drives, servers), internal storage media (e.g. RAM, ROM, EPROM, FLASH-EPROM, or any other memory chip or cartridge), removable storage media (e.g. CDs, DVDs, flash drives, memory cards, floppy disks, flexible disks), firmware, and/or other known or yet to be discovered storage media. Depending on its purpose, the memory may be transitory and/or non-transitory. Appropriate "messages," "communications," "signals," and/or "transmissions" (that includes various types of information and/or instructions including, but not limited to, data, commands, bits, symbols, voltages, currents, electromagnetic waves, magnetic fields or particles, optical fields or particles, and/or any combination thereof) over appropriate "communication paths," "transmission paths," and other means for signal transmission including any type of connection between two elements on the system (the system including, for example, the adapter module 100, mobile device 150, payment accepting unit 120, hardware systems and subsystems, and memory) would be used as appropriate to facilitate controls and communications.

- It should be noted that the terms "programs" and "subprograms" are defined as a series of instructions that may be implemented as software (i.e. computer program instructions or computer-readable program code) that may be loaded onto a computer to produce a "machine," such that the instructions that execute on the computer create structures for implementing the functions described herein or shown in the figures. Further, these programs and subprograms may be loaded onto a computer so that they can direct the computer to function in a particular manner, such that the instructions produce an article of manufacture including instruction structures that implement the function specified in the flow chart block or blocks. The programs and subprograms may also be loaded onto a computer to cause a series of operational steps to be performed on or by the computer to produce a computer implemented process such that the instructions that execute on the computer provide steps for implementing the functions specified in the flow chart block or blocks. The phrase "loaded onto a computer" also includes being loaded into the memory of the computer or a memory associated with or accessible by the computer. Separate, albeit interacting, programs and subprograms may be associated with the adapter modules 100, the server 130, and the mobile device 150 (including the mobile application 140) and these programs and subprograms may be divided into smaller subprograms to perform specific functions.

- The terms "messages," "communications," "signals," and/or "transmissions" include various types of information and/or instructions including, but not limited to, data, commands, bits, symbols, voltages, currents, electromagnetic waves, magnetic fields or particles, optical fields or particles, and/or any combination thereof. Appropriate technology may be used to implement the "communications," "signals," and/or "transmissions" including, for example, transmitters, receivers, and transceivers. "Communications," "signals," and/or "transmissions" described herein would use appropriate technology for their intended purpose. For example, hard-wired communications (e.g. wired serial communications) would use technology appropriate for hard-wired communications, short-range communications (e.g. Bluetooth) would use technology appropriate for close communications, and long-range

communications (e.g. WiFi or Cellular) would use technology appropriate for remote communications over a distance. Appropriate security (e.g. SSL or TLS) for each type of communication is included herein. Security units 755 and 955 include technology for securing messages. The security technology may be, for example, encryption/decryption technology (e.g. software or hardware). Although encryption/decryption is discussed primarily as being performed using a unique private key, alternative strategies include, but are not limited to encryption/decryption performed using public/private keys, or other encryption/decryption strategies known or yet to be discovered. Appropriate input mechanisms and/or output mechanisms, even if not specifically described, are considered to be part of the technology described herein. The exemplary communications unit 770 (shown in FIG. 56) of the adapter module 100 is shown as including appropriate input and output mechanisms 772, 774 that may be implemented in association (e.g. directly or indirectly in functional communication) with male and female adapters 720, 730 of the adapter module 100. The exemplary communications unit 870 (shown in FIG. 57) of the mobile device 150 includes mechanisms for both long-range communications (shown as Cellular and/or WiFi mechanisms 872) for communicating with the server 130 and short-range communications (shown as Bluetooth mechanisms 876) for communicating with the adapter module 100.

- When used in relation to "communications," "signals," and/or "transmissions," the terms "provide" and "providing" (and variations thereof) are meant to include standard means of provision including "transmit" and "transmitting," but can also be used for non-traditional provisions as long as the "communications," "signals," and/or "transmissions" are "received" (that can also mean obtained). The terms "transmit" and "transmitting" (and variations thereof) are meant to include standard means of transmission, but can also be used for non-traditional transmissions as long as the "communications," "signals," and/or "transmissions" are "sent." The terms "receive" and "receiving" (and variations thereof) are meant to include standard means of reception, but can also be used for non-traditional methods

of obtaining as long as the "communications," "signals," and/or "transmissions" are "obtained."

- The term "associated" is defined to mean integral or original, retrofitted, attached, connected (including functionally connected), positioned near, and/or accessible by. For example, if the user interface (e.g. a traditional display 122 (FIG. 19), a touch screen display 124 (FIG. 19), a key pad 126 (FIG. 19), buttons 126 (FIG. 19, shown as part of the key pad 126), a keyboard (not shown), and/or other input or output mechanism) is associated with a payment accepting unit 120, the user interface may be original to the payment accepting unit 120, retrofitted into the payment accepting unit 120, attached to the payment accepting unit 120, and/or a nearby the payment accepting unit 120. Similarly, adapter modules 100 may be associated with payment accepting units 120 in that the adapter modules 100 may be original to the payment accepting unit 120, retrofitted into the payment accepting unit 120, attached to the payment accepting unit 120, and/or a nearby the payment accepting unit 120.
- It should be noted that relative terms are meant to help in the understanding of the technology and are not meant to limit the scope of the invention. Similarly, unless specifically stated otherwise, the terms used for labels (e.g. "first," "second," and "third") are meant solely for purposes of designation and not for order or limitation. The term "short" in the phrase "short-range" (in addition to having technology specific meanings) is relative to the term "long" in the phrase "long-range."
- The terms "may," "might," "can," and "could" are used to indicate alternatives and optional features and only should be construed as a limitation if specifically included in the claims.
- It should be noted that, unless otherwise specified, the term "or" is used in its nonexclusive form (e.g. "A or B" includes A, B, A and B, or any combination thereof, but it would not have to include all of these possibilities). It should be noted that, unless otherwise specified, "and/or" is used similarly (e.g. "A and/or B" includes A, B, A and B, or any combination thereof, but it would not have to include all of these possibilities). It should be noted that, unless

otherwise specified, the terms "includes" and "has" mean "comprises" (e.g. a device that includes, has, or comprises A and B contains A and B, but optionally may contain C or additional components other than A and B). It should be noted that, unless otherwise specified, the singular forms "a," "an," and "the" refer to one or more than one, unless the context clearly dictates otherwise.

System Overview

[00103] FIGS. 5, 6, and 7 together show exemplary major components of the mobile-device-to-machine payment system and the interactions therebetwen.

[00104] As shown, the adapter module 100 functionally connected bi-directionally to the payment accepting unit 120 via a wired serial connection such that no security is necessary. The adapter module 100 is also functionally connected bi-directionally to the mobile device 150 (and its installed mobile application 140) via short-range communication technology (e.g. a Bluetooth connection). Because the mobile device 150 is not a "trusted" link (e.g. it could be hacked by a user), only secured communications (transmissions) are passed between the adapter module 100 and the mobile device 150. This keeps the passed communications secured and safe from hacking. The mobile device 150 (and its installed mobile application 140) is also functionally connected bi-directionally to a system management server 130 and/or a funding source server 160 via long-range communication technology (e.g. WiFi or Cellular connection) that preferably has appropriate security (e.g. SSL security). Security between the mobile device 150 and the system management server 130 has the advantage of protecting communications from the mobile device 150 to the system management server 130 that may include sensitive data and may not be encrypted. The system management server 130 and the funding source server 160 may be connected via a wired Internet connection with SSL security. The system management server 130 may be connected via a wired Internet connection with SSL security to an operators' server 170. Although not necessary to implement a purchase transaction, for other purposes (e.g. inventory), the operators' server 170 may be connected to the payment accepting unit 120 using a handheld computer sync or a cellular connection.

[00105] Also, a unique private key may be used to securely transmit encrypted messages between the adapter module 100 and the system management server 130 (although the encrypted transmissions would most likely be routed through the mobile device 150).

The server 130 stores a private key for each adapter module 100, and this key is only known to the adapter module 100 and the server 130. No intermediary is privy to this key (especially not the mobile device 150). When the adapter module 100 and server 130 communicate messages (e.g. AuthRequest and AuthGrant), the security unit 755 of the adapter module 100 encrypts the message with its private key and passes the message to the mobile device 150. The mobile device 150 (which preferably cannot decrypt the message) passes the encrypted message to the server 130. The server 130 is able to decrypt the message using the security unit 955 of the adapter module 100 and the unique private key. The security unit 955 of the server 130 uses this same unique private key to encrypt messages to the adapter module 100 and sends the message to the mobile device 150 to relay to the adapter module 100 that is able to decrypt the message using the security unit 755 of the adapter module 100 and the unique private key.

[00106] FIG. 7 shows specific exemplary communications and messaging with an exemplary vending sequence (the numbers to the left of the communications and messaging) between the adapter module 100, the mobile device 150, and the system management server 130. These communications are discussed in more detail in the discussion pertaining to the timing schematics (FIGS. 8A-8G) and the flow charts (FIGS. 9A-9E).

[00107] It should be noted that FIGS. 5, 6, and 7 are meant to be exemplary and to help in the understanding of the mobile-device-to-machine payment system. For example, the shown long-range communications technology may be replaced with alternative long-range communications technology known or yet to be discovered, the shown short-range communication technology may be replaced with alternative short-range communication technology known or yet to be discovered, and the shown security may be replaced with alternative security known or yet to be discovered. The shown connections are meant to be exemplary in that, for example, there may be intermediaries that are not shown. The shown components have been simplified in that, for example, only one mobile device 150 (or machine 120, adapter module 100, or server 130) is shown where many may be included. Finally, the order of the steps may be changed and some steps may be eliminated.

Adapter Module

[00108] FIGS. 11-55 show exemplary adapter modules 100a-100e (referred to generally as adapter modules 100). These are relatively low cost hardware that are pre-configured to work with industry standard a multi-drop bus (MDB). On machines without

MDB technology, the adapter module 100 can be configured or designed to work with other serial protocols or activate a switch. In essence the adapter module 100 simulates establishing payment on payment accepting unit 120 in much the same manner as other alternative forms of payment (e.g. cash).

[00109] The shown exemplary adapter modules 100 are preferably designed to be used as an in-line dongle for in-line insertion within, for example, a MDB of a machine 120. The wire used in MDB technology uses male and female connection ends or adapters to allow the attachment of peripherals. In the case of a vending machine, the wire with the connection ends or adapters would be present to allow the attachment of a payment receiving mechanism (e.g. a coin mechanism). The MDB male and female adapters 700, 710 may be separated (as shown in FIGS. 17, 18, 26, 27, 35, 36, 44, 45, 53, and 54). The adapter modules 100 have male and female adapters 720, 730. The adapter module may be plugged (inserted) in serial ("in-line") with the wire. For example, the MDB female adapter 710 may be connected to the male adapter 720 of the adapter module 100 and the MDB male adapter 700 may be connected to the female adapter 730 of the adapter module 100. The resulting in-line configuration is shown in FIGS. 19, 28, 37, 46, and 55. It should be noted that the adapter modules 100 are designed to allow pass-through communications so that if the mobile-device-to-machine payment systems is not enabled (e.g. for a particular purchase or simply turned off) the MDB functions as though the adapter module 100 is not there and the machine 120 can function normally.

Hands-Free

[00110] Summarily, if it is available, a hands-free mode, from the user's perspective, would allow the user to approach a favorite payment accepting unit 120 and notice that the display (e.g. the displays 122 or 124 shown in FIG. 19) associated with the payment accepting unit 120 shows funds available (e.g. the wallet balance), he would select the product or service using input mechanisms (e.g. buttons 126 or a touch screen display 124 shown in FIG. 19) associated with the payment accepting unit 120, and he would retrieve his dispensed services or products.

[00111] During an initial handshake with the mobile device 150 (when the user is within range), the adapter module 100 reports to the mobile device 150 whether or not hands-free mode is available. If it is available, the installed mobile application 140 automatically connects to the payment accepting unit 120 without the user having to interact with the

mobile device 150. The user observes that funds are available on the display 122, 124 of the payment accepting unit 120 and completes the purchase transaction as if cash was inserted in the machine 120 by inputting his selection on the payment accepting unit 120. The payment accepting unit 120 dispenses the product or service. After the selection is made, the change is returned to the mobile device 150.

[00112] Whether hands-free payment is available is determined by factors including, but not limited to whether if other mobile devices 150 are in range, if other adapter modules 100 are in range, if there are any alerts, if the payment trigger threshold is having wide variances and so deemed unstable, or if the payment accepting unit operator (e.g. a vending machine operator) has opted to disable hands-free mode for the payment accepting unit 120. In the latter instance, operators can disable via a maintenance mobile device 150, as well as through the operators' server 170 and/or the system management server 130.

[00113] FIG. 3 is a table that showing exemplary considerations, conditions, or factors that may be used to determine whether the hands-free pay feature is available. Starting at the "Favorite?" column, this indicates whether the payment accepting unit 120 is a favorite machine. Preferably the hands-free pay feature is only available for use with "favorite" payment accepting units 120 (e.g. a vending machine at work or school). The "Alert" column has to do with whether there is some reason (e.g. there are too many users in range) that the hands-free pay feature should not work and, if there is such a reason, the user will be notified (alerted) and may be able to use the manual mode to resolve the alert and/or complete the transaction. FIG. 3 shows situations in which a user is or is not able to make hands-free purchases from a machine 120 using a mobile application 140 on his mobile device 150. It should be noted that the shown interface is meant to be exemplary. For example, some of the features could be automated or pre-selected. (It should be noted that the left hand column, the "Tab" column, relates to whether the selected tab on the mobile application 140 is "all" or "favorite." FIGS. 10A-10D all show these tabs. Unlike the other columns in FIG. 3, this column has more to do with the functionality and view of the application 140 than specifically with the hands-free feature. The tabs would allow a user to select whether he wanted to be alerted when he was in range of all payment accepting units 120 or just "favorite" payment accepting units 120 and the application 140 would show the appropriate view.)

[00114] Balance Display: An optional feature of the mobile-device-to-machine payment system that is particularly helpful in the hands-free mode (although it may be

available in the manual mode and/or in a multiple-vend scenarios) is when the user's mobile device 150 sends "credit" to the payment accepting unit 120 (either via hands-free payment or through a manual swipe), the wallet balance is sent to the payment accepting unit 120 that is then displayed to the user on a display 122, 124 of the machine 120. This is particularly beneficial during hands-free mode when the user does not retrieve the mobile device 150 and, therefore, may not know the balance. Also, in a multiple-vend scenario the user would not have to calculate a remaining balance.

[00115] An exemplary hands-free and multiple-vend scenario with a balance display might be as follows: The user has $5.00 in his virtual wallet as that is the amount that has been authorized (the AuthGrant being stored on the mobile device 150). He walks up to the payment accepting unit 120 and $5.00 is displayed on the display 122, 124 of the payment accepting unit 120 since hands-free mode was enabled and credit was sent (e.g. via short-range communication technology) to the payment accepting unit 120. The user makes a selection of $1.50 by interacting (e.g. pressing buttons) with the machine 120. The item (product or service) is dispensed and the "change" is "returned" (e.g. via short-range communication technology) to the virtual wallet. But since user is still standing in the payment zone 102, the remaining wallet balance of $3.50 is sent to the payment accepting unit 120 and displayed so that the user can now see he has a $3.50 balance. (It should be noted that the authorized funds may remain on the machine 120 and not be transferred back to the mobile device 150 between transactions.) The user decides to purchase a $1.50 item, and the transaction is completed as usual (e.g. by interacting with the machine 120). Now the user is still standing in the payment zone 102 and he sees the wallet balance of $2.00 on the display 122, 124 of the payment accepting unit 120. Deciding he does not wish to purchase anything else, the user walks away. As he walks out of the payment zone 102, the credit is cleared from the machine 120. But he is left with the knowledge that his wallet balance is $2.00 even though he never touched the mobile device 150. Communications between the payment accepting unit 120 and the adapter module 100 (via the mobile device 150) handle the accounting incidental to the transaction. The remaining balance ($2.00) is technically stored on the server 130, and may be reflected on the application 140 on the mobile device 150.

Multiple Distinct Zones

[00116] As shown in FIGS. 1 and 2, the functions performed by the adapter module 100 can be divided into distinct zones: a first "communication zone" (e.g. "Bluetooth range"

106), a second "authorization zone" 104, and a third "payment zone" 102. The payment zone102 (that can not be zero) is smaller than or equal to (overlapping completely) the authorization zone 104. (Put another way, the payment zone 102 is within or coextensive with the authorization zone 104.) The payment zone 102 is a subset of the authorization zone 104 with a ratio of the payment zone 102 to the authorization zone 104 ranging from 0.01:1 to 1:1. It is not necessarily a fixed ratio and can vary between different payment accepting units 120, different mobile devices 150, different users, and over time. While the zones 102, 104, 106 are depicted as having a uniform shape, the zones may not necessarily be uniform (or constant over time) in that the shape can vary. For example, the shape of the Bluetooth range 106 may vary depending on environmental conditions such as obstacles in the room and payment accepting unit 120 door/wall materials.

[00117] Bluetooth Range 106: The outermost range is the Bluetooth range 106. This is the area in which the adapter module 100 is able to broadcast its presence. In most situations, the Bluetooth range 106 is a passive range in that no actual data is exchanged between the mobile device 150 and the adapter module 100. While in the Bluetooth range 106, the mobile device 150 monitors the RSSI (Received Signal Strength Indicator).

[00118] Authorization Zone 104: The middle region is the authorization zone 104. This is a computed area based on the RSSI. As mentioned, the mobile device 150 monitors the RSSI while it is in the Bluetooth range 106. When the RSSI reaches a certain predetermined threshold based on In-Range Heuristics, the mobile device 150 can be considered to be in the authorization zone 104. In the authorization zone 104 the mobile device 150 establishes a connection to the adapter module 100 (e.g. a Bluetooth connection (FIG. 5) with SSL protection (FIG. 6)) and informs the adapter module 100 of its presence. After a successful handshake with the adapter module 100, the mobile device 150 registers the adapter module 100 and the adapter module 100 requests an authorization to the server 130 via the mobile devices' network connection (e.g. a WiFi or cellular connection (FIG. 5) with SSL protection (FIG. 6)). It is important to note the mobile device 150 and the adapter module 100 have a non-exclusive relationship at this point. The adapter module 100 may collect registrations for all mobile devices 150 that are within the authorization zone 104.

[00119] An authorization occurs in preparation for when the user enters the payment zone 102. An authorization expires in a set period of time (for example, five minutes), so if the mobile device 150 is still in the authorization zone 104 at the time of expiration, the adapter module 100 submits for and receives another authorization. This will continue for a

set number of times (for example, the limit may be three times to limit cases of numerous authorizations for a mobile device that may remain in the authorization zone 104 for an extended period of time without completing a transaction). Should authorization fail (for instance if the limit had been reached) prior to the user entering the payment zone 102, the adapter module 100 will request authorization when the mobile device 150 enters the payment zone 102 (which adds a few seconds to the experience).

[00120] Payment Zone 102: As a user enters the payment zone 102, the mobile device 150 establishes exclusive control of the adapter module 100. Once established, any other user in the payment zone 102 is put into a "waiting" status.

[00121] In the payment zone 102, the payment can be triggered automatically if the system has and is in hands-free mode. In such instances, the mobile device 150 is running the app 140 in background mode and will send credit to the payment accepting unit 120 without any explicit user interaction. The user completes the transaction on the payment accepting unit 120 in much the same manner as if cash had been inserted into the payment accepting unit 120 to establish credit. After the user completes the transaction (that may include one or more purchases), details of the transaction are preferably returned to the mobile device 150 and server 130 in separate messages. The message to the server 130 is preferably encrypted with the adapter module's 100 private key (FIG. 6) to ensure data integrity. As shown in FIG. 7, the "private key" coded message (Encrypted VendDetails) is preferably sent via the mobile device 150. The message to the mobile device 150 may be sent solely for the purpose of closing the transaction. The transaction history and balance are updated server-side via the encrypted message sent to the server 130.

[00122] The other mode of operation is manual mode. In manual mode, the user launches the mobile device 150 and is able to swipe to send payment to the payment accepting unit 120. The user can also swipe back to cancel the payment. Like in hands-free mode, the purchase transaction is completed on the payment accepting unit 120 in the same manner as if cash were inserted into the payment accepting unit 120. The mobile device 150 is only used to send payment. Selection is made directly on the payment accepting unit 120.

[00123] Self-Calibrating Zone Threshold: A key, but optional feature, of the system is a self-calibrating payment zone RSSI threshold. Because RSSI can vary machine to machine, environment to environment, and device to device, having a fixed threshold at which payment is triggered can be problematic. The approach suggested herein is the creation of a

self-calibrating threshold. When the user is interacting with the payment accepting unit 120 (such as when he makes his selection on the payment accepting unit 120), the payment accepting unit 120 notifies the adapter module 100 and the adapter module 100 logs the conditions such as RSSI, type of user mobile device 150, accelerometer data, and other information. It is at this point that it can be ascertained safely that the user is within arms-length from the payment accepting unit 120 (by necessity the user is arms-length because he is making some physical interaction with the payment accepting unit 120). This is the only point in the entire transaction in which it can be certain that the user is within arms-length from the payment accepting unit 120.

[00124] FIG. 4 shows a simplified set of exemplary steps involved when users enter the payment zone 102. Specifically, FIG. 4 shows that credit is established 200 (this may have been done in the authorization zone 104, but if not it would be handled in the payment zone 102), that the user makes a selection using the machine 202, that the machine notifies the adapter module of the selection 204, that the adapter module (optionally) logs the RSSI 206, and that the purchase process(es) continues 208. Using the historically logged RSSI data, the adapter module 100 calculates one of several "average" RSSI using various mathematical models. This "average" could be a traditional average, a moving average, a weighted average, a median, or other similar summary function. The adapter module 100 could pre-process the historical data before running the function, such as to eliminate top and bottom data points, suspect data points, etc.

[00125] Optionally, during the handshake between the mobile device 150 and the adapter module 100, the information transmitted to the adapter module 100 may include, for example, the model of the mobile device 150. Using the received information pertaining to the mobile device models, the adapter module 100 can create multiple payment thresholds, one for each mobile device model. This allows for variances that may be inherent in different types of Bluetooth radios. An alternative to this method is for the adapter module 100 to broadcast a baseline payment zone threshold, and the mobile device 150 can use an offset from this baseline based on its specific model type. The payment zone thresholds (or baseline offsets) can be unique to specific types of mobile devices (e.g. by manufacturer, operating system, or component parts), models of mobile devices, or individual mobile devices (unique to each user).

[00126] In a typical scenario in which the payment zone threshold has been calibrated, the adapter module 100 advertises its presence along with the threshold at which it considers

any mobile device 150 to be in the authorization zone 104. This is a one-way communication from adapter module 100 to mobile device 150. Once the mobile device 150 enters the authorization zone 104, there is a handshake that is established between the adapter module 100 and the mobile device 150. During this handshake, the mobile device 150 can share its model information with the adapter module 100, and the adapter module 100 can return the payment zone 102 threshold for that specific model.

[00127] Optionally, in addition to calibrating the payment zone threshold, the adapter module 100 can apply the self-calibrating model to the authorization zone 104 to calibrate the authorization zone threshold. As with the payment zone thresholds, the authorization zone thresholds can be unique to specific types of mobile devices, models of mobile devices, or individual mobile devices. In this scenario, the adapter module 100 would broadcast multiple thresholds by device type and the mobile device 150 would determine which threshold to apply (or alternatively broadcast a baseline and the mobile device 150 uses an offset based on its device model). Even in this scenario, the authorization zone 104 is a one-way communication.

[00128] Optionally, along with the threshold that is calculated (in the payment and/or the authorization zone(s)), a safety margin can be added to minimize scenarios in which a user is within range, but the mobile-device-to-machine payment systems do not recognize it because the threshold may not have been reached. For example, if the calculated RSSI for an iPhone 5 on machine 4567 is -68db, the mobile-device-to-machine payment systems may add a safety margin of -5db, and establish the threshold at -73db. So when a user's phone is communicating with the adapter module 100 at an RSSI of -73db or better, the mobile-device-to-machine payment systems will allow the mobile device 150 to credit the payment accepting unit 120. The safety margin can be set on the server 130 and downloaded to the adapter module 100, or set on the mobile device 150, or set on the adapter module 100 itself.

[00129] Optionally, in the payment zone threshold, the mobile device 150 can use other data to determine when to cancel the exclusive control of the payment accepting unit 120, to identify when the user is moving out of the payment zone 102. External data could include accelerometer data from the mobile device 150. Using that data, the mobile device 150 can determine whether the user is standing relatively still in front of the payment accepting unit 120, or if the user is in motion – effectively walking away from the payment accepting unit 120.

Signal Unavailability Adaptation

[00130] The mobile-device-to-machine payment systems described herein use a mobile device's 150 short-range communication technology (shown as Bluetooth mechanisms 876 in FIG. 57) and a mobile device's 150 long-range communications technology (shown as Cellular and/or WiFi mechanisms 872 in FIG. 57). The short-range communication technology 876 communicates with the adapter module's 100 short-range communication technology (shown as Bluetooth mechanisms 776 in FIG. 56). The long-range communications technology 872 communicates with the server's 130 communication technology (not shown). The mobile device 150 (with a mobile application 140 thereon) acts as a communication bridge between the adapter module 100 (associated with a payment accepting unit 120) and the server 130. This process is described herein and works properly if there is cellular or WiFi coverage within the payment zone 102.

[00131] One option if there is no cellular or WiFi coverage within the payment zone 102 is to determine whether there is cellular or WiFi coverage within the authorization zone 104 or the Bluetooth range 106. If there is, then the sizes of the zones 102, 104, 106 could be adapted and the timing could be adapted. For example, if the mobile devices 150 detected problems with the cellular or WiFi coverage within the payment zone 102, the user could carry his mobile device 150 into the other zones (or the mobile device 150 could use short-range communication technology to communicate with other mobile devices 150 within the authorization zone 104 or the Bluetooth range 106) to determine whether the zones have cellular or WiFi coverage. If they do have coverage, communication between the mobile device 150 and the server 130 can be advanced (conducted earlier when the mobile device 150 is further from the machine 120) or delayed (conducted later when the mobile device 150 is further from the machine 120). This can be thought of as changing the size or shapes of the zones 102, 104, 106. The timing would also have to be adjusted so that the authorization of funds (AuthGrant) does not expire before the user has a chance to make a purchase. It also means that balance updates to the server 130 may happen after the user has moved away from the machine 120 and has cellular or WiFi coverage again.

[00132] Another option if there is no cellular or WiFi coverage within any of the zones 102, 104, 106 is for the user to obtain authorization while outside of the zones in a place with cellular or WiFi coverage. This may occur, for example, if a user knows that he will be going to a place with a payment accepting unit 120 equipped with an adapter module 100 (perhaps to a favorite payment accepting unit 120) that does not have (or rarely has) cellular or WiFi

coverage. A user may also use the mobile application 140 to query payment accepting units 120 in a given range (e.g. within 50 miles) or at a given location (e.g. at a campground or in a particular remote city) to determine whether there is cellular or WiFi coverage within the zones 102, 104, 106. The user can then obtain pre-authorization from the server 130 using the mobile application 140. Again, the timing would also have to be adjusted so that the authorization of funds (AuthGrant) does not expire before the user has a chance to make a purchase. It also means that balance updates to the server 130 may happen after the user has moved away from the machine 120 and has cellular or WiFi coverage again. A mobile-device-to-machine payment system having the ability to implement this option would be able to accept cashless payments without requiring any network connection near the payment accepting unit 120. Mobile-device-to-machine payment systems described herein that are located in a remote location where no signal is available, therefore, can accept cashless payments.

[00133] As an example of a situation in which there might be no cellular or WiFi coverage within any of the zones 102, 104, 106 of a particular payment accepting unit 120, the user (a teenager) may be traveling to a remote location to attend summer camp where there is no cellular or WiFi coverage. The camp may have several payment accepting units 120 (e.g. a machine that creates a dedicated "hot spot" that requires payment for use, vending machines, or machines for renting equipment (e.g. bikes, kayaks, or basket balls)). The camp facility might notify parents that the mobile-device-to-machine payment system is available. The parents, while at home, could obtain authorization for a particular amount (that could be doled out a certain amount per day or limited to type of machine or location) to be authorized and "loaded" into the user's mobile device 150 and specify that the authorization will not expire for a certain period or until a certain date. Thereafter, while at camp, the user could use the mobile application 140 on his mobile device 150 in a manner similar to those discussed elsewhere herein. Short-range communications may be used for communications between the adapter modules 100 (associated with the machines 120) and users' mobile devices 150.

[00134] One subtle but powerful component of the systems described herein is that they require internet network connection only in the authorization zone 104 and only for the time period required to send the AuthRequest and receive the AuthGrant. Once a valid AuthGrant is received by the mobile device 150, an internet network connection is not required by either the mobile device 150 or the adapter module 100 in the payment zone 102

as long as the AuthGrant is valid (unexpired). This mechanism allows the system to seamlessly handle authenticated transactions in (temporary) offline mode, with the deferred acknowledgement and transaction messages performing the bookkeeping and cleanup when network connection is regained. The alternatives described above provide a unique way to artificially extend the authorization zone to include any location where the mobile device 150 can communicate with the server 130.

Multiple User Resolution

[00135] As shown in FIG. 2, in likely practical scenarios, there will be multiple users in the zones 102, 104, 106. As shown, users 1, 2, and 3 are in the payment zone 102 near the machine 120, users 5 and 6 are shown as positioned between the authorization zone 104 and the Bluetooth range 106, users 4 and 7 are in the Bluetooth range 106, user 10 is positioned on the edge of the Bluetooth range 106, and users 8 and 9 are positioned outside of Bluetooth range 106. The mobile-device-to-machine payment systems provide for managing, and resolving issues pertaining to multiple users.

[00136] Users 4 and 7 are within the Bluetooth range 106 and user 10 is either entering or leaving the Bluetooth range 106. Within the Bluetooth range 106 the users' mobile devices 150 are able to see the adapter module's 100 advertisement. In this zone, the mobile device 150 preferably does not initiate a connection. The adapter module 100 is preferably unaware of the users in the Bluetooth range 106. All the adapter module 100 is doing is advertising its presence to any multitude of users that may be in Bluetooth range 106.

[00137] The adapter module 100 begins to log users as the users (and their respective mobile devices 150) enter the authorization zone 104 (shown in FIG. 2 as users 5 and 6). At this point, there is a non-exclusive connection initiated by the mobile device 150 to the adapter module 100. It does a handshake (e.g. to exchange information needed to obtain authorization and, optionally, to log information needed for a self-calibrating authorization zone threshold) and the mobile device 150 contacts the server 130 for an authorization (e.g. sending an AuthRequest and receiving an AuthGrant). The adapter module 100 registers all mobile devices 150 that have requested and received AuthGrants. The adapter module 100 continues communicating with any other mobile device 150 that enters the authorization zone 104. After initial contact, the adapter module 100 may provide the mobile device 150 with a deferral delay of when to check back in with the adapter module 100 allowing opportunity for other mobile devices 150 to communicate with the adapter module 100.

[00138] If there is only one user in the payment zone 102, a purchase transaction may be performed. If there are multiple users in the payment zone 102, the mobile-device-to-machine payment system must handle the situation.

[00139] One optional exemplary solution for handling the situation of the multiple users in the payment zone 102 is queuing users in the payment zone 102. Once any mobile device 150 enters the payment zone 102, it establishes exclusivity to a particular mobile device 150 (first come first serve). Technically, however, the adapter module 100 is not establishing an exclusive connection to the mobile device 150. The adapter module 100 can still perform a round-robin poll and communicate with and advertise to other mobile devices 150. Instead, the adapter module 100 establishes a queue prioritized by RSSI and time (e.g. who was first and whether the authorization has expired) and it notifies (e.g. alerts) other mobile devices 150 to wait. The earliest valid (unexpired) authorization takes precedence when there is any tie in the RSSI. Otherwise, for example, the strongest average RSSI takes priority. Preferably the queue is not a static measure of the RSSI but an averaged measure over the period of time in the queue. This compensates for a scenario in which a user may be walking around in the queue and then shows up at the payment accepting unit 120 just as the previous user is finishing. If another user was also in the payment zone 102 and stood there the entire time, but may have newer authorization, he could win out.

[00140] Anytime that the adapter module 100 cannot determine exactly which user is in the payment zone 102 in front of the payment accepting unit 120, the adapter module 100 will disable hands-free payment. The mobile device 150 will send an alert to the user and he can use swipe to pay (manual mode). All users in payment zone 102 will show "Connected" and the first to swipe payment to the payment accepting unit 120 then locks out other users.

Multiple Module Resolution

[00141] In the scenario where there are multiple modules present, determining which payment accepting unit 120 a user is in front of can be a challenge. The mobile-device-to-machine payment systems described herein allow for adapter modules 100 to communicate to other adapter modules 100 in range via Bluetooth. Each user receives authorization grants for specific payment accepting units 120. This means if there are multiple adapter modules 100 within the same authorization zone 104, there will be multiple authorization grants for the user. When the user enters the payment zone 102, it can be difficult to differentiate which payment accepting unit 120 the user is in front of if the payment zones 102 overlap.

[00142] To solve this problem, when the user enters the payment zone 102, the adapter modules 100 communicate with each other to determine the RSSI for the particular user (based on the signal from his mobile device 150) to triangulate which adapter module 100 (and the associated payment accepting unit 120) is closer to the user. Optionally, the inter-module communications can restrict the user to establishing an exclusive connection with only one payment accepting unit 120.

[00143] Optionally, when the user connects to a payment accepting unit 120, the mobile device 150 can send a communication to the payment accepting unit 120 for momentary display to the user on the display 122, 124 of the payment accepting unit 120. For example, the mobile device 150 can send a communication (e.g. "connected" or "Fred's Mobile Device Connected") to the payment accepting unit's display 122, 124 for a predetermined period of time (e.g. 1-3 seconds) so when the user is in payment zone 102, it is clear which payment accepting unit 120 the user is connected to prior to making a purchase (either in hands-free or manual mode).

[00144] In addition, when the user is in manual mode, the mobile device 150 can display (e.g. on the touch screen 152 as shown in FIGS. 10A-10D) a visual indication of the payment accepting unit 120 (e.g. a picture and/or a payment accepting unit ID of the payment accepting unit 120) for visual confirmation. If the user is in manual mode, the user can manually change the payment accepting unit 120.

Descriptive Scenario

[00145] FIG. 7, FIGS. 8A-8G, and 9A-E (as well as other figures) can be used to understand a detailed exemplary scenario of the mobile-device-to-machine payment systems described herein. An exemplary flow of communications and steps are loosely described below with reference to these (and other figures). It should be noted that alternative scenarios could include, for example, a modified order of the steps performed.

[00146] Prior to vending transactions, a user downloads a mobile app 140 onto his mobile device 150, creates an account, and configures a funding source via, for example, a funding source server 160. A funding source may be, for example, a debit card, a credit card, campus cards, rewards points, bank accounts, payment services (e.g. PayPal®) or other payment option or combination of payment options known or yet to be discovered. The funding sources may be traditional and/or nontraditional payment sources that are integrated into the ecosystem described herein and then used indirectly as a source of funds. Funds

from the funding source are preferably held on the server 130 such that when an AuthRequest is received by the server 130, the server 130 can send an AuthGrant authorizing funds for a purchase.

[00147] The user can specify one or more "favorite" adapter module(s) 100 (that has a one-to-one relationship to the payment accepting unit 120) that he may visit regularly, such as a vending machine at school or work. Favorite adapter modules 100 appear on a pre-filtered list and allow for additional rich features such as hands-free payment.

[00148] The payment accepting unit 120 may be equipped with an adapter module 100 that is constantly advertising its availability via Bluetooth (or other "signals," "communications," and/or "transmissions"). This ongoing advertising and scanning for adapter modules is shown in FIG. 8A. As shown, the mobile device 150 is continuously scanning for any adapter module 100 within Bluetooth (or other "signal," "communication," and/or "transmission") range. When the user is within range of that adapter module 100, the mobile device 150 tracks and monitors the signal strength until a predetermined "authorization zone" threshold is achieved.

[00149] FIGS. 8B and 9A generally show that when the authorization zone threshold is reached, the mobile device 150 enters the authorization zone (block 302) and registers the adapter module 100. The mobile device 150 connects to the server 130 (block 304). The app 140 on the mobile device 150 creates a request for authorization (AuthRequest) and passes the AuthRequest to the server 130 using appropriate communication technology (e.g. cellular or WiFi) (block 306). The server 130 responds with an authorization grant (AuthGrant) encrypted with the specific adapter module's private key (block 306). This authorization token may minimally include the Userl D, Apparatusl D (for the adapter module 100), authorization amount, and expiration time. The mobile device 150 receives the AuthGrant from the server 130, and retains it until the mobile device 150 is ready to issue payment to an adapter module 100. The mobile device 150 collects all pending AuthGrants that may be one or more depending on how many adapter modules 100 are in-range. Unused AuthGrants that expire are purged from the mobile device 150 and the server 130. It is important to note that the mobile device 150 is unable to read the AuthGrant because it is encrypted with the adapter module's unique private key that is only known to server 130 and adapter module 100. This provides a preferred key element of security in the system as the adapter module 100 only trusts AuthGrants that are issued by the server, and the AuthGrants cannot be read or modified by the mobile device 150 or any other party in between the server and the adapter

module 100. Additional mobile devices 150 may enter the authorization zone 104 (block 308).

[00150] As the user approaches a specific adapter module 100, the user enters the payment zone 102 and an event threshold is triggered based on heuristics performed by the mobile device 150. Blocks 310 and 312 show the loop steps of waiting for a mobile device 150 from the authorization zone 104 to enter the payment zone 102. If the user leaves the authorization zone 104 without entering the payment zone 102, the adapter module 100 returns to advertising its presence (block 300).

[00151] FIGS. 8C and 9B generally show the user entering the payment zone. The mobile device 150 verifies that it has an unexpired and valid AuthGrant. If the AuthGrant is not good, it may be requested again, repeating the Auth Request process (block 315). If the AuthGrant is good, the mobile device 150 sends the valid AuthGrant (including the wallet balance (block 322)) to the adapter module 100 to initiate a transaction. The mobile device 150 may issue the AuthGrant automatically without specific user interaction if the hands-free mode is supported (and the device is a favorite (block 318), there is only one device in the payment zone 102 (block 318), and (optionally) there is only one user in the authorization zone 104 (block 320). If any of these factors are not present, the mobile device 150 will prompt and/or wait for the user to begin the transaction manually (block 324).

[00152] FIGS. 8D, 9C, and 9D generally show the transaction process. As shown in FIG. 9C, the adapter module 100 runs through a series of questions to determine if there are any issues that would prevent vending including: has the user canceled in-app? (block 326), has the user walked away? (block 328), is the coin return pressed? (block 330), has more than a predetermined period of time elapsed? (block 332). If the answer to any of these questions is "yes," the transaction does not proceed. If the answers to all of these questions is "no," the user makes a selection (block 334) on the payment accepting unit 120 in the same or similar manner as compared to if cash or credit were presented to the payment accepting unit 120. If the machine 120 is able to vend (block 336), it attempts to release the product. If the vend fails (block 338) it is reported by the machine (block 340) and a credit is returned to the virtual wallet (block 342). If the vend is successful (block 338) it is reported by the machine (block 344). Put another way, after the transaction is complete, the adapter module 100 returns to the mobile device 150 the details of the transaction as well as an encrypted packet containing the vend details to be sent to the server 130 via the mobile device 150.

Optionally, the adapter module 100 can pass additional information not directly related to the transaction such as payment accepting unit health, sales data, error codes, etc.

[00153] FIGS. 8D and 9E generally show the multi-vend function. If the machine has enabled multi-vend capabilities (block 350) and the multi-vend limit has not been reached, the process returns to the question of whether the user is in the payment zone (block 310 of FIG. 9A). If the machine does not have enabled multi-vend capabilities (block 350) or the multi-vend limit has been reached, the wallet is decremented by the vend amount(s) and "change" is returned to the virtual wallet (block 354) and the process ends (block 356).

[00154] FIG. 8E is a timing schematic showing an exemplary Login process. FIG. 8F is a timing schematic showing an exemplary bootup process. FIG. 8G is a timing schematic showing an exemplary Account Check/Update process.

[00155] Several of the figures are flow charts (e.g. FIGS. 9A-9E) illustrating methods and systems. It will be understood that each block of these flow charts, components of all or some of the blocks of these flow charts, and/or combinations of blocks in these flow charts, may be implemented by software (e.g. coding, software, computer program instructions, software programs, subprograms, or other series of computer-executable or processor-executable instructions), by hardware (e.g. processors, memory), by firmware, and/or a combination of these forms. As an example, in the case of software, computer program instructions (computer-readable program code) may be loaded onto a computer to produce a machine, such that the instructions that execute on the computer create structures for implementing the functions specified in the flow chart block or blocks. These computer program instructions may also be stored in a memory that can direct a computer to function in a particular manner, such that the instructions stored in the memory produce an article of manufacture including instruction structures that implement the function specified in the flow chart block or blocks. The computer program instructions may also be loaded onto a computer to cause a series of operational steps to be performed on or by the computer to produce a computer implemented process such that the instructions that execute on the computer provide steps for implementing the functions specified in the flow chart block or blocks. Accordingly, blocks of the flow charts support combinations of steps, structures, and/or modules for performing the specified functions. It will also be understood that each block of the flow charts, and combinations of blocks in the flow charts, may be divided and/or joined with other blocks of the flow charts without affecting the scope of the invention. This may result, for example, in computer-readable program code being stored in

whole on a single memory, or various components of computer-readable program code being stored on more than one memory.

Distinction From Known Systems

[00156] Many of the known systems and methods require that the payment accepting unit be persistently (continuously) connected to and/or connectable on demand to some sort of remote server in order to function. As an example, the Carlson reference describes a system and a method for using a portable consumer device. Described embodiments include a consumer using the portable consumer device to dial a number to purchase an item (product or service) in a vending machine, to send an SMS to purchase an item in a vending machine, or to use a mobile wallet to purchase an item in a vending machine. It is mentioned in one embodiment that the consumer may launch an application in the portable consumer device or, alternatively, the portable consumer device may automatically detect the vending machine and prompt the consumer to enter information associated with the vending machine. It should be noted, however, that even when there is automatic detection, the user is prompted to enter information (e.g. a machine alias, payment information, or a PIN) and it can be inferred that this is entered on the portable consumer device. Once connected to a payment processing network, the authorization process begins using a payment processing network and/or payment server. Significantly, all of the embodiments described in the Carlson reference specify that the payment server sends an authorization response message to the vending machine. This means that, unlike the mobile-device-to-machine payment systems described herein, a persistent network connection is required for the Carlson system to function. Other references that disclose systems that require a persistent network connection include the Khan reference (the MicroAdapter having the persistent connection), the Garibaldi reference, and the Weiner reference.

[00157] Many of the known systems and methods require the user to significantly interact with their mobile devices. As an example, the Whigham reference is directed to a system that eliminates the need for currency for a vending machine and also eliminates the need for a dedicated online connection between the vending machine and the issuer of a credit card or a debit card. Instead the Whigham system and method allows a consumer to purchase a product from an automatic vending machine by using the consumer's cellular telephone, personal digital assistant (P DA), or similar wireless communication device as a link between the provider of the products in the vending machine and the vending machine. The Whigham reference, however, sets forth a system and method requires significant

interaction between the consumer and his telephone including dialing a telephone number to a server (that, in turn, provides a vend code to the consumer), requesting a specific product (e.g. by dialing additional digits, although this step is optional if a unique number was dialed for a specific product), and transmitting a vend code to the vending machine. (Other references that disclose systems that require user interaction with the phone include the Offer reference, the Khan reference, the Belfer reference, and the Carlson reference.) In addition to other differences, some of the mobile-device-to-machine payment systems described herein do not require the user to interact with his mobile device at all, which can be contrasted to known systems and methods that require the consumer to, for example, dial a telephone number, enter a machine identification, and/or enter a product identifier using the mobile device to purchase a product.

[00158] The known systems and methods that use a cellular telephone to facilitate cashless transactions at a vending machine use the cellular telephone to authorize a particular transaction. For example, once the user knows what he wants from a vending machine, he can dial a server and receive authorization to make a specific purchase. Sometimes this includes dialing additional numbers on the cellular telephone to specify a particular product. The mobile-device-to-machine payment systems described herein take a completely different approach. The mobile-device-to-machine payment systems described herein are not specifically interested in the details of the transaction to authorize the transaction. Instead, the mobile-device-to-machine payment systems function more like a gift card, a credit card, or a debit card in that they allow the user to have funds to make a purchase. When a user is in range, the adapter module 100 (via a mobile device 150) sends an AuthRequest to the server 130 to preemptively obtain authorization to make funds available. The server 130 returns the AuthGrant for funds to the adapter module 100 (via a mobile device 150) so that the user may use the funds to make a purchase. The AuthGrant may remain valid until it expires. This gives the user significantly more flexibility than known systems and methods.

Miscellaneous

[00159] It is to be understood that the inventions, examples, and embodiments described herein are not limited to particularly exemplified materials, methods, and/or structures. It is to be understood that the inventions, examples, and embodiments described herein are to be considered preferred inventions, examples, and embodiments whether specifically identified as such or not.

[00160] All references (including, but not limited to, foreign and/or domestic publications, patents, and patent applications) cited herein, whether supra or infra, are hereby incorporated by reference in their entirety.

[00161] The terms and expressions that have been employed in the foregoing specification are used as terms of description and not of limitation, and are not intended to exclude equivalents of the features shown and described. While the above is a complete description of selected embodiments of the present invention, it is possible to practice the invention using various alternatives, modifications, adaptations, variations, and/or combinations and their equivalents. It will be appreciated by those of ordinary skill in the art that any arrangement that is calculated to achieve the same purpose may be substituted for the specific embodiment shown. It is also to be understood that the following claims are intended to cover all of the generic and specific features of the invention herein described and all statements of the scope of the invention that, as a matter of language, might be said to fall therebetween.

WHAT IS CLAIMED IS:

1. A method of payment processing, comprising:

at a device with one or more processors, memory, and two or more communication capabilities:

obtaining, from a payment module, an authorization request via a first communication capability;

sending, to a server, the authorization request via a second communication capability distinct from the first communication capability;

in response to sending the authorization request, obtaining, from the server, authorization information via the second communication capability;

after obtaining the authorization information, detecting a trigger condition to perform a transaction with a payment accepting unit associated with the payment module; and

in response to detecting the trigger condition, sending, to the payment module, at least a portion of the authorization information via the first communication capability.

2. The method of claim 1, wherein the first communication capability corresponds to a short-range communication protocol and the second communication capability corresponds to a long-range communication protocol.

3. The method of claim 1, further comprising:

obtaining, from the payment module, advertised information indicating the payment module's presence via the first communication capability that at least includes authorization zone threshold criterion.; and

after obtaining the advertised information, initiating a handshake process with the payment module, wherein the handshake process includes:

sending, to the payment module, device information at least including user identification information corresponding to the user of the device via the first communication capability; and

receiving, from the payment module, payment module information, wherein the payment module information at least includes an identifier corresponding to the payment module.

4. The method of claim 3, further comprising:

prior to obtaining the authorization request:

in accordance with a determination that the authorization zone threshold criterion is satisfied, sending notification information to the payment module via the first communication capability, wherein the notification information indicates that the authorization zone threshold criterion is satisfied;

wherein the device obtains the authorization request in response to sending the notification information.

5. The method of claim 3, wherein the payment module information further includes an indication that hands-free mode is available and payment zone threshold criterion.

6. The method of claim 5, wherein the device information further includes device identification information corresponding to a model type of the device; and

wherein the payment zone threshold criterion is based at least in part on the device identification information.

7. The method of claim 5, wherein detecting the trigger condition comprises:

determining whether the payment zone threshold criterion is satisfied; and

in accordance with a determination that the payment zone threshold criterion is satisfied, detecting the trigger condition without interaction from a user of the device.

8. The method of claim 1, wherein detecting the trigger condition comprises:

detecting a user input from a user of the device; and

in response to detecting the user input, detecting the trigger condition to perform a transaction with the payment accepting unit.

9. The method of claim 1, further comprising:

in response to obtaining the authorization information, presenting a notification to the user of the device that a connection has been established with the payment module.

10. The method of claim 9, wherein the notification further indicates an authorized amount for the transaction.

11. The method of claim 1, wherein the authorization information includes an identifier corresponding to the payment module, an identifier corresponding to the user of the device,

an authorized amount, an authorization grant token, and an expiration period for the authorization grant token.

12. The method of claim 11, wherein at least a portion of the authorization request and the authorization grant token are encrypted with a unique encryption key corresponding to the payment module.

13. A device, comprising:

two or more communication capabilities;

one or more processors; and

memory storing one or more programs to be executed by the one or more processors, the one or more programs comprising instructions for:

obtaining, from a payment module, an authorization request via a first communication capability;

sending, to a server, the authorization request via a second communication capability distinct from the first communication capability;

in response to sending the authorization request, obtaining, from the server, authorization information via the second communication capability;

after obtaining the authorization information, detecting a trigger condition to perform a transaction with a payment accepting unit associated with the payment module; and

in response to detecting the trigger condition, sending, to the payment module, at least a portion of the authorization information via the first communication capability.

14. The device of claim 13, wherein the first communication capability corresponds to a short-range communication protocol and the second communication capability corresponds to a long-range communication protocol.

15. The device of claim 13, wherein the one or more programs further comprise instructions for:

obtaining, from the payment module, advertised information indicating the payment module's presence via the first communication capability that at least includes authorization zone threshold criterion; and

after obtaining the advertised information, initiating a handshake process with the payment module, wherein the handshake process includes:

sending, to the payment module, device information at least including user identification information corresponding to the user of the device via the first communication capability; and

receiving, from the payment module, payment module information, wherein the payment module information at least includes an identifier corresponding to the payment module.

16. The device of claim 15, wherein the one or more programs further comprise instructions for:

prior to obtaining the authorization request:

in accordance with a determination that the authorization zone threshold criterion is satisfied, sending notification information to the payment module via the first communication capability, wherein the notification information indicates that the authorization zone threshold criterion is satisfied;

wherein the device obtains the authorization request in response to sending the notification information.

17. The device of claim 15, wherein the payment module information further includes an indication that hands-free mode is available and payment zone threshold criterion.

18. The device of claim 17, wherein the device information further includes device identification information corresponding to a model type of the device; and

wherein the payment zone threshold criterion is based at least in part on the device identification information.

19. The device of claim 17, wherein detecting the trigger condition comprises:

determining whether the payment zone threshold criterion is satisfied; and

in accordance with a determination that the payment zone threshold criterion is satisfied, detecting the trigger condition without interaction from a user of the device.

20. The device of claim 13, wherein detecting the trigger condition comprises:

detecting a user input from a user of the device; and

in response to detecting the user input, detecting the trigger condition to perform a transaction with the payment accepting unit.

21. A non-transitory computer readable storage medium storing one or more programs, the one or more programs comprising instructions, which, when executed by a device with one or more processors and two or more communication capabilities, cause the device to perform operations comprising:

obtaining, from a payment module, an authorization request via a first communication capability;

sending, to a server, the authorization request via a second communication capability distinct from the first communication capability;

in response to sending the authorization request, obtaining, from the server, authorization information via the second communication capability;

after obtaining the authorization information, detecting a trigger condition to perform a transaction with a payment accepting unit associated with the payment module; and

in response to detecting the trigger condition, sending, to the payment module, at least a portion of the authorization information via the first communication capability.

22. The non-transitory computer readable storage medium of claim 21, wherein the first communication capability corresponds to a short-range communication protocol and the second communication capability corresponds to a long-range communication protocol.

23. The non-transitory computer readable storage medium of claim 21, wherein the instructions cause the device to perform operations further comprising:

obtaining, from the payment module, advertised information indicating the payment module's presence via the first communication capability that at least includes authorization zone threshold criterion; and

after obtaining the advertised information, initiating a handshake process with the payment module, wherein the handshake process includes:

sending, to the payment module, device information at least including user identification information corresponding to the user of the device via the first communication capability; and

receiving, from the payment module, payment module information, wherein the payment module information at least includes an identifier corresponding to the payment module.

24. The non-transitory computer readable storage medium of claim 23, wherein the instructions cause the device to perform operations further comprising:

prior to obtaining the authorization request:

in accordance with a determination that the authorization zone threshold criterion is satisfied, sending notification information to the payment module via the first communication capability, wherein the notification information indicates that the authorization zone threshold criterion is satisfied;

wherein the device obtains the authorization request in response to sending the notification information.

25. The non-transitory computer readable storage medium of claim 23, wherein the payment module information further includes an indication that hands-free mode is available and payment zone threshold criterion.

26. The non-transitory computer readable storage medium of claim 25, wherein the device information further includes device identification information corresponding to a model type of the device; and

wherein the payment zone threshold criterion is based at least in part on the device identification information.

27. The non-transitory computer readable storage medium of claim 25, wherein detecting the trigger condition comprises:

determining whether the payment zone threshold criterion is satisfied; and

in accordance with a determination that the payment zone threshold criterion is satisfied, detecting the trigger condition without interaction from a user of the device.

28. The non-transitory computer readable storage medium of claim 21, wherein detecting the trigger condition comprises:

detecting a user input from a user of the device; and

in response to detecting the user input, detecting the trigger condition to perform a transaction with the payment accepting unit.

METHOD AND SYSTEM FOR PERFORMING MOBILE DEVICE-TO-MACHINE PAYMENTS

ABSTRACT OF THE DISCLOSURE

A device with one or more processors, memory, and two or more communication capabilities obtains, from a payment module, an authorization request via a first communication capability (e.g., Bluetooth). The device sends, to a server, the authorization request via a second communication capability distinct from the first communication capability (e.g., cellular or WiFi technology). In response to sending the authorization request, the device obtains, from the server, authorization information via the second communication capability. After obtaining the authorization information, the device detects a trigger condition to perform a transaction with a payment accepting unit associated with the payment module. In response to detecting the trigger condition, the device sends, to the payment module, at least a portion of the authorization information via the first communication capability.

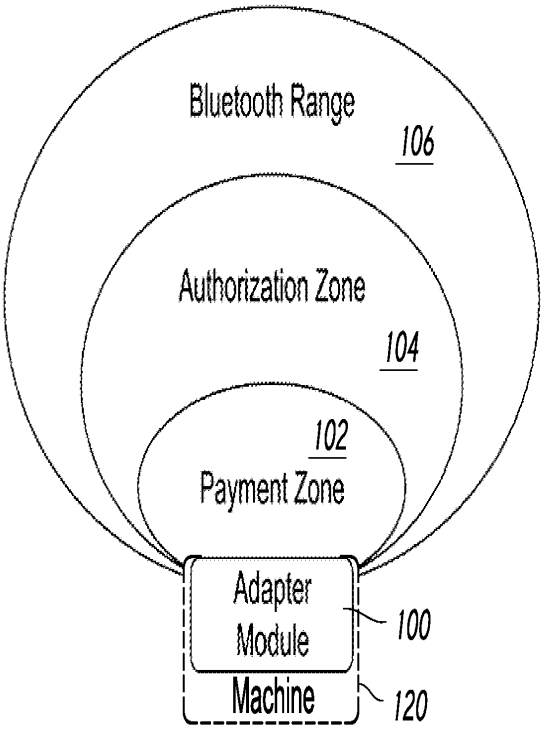

Bluetooth Range
106
Authorization Zone
104
102
Payment Zone
Adapter
Module
100
Machine
120

FIG. 1

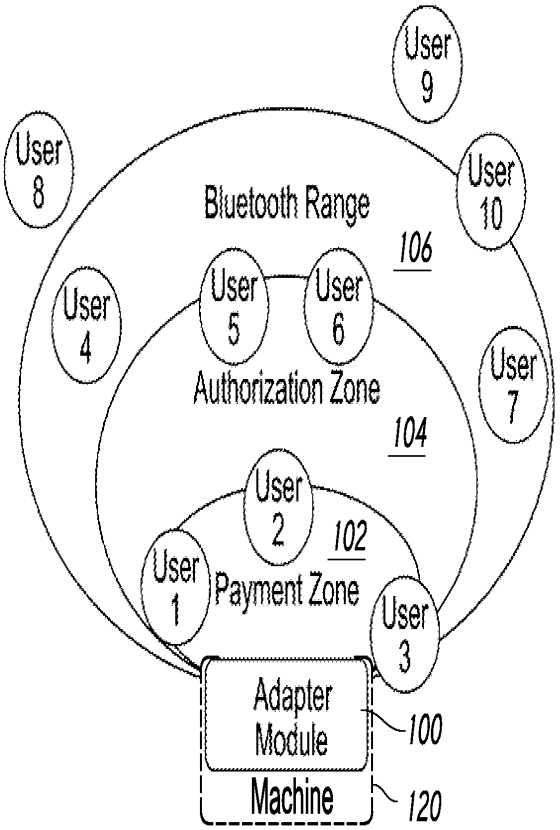

User
9
User
8
User
10
Bluetooth Range
106
User
4
User
5
User
6
User
7
Authorization Zone
104
User
2
102
User
1
Payment Zone
User
3
Adapter
Module
100
Machine
120

FIG. 2

Tab	Favorite?	Alert	View to User
All	Yes	No	User can make Hands-free Credit with the connected vending machine
All	No	Yes	User needs to launch Mobile Device and then swipe to make transaction manually
Favorite	Yes	No	Hands-free transction will be available to the user via vending machine
Favorite	No	No	User is not alerted for the vending machine which is not a favorite machine. Hands-free mode will not work, manual swipe for transaction required by user.
Either All or Favorite	Yes	Yes	BUT Hands-free Credit is not available (disabled by module, expired AuthGrant, insufficient balance, or other issue), then user will get an alert so that user can swipe credit manually.

FIG. 3

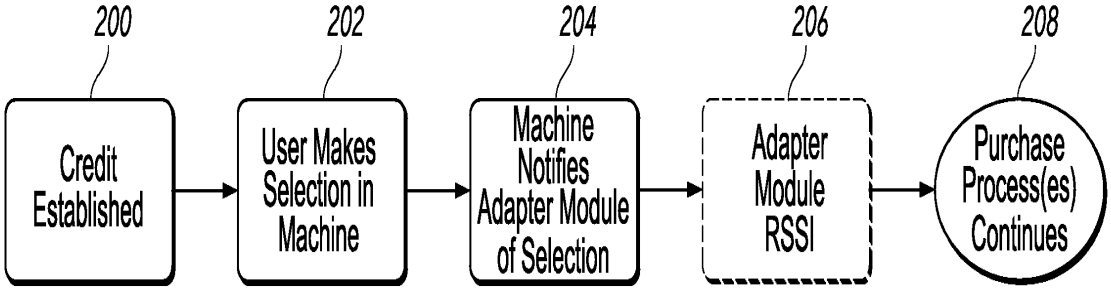


FIG. 4

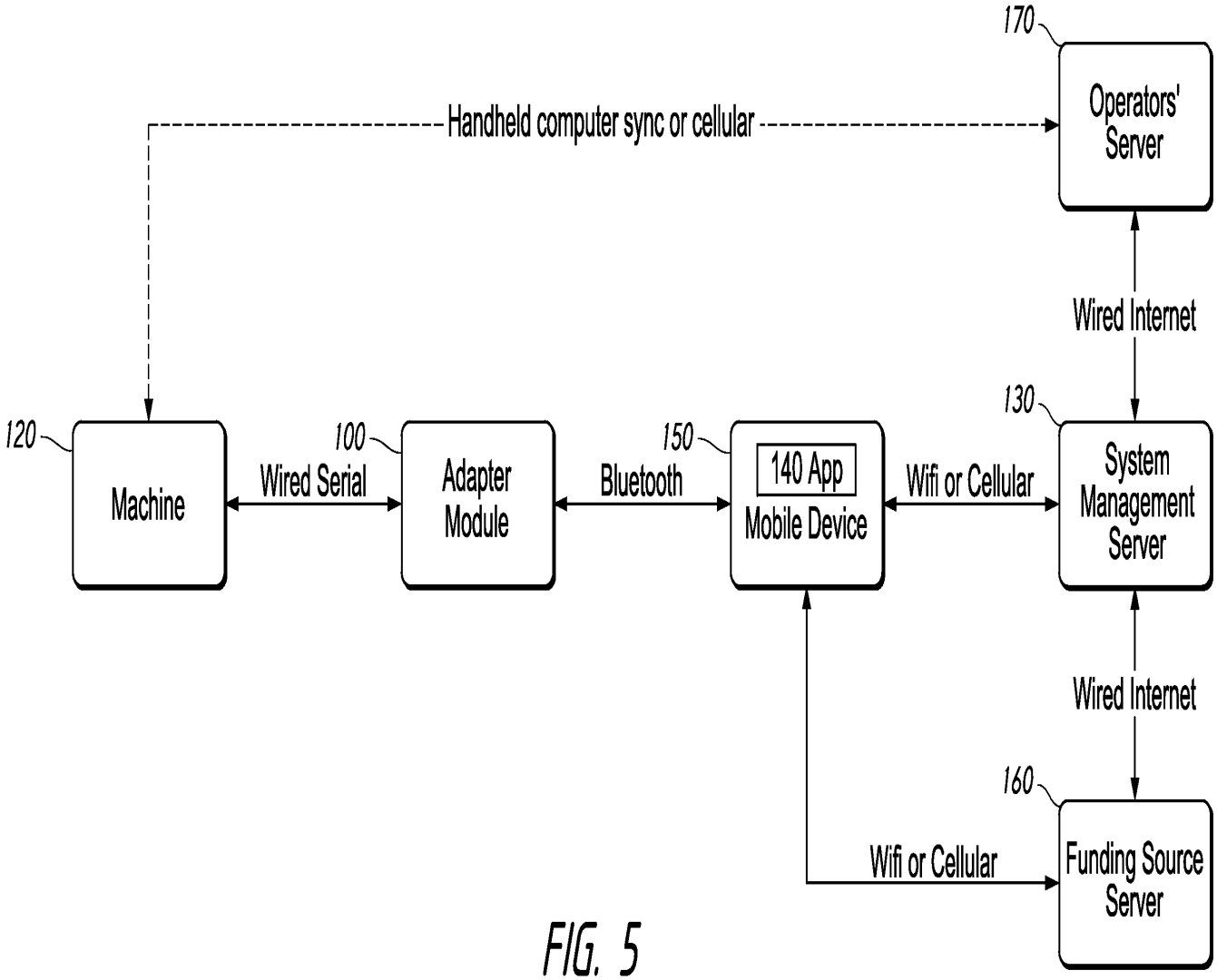

170
Operators' Server
Handheld computer sync or cellular
Wired Internet
130
120
100
150
Machine
Wired Serial
Adapter Module
Bluetooth
140 App
Mobile Device
Wifi or Cellular
System Management Server
Wired Internet
160
Wifi or Cellular
Funding Source Server

FIG. 5

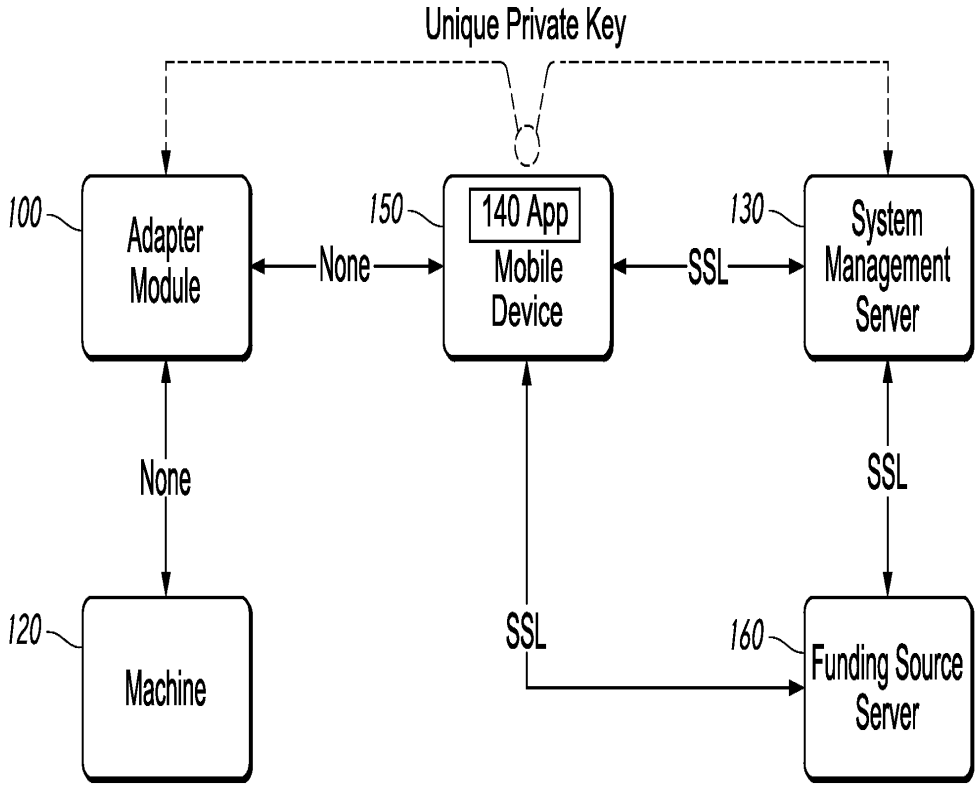

Unique Private Key
100
Adapter Module
None
150
140 App
Mobile Device
SSL
130
System Management Server
None
SSL
120
Machine
SSL
160
Funding Source Server

FIG. 6

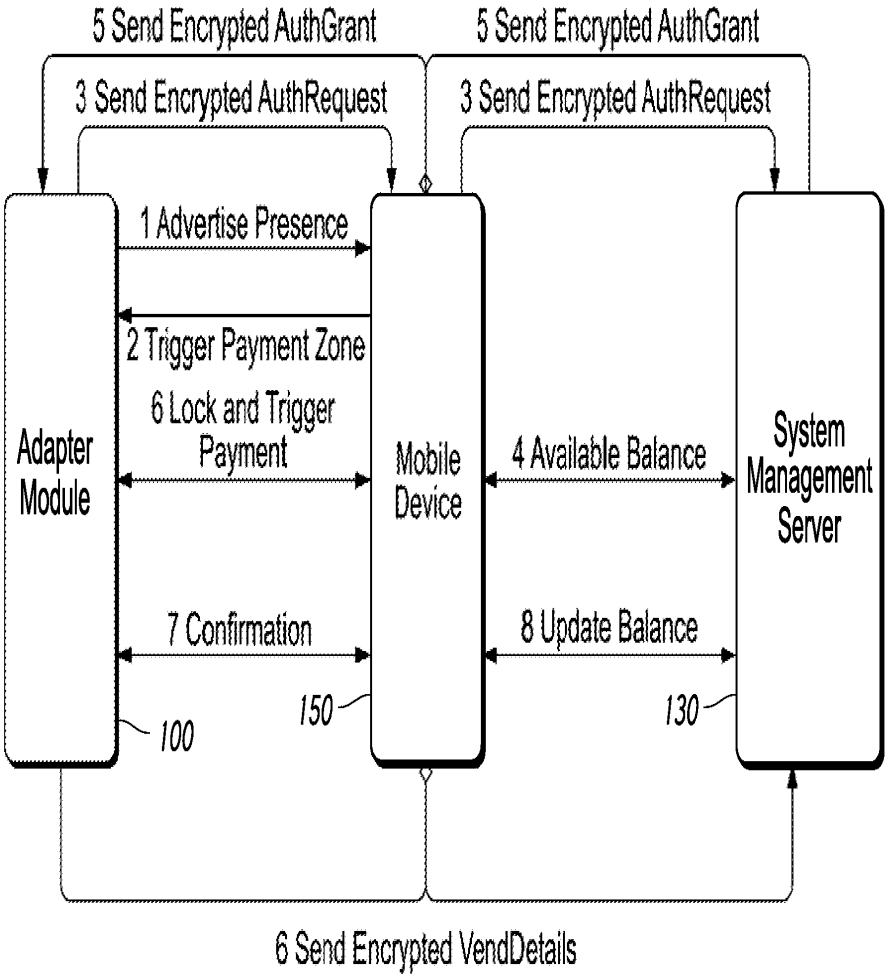

5 Send Encrypted AuthGrant
5 Send Encrypted AuthGrant
3 Send Encrypted AuthRequest
3 Send Encrypted AuthRequest
1 Advertise Presence
2 Trigger Payment Zone
6 Lock and Trigger Payment
Adapter Module
Mobile Device
4 Available Balance
System Management Server
7 Confirmation
8 Update Balance
100
150
130
6 Send Encrypted VendDetails

FIG. 7

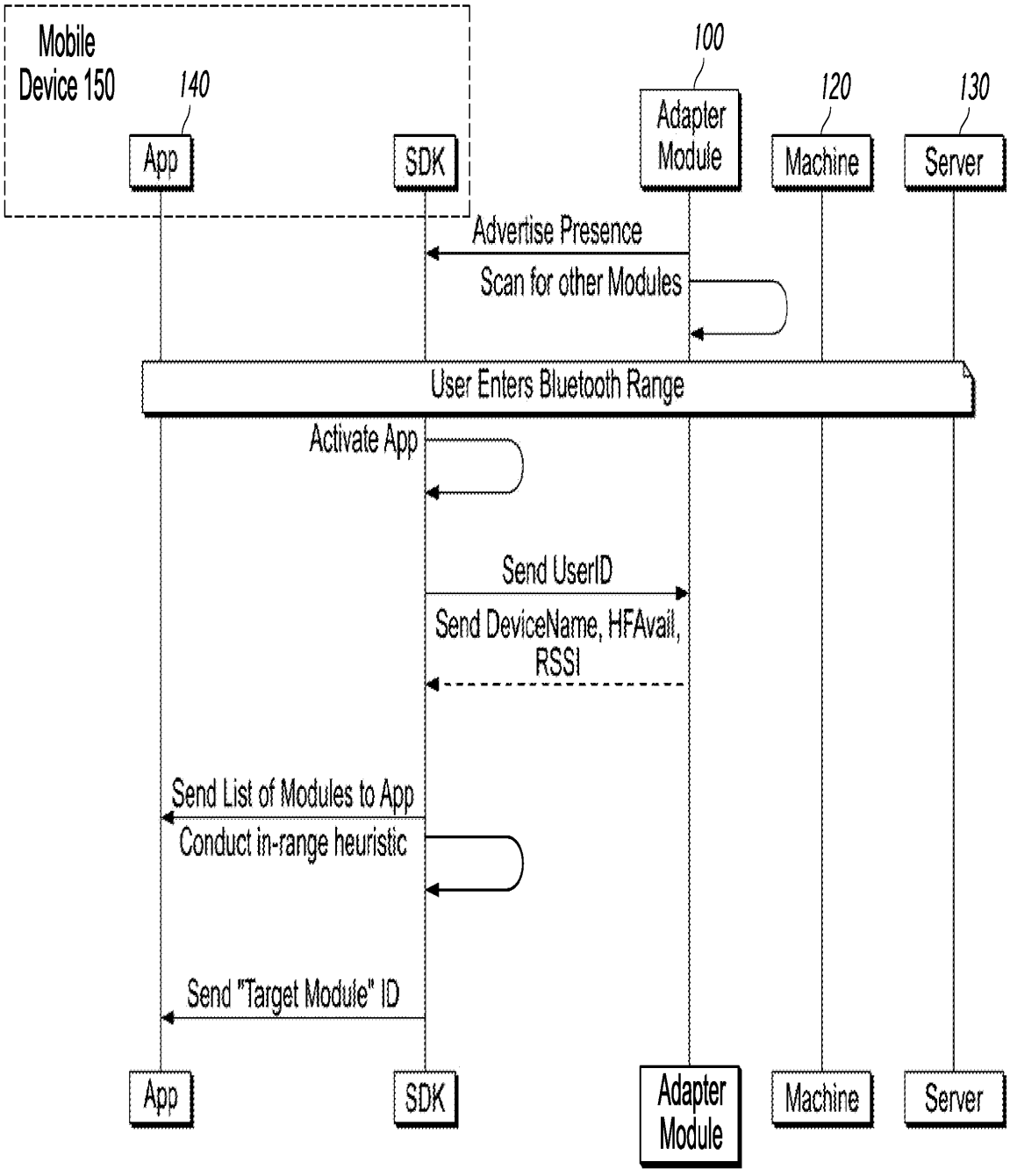

Mobile Device 150
140
App
SDK
100
Adapter Module
120
Machine
130
Server
Advertise Presence
Scan for other Modules
User Enters Bluetooth Range
Activate App
Send UserID
Send DeviceName, HFAvail, RSSI
Send List of Modules to App
Conduct in-range heuristic
Send "Target Module" ID
App
SDK
Adapter Module
Machine
Server

FIG. 8A

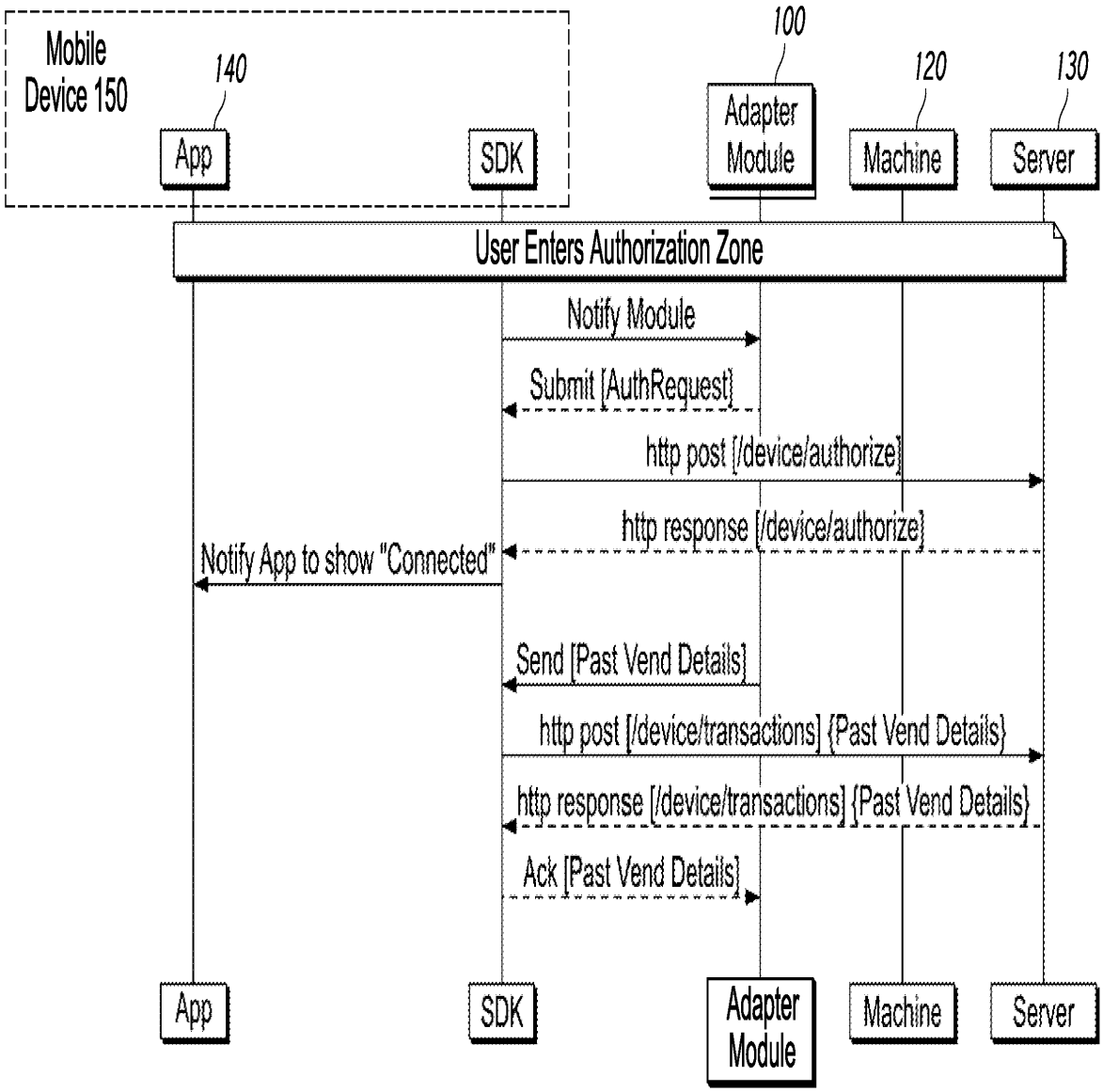

Mobile Device 150
140
100
120
130
App
SDK
Adapter Module
Machine
Server
User Enters Authorization Zone
Notify Module
Submit [AuthRequest]
http post [/device/authorize]
http response [/device/authorize]
Notify App to show "Connected"
Send [Past Vend Details]
http post [/device/transactions] {Past Vend Details}
http response [/device/transactions] {Past Vend Details}
Ack [Past Vend Details]
App
SDK
Adapter Module
Machine
Server

FIG. 8B

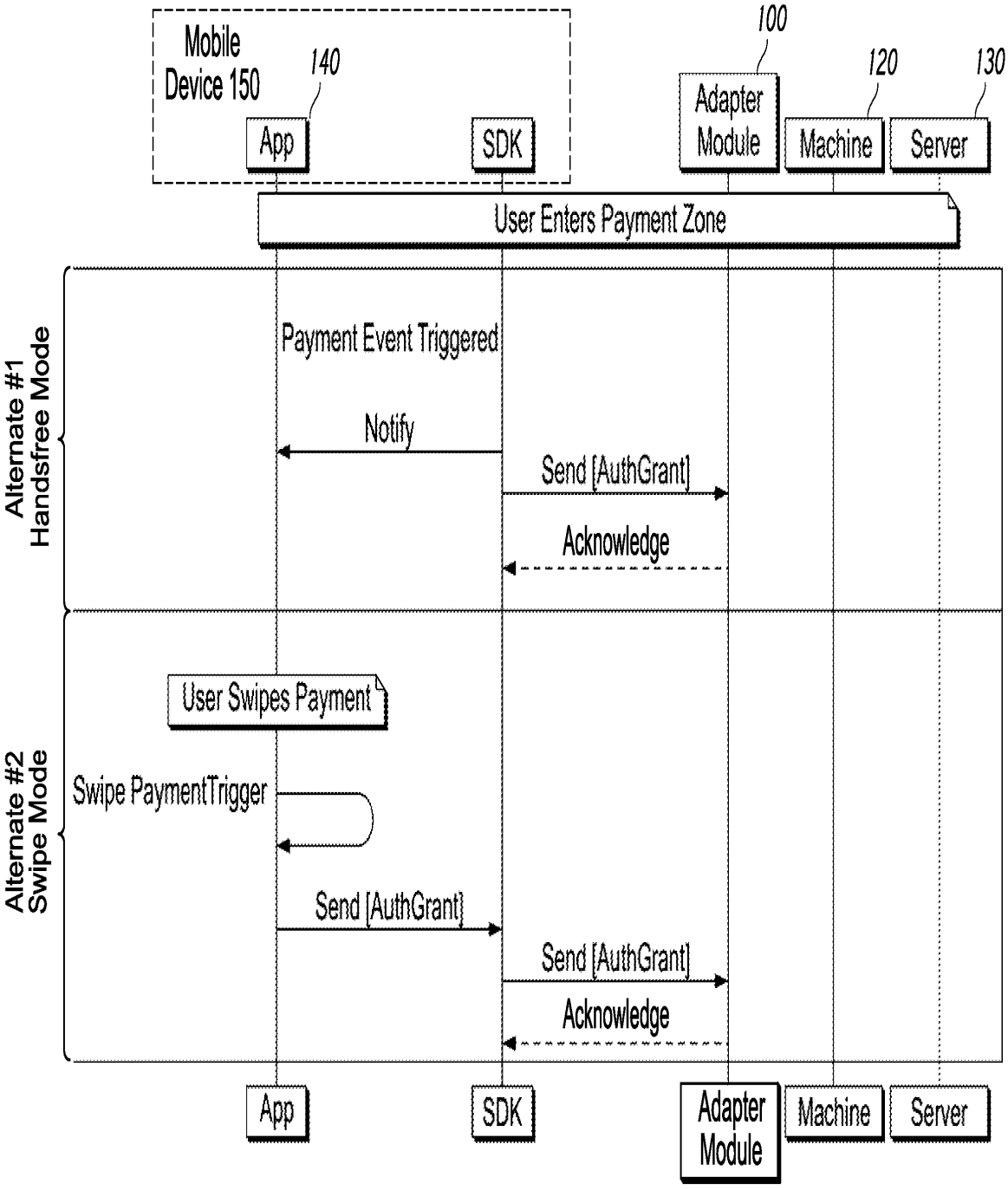

Mobile Device 150
140
App
SDK
100
Adapter Module
120
Machine
130
Server
User Enters Payment Zone
Alternate #1 Handsfree Mode
Payment Event Triggered
Notify
Send [AuthGrant]
Acknowledge
Alternate #2 Swipe Mode
User Swipes Payment
Swipe PaymentTrigger
Send [AuthGrant]
Send [AuthGrant]
Acknowledge
App
SDK
Adapter Module
Machine
Server

FIG. 8C

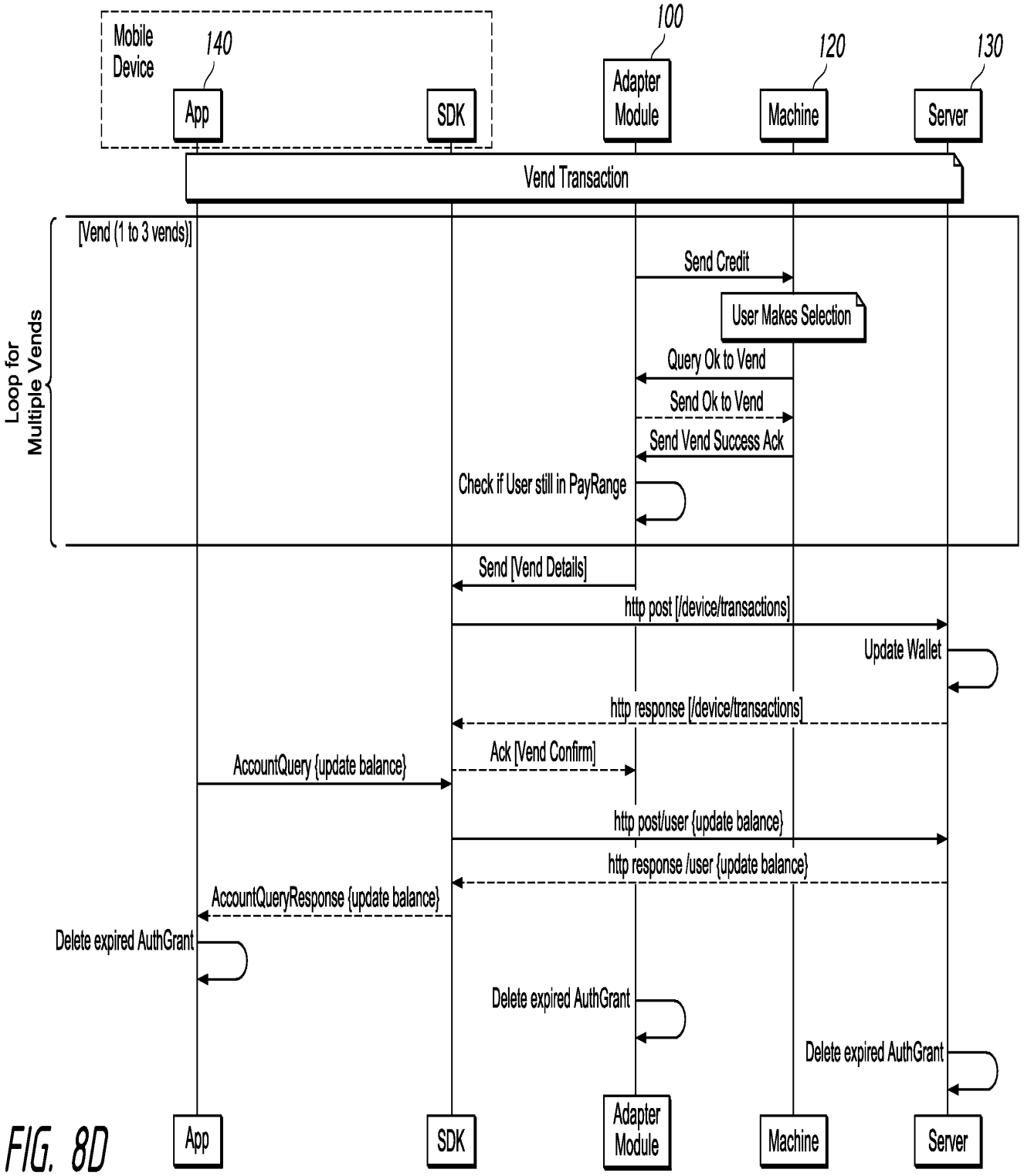

Mobile Device
140
App
SDK
100
Adapter Module
120
Machine
130
Server
Vend Transaction
Loop for Multiple Vends
[Vend (1 to 3 vends)]
Send Credit
User Makes Selection
Query Ok to Vend
Send Ok to Vend
Send Vend Success Ack
Check if User still in PayRange
Send [Vend Details]
http post [/device/transactions]
Update Wallet
http response [/device/transactions]
Ack [Vend Confirm]
AccountQuery {update balance}
http post/user {update balance}
http response /user {update balance}
AccountQueryResponse {update balance}
Delete expired AuthGrant
Delete expired AuthGrant
Delete expired AuthGrant
App
SDK
Adapter Module
Machine
Server

FIG. 8D

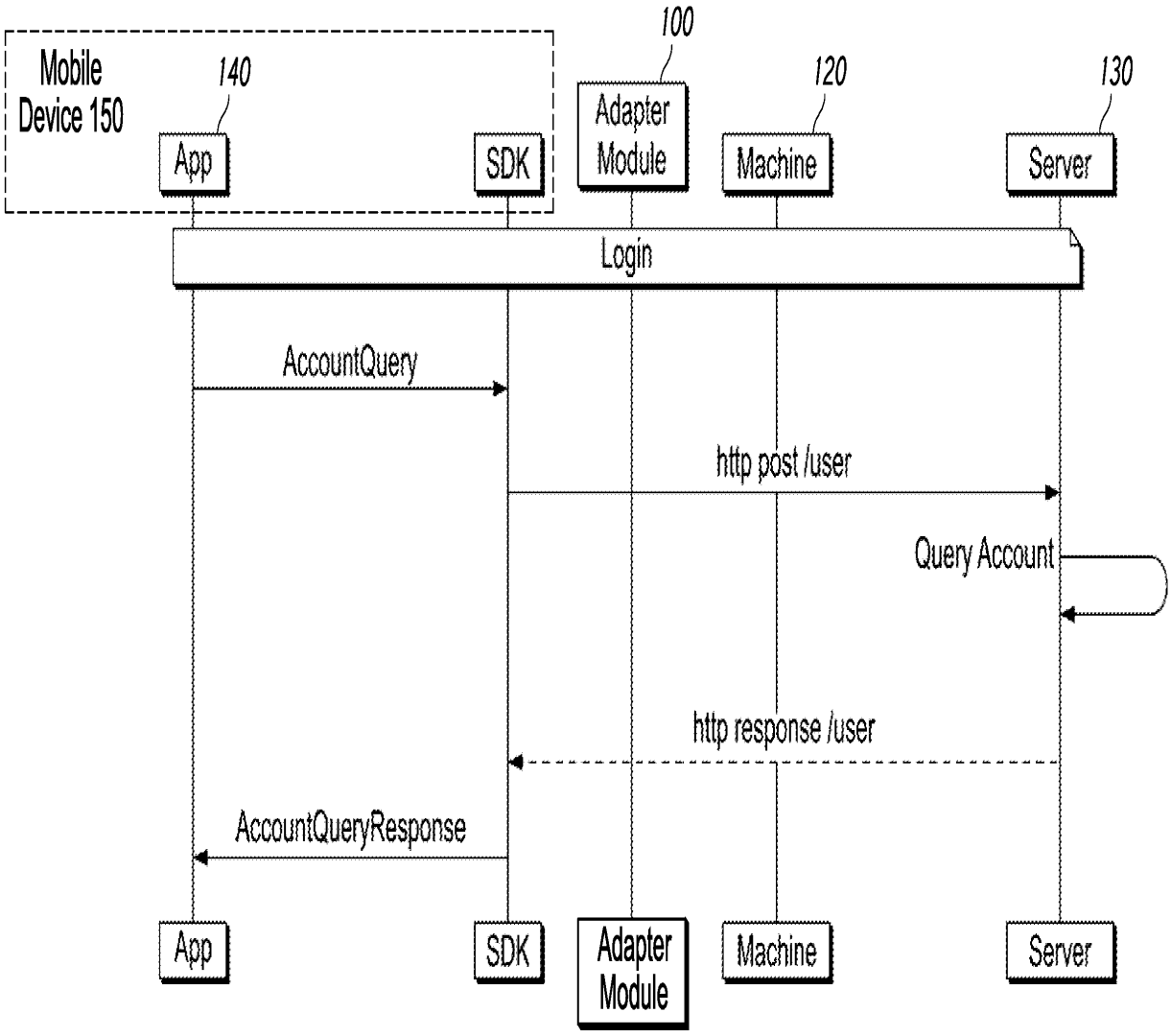

Mobile
Device 150
140
100
120
130
App
SDK
Adapter
Module
Machine
Server
Login
AccountQuery
http post /user
Query Account
http response /user
AccountQueryResponse
App
SDK
Adapter
Module
Machine
Server

FIG. 8E

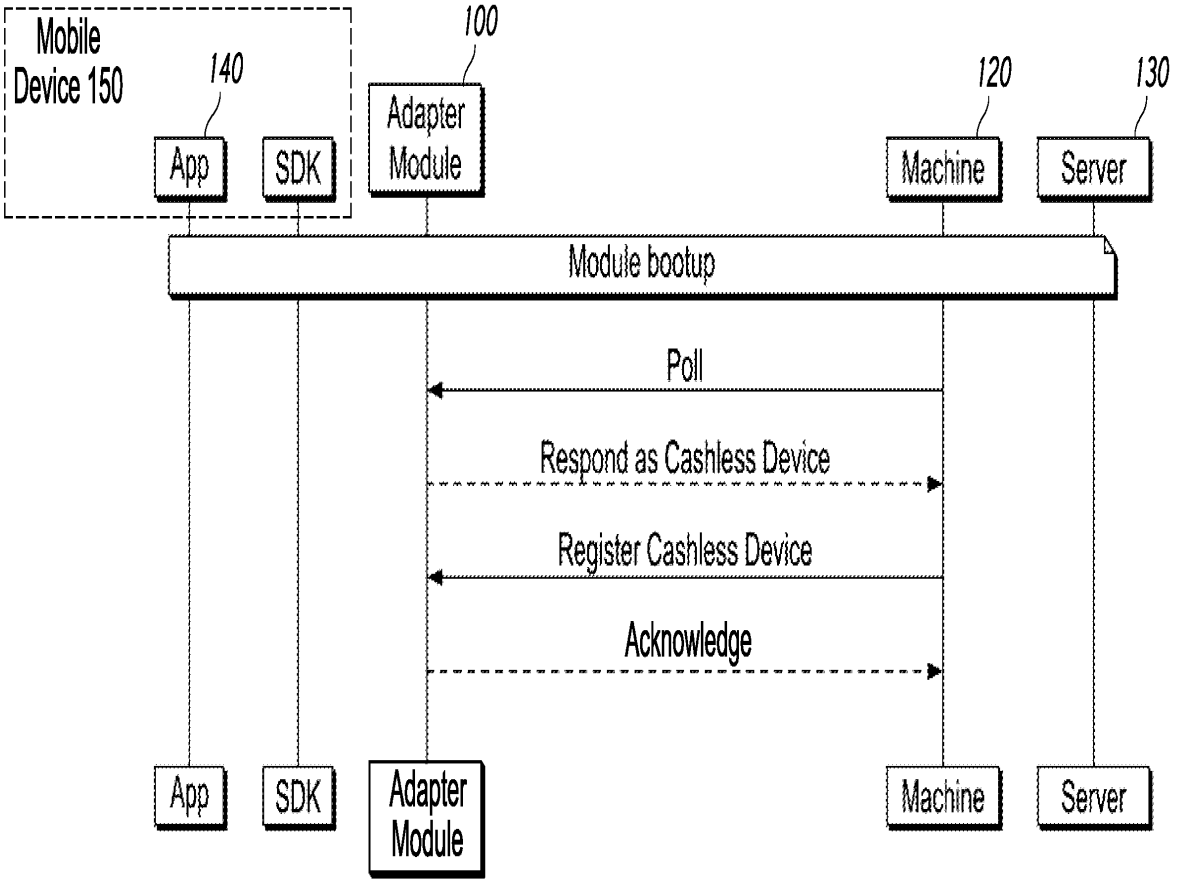

Mobile
Device 150
140
100
120
130
App
SDK
Adapter
Module
Machine
Server
Module bootup
Poll
Respond as Cashless Device
Register Cashless Device
Acknowledge
App
SDK
Adapter
Module
Machine
Server

FIG. 8F

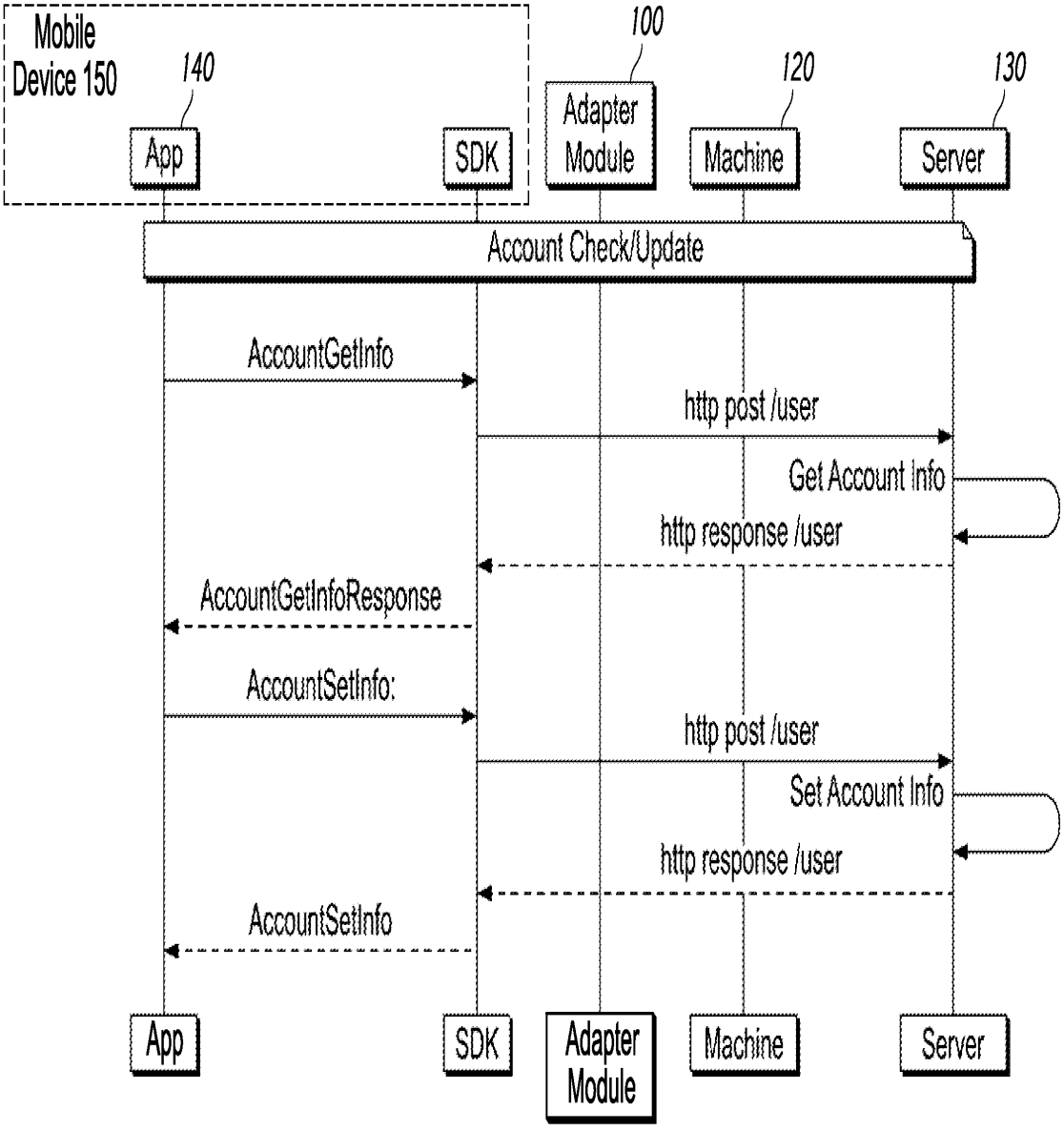

Mobile
Device 150
140
100
120
130
App
SDK
Adapter
Module
Machine
Server
Account Check/Update
AccountGetInfo
http post /user
Get Account Info
http response /user
AccountGetInfoResponse
AccountSetInfo:
http post /user
Set Account Info
http response /user
AccountSetInfo
App
SDK
Adapter
Module
Machine
Server

FIG. 8G

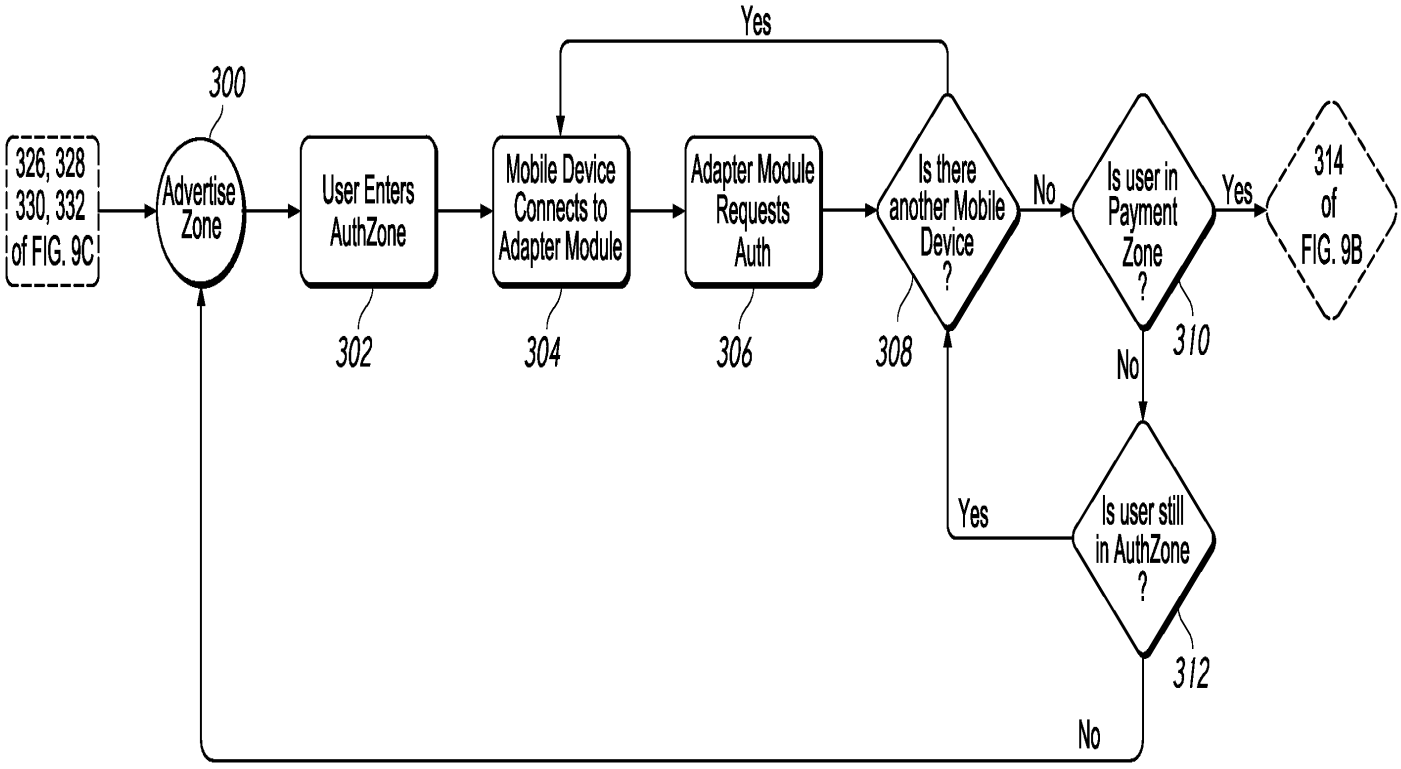

326, 328
330, 332
of FIG. 9C
Advertise Zone
300
User Enters AuthZone
302
Mobile Device Connects to Adapter Module
304
Adapter Module Requests Auth
306
Is there another Mobile Device ?
308
Yes
No
Is user in Payment Zone ?
310
Yes
314
of
FIG. 9B
No
Is user still in AuthZone ?
312
Yes
No

FIG. 9A

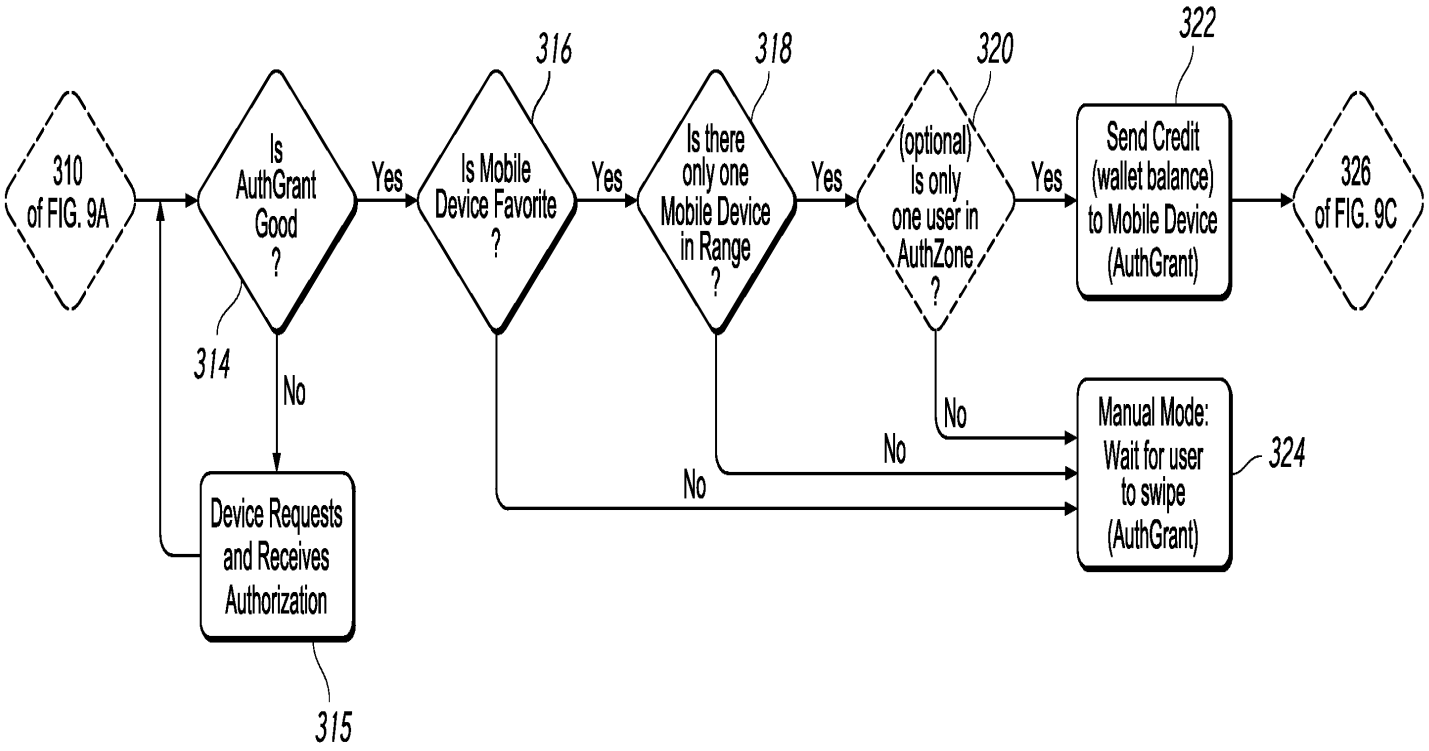
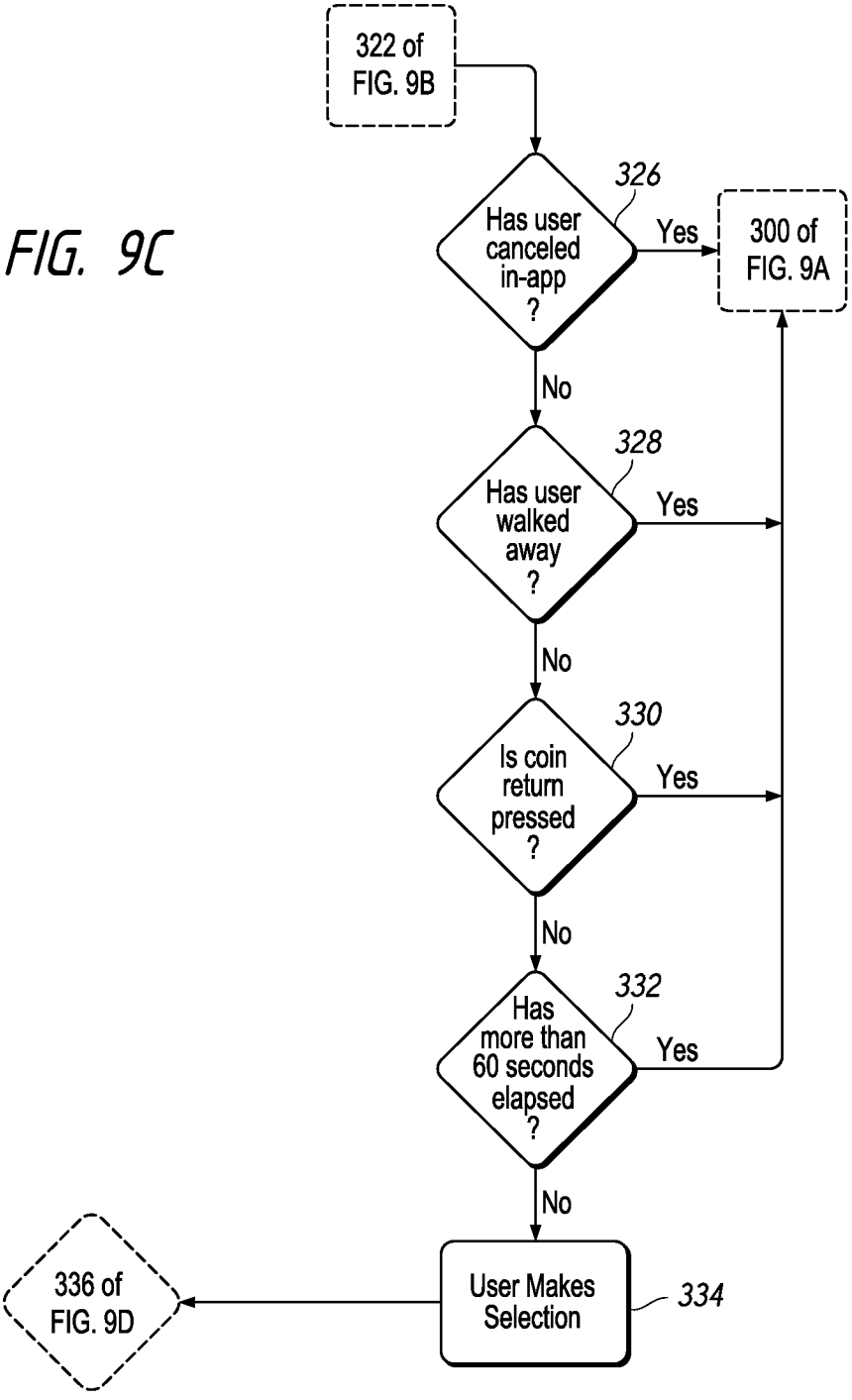

310 of FIG. 9A
Is AuthGrant Good ?
314
Yes
No
Device Requests and Receives Authorization
315
316
Is Mobile Device Favorite ?
Yes
318
Is there only one Mobile Device in Range ?
Yes
320
(optional) Is only one user in AuthZone ?
Yes
322
Send Credit (wallet balance) to Mobile Device (AuthGrant)
326 of FIG. 9C
No
No
No
Manual Mode: Wait for user to swipe (AuthGrant)
324

FIG. 9B

FIG. 9C


322 of FIG. 9B
326
Has user canceled in-app ?
Yes
300 of FIG. 9A
No
328
Has user walked away ?
Yes
No
330
Is coin return pressed ?
Yes
No
332
Has more than 60 seconds elapsed ?
Yes
No
User Makes Selection
334
336 of FIG. 9D

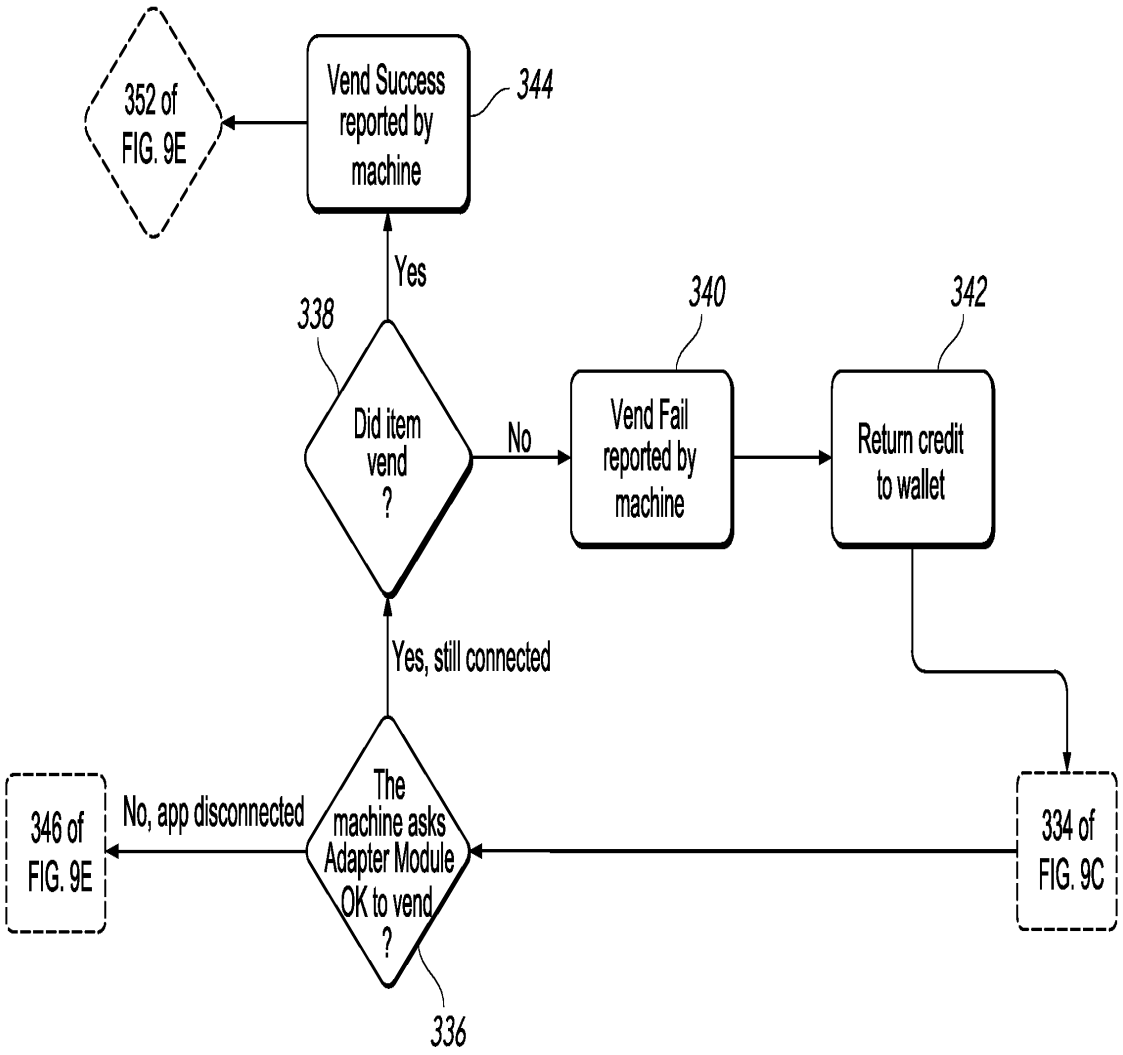

352 of FIG. 9E
Vend Success reported by machine
344
Yes
338
Did item vend ?
No
340
Vend Fail reported by machine
342
Return credit to wallet
Yes, still connected
346 of FIG. 9E
No, app disconnected
The machine asks Adapter Module OK to vend ?
336
334 of FIG. 9C

FIG. 9D

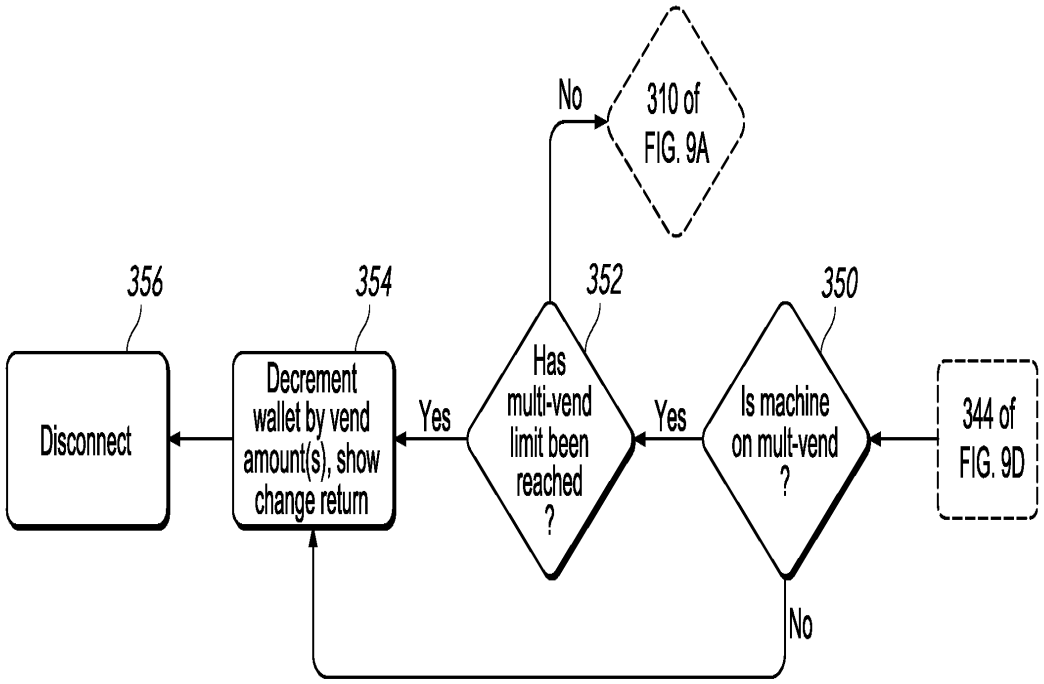

No
310 of FIG. 9A
356
354
352
350
Disconnect
Decrement wallet by vend amount(s), show change return
Yes
Has multi-vend limit been reached ?
Yes
Is machine on mult-vend ?
344 of FIG. 9D
No

FIG. 9E

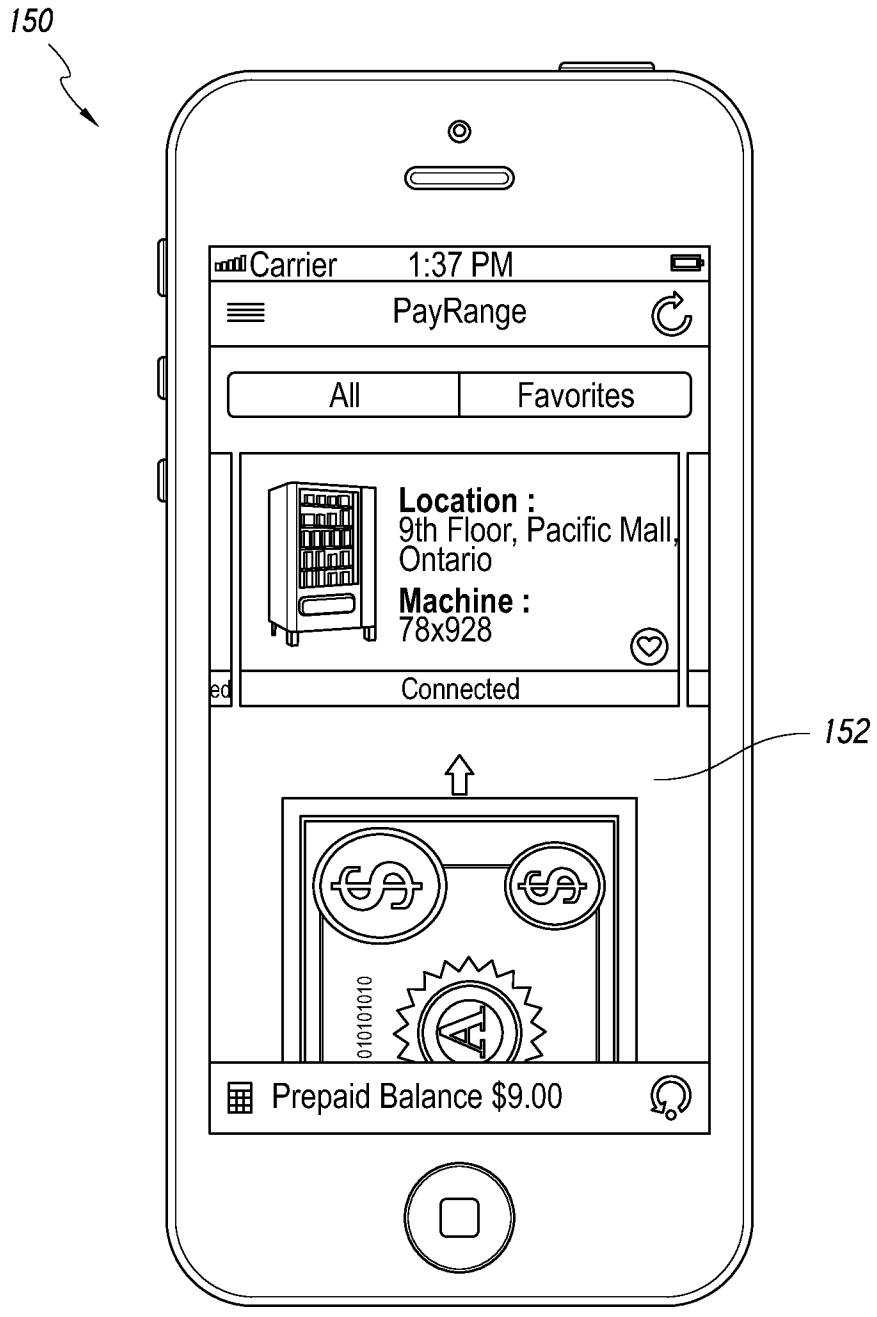

150
Carrier
1:37 PM
PayRange
All
Favorites
Location :
9th Floor, Pacific Mall, Ontario
Machine :
78x928
Connected
152
Prepaid Balance $9.00

FIG. 10A

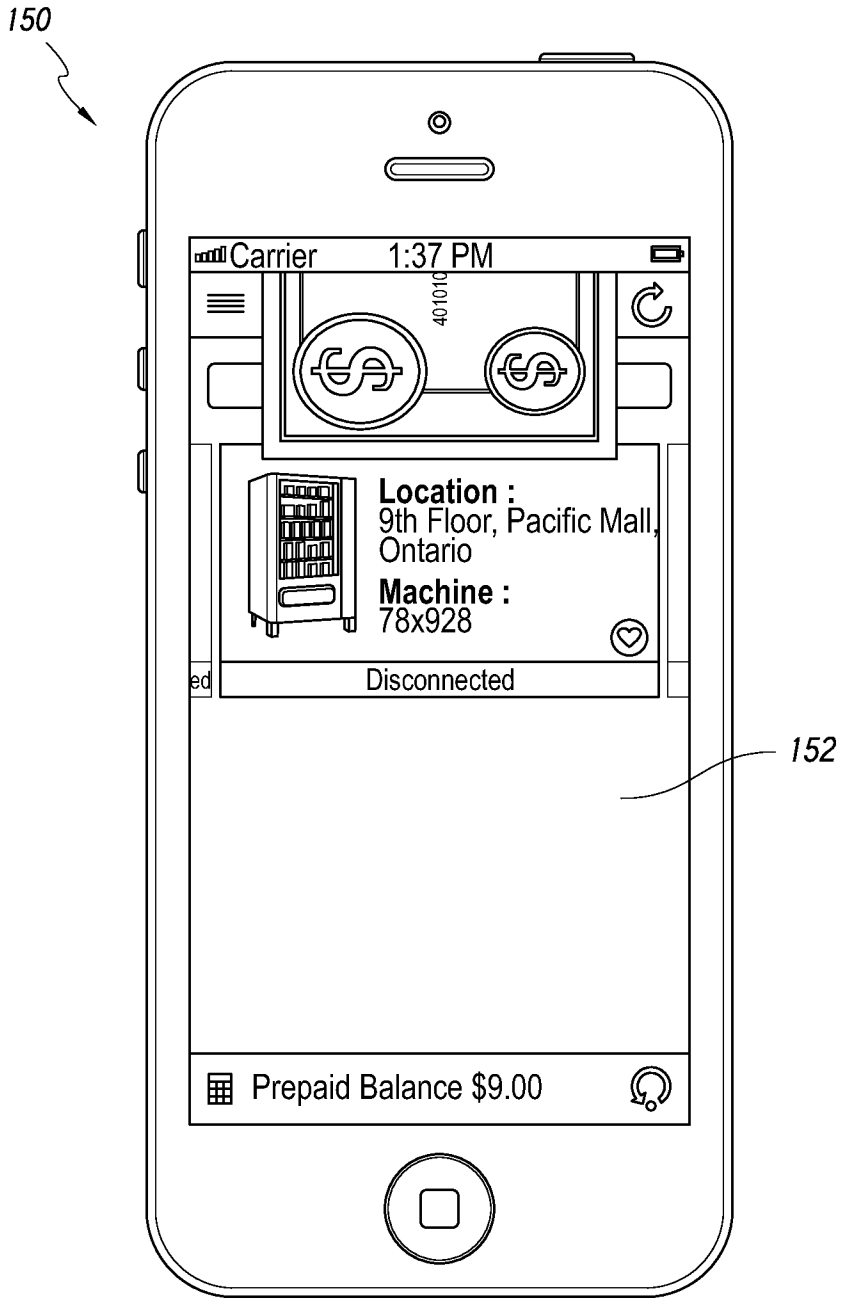

150
Carrier
1:37 PM
401010
Location :
9th Floor, Pacific Mall,
Ontario
Machine :
78x928
ed
Disconnected
152
Prepaid Balance $9.00

FIG. 10B

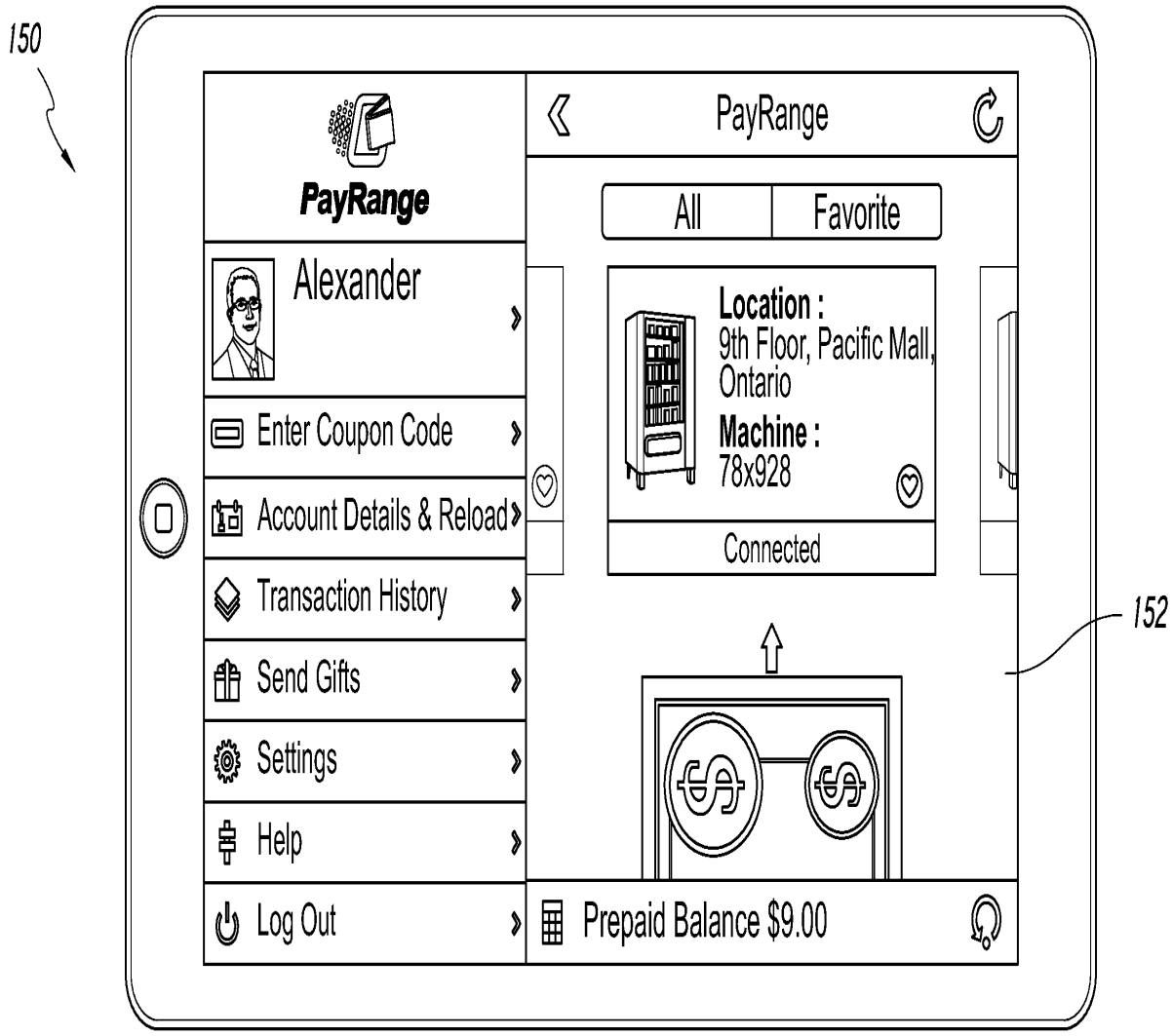

150
PayRange
Alexander
Enter Coupon Code
Account Details & Reload
Transaction History
Send Gifts
Settings
Help
Log Out
PayRange
All
Favorite
Location :
9th Floor, Pacific Mall, Ontario
Machine :
78x928
Connected
Prepaid Balance $9.00
152

FIG. 10C

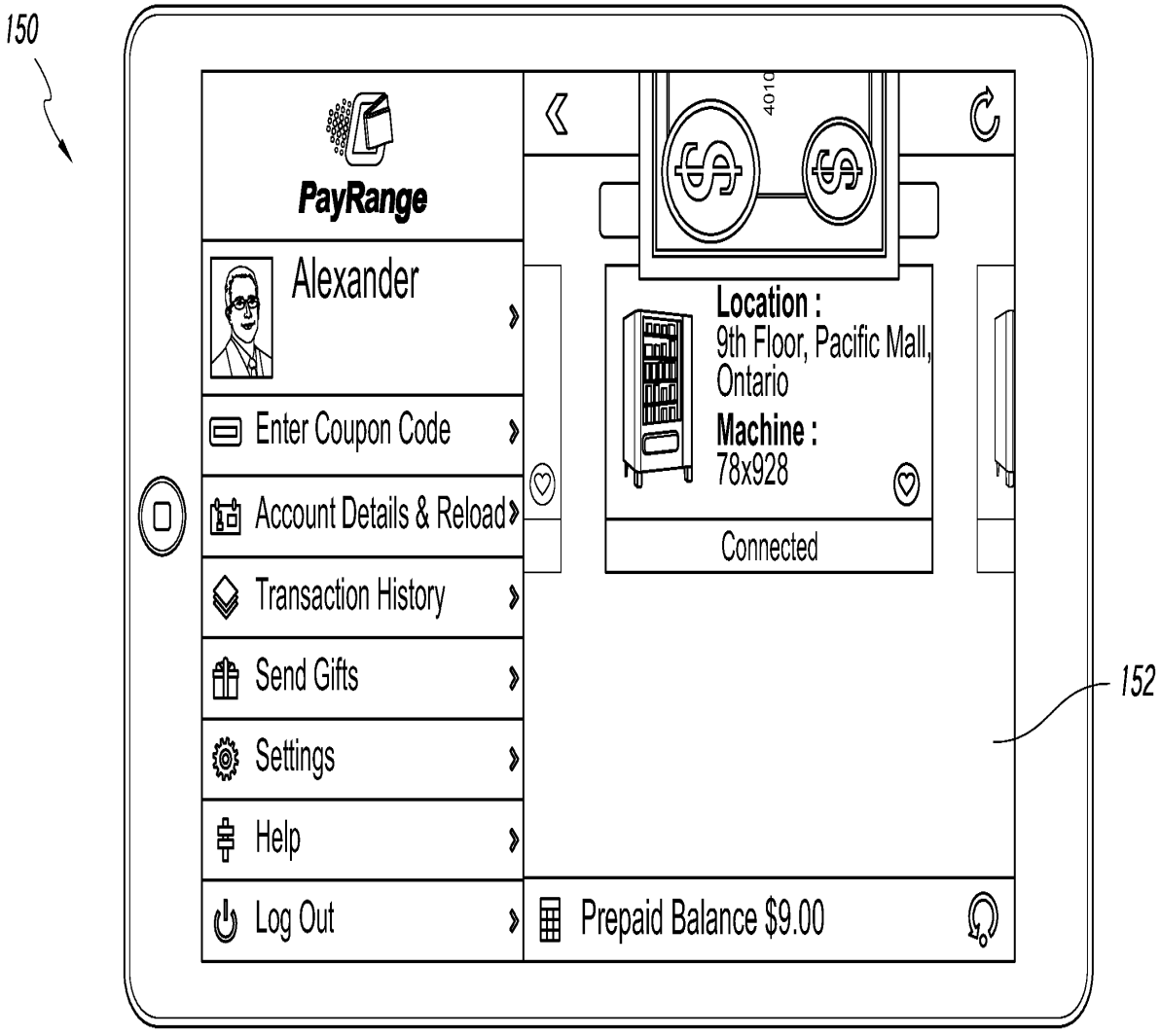

150
PayRange
Alexander
Enter Coupon Code
Account Details & Reload
Transaction History
Send Gifts
Settings
Help
Log Out
Location :
9th Floor, Pacific Mall, Ontario
Machine :
78x928
Connected
Prepaid Balance $9.00
152

FIG. 10D

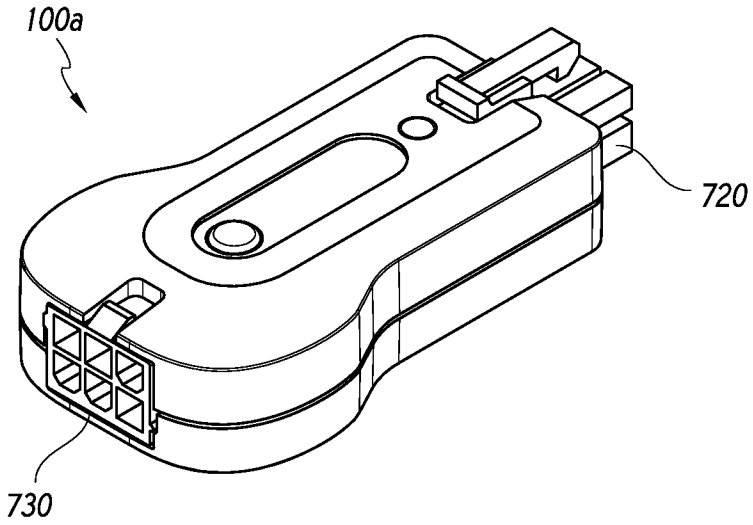


FIG. 11

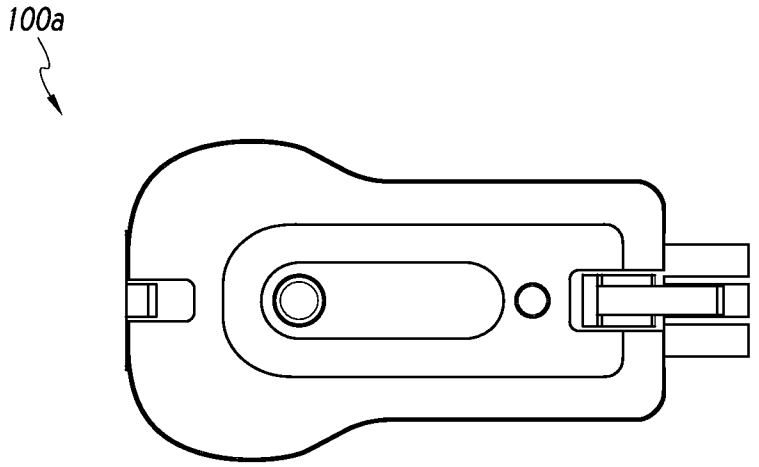


FIG. 12

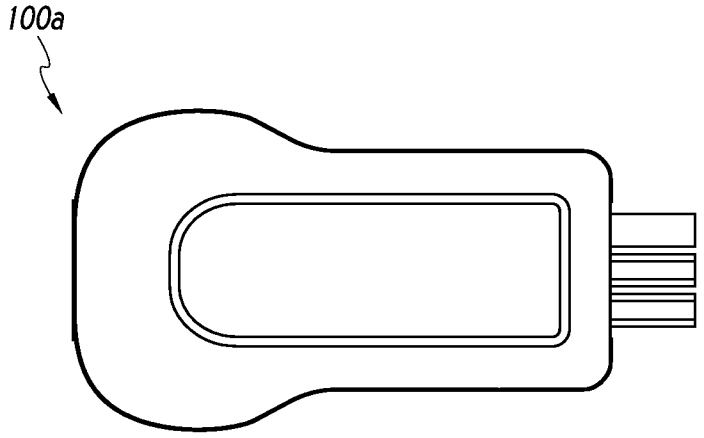


FIG. 13

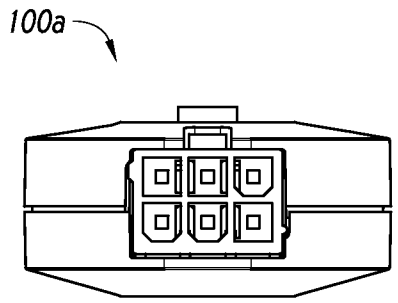


FIG. 15

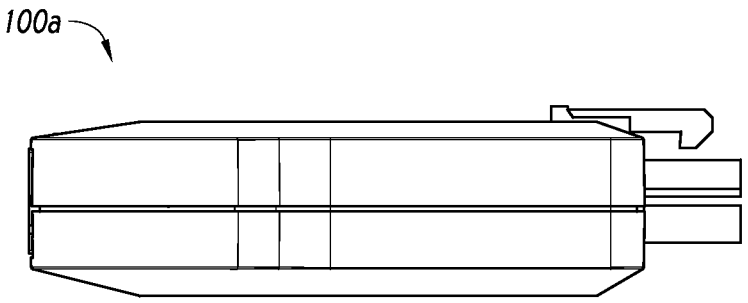


FIG. 14

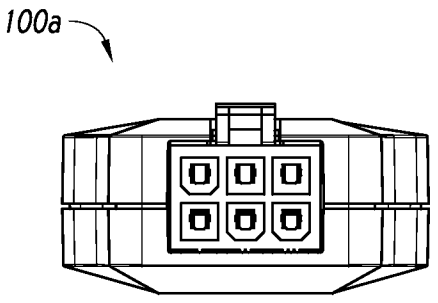


FIG. 16

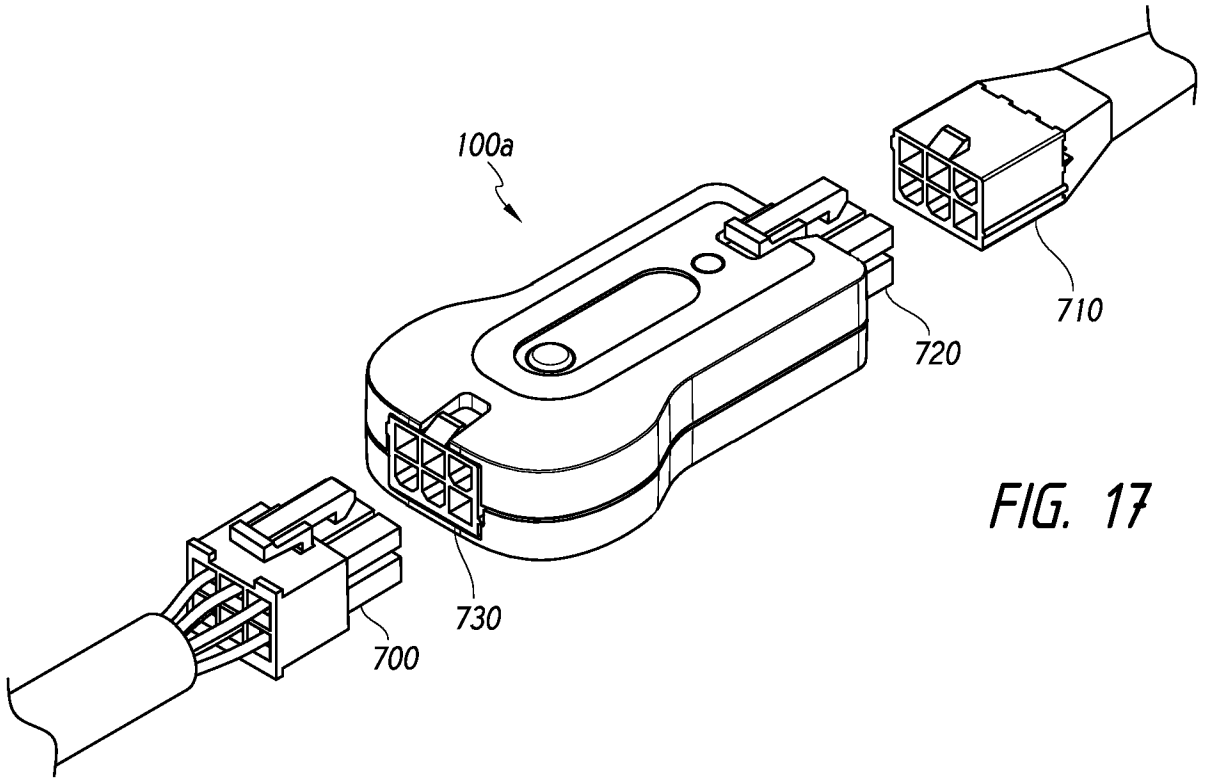


FIG. 17

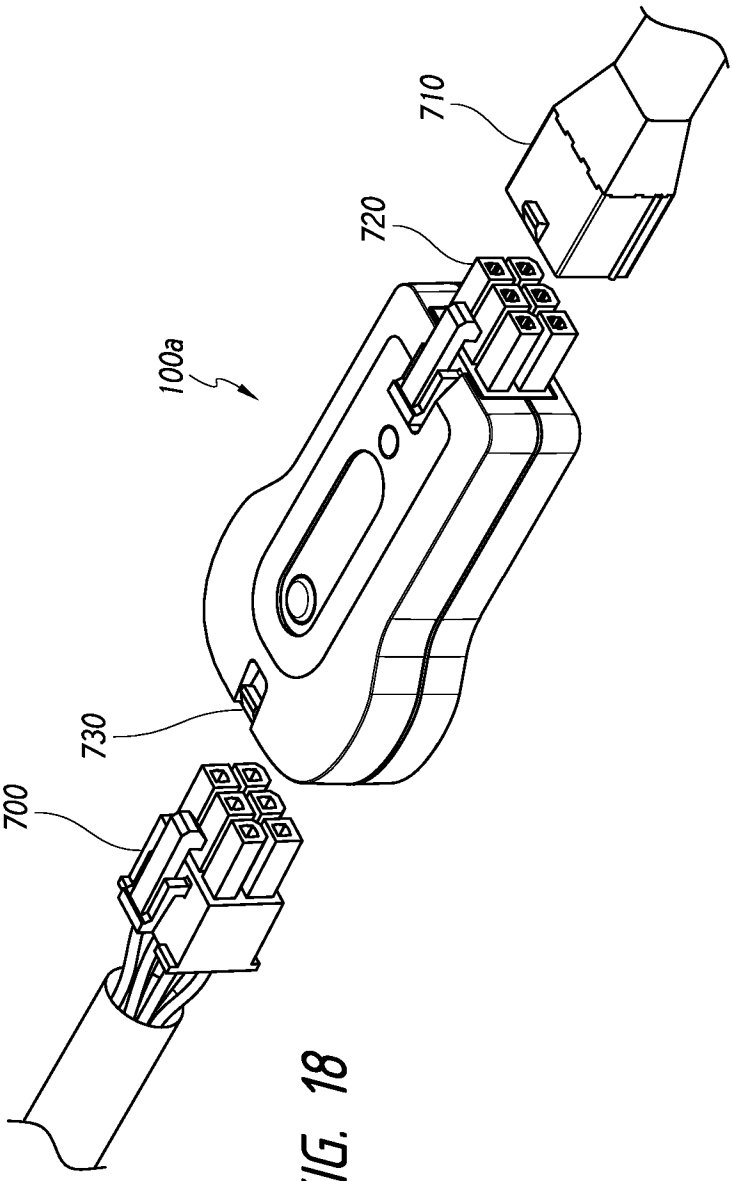


FIG. 18

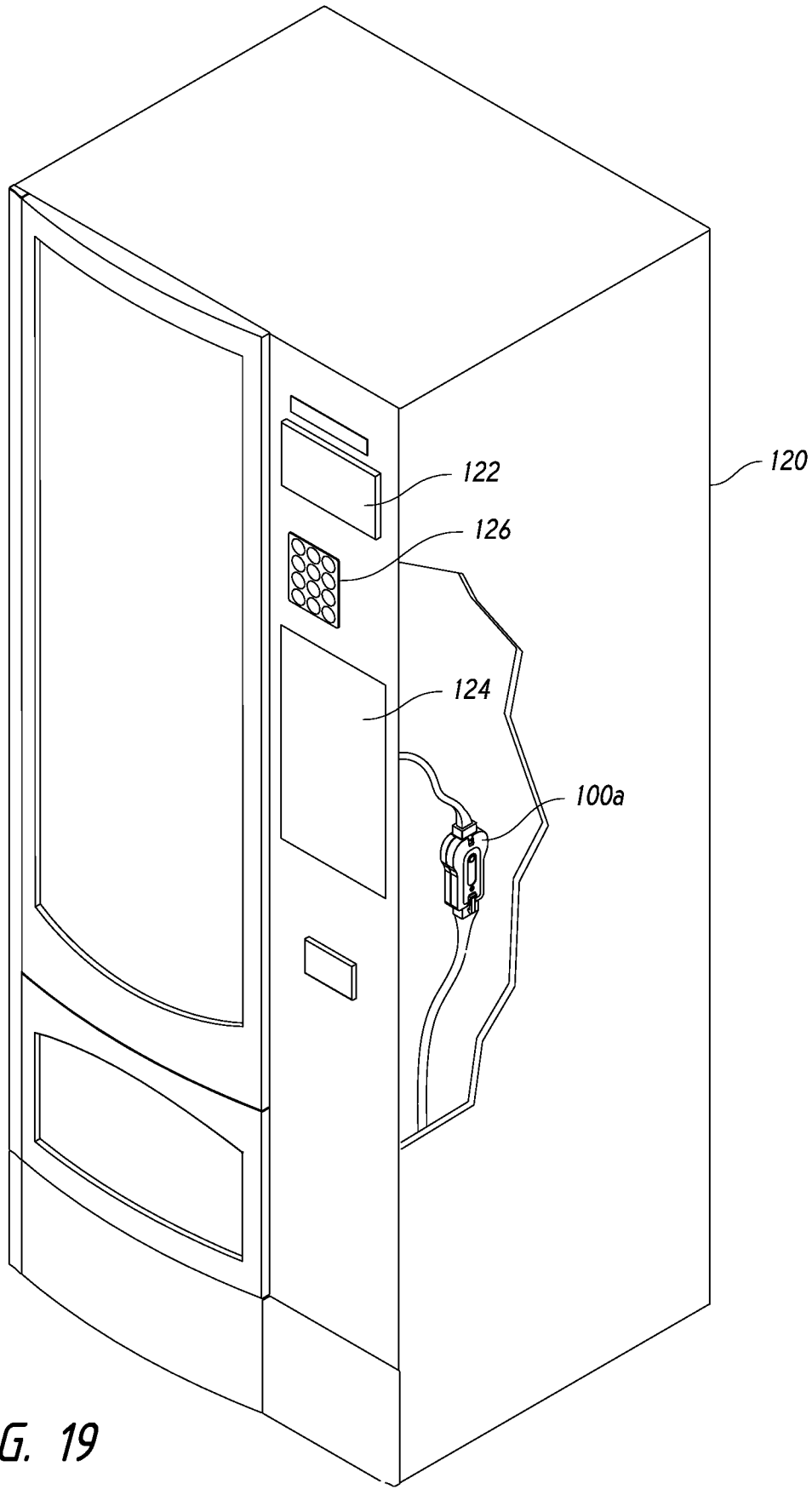


FIG. 19

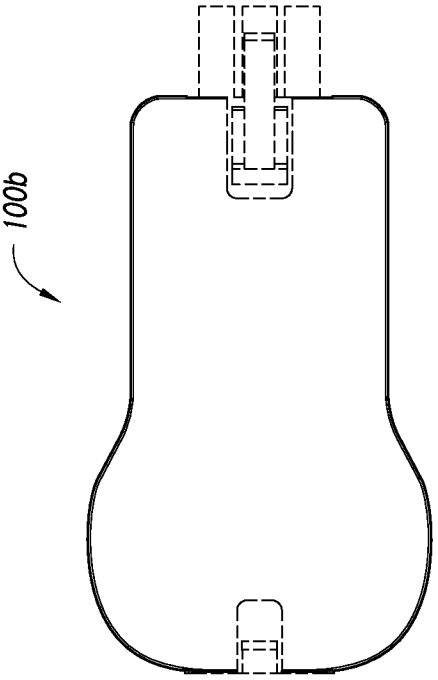


FIG. 21

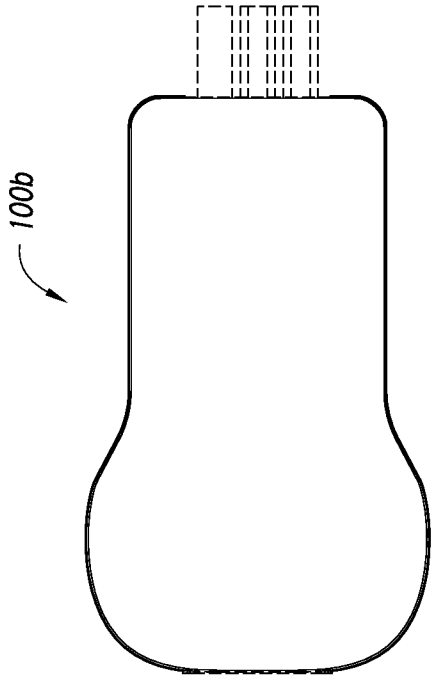


FIG. 22

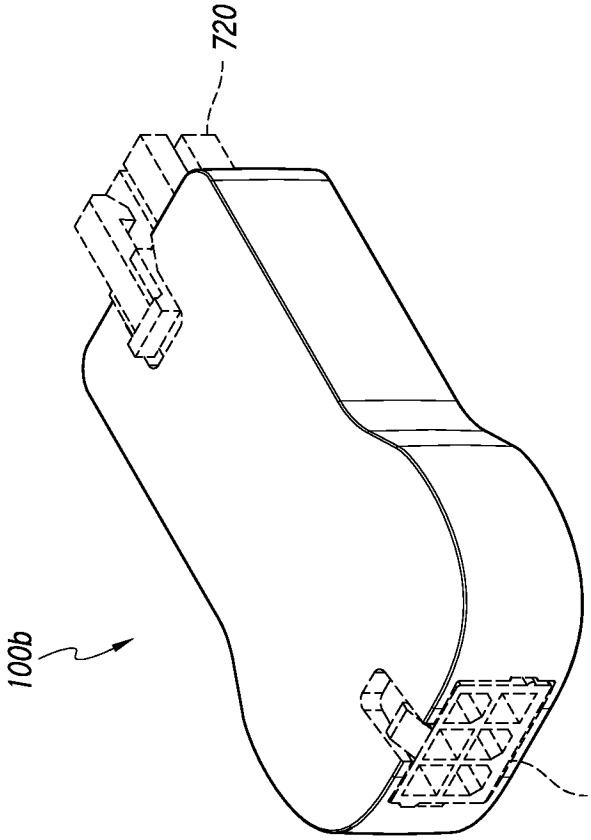


FIG. 20

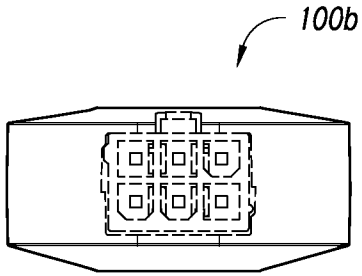


FIG. 24

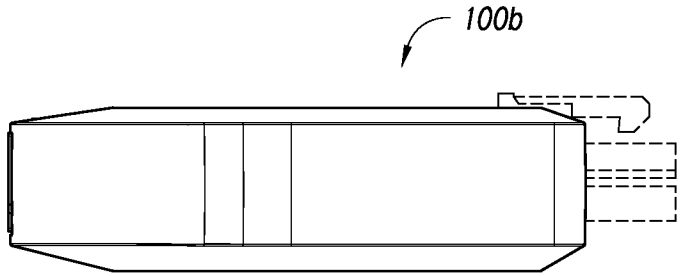


FIG. 23

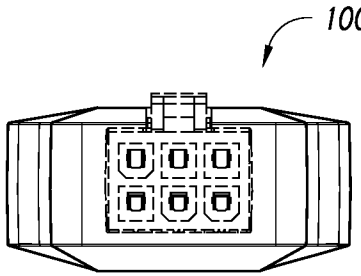


FIG. 25

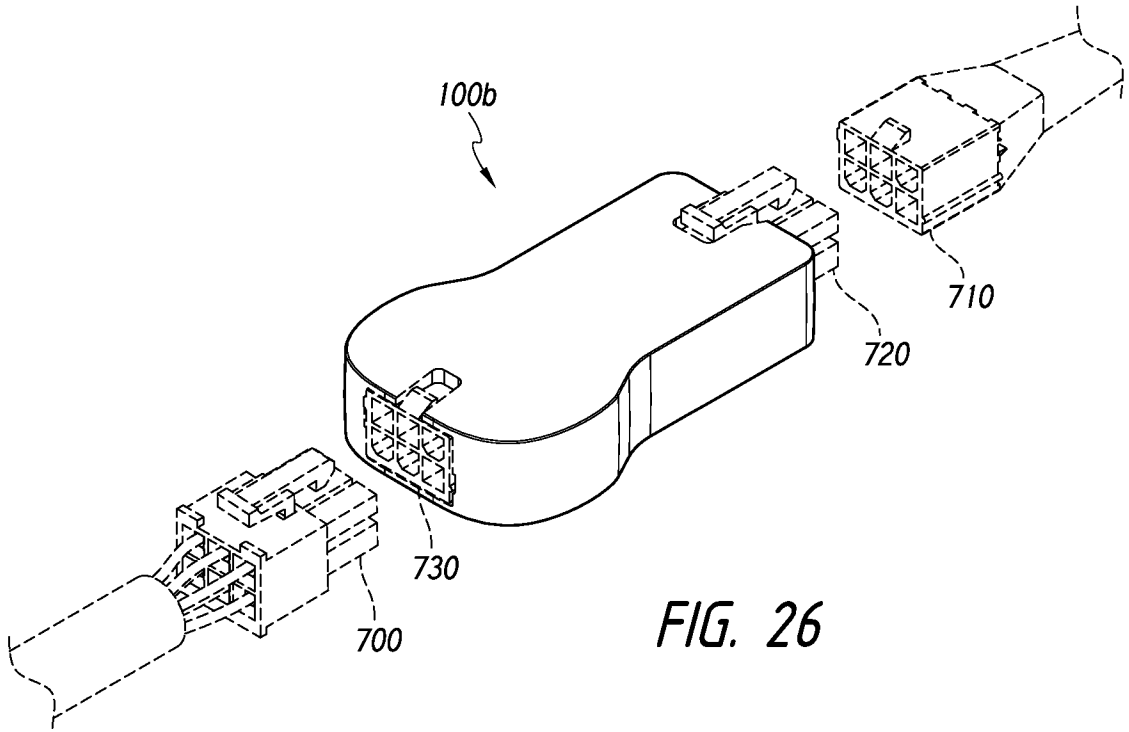


FIG. 26

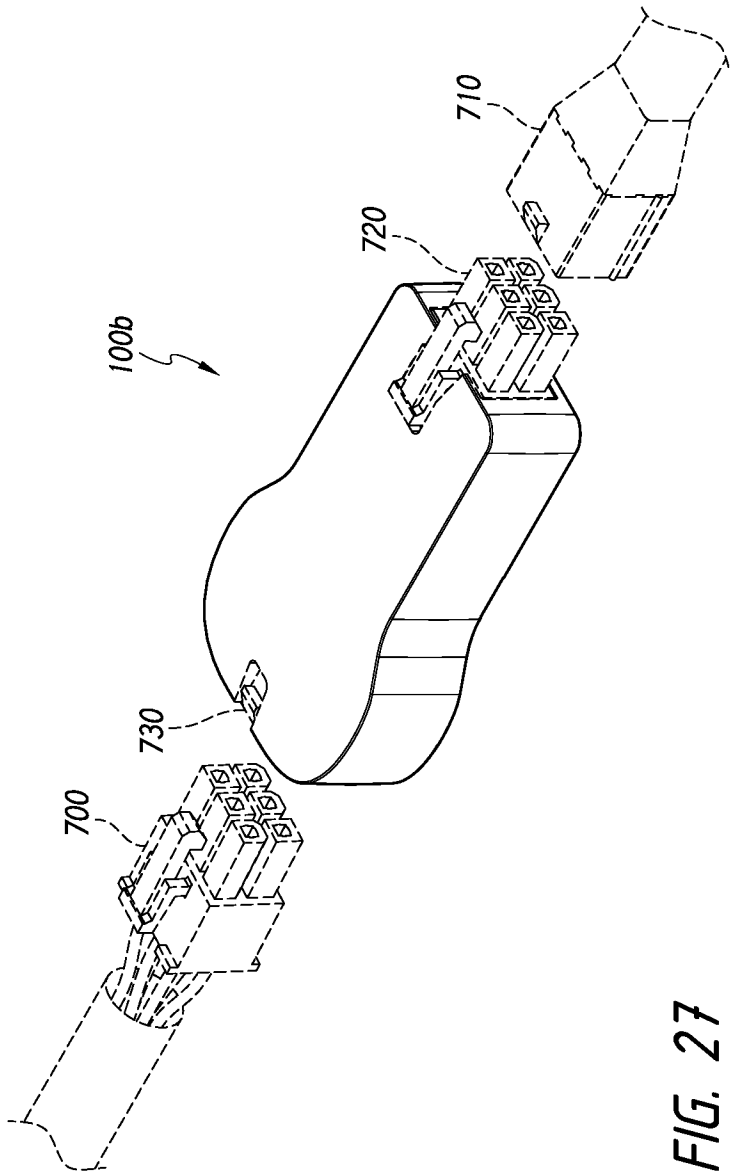


FIG. 27

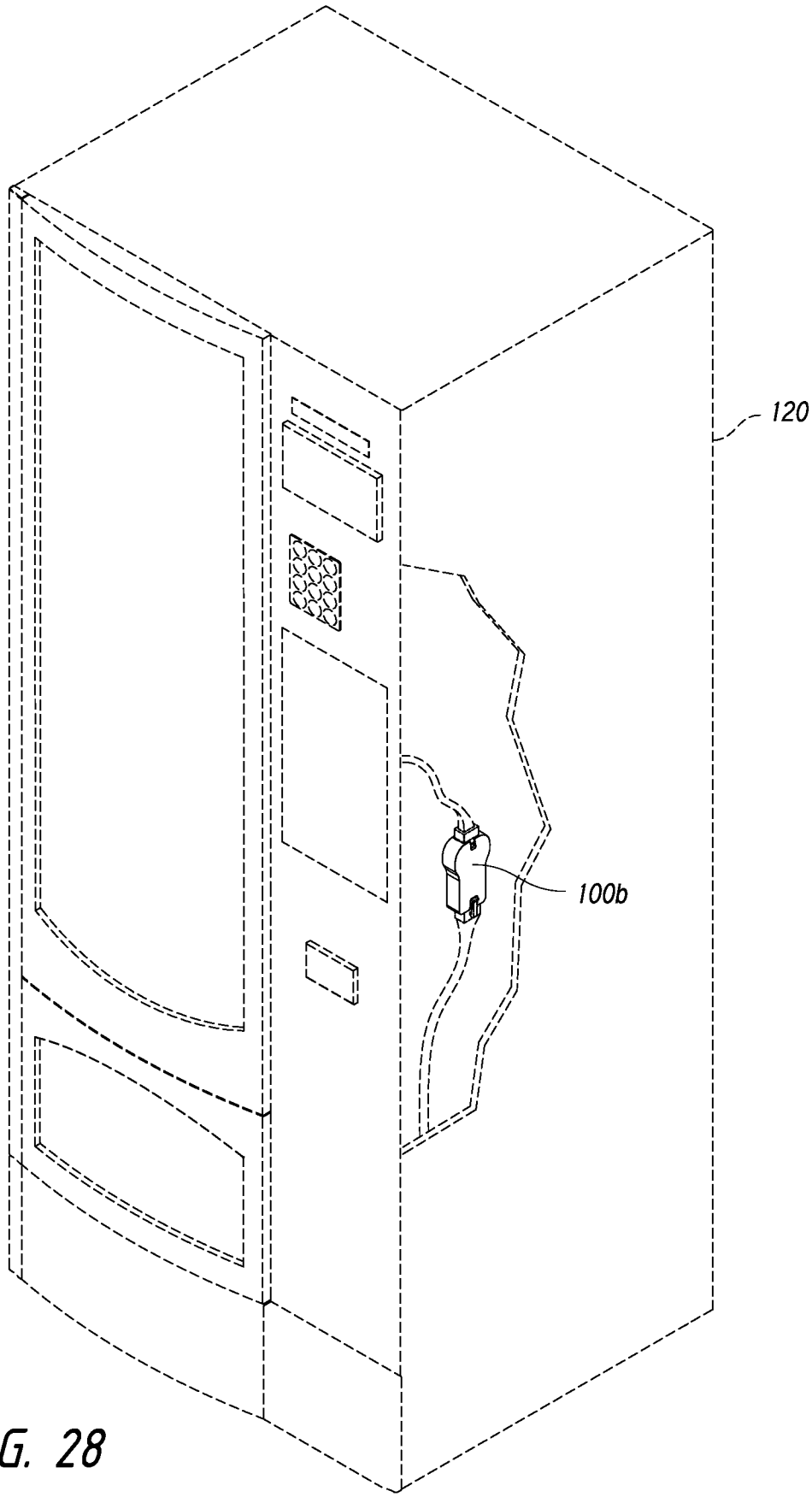


FIG. 28

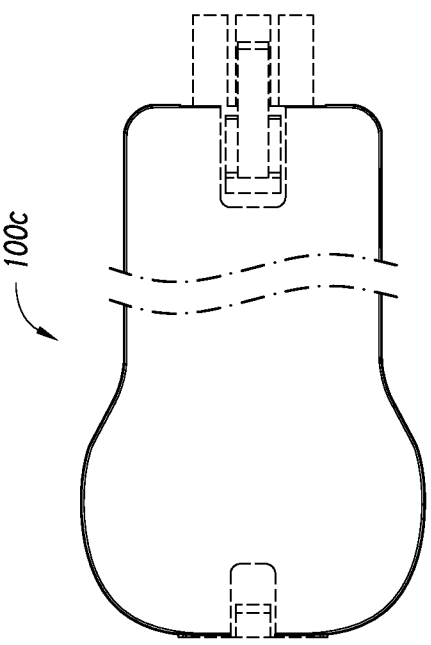


FIG. 30

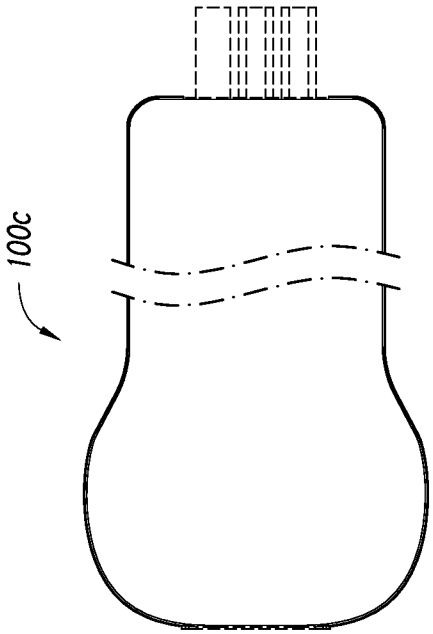


FIG. 31

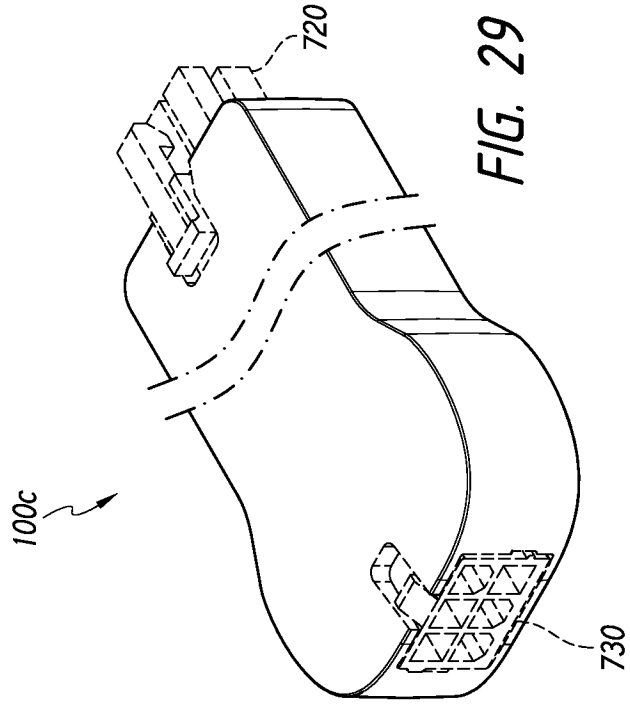


FIG. 29

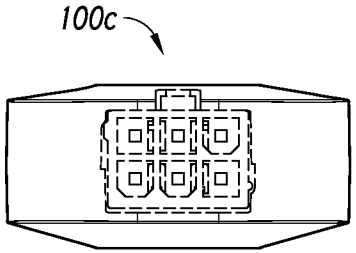


FIG. 33

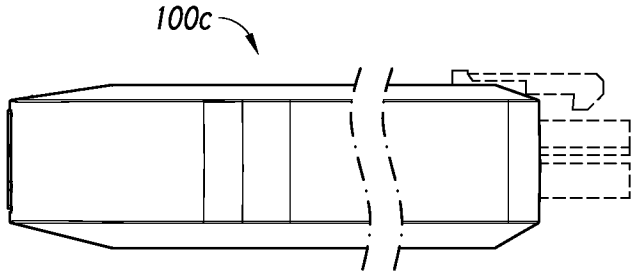


FIG. 32

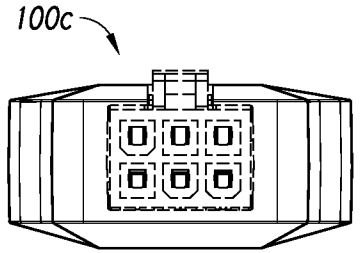


FIG. 34

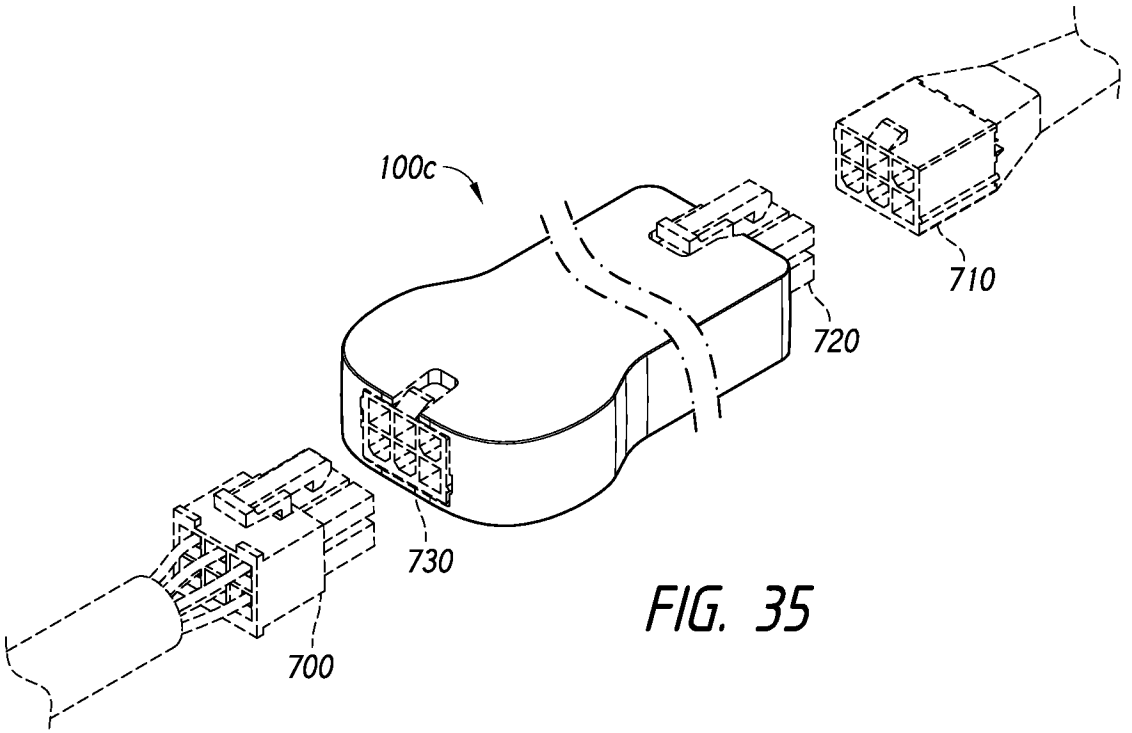


FIG. 35

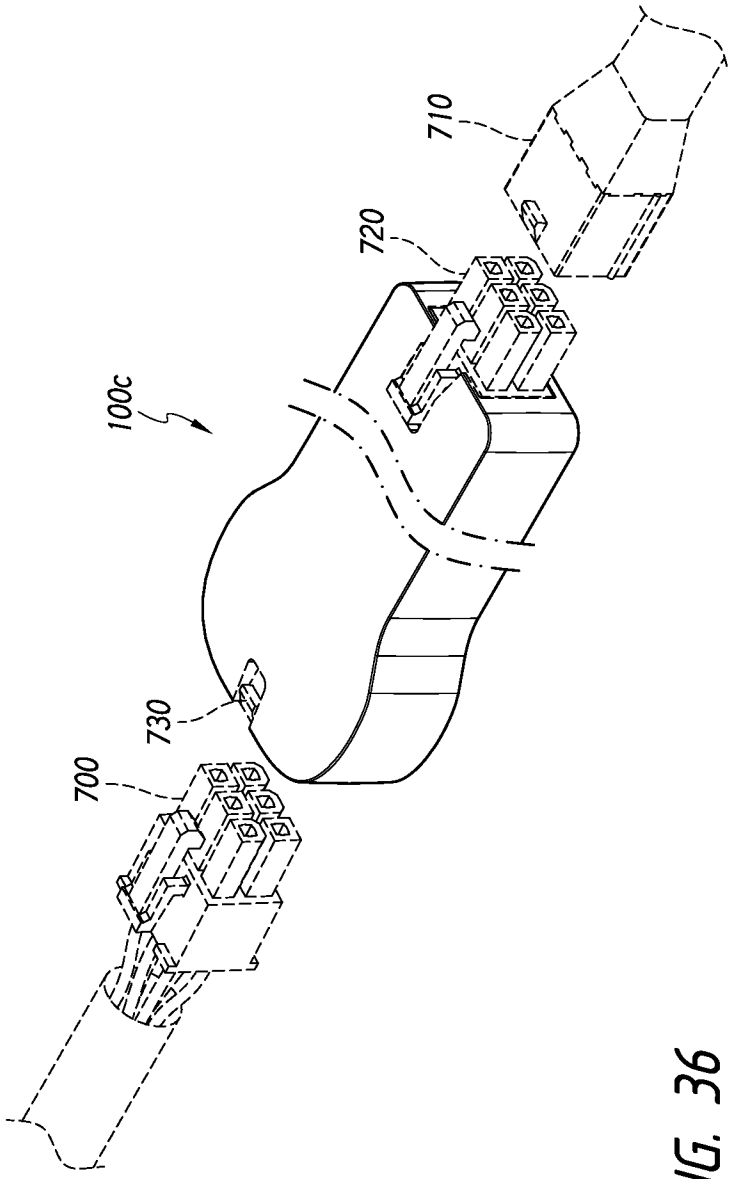


FIG. 36

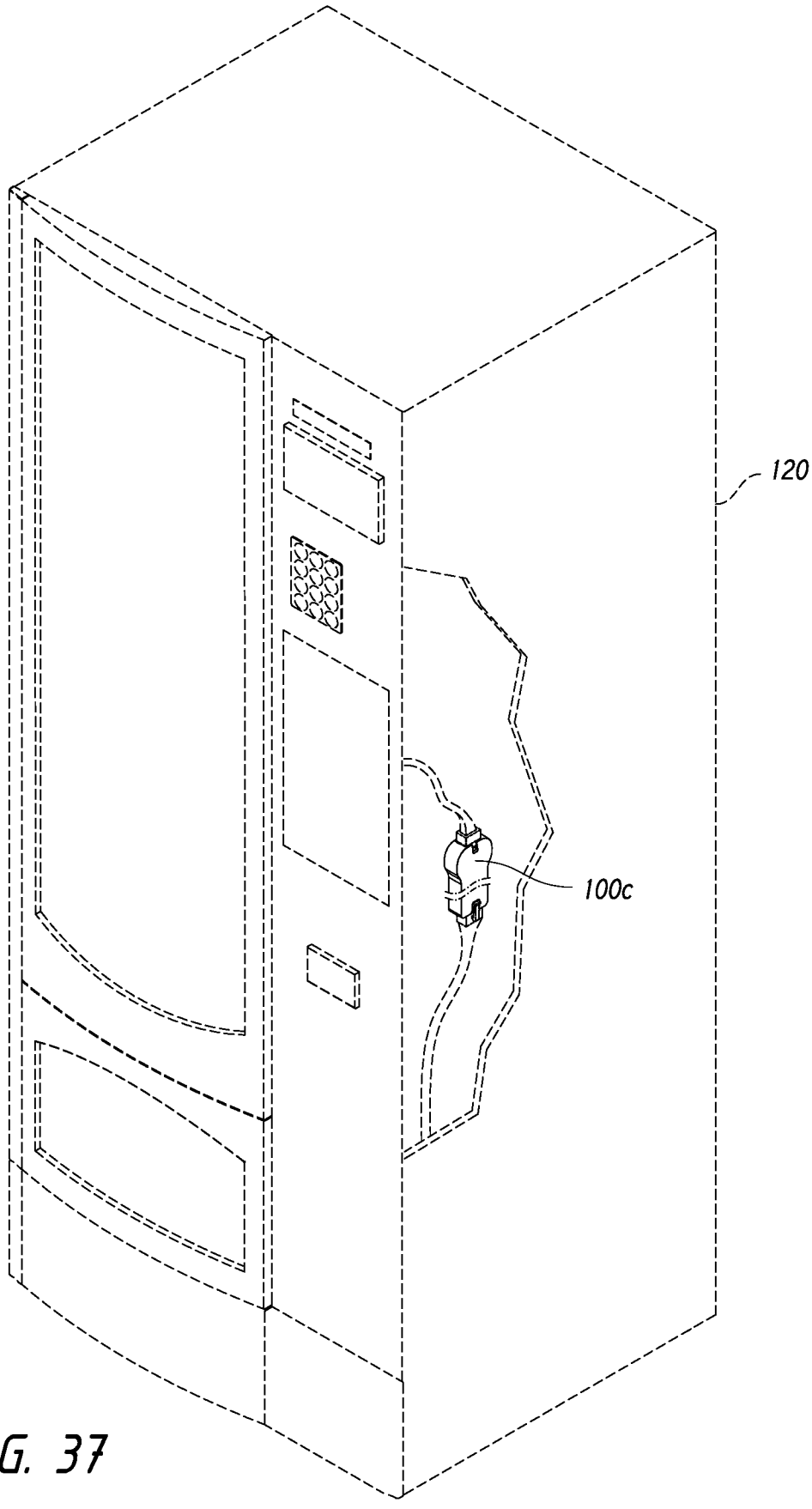


FIG. 37

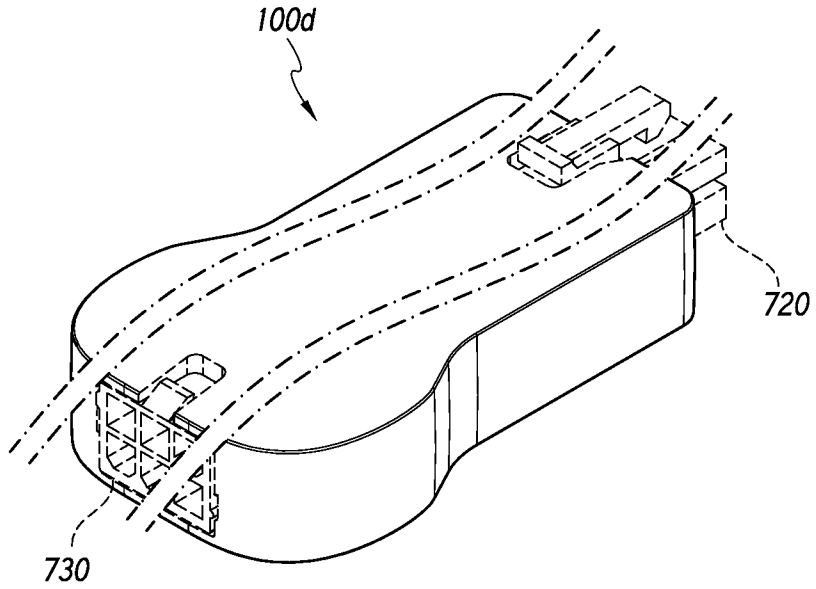


FIG. 38

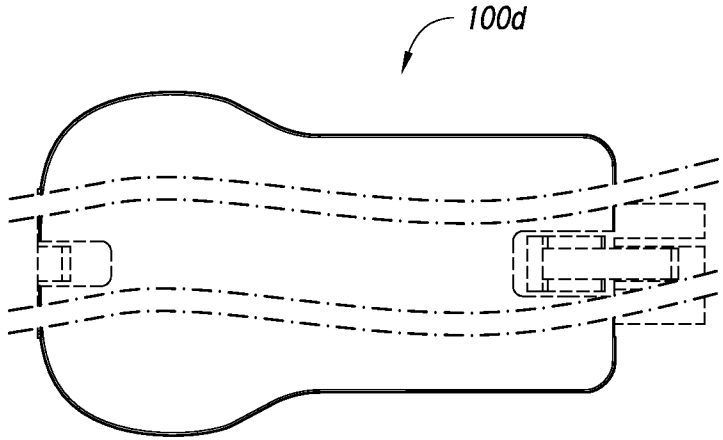


FIG. 39

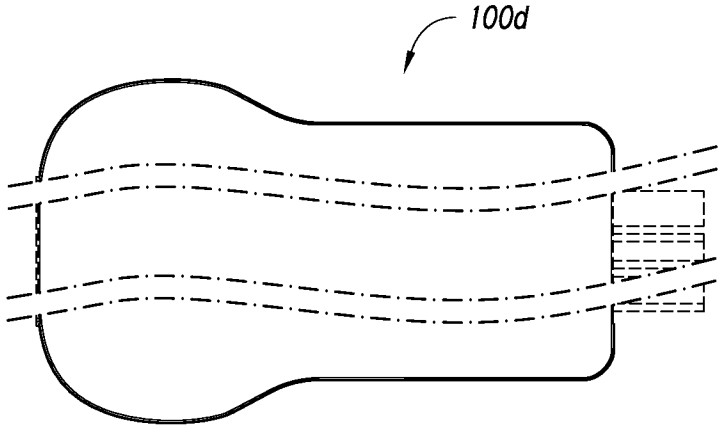


FIG. 40

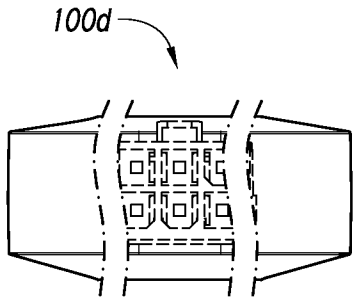


FIG. 42

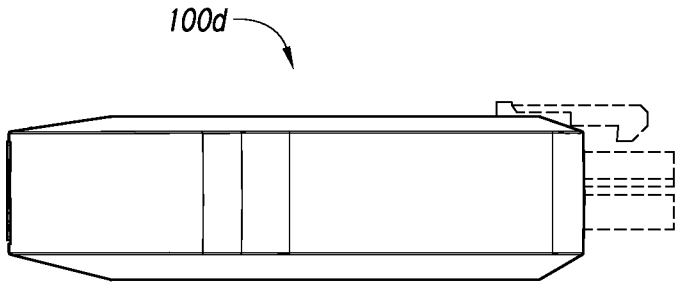


FIG. 41

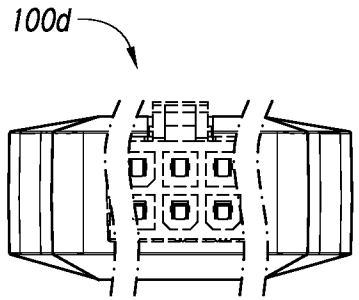


FIG. 43

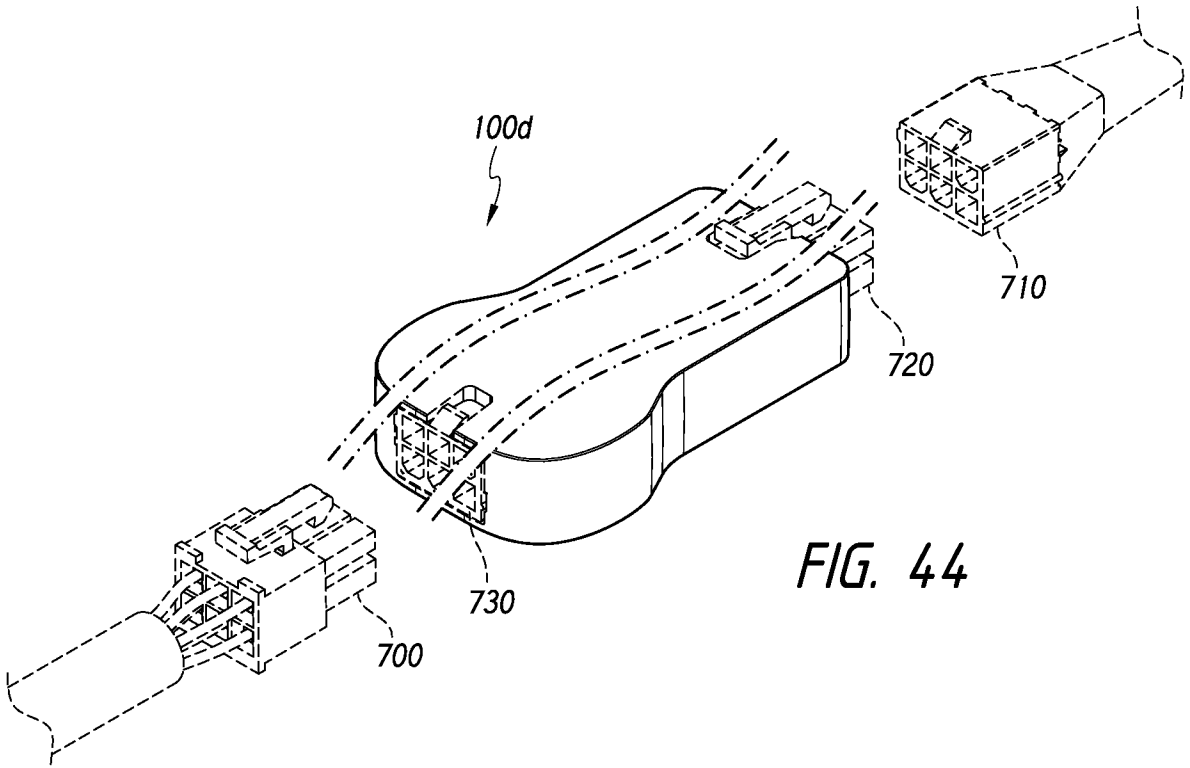


FIG. 44

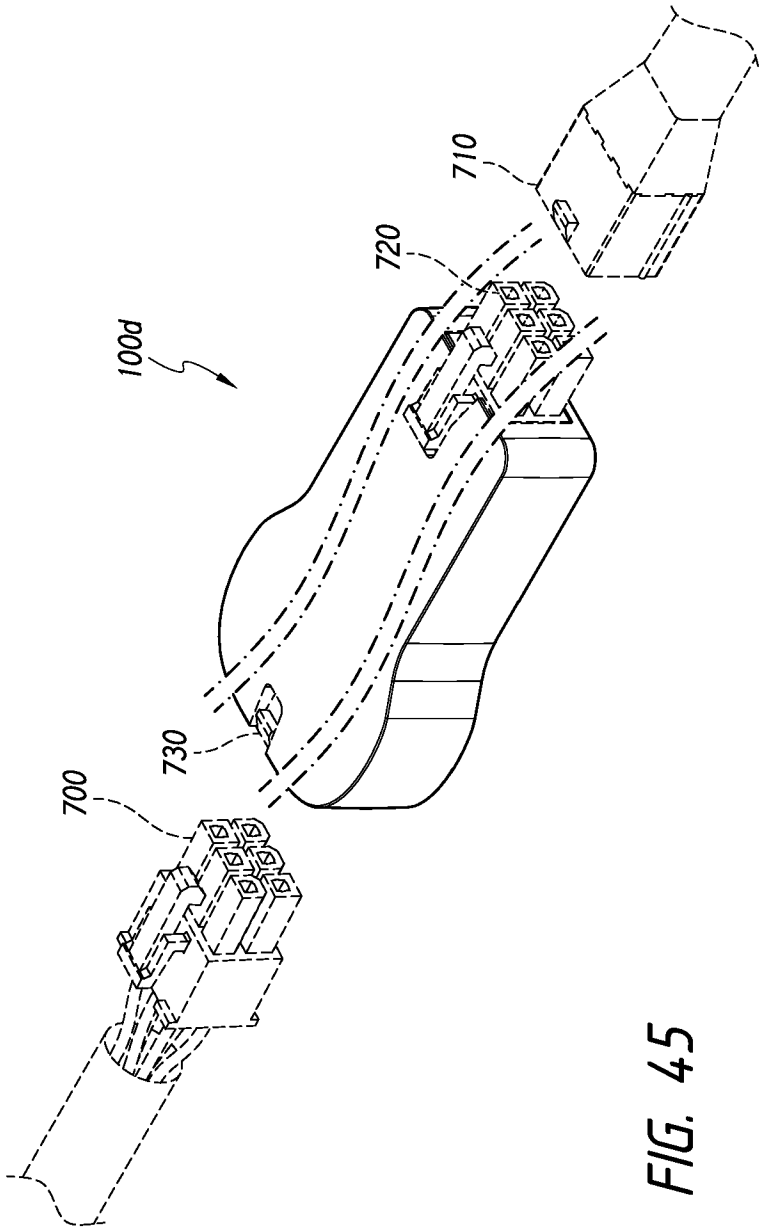


FIG. 45

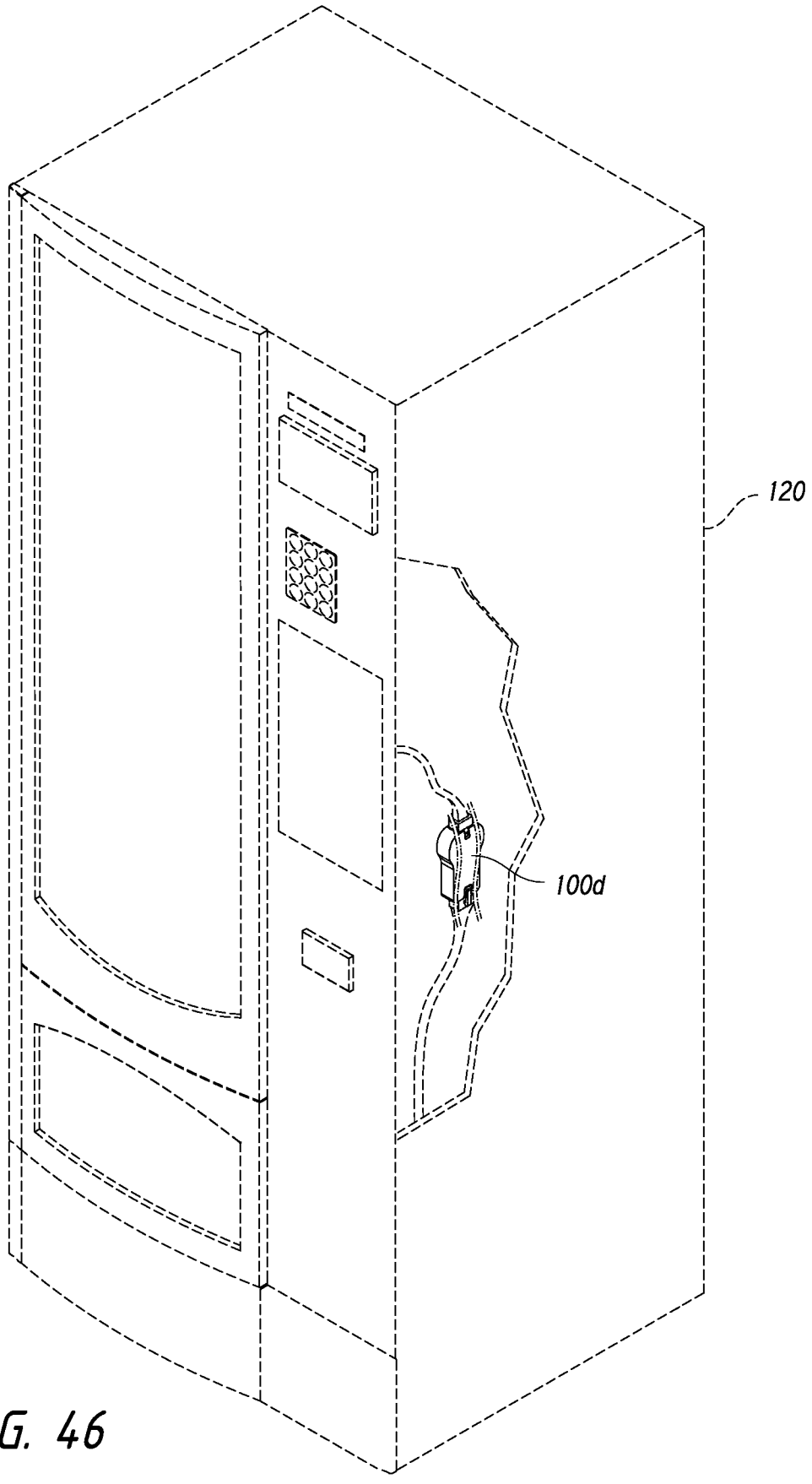


FIG. 46

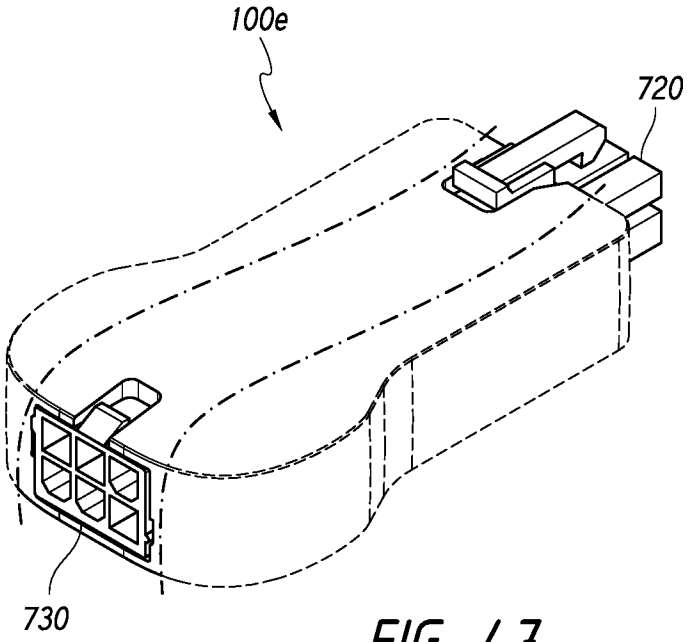


FIG. 47

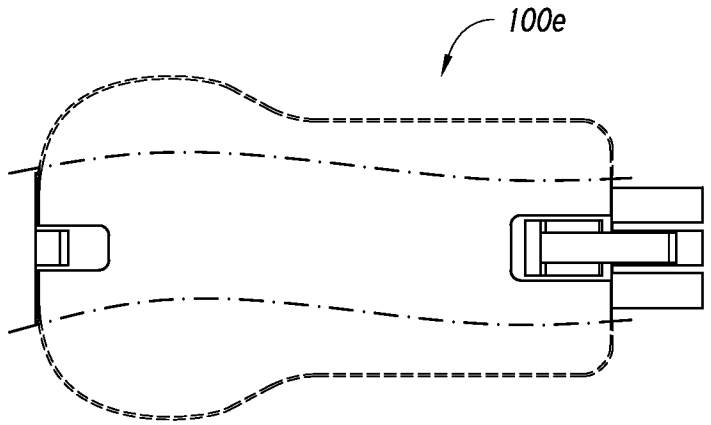


FIG. 48

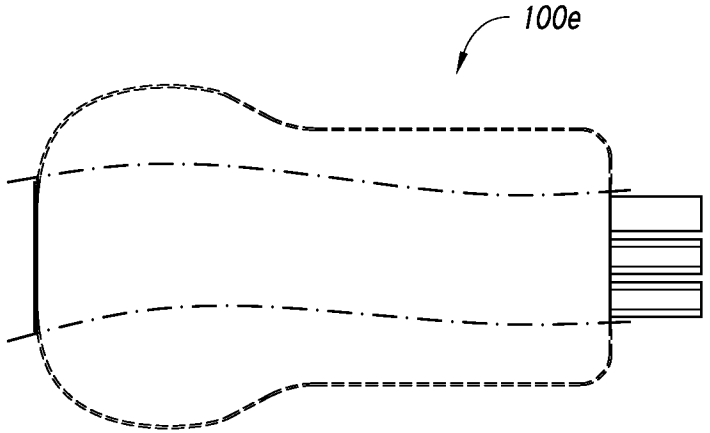


FIG. 49

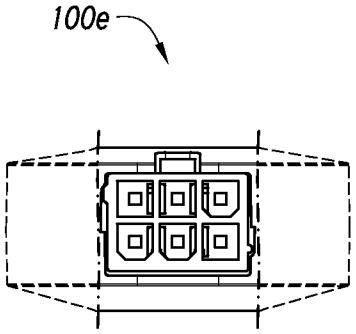


FIG. 51

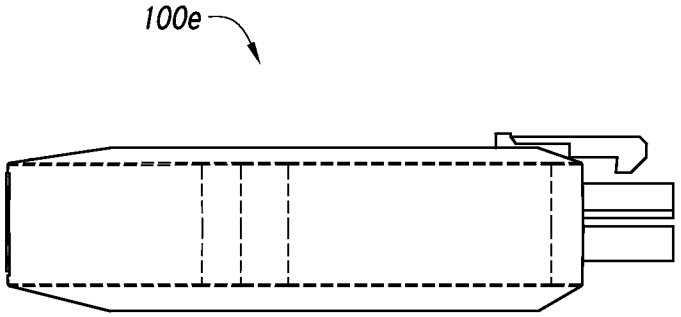


FIG. 50

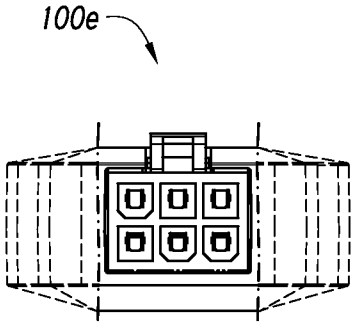


FIG. 52

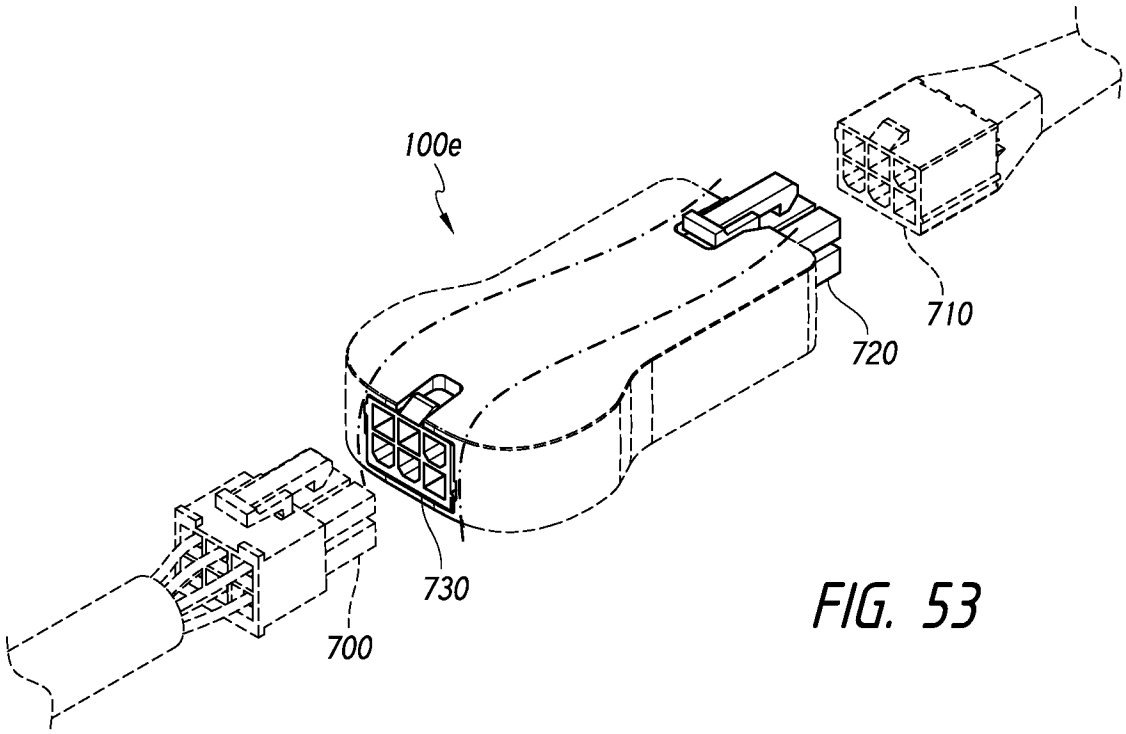


FIG. 53

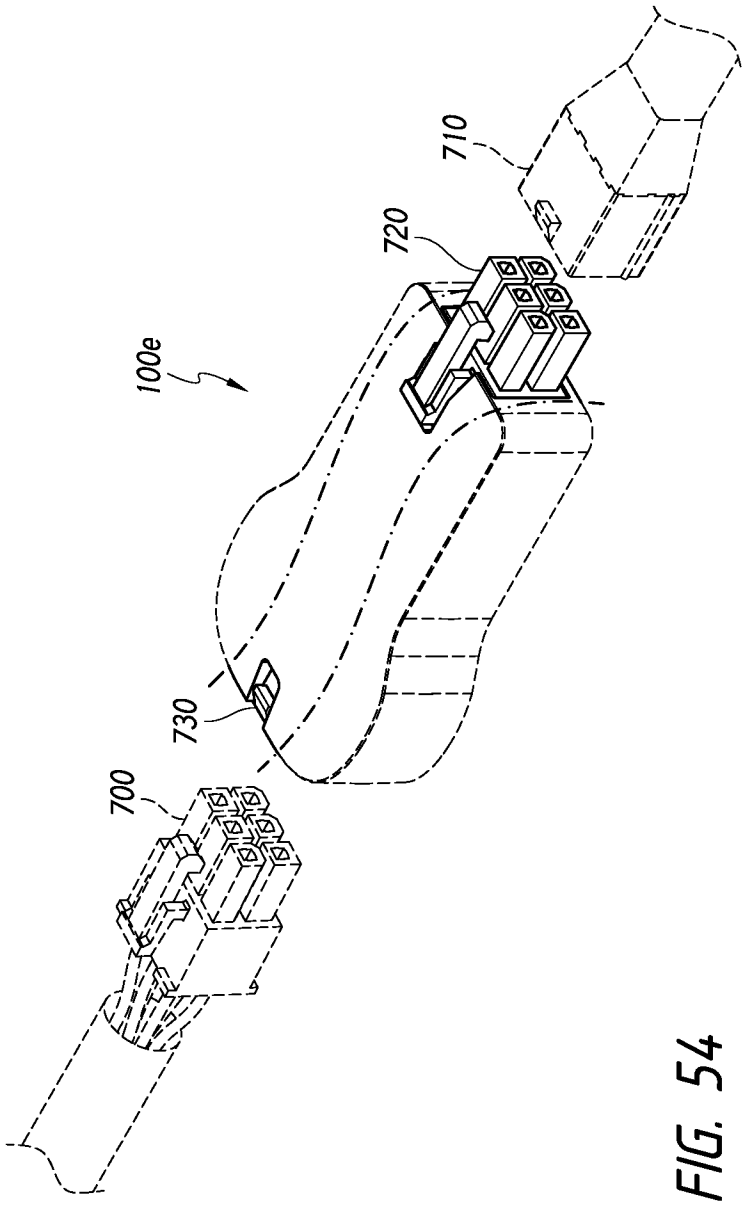


FIG. 54

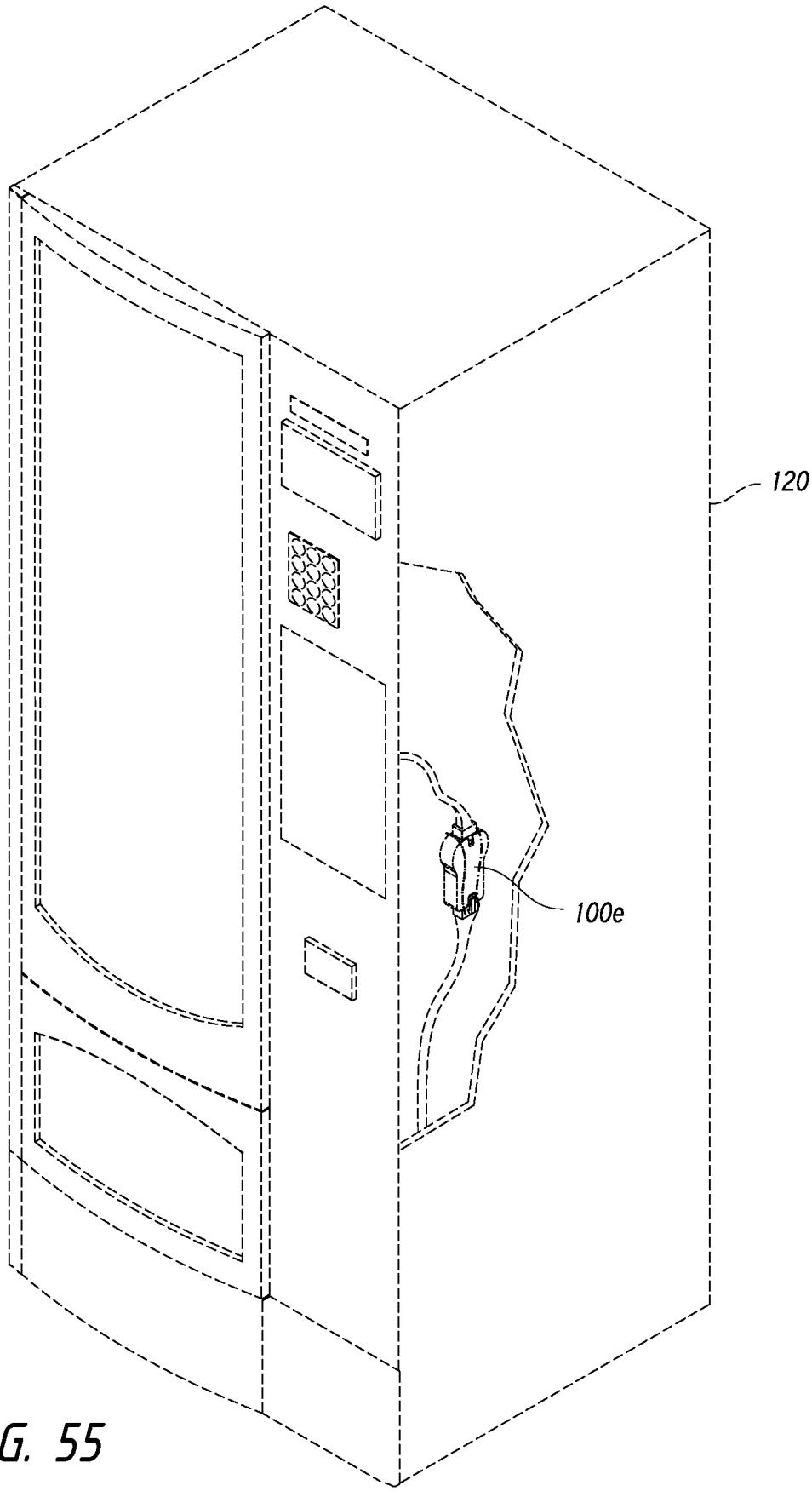


FIG. 55

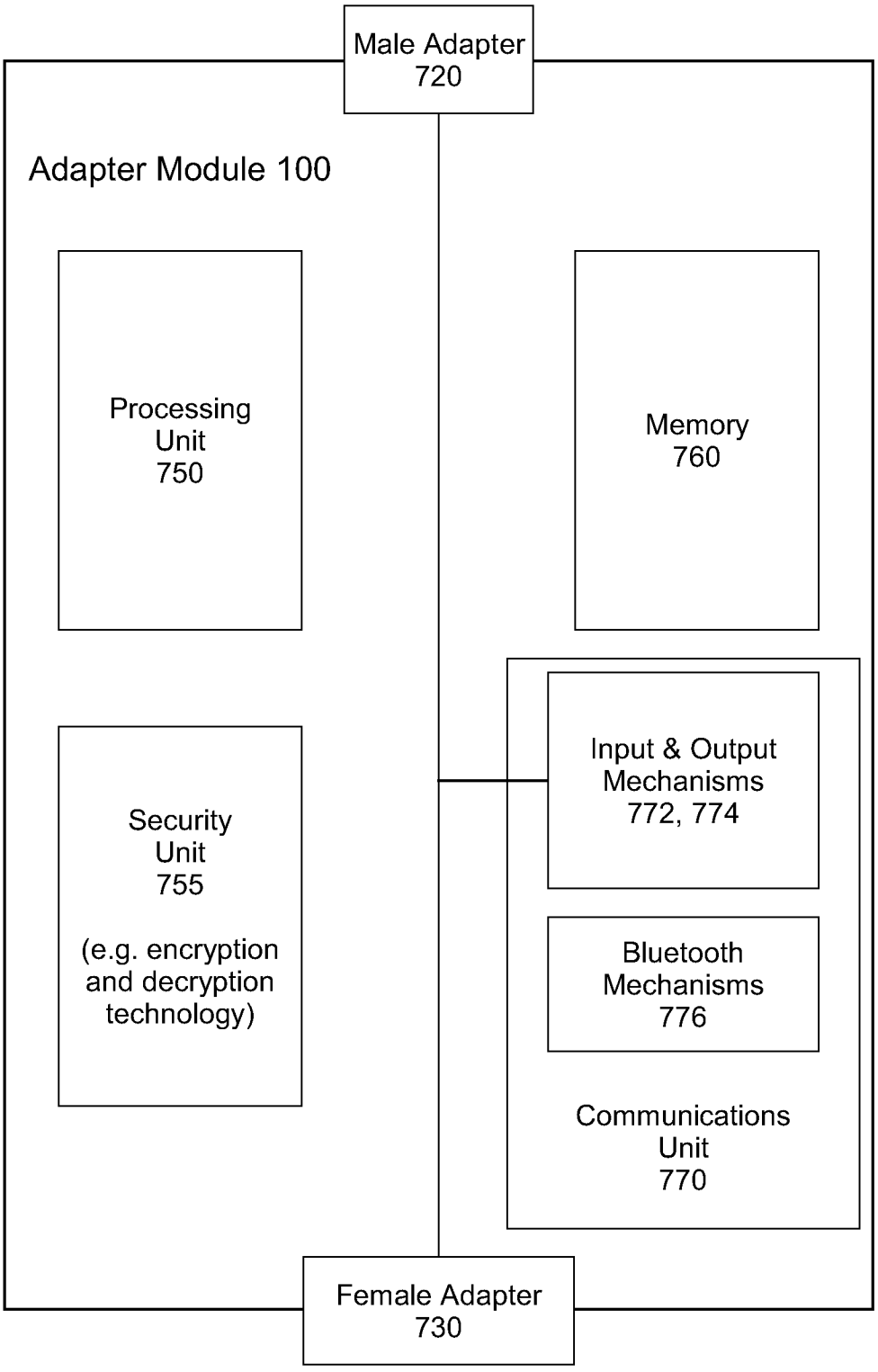

Male Adapter
720
Adapter Module 100
Processing
Unit
750
Memory
760
Input & Output
Mechanisms
772, 774
Security
Unit
755
(e.g. encryption
and decryption
technology)
Bluetooth
Mechanisms
776
Communications
Unit
770
Female Adapter
730

FIG. 56

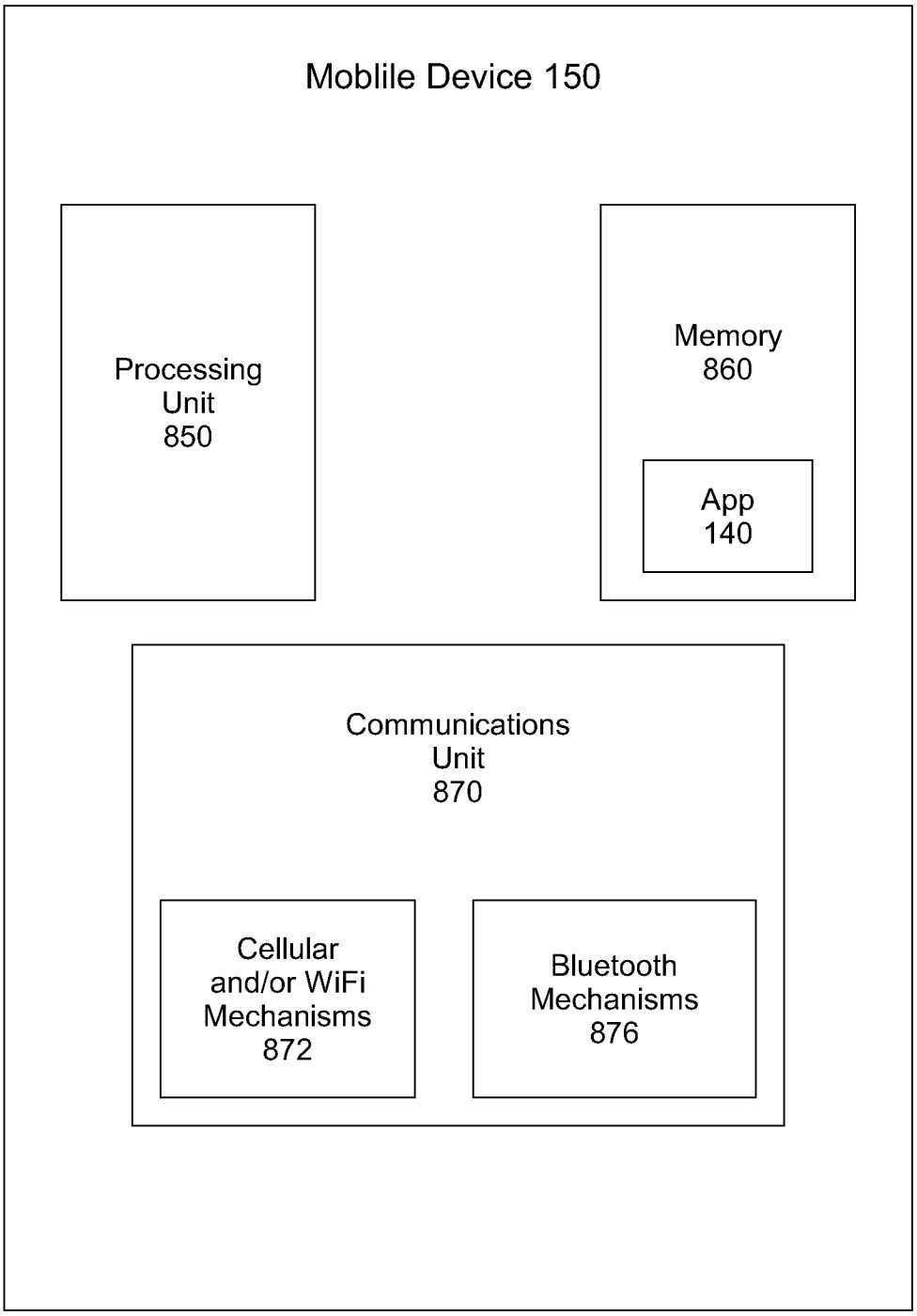

Moblile Device 150
Processing Unit 850
Memory 860
App 140
Communications Unit 870
Cellular and/or WiFi Mechanisms 872
Bluetooth Mechanisms 876

FIG. 57

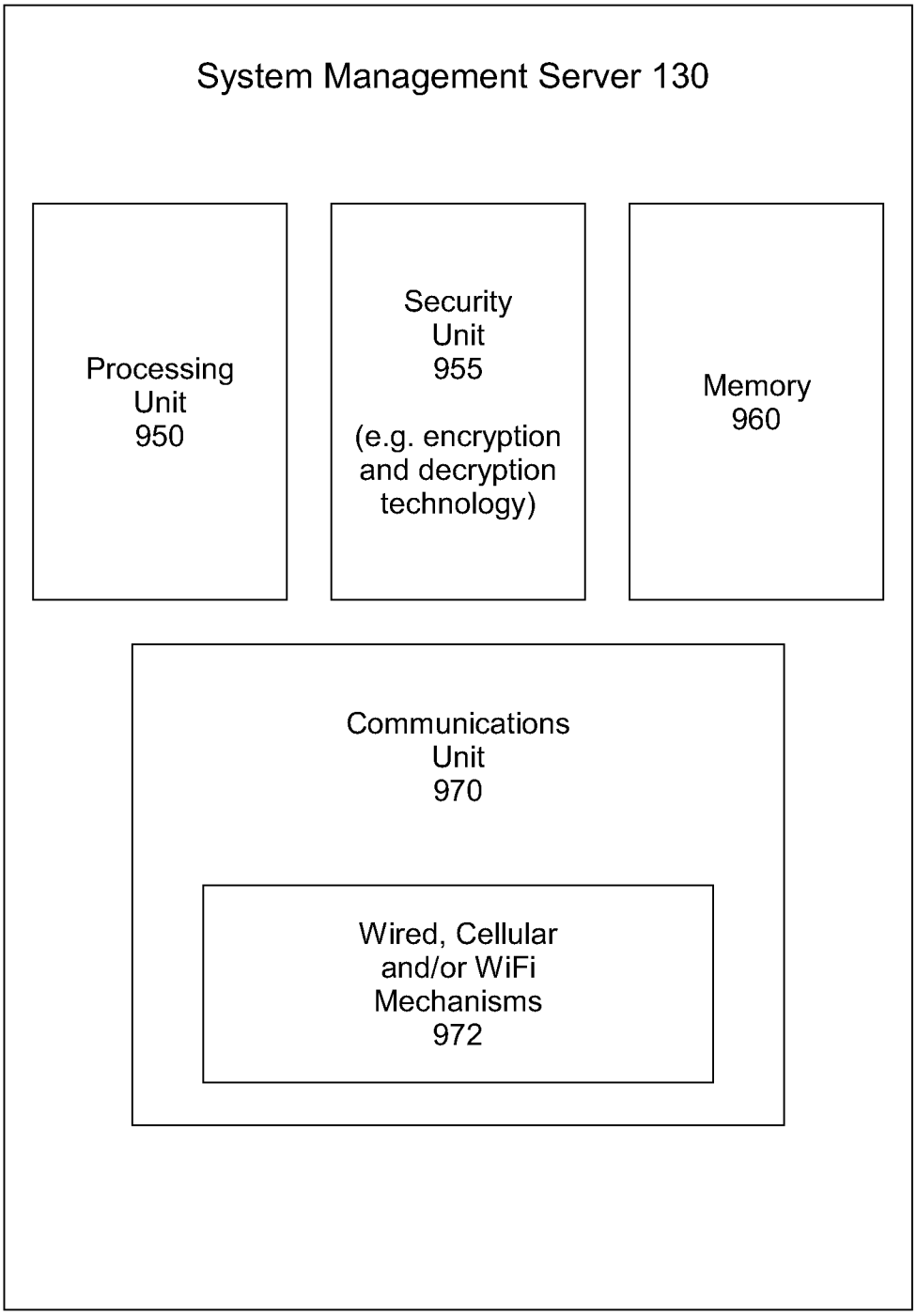

System Management Server 130
Processing Unit 950
Security Unit 955
(e.g. encryption and decryption technology)
Memory 960
Communications Unit 970
Wired, Cellular and/or WiFi Mechanisms 972

FIG. 58

PTO/AIA/14 (11-13)
Approved for use through 01/31/2014. OMB 0651-0032
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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	104402-5002-US
	Application Number	
Title of Invention	Method and System for Performing Mobile Device-To-Machine Payments	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
Dr.	Paresh	K.	Patel	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Portland	State/Province	OR	Country of Residence i	US

Mailing Address of Inventor:

Address 1	12815 NE Marx Street		
Address 2			
City	Portland	State/Province	OR
Postal Code	97230	Country i	US

Inventor 2 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Chau	M.	Doan	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Beaverton	State/Province	OR	Country of Residence i	US

Mailing Address of Inventor:

Address 1	12815 NE Marx Street		
Address 2			
City	Portland	State/Province	OR
Postal Code	97230	Country i	US

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

PTO/AIA/14 (11-13)
Approved for use through 01/31/2014. OMB 0651-0032
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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	104402-5002-US
	Application Number	
Title of Invention	Method and System for Performing Mobile Device-To-Machine Payments	

☐ **An Address is being provided for the correspondence Information of this application.**			
Customer Number	24341		
Email Address		Add Email	Remove Email

Application Information:

Title of the Invention	Method and System for Performing Mobile Device-To-Machine Payments		
Attorney Docket Number	104402-5002-US	**Small Entity Status Claimed**	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	44	**Suggested Figure for Publication (if any)**	

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)
☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	24341		

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) 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.
When referring to the current application, please leave the application number blank.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Continuation of	14/214644	2014-03-14
Prior Application Status	Pending		Remove

PTO/AIA/14 (11-13)
Approved for use through 01/31/2014. OMB 0651-0032
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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	104402-5002-US
	Application Number	
Title of Invention	Method and System for Performing Mobile Device-To-Machine Payments	

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
14/214644	Claims benefit of provisional	61/917936	2013-12-18
Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
14/214644	Continuation in part of	29/477025	2013-12-18
Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button.			Add

Foreign Priority Information:

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(d). When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX) [i] the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(h)(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).

Remove

Application Number	Country [i]	Filing Date (YYYY-MM-DD)	Access Code [i] (if applicable)

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button. Add

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Authorization to Permit Access:

☐ Authorization to Permit Access to the Instant Application by the Participating Offices

PTO/AIA/14 (11-13)
Approved for use through 01/31/2014. OMB 0651-0032
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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	104402-5002-US
	Application Number	
Title of Invention	Method and System for Performing Mobile Device-To-Machine Payments	

If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the instant patent application is filed access to the instant patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the instant patent application is filed to have access to the instant patent application.

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the instant patent application with respect to: 1) the instant patent application-as-filed; 2) any foreign application to which the instant patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the instant patent application; and 3) any U.S. application-as-filed from which benefit is sought in the instant patent application.

In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date of filing this Authorization.

Applicant 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.

Applicant 1 Remove

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. 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. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

◯ Assignee	◯ Legal Representative under 35 U.S.C. 117	◯ Joint Inventor
◯ Person to whom the inventor is obligated to assign.	◯ Person who shows sufficient proprietary interest	

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 :

If the Applicant is an Organization check here. ☒

Organization Name	PayRange Inc.

Mailing Address Information:

Address 1	12815 NE Marx Street		
Address 2			
City	Portland	**State/Province**	OR
Country [i]	US	Postal Code	97230
Phone Number		Fax Number	

PTO/AIA/14 (11-13)
Approved for use through 01/31/2014. OMB 0651-0032
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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	104402-5002-US
	Application Number	
Title of Invention	Method and System for Performing Mobile Device-To-Machine Payments	

Email Address	

Additional Applicant Data may be generated within this form by selecting the Add button. Add

Assignee Information including Non-Applicant Assignee Information:

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

Assignee 1

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication . An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

Remove

If the Assignee or Non-Applicant Assignee is an Organization check here. ☐

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information For Assignee including Non-Applicant Assignee:

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

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button. Add

Signature:

Remove

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

Signature	/ Douglas J. Crisman /			Date (YYYY-MM-DD)	2014-07-18
First Name	Douglas J.	Last Name	Crisman	Registration Number	

Additional Signature may be generated within this form by selecting the Add button. Add

PTO/AIA/14 (11-13)
Approved for use through 01/31/2014. OMB 0651-0032
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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	104402-5002-US
	Application Number	
Title of Invention	Method and System for Performing Mobile Device-To-Machine Payments	

This collection of information is required by 37 CFR 1.76. 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 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet 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 records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	METHOD AND SYSTEM FOR PERFORMING MOBILE DEVICE-TO-MACHINE PAYMENTS
First Named Inventor/Applicant Name:	Paresh K. Patel
Filer:	Douglas James Crisman/Sherri Ballbach
Attorney Docket Number:	104402-5002-US

Filed as Small Entity

Track I Prioritized Examination - Nonprovisional Application under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility filing Fee (Electronic filing)	4011	1	70	70
Utility Search Fee	2111	1	300	300
Utility Examination Fee	2311	1	360	360
Request for Prioritized Examination	2817	1	2000	2000
Pages:				
Claims:				
Claims in excess of 20	2202	8	40	320
Miscellaneous-Filing:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Publ. Fee- Early, Voluntary, or Normal	1504	1	0	0
PROCESSING FEE, EXCEPT PROV. APPLS.	2830	1	70	70

Petition:	
Patent-Appeals-and-Interference:	
Post-Allowance-and-Post-Issuance:	
Extension-of-Time:	
Miscellaneous:	
Total in USD ($)	**3120**

Electronic Acknowledgement Receipt

EFS ID:	19625628
Application Number:	14335762
International Application Number:	
Confirmation Number:	6199
Title of Invention:	METHOD AND SYSTEM FOR PERFORMING MOBILE DEVICE-TO-MACHINE PAYMENTS
First Named Inventor/Applicant Name:	Paresh K. Patel
Customer Number:	24341
Filer:	Douglas James Crisman/Sherri Ballbach
Filer Authorized By:	Douglas James Crisman
Attorney Docket Number:	104402-5002-US
Receipt Date:	18-JUL-2014
Filing Date:	
Time Stamp:	19:13:13
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$3120
RAM confirmation Number	4753
Deposit Account	500310
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if app

1		104402-5002-US_ApplicationAsFiled.pdf	1373441 48a376f75249a1fd5953154c88c0fb9c087730b9	yes	100

Multipart Description/PDF files in .zip description		
Document Description	**Start**	**End**
Transmittal of New Application	1	1
Fee Worksheet (SB06)	2	2
TrackOne Request	3	3
Specification	4	49
Claims	50	55
Abstract	56	56
Drawings-only black and white line drawings	57	100

Warnings:					
Information:					
2	Application Data Sheet	104402-5002-US_ADS_AsFiled.pdf	1265267 d5e20651d37a7443e4de5fca1de1fe3bde97822f	no	7
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	41719 3a3322dff9e508d3d74f9dcb6dcbdc76626ac654	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	2680427		

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.

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR § 1.53(b))

Attorney Docket No.	104402-5002-US
First Inventor	Dr. Paresh K. Patel
Title	METHOD AND SYSTEM FOR PERFORMING MOBILE DEVICE-TO-MACHINE PAYMENTS
Electronically filed	July 18, 2014

APPLICATION ELEMENTS

See MPEP Chapter 600 concerning utility patent application contents.

1. ☒ Fee Transmittal Form *(with duplicate for fee processing)*
2. ☒ Applicant claims Small Entity status, see 37 C.F.R. § 1.27
3. ☒ Specification [Total Pages 53]
4. ☒ Drawing(s) *(35 USC § 113)* [Total Sheets 44]
5. ☐ Oath or Declaration [Total Pages]
   a. ☐ Newly executed *(original or copy)*
   b. ☐ Copy from a prior application *(37 CFR § 1.63(d))*
6. ☒ Application Data Sheet, see 37 C.F.R. § 1.76
7. ☐ CD-ROM or CD-R in duplicate, large table or Computer Program *(Appendix)*
   ☐ Landscape Table on CD
8. ☐ Nucleotide and/or Amino Acid Sequence Submission *(if applicable, all necessary)*
   a. ☐ Computer Readable Form (CRF)
   b. ☐ Specification Sequence Listing on
      i. ☐ CD-ROM or CD-R (2 copies); or
      ii. ☐ Paper
   c. ☐ Statement verifying identity of above copies

Address to: **Commissioner for Patents**
P.O. Box 1450
Alexandria, VA 22313-1450

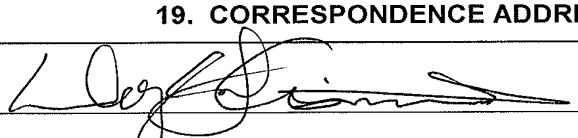
ACCOMPANYING APPLICATION PARTS

9. ☐ Assignment Papers *(cover sheet & document(s))*
   Name of Assignee:
10. ☐ 37 CFR § 3.73(c) Statement
    a. ☐ Power of Attorney
11. ☐ English Translation Document *(if applicable)*
12. ☐ Information Disclosure Statement and PTO-1449
    a. ☐ Copies of citations attached
13. ☐ Preliminary Amendment
14. ☐ Return Receipt Postcard *(MPEP 503)*
15. ☐ Certified Copy of Priority Document(s)
    (if foreign priority is claimed)
16. ☐ Non-Publication Request under 35 U.S.C. § 122 (b)(2)(B)(i)
17. ☒ Other: Track-1 Certification and Request for Prioritized Examination (1 page)

Note: (1) Benefit claims under 37 CFR 1.78 and foreign priority claims under 1.55 MUST be included in an Application Data Sheet (ADS).

(2) For applications filed under 35 U.S.C. 111, the application must contain an ADS specifying the applicant if the applicant is an assignee, person to whom the inventor is under an obligation to assign, or person who otherwise shows sufficient proprietary interest in the matter. See 37 CFR 1.46(b).

19. CORRESPONDENCE ADDRESS: Customer Number 24341

Signature		Date	July 18, 2014
Name (Print/Type)	Douglas J. Crisman	Registration No. (Attorney/Agent)	39,951

UTILITY PATENT APPLICATION FEE TRANSMITTAL *(Only for new nonprovisional applications under 37 CFR § 1.53(b))*	Attorney Docket No.	104402-5002-US
	First Inventor	Dr. Paresh K. Patel
	Title	METHOD AND SYSTEM FOR PERFORMING MOBILE DEVICE-TO-MACHINE PAYMENTS
	Electronically filed	July 18, 2014

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

BASIC FILING, SEARCH AND EXAMINATION FEES

Application Type	Filing Fees	Search Fees	Examination Fees	Fees Paid ($)
Utility	$ 140	$ 600	$ 720	$ 1460

EXCESS CLAIM FEES

Type	No. Filed	Less	Extra	Extra Rate ($)	Fee ($)
Total Claims	28	- 20	8	$ 80 each	640
Independent	3	- 3	0	$ 4200 each	0
			Multiple Dependency Fee If Applicable ($780)		0

APPLICATION SIZE FEE (Specification and Drawings)

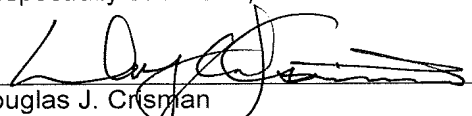
Total Sheets	Extra Sheets	No. of each add'l 50 or fraction thereof	Fee ($)
97 x .75- 100	0 / 50	0 (round up to whole no.) x $400	0

Sub Total	2100
Request for Prioritized Examination	4000
Processing Fee	140
TOTAL FILING FEE	**6240**
Small Entity Fee	**3120**

Please charge the total filing fee and any other additional fees to Morgan, Lewis & Bockius LLP Deposit Account 50-0310 (order no. 104402-5002-US).

Respectfully submitted,

Date: July 18, 2014



39,951
(Reg. No.)

Douglas J. Crisman
MORGAN, LEWIS & BOCKIUS LLP
2 Palo Alto Square
3000 El Camino Real, Suite 700
Palo Alto, California 94306
(650) 843-4000

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
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.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 14/335,762	Filing Date 07/18/2014	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	

AMENDMENT

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
/TAMMY d. MCBETH BROWN/

This collection of information is required by 37 CFR 1.16. 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 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.

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	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/335,762	07/18/2014	Paresh K. Patel	104402-5002-US

CONFIRMATION NO. 6199

24341
MORGAN, LEWIS & BOCKIUS LLP (PA)
2 PALO ALTO SQUARE
3000 EL CAMINO REAL, SUITE 700
PALO ALTO, CA 94306

FORMALITIES LETTER

OC00000069896676

Date Mailed: 07/31/2014

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The inventor's oath or declaration or an application data sheet (ADS) naming each inventor has not been submitted. An inventor's oath or declaration in compliance with 37 CFR 1.63 or 1.64 executed by or with respect to each inventor, or a properly executed ADS in compliance with 37 CFR 1.76 identifying each inventor by his or her legal name, mailing address, and residence (if an inventor lives at a location which is different from where the inventor customarily receives mail) is required. If an ADS as set forth above is provided, the filing of the inventor's oath or declaration may be postponed until the application is otherwise in condition for allowance. See 37 CFR 1.53(f).

The application is informal since it does not comply with the regulations for the reason(s) indicated below.

The required item(s) identified below must be timely submitted to avoid abandonment:

- A substitute specification in compliance with 37 CFR 1.52, 1.121(b)(3), and 1.125, is required. The substitute specification must be submitted with markings and be accompanied by a clean version (without markings) as set forth in 37 CFR 1.125(c) and a statement that the substitute specification contains no new matter (see 37 CFR 1.125(b)). The specification, claims, and/or abstract page(s) submitted is not acceptable and cannot be scanned or properly stored because:
  - The application contains drawings, but the specification does not contain a brief description of the several views of the drawings as required by 37 CFR 1.74 and 37 CFR 1.77(b)(9).

Applicant is cautioned that correction of the above items may cause the specification and drawings page count to exceed 100 pages. If the specification and drawings exceed 100 pages, applicant will need to submit the required application size fee.

- Surcharge as set forth in 37 CFR 1.16(f) must be submitted.
  The surcharge is due for any one of:
  - late submission of the basic filing fee, search fee, or examination fee,
  - late submission of inventor's oath or declaration,
  - filing an application that does not contain at least one claim on filing, or
  - submission of an application filed by reference to a previously filed application.

SUMMARY OF FEES DUE:

The fee(s) required within **TWO MONTHS** from the date of this Notice to avoid abandonment is/are itemized below. Small entity discount is in effect. If applicant is qualified for micro entity status, an acceptable Certification of Micro Entity Status must be submitted to establish micro entity status. (See 37 CFR 1.29 and forms PTO/SB/15A and 15B.)

- $ **70** surcharge.
- $(**0**) previous unapplied payment amount.
- $ **70** TOTAL FEE BALANCE DUE.

Items Required To Avoid Processing Delays:

Applicant is notified that the above-identified application contains the deficiencies noted below. No period for reply is set forth in this notice for correction of these deficiencies. However, if a deficiency relates to the inventor's oath or declaration, the applicant must file an oath or declaration in compliance with 37 CFR 1.63, or a substitute statement in compliance with 37 CFR 1.64, executed by or with respect to each actual inventor no later than the expiration of the time period set in the "Notice of Allowability" to avoid abandonment. See 37 CFR 1.53(f).

- The ADS received on 07/18/2014 was not properly signed. Therefore, the Office will treat it only as a transmittal letter. See 37 CFR 1.76(e). Inventorship has not been set by this document and any foreign priority or domestic benefit claims contained therein are ineffective. See 37 CFR 1.55 or 37 CFR 1.78.

Replies must be received in the USPTO within the set time period or must include a proper Certificate of Mailing or Transmission under 37 CFR 1.8 with a mailing or transmission date within the set time period. For more information and a suggested format, see Form PTO/SB/92 and MPEP 512.

Replies should be mailed to:

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web, including a copy of this Notice and selecting the document description "Applicant response to Pre-Exam Formalities Notice". https://sportal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html

For more information about EFS-Web please call the USPTO Electronic Business Center at **1-866-217-9197** or visit our website at http://www.uspto.gov/ebc.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

/mkanno/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 14/335,762

APPLICATION AS FILED - PART I

	(Column 1)		(Column 2)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED		NUMBER EXTRA	RATE($)	FEE($)		RATE($)	FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A		N/A	N/A	70		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A		N/A	N/A	300		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A		N/A	N/A	360		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	28	minus 20 =	* 8	x 40 =	320	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3	minus 3 =	*	x 210 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).				0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))					0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL	1050		TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1)		(Column 2)	(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1)		(Column 2)	(Column 3)					
		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

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
14/335,762	07/18/2014	2876	1050	104402-5002-US	28	3

CONFIRMATION NO. 6199

24341
MORGAN, LEWIS & BOCKIUS LLP (PA)
2 PALO ALTO SQUARE
3000 EL CAMINO REAL, SUITE 700
PALO ALTO, CA 94306

FILING RECEIPT



Date Mailed: 07/31/2014

Receipt is acknowledged of this non-provisional 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 APPLICANT, 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 Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections 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**

Inventor(s)

Paresh K. Patel, Portland, OR;
Chau M. Doan, Beaverton, OR;

Applicant(s)

Paresh K. Patel, Portland, OR;
Chau M. Doan, Beaverton, OR;

Power of Attorney: None

Domestic Applications for which benefit is claimed - None.
A proper domestic benefit claim must be provided in an Application Data Sheet in order to constitute a claim for domestic benefit. See 37 CFR 1.76 and 1.78.

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.

If Required, Foreign Filing License Granted: 07/29/2014

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 14/335,762**

Projected Publication Date: To Be Determined - pending completion of Missing Parts

Non-Publication Request: No

Early Publication Request: No
** **SMALL ENTITY** **

Title

Method and System for Performing Mobile Device-To-Machine Payments

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

Electronically filed: August 13, 2014

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application of:	Patel et al.	Confirmation No.:	6199
Serial No.:	14/335,762	Art Unit:	2876
Filed:	July 18, 2014	Examiner:	To be assigned
For:	*Method and System for Performing Mobile Device-To-Machine Payments*	Attorney Docket No:	104402-5002-US

PRELIMINARY AMENDMENT

Mail Stop: Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This preliminary amendment is for the application identified above. Please enter this amendment prior to examination on the merits.

IN THE SPECIFICATION:

Please revise the specification as follows:

Please add a paragraph between current paragraph numbers [0049] and [0050] as follows:

[0049.1] FIG. 14 is a side view of the in-line dongle adapter module of FIG. 11 in accordance with some implementations.

Please add a paragraph between current paragraph numbers [0084] and [0085] as follows:

[0084.1] FIG. 50 is a side view of the in-line dongle adapter module of FIG. 47 in accordance with some implementations.

REMARKS

Amendments to the Specification

New paragraph [0049.1] has been added to correct a typographical error. Support is found in at least paragraphs [00108]-[00109] and Figure 14 of the application as filed.

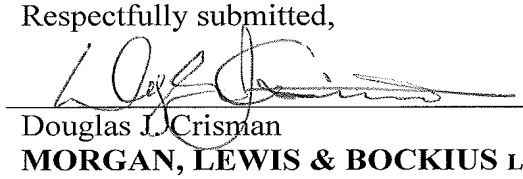
New paragraph [0084.1] has been added to correct a typographical error. Support is found in at least paragraphs [00108]-[00109] and Figure 50 of the application as filed.

Conclusions

No fee is believed to be due at this time, however, the Commissioner is hereby authorized to charge any additional fees associated with this paper communication or credit any overpayment to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no. 104402-5002-US).

Respectfully submitted,

Date: August 13, 2014



39,951

Douglas J. Crisman (Reg. No.)
MORGAN, LEWIS & BOCKIUS LLP
2 Palo Alto Square
3000 El Camino Real, Suite 700
Palo Alto, CA 94306
(650) 843-4000

Electronic Acknowledgement Receipt

EFS ID:	19860784
Application Number:	14335762
International Application Number:	
Confirmation Number:	6199
Title of Invention:	Method and System for Performing Mobile Device-To-Machine Payments
First Named Inventor/Applicant Name:	Paresh K. Patel
Customer Number:	24341
Filer:	Douglas James Crisman/Sherri Ballbach
Filer Authorized By:	Douglas James Crisman
Attorney Docket Number:	104402-5002-US
Receipt Date:	13-AUG-2014
Filing Date:	18-JUL-2014
Time Stamp:	19:24:21
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	Preliminary Amendment	104402-5002-US_PreliminaryAmendment.pdf	65125 d749b50366e42404415818d6c546da752b52f9d8	no	3

Warnings:	
Information:	

Total Files Size (in bytes):	65125

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.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 14/335,762

APPLICATION AS FILED - PART I

	(Column 1)		(Column 2)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED		NUMBER EXTRA	RATE($)	FEE($)		RATE($)	FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A		N/A	N/A	70		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A		N/A	N/A	300		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A		N/A	N/A	360		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	28	minus 20 =	* 8	x 40 =	320	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3	minus 3 =	*	x 210 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).				0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))					0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL	1050		TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1)		(Column 2)	(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1)		(Column 2)	(Column 3)					
		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

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	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/335,762	07/18/2014	Paresh K. Patel	104402-5002-US

CONFIRMATION NO. 6199

24341
MORGAN, LEWIS & BOCKIUS LLP (PA)
2 PALO ALTO SQUARE
3000 EL CAMINO REAL, SUITE 700
PALO ALTO, CA 94306

MISCELLANEOUS NOTICE

OC000000070284450

Date Mailed: 08/21/2014

A communication which cannot be delivered in electronic form has been mailed to the applicant.

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	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/335,762	07/18/2014	Paresh K. Patel	104402-5002-US

CONFIRMATION NO. 6199

24341
MORGAN, LEWIS & BOCKIUS LLP (PA)
2 PALO ALTO SQUARE
3000 EL CAMINO REAL, SUITE 700
PALO ALTO, CA 94306

FORMALITIES LETTER

OC000000070284662

Date Mailed: 08/21/2014

NOTICE OF INCOMPLETE REPLY (NONPROVISIONAL)

Filing Date Granted

The U.S. Patent and Trademark Office has received your reply on 08/13/2014 to the Notice to File Missing Parts (Notice) mailed 07/31/2014 and it has been entered into the nonprovisional application. The reply, however, does not include the following items required in the Notice. A complete reply must be timely filed to prevent ABANDONMENT of the above-identified application. Replies should be mailed to: Mail Stop Missing Parts, Commissioner for Patents, P.O. Box 1450, Alexandria VA 22313-1450.

Applicant is given **TWO MONTHS** from the date of the Notice to File Missing Parts (Notice) mailed 07/31/2014 within which to file all required items and pay any fees required below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The inventor's oath or declaration or an application data sheet (ADS) naming each inventor has not been submitted. An inventor's oath or declaration in compliance with 37 CFR 1.63 or 1.64 executed by or with respect to each inventor, or a properly executed ADS in compliance with 37 CFR 1.76 identifying each inventor by his or her legal name, mailing address, and residence (if an inventor lives at a location which is different from where the inventor customarily receives mail) is required. If an ADS as set forth above is provided, the filing of the inventor's oath or declaration may be postponed until the application is otherwise in condition for allowance. See 37 CFR 1.53(f).
- Surcharge as set forth in 37 CFR 1.16(f) was not received.
  The surcharge is due for any one of:
  - late submission of the basic filing fee, search fee, or examination fee,
  - late submission of inventor's oath or declaration,
  - filing an application that does not contain at least one claim on filing, or
  - submission of an application filed by reference to a previously filed application.

The application is informal since it does not comply with the regulations for the reason(s) indicated below.

The required item(s) identified below must be timely submitted to avoid abandonment:

- A substitute specification in compliance with 37 CFR 1.52, 1.121(b)(3), and 1.125, is required. The substitute specification must be submitted with markings and be accompanied by a clean version (without markings) as set forth in 37 CFR 1.125(c) and a statement that the substitute specification contains no new matter (see 37 CFR 1.125(b)). The specification, claims, and/or abstract page(s) submitted is not acceptable and cannot be scanned or properly stored because:
  - The application contains drawings, but the specification does not contain a brief description of the several views of the drawings as required by 37 CFR 1.74 and 37 CFR 1.77(b)(9).

Applicant is cautioned that correction of the above items may cause the specification and drawings page count to exceed 100 pages. If the specification and drawings exceed 100 pages, applicant will need to submit the required application size fee.

SUMMARY OF FEES DUE:

The fee(s) required within **TWO MONTHS** from the date of the Notice to avoid abandonment is/are itemized below. Small entity discount is in effect. If applicant is qualified for micro entity status, an acceptable Certification of Micro Entity Status must be submitted to establish micro entity status. (See 37 CFR 1.29 and forms PTO/SB/15A and 15B.)

- $ **70** surcharge.
- $(**0**) previous unapplied payment amount.
- $ **70** TOTAL FEE BALANCE DUE.

Items Required To Avoid Processing Delays:

Applicant is notified that the above-identified application contains the deficiencies noted below. No period for reply is set forth in this notice for correction of these deficiencies. However, if a deficiency relates to the inventor's oath or declaration, the applicant must file an oath or declaration in compliance with 37 CFR 1.63, or a substitute statement in compliance with 37 CFR 1.64, executed by or with respect to each actual inventor no later than the expiration of the time period set in the "Notice of Allowability" to avoid abandonment. See 37 CFR 1.53(f).

- The ADS received on 08/13/2014 was not properly signed. Therefore, the Office will treat it only as a transmittal letter. See 37 CFR 1.76(e). Inventorship has not been set by this document and any foreign priority or domestic benefit claims contained therein are ineffective. See 37 CFR 1.55 or 37 CFR 1.78.

Replies must be received in the USPTO within the set time period or must include a proper Certificate of Mailing or Transmission under 37 CFR 1.8 with a mailing or transmission date within the set time period. For more information and a suggested format, see Form PTO/SB/92 and MPEP 512.

Replies should be mailed to:

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web, including a copy of this Notice and selecting the document description "Applicant response to Pre-Exam Formalities Notice". https://sportal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html

For more information about EFS-Web please call the USPTO Electronic Business Center at **1-866-217-9197** or visit our website at http://www.uspto.gov/ebc.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

/ydemisse/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

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 DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/335,762	07/18/2014	Paresh K. Patel	104402-5002-US

CONFIRMATION NO. 6199

24341
MORGAN, LEWIS & BOCKIUS LLP (PA)
2 PALO ALTO SQUARE
3000 EL CAMINO REAL, SUITE 700
PALO ALTO, CA 94306

OC000000070284450

Date Mailed: 8/21/2014

NOTICE OF INCOMPLETE REPLY

Filing Date Granted

Applicant's reply to the Notice mailed on 7/31/2014 was received in the U.S. Patent and Trademark Office on 8/13/2014 and has been entered into the application. The reply, however, does not include the following item(s) required in the Notice.

The period for reply continues to run from the mailing date of the prior Notice. The item(s) listed below must be timely filed to avoid abandonment of the application. No new time period for reply is provided in this communication. If the period for reply set forth in the prior Notice has expired, this application will become abandoned unless applicant: (1) submits the following checked item(s), **and** (2) obtains an extension of time under 37 CFR 1. 136(a) (including the appropriate fee (37 CFR 1.17(a)). In no case may an applicant obtain an extension of time for more than FIVE (5) MONTHS beyond the date for reply set forth in the prior Notice.

A complete reply which includes the following checked item(s) must be timely filed to prevent ABANDONMENT of the above-identified application:

- ☒ A substitute specification.
- ☒ A statement that the substitute specification contains no new matter.
- ☐ A replacement abstract commencing on a separate sheet in compliance with 37 CFR 1.72(b) and 1.121 (deleting the drawings or flow diagrams).
- ☐ New and replacement drawing sheets.
- ☐ Replacement drawing sheets with the figures renumbered.
- ☐ A complete claim listing or a replacement claim listing with the claims renumbered.
- ☐ An amendment to the claims in compliance with 37 CFR 1.121 (deleting the drawings or flow diagrams).
- ☐ A replacement transmittal letter listing all of the files except the missing or unreadable file.
- ☐ A duplicate copy of the CD.
- ☐ A statement that the replacement CD contains no new matter.

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

Replies should be mailed to: Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web.
https://sportal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html

For more information about EFS-Web, please call the USPTO Electronic Business Center at 1-866-217-9197 or visit our website at http://www.uspto.gov/ebc.

Application Assistance Unit (571) 272-4200

Electronically filed: August 26, 2014

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application of:	Paresh K. Patel et al.	Confirmation No.:	6199
Serial No.:	14/335,762	Art Unit:	2876
Filed:	July 18, 2014	Examiner:	To Be Assigned
For:	*Method and System for Performing Mobile-Device-To-Machine Payments*	Attorney Docket No:	104402-5002-US

RESPONSE TO THE NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

Mail Stop: MISSING PARTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In Response to the Notice to File Missing Parts of Nonprovisional Application mailed July 31, 2014, enclosed is the Notice to File Missing Parts of Nonprovisional Application for the above-identified application and the executed declaration. The fee for the late oath or declaration surcharge is $70 for a small entity. The Commissioner is hereby authorized to charge the required fees or credit any overpayments to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no. 104402-5002-US).

A Supplemental Application Data Sheet, Substitute Specification with Markings as well as a clean version of the Specification are also submitted herewith.

Respectfully submitted,

Date: August 26, 2014



39,951

Douglas J. Crisman (Reg. No.)
MORGAN, LEWIS & BOCKIUS LLP
2 Palo Alto Square
3000 El Camino Real, Suite 700
Palo Alto, CA 94306
(650) 843-4000

WORKING COPY 104402-5002-US
ASG/DJC/JTS

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	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/335,762	07/18/2014	Paresh K. Patel	104402-5002-US

CONFIRMATION NO. 6199

24341
MORGAN, LEWIS & BOCKIUS LLP (PA)
2 PALO ALTO SQUARE
3000 EL CAMINO REAL, SUITE 700
PALO ALTO, CA 94306

FORMALITIES LETTER

OC000000069896676

Date Mailed: 07/31/2014

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The inventor's oath or declaration or an application data sheet (ADS) naming each inventor has not been submitted. An inventor's oath or declaration in compliance with 37 CFR 1.63 or 1.64 executed by or with respect to each inventor, or a properly executed ADS in compliance with 37 CFR 1.76 identifying each inventor by his or her legal name, mailing address, and residence (if an inventor lives at a location which is different from where the inventor customarily receives mail) is required. If an ADS as set forth above is provided, the filing of the inventor's oath or declaration may be postponed until the application is otherwise in condition for allowance. See 37 CFR 1.53(f).

The application is informal since it does not comply with the regulations for the reason(s) indicated below.

The required item(s) identified below must be timely submitted to avoid abandonment:

- A substitute specification in compliance with 37 CFR 1.52, 1.121(b)(3), and 1.125, is required. The substitute specification must be submitted with markings and be accompanied by a clean version (without markings) as set forth in 37 CFR 1.125(c) and a statement that the substitute specification contains no new matter (see 37 CFR 1.125(b)). The specification, claims, and/or abstract page(s) submitted is not acceptable and cannot be scanned or properly stored because:
  - The application contains drawings, but the specification does not contain a brief description of the several views of the drawings as required by 37 CFR 1.74 and 37 CFR 1.77(b)(9).

Applicant is cautioned that correction of the above items may cause the specification and drawings page count to exceed 100 pages. If the specification and drawings exceed 100 pages, applicant will need to submit the required application size fee.

DOCKETED
FILE MISSING PARTS
DUE 30 SEP 2014
FINAL 28 FEB 2015

RECEIVED DOCKETING
JUL 31 2014
MORGAN LEWIS
PALO ALTO OFFICE

- Surcharge as set forth in 37 CFR 1.16(f) must be submitted.
  The surcharge is due for any one of:
  - late submission of the basic filing fee, search fee, or examination fee,
  - late submission of inventor's oath or declaration,
  - filing an application that does not contain at least one claim on filing, or
  - submission of an application filed by reference to a previously filed application.

SUMMARY OF FEES DUE:

The fee(s) required within **TWO MONTHS** from the date of this Notice to avoid abandonment is/are itemized below. Small entity discount is in effect. If applicant is qualified for micro entity status, an acceptable Certification of Micro Entity Status must be submitted to establish micro entity status. (See 37 CFR 1.29 and forms PTO/SB/15A and 15B.)

- $ **70** surcharge.
- $(**0**) previous unapplied payment amount.
- $ **70** TOTAL FEE BALANCE DUE.

Items Required To Avoid Processing Delays:

Applicant is notified that the above-identified application contains the deficiencies noted below. No period for reply is set forth in this notice for correction of these deficiencies. However, if a deficiency relates to the inventor's oath or declaration, the applicant must file an oath or declaration in compliance with 37 CFR 1.63, or a substitute statement in compliance with 37 CFR 1.64, executed by or with respect to each actual inventor no later than the expiration of the time period set in the "Notice of Allowability" to avoid abandonment. See 37 CFR 1.53(f).

- The ADS received on 07/18/2014 was not properly signed. Therefore, the Office will treat it only as a transmittal letter. See 37 CFR 1.76(e). Inventorship has not been set by this document and any foreign priority or domestic benefit claims contained therein are ineffective. See 37 CFR 1.55 or 37 CFR 1.78.

Replies must be received in the USPTO within the set time period or must include a proper Certificate of Mailing or Transmission under 37 CFR 1.8 with a mailing or transmission date within the set time period. For more information and a suggested format, see Form PTO/SB/92 and MPEP 512.

Replies should be mailed to:

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web, including a copy of this Notice and selecting the document description "Applicant response to Pre-Exam Formalities Notice". https://sportal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html

For more information about EFS-Web please call the USPTO Electronic Business Center at **1-866-217-9197** or visit our website at http://www.uspto.gov/ebc.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

/mkanno/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	**METHOD AND SYSTEM FOR PERFORMING MOBILE-DEVICE-TO-MACHINE PAYMENTS**

As the below named inventor, I hereby declare that:

This declaration is directed to:

☐ The attached application, or

☒ United States application or PCT international application number 14/335,762 filed on July 18, 2014

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby state that I have reviewed and understand the contents of the above identified application, including the claims.

I acknowledge the duty to disclose information known to me to be material to patentability as defined by 37 CFR 1.56.

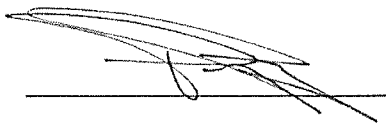
I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: **Dr. Paresh K. Patel** Date: 07/24/2014

Signature: 

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	**METHOD AND SYSTEM FOR PERFORMING MOBILE-DEVICE-TO-MACHINE PAYMENTS**

As the below named inventor, I hereby declare that:

This declaration is directed to:

☐ The attached application, or

☒ United States application or PCT international application number 14/335,762 filed on July 18, 2014

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby state that I have reviewed and understand the contents of the above identified application, including the claims.

I acknowledge the duty to disclose information known to me to be material to patentability as defined by 37 CFR 1.56.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: **Chau M. Doan** Date: 07/24/2014

Signature: Chau Doan

PTO/AIA/14 (11-13)
Approved for use through 01/31/2014. OMB 0651-0032
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.

SUPPLEMENTAL Application Data Sheet 37 CFR 1.76	Attorney Docket Number	104402-5002-US
	Application Number	14/335,762
Title of Invention	Method and System for Performing Mobile Device-To-Machine Payments	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
Dr.	Paresh	K.	Patel	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Portland	State/Province	OR	Country of Residence	US

Mailing Address of Inventor:

Address 1	12815 NE Marx Street		
Address 2			
City	Portland	State/Province	OR
Postal Code	97230	Country	US

Inventor 2 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Chau	M.	Doan	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Beaverton	State/Province	OR	Country of Residence	US

Mailing Address of Inventor:

Address 1	12815 NE Marx Street		
Address 2			
City	Portland	State/Province	OR
Postal Code	97230	Country	US

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

PTO/AIA/14 (11-13)
Approved for use through 01/31/2014. OMB 0651-0032
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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	104402-5002-US
	Application Number	14/335,762
Title of Invention	Method and System for Performing Mobile Device-To-Machine Payments	

☐ An Address is being provided for the correspondence Information of this application.			
Customer Number	24341		
Email Address		Add Email	Remove Email

Application Information:

Title of the Invention	Method and System for Performing Mobile Device-To-Machine Payments		
Attorney Docket Number	104402-5002-US	**Small Entity Status Claimed**	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	44	**Suggested Figure for Publication (if any)**	

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)
☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	24341		

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) 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.
When referring to the current application, please leave the application number blank.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Continuation of	14/214644	2014-03-14
Prior Application Status	Pending		Remove

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	104402-5002-US
	Application Number	14/335,762
Title of Invention	Method and System for Performing Mobile Device-To-Machine Payments	

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
14/214644	Claims benefit of provisional	61/917936	2013-12-18
Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
14/214644	Continuation in part of	29/477025	2013-12-18

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button.

Foreign Priority Information:

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(d). When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX)[i] the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(h)(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).

Remove

Application Number	Country[i]	Filing Date (YYYY-MM-DD)	Access Code[i] (if applicable)

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button.

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Authorization to Permit Access:

☐ Authorization to Permit Access to the Instant Application by the Participating Offices

PTO/AIA/14 (11-13)
Approved for use through 01/31/2014. OMB 0651-0032
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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	104402-5002-US
	Application Number	14/335,762
Title of Invention	Method and System for Performing Mobile Device-To-Machine Payments	

If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the instant patent application is filed access to the instant patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the instant patent application is filed to have access to the instant patent application.

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the instant patent application with respect to: 1) the instant patent application-as-filed; 2) any foreign application to which the instant patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the instant patent application; and 3) any U.S. application-as-filed from which benefit is sought in the instant patent application.

In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date o f filing this Authorization.

Applicant 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.

Applicant 1

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. 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. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

◯ Assignee	◯ Legal Representative under 35 U.S.C. 117	◯ Joint Inventor
◯ Person to whom the inventor is obligated to assign.	◯ Person who shows sufficient proprietary interest	

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 :	
If the Applicant is an Organization check here. ☒	
Organization Name	PayRange Inc.

Mailing Address Information For Applicant:

Address 1	12815 NE Marx Street		
Address 2			
City	Portland	**State/Province**	OR
Country	US	Postal Code	97230
Phone Number		Fax Number	

PTO/AIA/14 (11-13)
Approved for use through 01/31/2014. OMB 0651-0032
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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	104402-5002-US
	Application Number	14/335,763
Title of Invention	Method and System for Performing Mobile Device-To-Machine Payments	

Email Address	

Additional Applicant Data may be generated within this form by selecting the Add button.

Assignee Information including Non-Applicant Assignee Information:

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

Assignee 1

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication . An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

If the Assignee or Non-Applicant Assignee is an Organization check here. ☐

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information For Assignee including Non-Applicant Assignee:

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

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button.

Signature:

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

Signature				Date (YYYY-MM-DD)	2014-08-26
First Name	Douglas J.	Last Name	Crisman	Registration Number	39951

Additional Signature may be generated within this form by selecting the Add button.

PTO/AIA/14 (11-13)
Approved for use through 01/31/2014. OMB 0651-0032
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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	104402-5002-US
	Application Number	14/335,762
Title of Invention	Method and System for Performing Mobile Device-To-Machine Payments	

This collection of information is required by 37 CFR 1.76. 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 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet 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.**

METHOD AND SYSTEM FOR PERFORMING MOBILE DEVICE-TO-MACHINE PAYMENTS

PRIORITY CLAIM

[0001] The present application is an continuation of U.S. Patent Application Number 14/214,644, filed March 14, 2014, which claims priority to U.S. Provisional Patent Application Number 61/917,936, filed December 18, 2013, and is a continuation-in-part of U.S. Design Patent Application Number 29/477,025, filed December 18, 2013. The present application is based on and claims priority from these applications, the disclosures of which are hereby expressly incorporated herein by reference.

BACKGROUND OF THE INVENTION

[0002] Disclosed herein are mobile-device-to-machine payment systems and, more specifically, mobile-device-to-machine payment systems over a non-persistent network connection and featuring hands-free and manual modes.

[0003] Vending machines (or "automatic retailing" machines), in the broadest sense, have been around for thousands of years. The first simple mechanical coin operated vending machines were introduced in the 1880s. Modern vending machines stock many different types of products including, but not limited to drinks (e.g. water, juice, coffee, and soda) and edible food products/items (e.g. snacks, candy, fruit, and frozen meals), as well as a wide variety of non-food items. In this fast paced world, vending machines are ubiquitous.

[0004] Vending machines are one type of "payment accepting unit" (payment accepting units are also referred to herein generically as "machines"). A payment accepting unit (or machine) is equipment that requires payment for the dispensing of products and/or services. In addition to vending machines, payment accepting units can also be other machines that require payment for the dispensing of a product and/or services including, but not limited to parking meters, toll booths, laundromat washers and dryers, arcade games, kiosks, photo booths, toll booths, transit ticket dispensing machines, and other known or yet to be discovered payment accepting units.

[0005] In using a payment accepting unit, a user will (1) approach the payment accepting unit, (2) determine from the face of the payment accepting unit the product (or service) he desires, (3) insert payment (e.g. coins, bills, or payment cards), and (4) input his

selection into the payment accepting unit using a user interface (e.g. a series of buttons, a key pad, touch screen, or other input mechanism using, for example, the column and row at which a product is located). Based on the user's inputted selection, technology within the payment accepting unit provides the desired product (or service) to the user.

[0006] As the number of people with internet-connected mobile devices proliferates, so does the variety of uses for such devices. Mobile payment is a logical extension.

[0007] There is a large development effort around bringing mobile payment to the retail sector in an effort to not only provide options to the user, but also increased convenience.

[0008] In recent years, many improvements to modern vending machines have been suggested. Many of the innovations relate to means for communicating with the vending machine. Some of these communication innovations are detailed in U.S. Patent No. 6,584,309 to Whigham (the "Whigham reference"), U.S. Patent No. 7,085,556 to Offer (the "Offer reference"), U.S. Patent No. 7,127,236 to Khan et al. (the "Khan reference"), U.S. Patent No. 7,721,958 to Belfer et al. (the "Belfer reference"), U.S. Patent No. 8,396,589 to Katzenstein Garibaldi et al. (the "Garibaldi reference"), U.S. Patent No. 8,489,140 to Weiner et al. (the "Weiner reference"), and International Publication No. WO/2008/083025 to Carlson (the "Carlson reference").

[0009] The Whigham reference is directed to a system and method for purchasing a product from an automatic vending machine by means of a consumer's cellular telephone. The consumer requests a product available from the vending machine by dialing a specified telephone number that connects the consumer's cellular telephone to a server operated by a billing agency. The server recognizes the request for the product, creates a transaction record, and communicates a vend code to the consumer. Upon receiving the vend code from the server, the consumer transmits the vend code to the vending machine. The vend code may be an RF code, an audible tone code, or a manual code. Upon receipt of the vend code from the consumer, the vending machine dispenses the requested product.

[0010] The Offer reference is directed to a vending machine that is designed to communicate with a cellular phone such that it dispenses a product when it receives information indicating that the product has been selected. The Offer reference teaches permitting the cashless utilization of a vending machines via a communications service, such as a cellular telephone. A response to a signal from the cellular telephone from

[0011] the vending machine that indicates that a connection has been established between the vending machine and the cellular phone may be a visual indication that is displayed on the cellular telephone. The vending machine outputs the cost of the product and that cost is debited from an account to pay for the product.

[0012] The Khan reference describes a point of sale MicroAdapter device that enables payment transactions to be effected through a purchaser's personal trusted device (e.g. the user selecting the micropayment application on his personal trusted device and confirming or cancelling the purchase thereon) without relying upon tokens or prepayment cards. In one embodiment, the MicroAdapter includes a transceiver configured to receive a purchase signal from the personal trusted device including order and payment information. In response, the MicroAdapter communicates via wireless telephony with a transaction authorizer to receive authorization for effectuating the purchase transaction. The MicroAdapter can effectuate micropayment transactions authorized by a Billing On Behalf of Others program administered through a wireless carrier/ISP or third party.

[0013] The Belfer reference is directed to a system wherein a vending machine has an audio code collector and a code validator that is adapted to receive audio tones from a mobile device. The audio tones include authentication codes and dispense codes to control dispensing of product from the vending machine. To start the transaction, the consumer dials a unique set of symbols and digits to route the call to a verification server. The symbols and digits may correspond to a unique vending machine identification number and product identification numbers.

[0014] The Garibaldi reference is directed to an electronic device for the sale of intangible products through vending machines that include interfaces to communicate with external peripherals through the MDB protocol, the RS232 standard, and the DEX protocol, an interface to communicate with users, a communications system that enables it to act as part of a network and communicate with a central system, and a controller, that articulates the communication among the above-mentioned components, so as to enable a central system to perform diverse actions on a vending machine.

[0015] The Weiner reference is directed to a system and method for providing product or service with a cellular telephone. The problem identified in the Weiner reference is that mobile communication devices are long-range electronic devices designed to be used for long-range communications. Eschewing the use of near- field communication because it

requires special design or modification of the mobile station (e.g. the vending machine), the Weiner reference teaches a mobile communication device identifier, consisting of: a shielding defining a coverage area, the shielding arranged to reduce radio signals originating externally of the coverage area to be less than a pre-determined signal strength; an antenna associated within the defined coverage area; a transceiver coupled to the antenna, the transceiver communicating with a mobile station inserted within the defined coverage area utilizing a signal strength greater than the pre-determined signal strength; and a service control unit responsive to the transceiver, the service control unit responsive to the communication to output a signal indicative of an authorization to provide a product or service.

[0016] The Carlson reference is directed to a system and a method for using a portable consumer device such as a mobile phone for payments and the like. One embodiment of the Carlson system is directed to a method that includes the steps of receiving a payment request message (that includes a request to pay for a product from a vending machine) from a portable consumer device operated by a consumer, sending an authorization response message back to the vending machine wherein the vending machine subsequently prompts the consumer to enter a selection if the authorization response message indicates that the consumer is authorized to make a purchase, and receiving an acknowledgement message from the vending machine that the product was purchased. The step of "sending an authorization response message back to the vending machine" is performed by a remote payment server and would require a persistent network connection.

BRIEF SUMMARY OF THE INVENTION

[0017] Disclosed herein are mobile-device-to-machine payment systems and, more specifically, mobile-device-to-machine payment systems over a non-persistent network connection and featuring hands-free and manual modes.

[0018] Described herein is a mobile-device-to-machine payment system for facilitating a cashless transaction for purchase of at least one product or service by a user from a payment accepting unit that preferably has input mechanisms. The user has a mobile device that has both short-range communication technology and long-range communication technology. The payment accepting unit is capable of dispensing at least one product or service. The system includes an adapter module and a server. The adapter module is associated with the payment accepting unit and has short-range communication technology

for communicating with the short-range communication technology of the mobile device. The server has long-range communication technology for communicating with the long-range communication technology of the mobile device. The adapter module is for sending an authorization request for funds to the mobile device using short-range communication technology. The mobile device then forwards the authorization request for funds to the server using long-range communication technology. The server is for sending an authorization grant for funds to the mobile device using long-range communication technology. The mobile device the forwards the authorization grant for funds to the adapter module using short-range communication technology. The payment accepting unit dispenses the at least one product or service in response to receiving user input to the payment accepting unit input mechanism if the adapter module has received the authorization grant.

[0019] The adapter module may have security technology and the server may have security technology. The authorization request may be secured by the adapter module security technology to create a secured authorization request. The authorization grant may be secured by the server security technology to create a secured authorization grant. The secured authorization request and the secured authorization grant are preferably undecipherable to the mobile device.

[0020] The adapter module and the server may share a unique private key. The adapter module may have encryption/decryption technology and the server may have encryption/decryption technology. The authorization request may be encrypted by the adapter module encryption/decryption technology using the unique private key to create an encrypted authorization request. The encrypted authorization request may be decrypted by the server encryption/decryption technology using the unique private key. The authorization grant may be encrypted by the server encryption/decryption technology using the unique private key to create an encrypted authorization grant. The encrypted authorization grant may be decrypted by the adapter module encryption/decryption technology using the unique private key. The encrypted authorization request and the encrypted authorization grant are preferably undecipherable to the mobile device.

[0021] The adapter module is preferably surrounded by two zones, a payment zone and an authorization zone, wherein the payment zone is within the authorization zone. The adapter module sends the authorization request when the mobile device is within the authorization zone. The mobile device forwards the authorization grant for funds to the adapter module when the mobile device is within the payment zone. A third zone possible

zone is a communication zone, the authorization zone being within the communication zone. The mobile device preferably receives advertising broadcast signals from the adapter module within the communication zone.

[0022] The system may have a hands-free mode in which the payment accepting unit dispenses the at least one product or service without the user interacting with the mobile device. A display of the payment accepting unit may be used for displaying funds available based on information from the authorization grant. The input mechanisms of the payment accepting unit may be used for receiving user selection input when the user interacts with the input mechanisms to select the at least one product or service to be dispensed.

[0023] The adapter module may be an in-line dongle for in-line insertion within a multi-drop bus of the payment accepting unit. Further, the payment accepting unit may have a multi-drop bus to a payment receiving mechanism. The multi-drop bus may have a male adapter and a female adapter. The adapter module may have a male adapter and a female adapter. The adapter module is preferably insertable in serial with the multi-drop bus by connecting the male adapter of the adapter module to the female adapter of the multi-drop bus and by connecting the female adapter of the adapter module to the male adapter of the multi-drop bus.

[0024] Also described herein is a method for using a mobile-device-to-machine payment system for facilitating a cashless transaction for purchase of at least one product or service by a user from a payment accepting unit may have input mechanisms. The user may have a mobile device having both short-range communication technology and long-range communication technology. The payment accepting unit is preferably capable of dispensing at least one product or service. The method includes the steps of: (a) sending an authorization request for funds to the mobile device using short-range communication technology of an adapter module associated with the payment accepting unit; (b) receiving the authorization request for funds from the short-range communication technology of the adapter module at the short-range communication technology of the mobile device; (c) forwarding the authorization request for funds to a server using the long-range communication technology of the mobile device; (d) receiving the authorization request for funds from the long-range communication technology of the mobile device at long-range communication technology of the server; (e) sending an authorization grant for funds to the mobile device using the long-range communication technology of the server; (f) receiving the authorization grant for funds from long-range communication technology of the server at the

long-range communication technology of the mobile device; (g) forwarding the authorization grant for funds to the adapter module using the short-range communication technology of the mobile device; and (h) receiving the authorization grant for funds from the short-range communication technology of the mobile device at short-range communication technology of the adapter module. At least one product or service may then be dispensed from the payment accepting unit in response to receiving user input to the payment accepting unit input mechanism if the adapter module has received the authorization grant.

[0025] The method may include the steps of securing the authorization request using security technology associated with the adapter module to create a secured authorization request, securing the authorization grant using security technology associated with the server to create a secured authorization grant, and the secured authorization request and the secured authorization grant are preferably undecipherable to the mobile device.

[0026] The method may include the steps of (a) sharing a unique private key between the adapter module and the server, (b) encrypting using the unique private key the authorization request using encryption/decryption technology associated with the adapter module to create an encrypted authorization request, (c) decrypting using the unique private key the encrypted authorization request using encryption/decryption technology associated with the server, (d) encrypting using the unique private key the authorization grant using the encryption/decryption technology associated with the server to create an encrypted authorization grant, (e) decrypting using the unique private key the encrypted authorization grant using encryption/decryption technology associated with the adapter module, and (e) the encrypted authorization request and the encrypted authorization grant are preferably undecipherable to the mobile device.

[0027] The method may include the steps of (a) surrounding the adapter module with two zones, a payment zone and an authorization zone, wherein the payment zone is within the authorization zone, (b) the adapter module sending the authorization request when the mobile device is within the authorization zone; and (c) the mobile device forwarding the authorization grant for funds to the adapter module when the mobile device is within the payment zone. The adapter module may also include a third zone, a communication zone, wherein the authorization zone is within the communication zone. The mobile device receives advertising broadcast signals from the adapter module within the communication zone.

[0028] The method may have a hands-free mode in which the payment accepting unit dispenses the at least one product or service without the user interacting with the mobile device. The method may further include the steps of (a) displaying funds available on a display of the payment accepting unit, the funds available may be based on information from the authorization grant; and (b) receiving user selection input when the user interacts with input mechanisms of the payment accepting unit to select the at least one product or service to be dispensed.

[0029] The method may include the step of inserting the adapter module as an in-line dongle for in-line insertion within a multi-drop bus of the payment accepting unit. The method may include the step of inserting the adapter module in serial with the multi-drop bus by connecting a male adapter of the adapter module to a female adapter of the multi-drop bus and by connecting a female adapter of the adapter module to a male adapter of the multi-drop bus.

[0030] The subject matter described herein is particularly pointed out and distinctly claimed in the concluding portion of this specification. Objectives, features, combinations, and advantages described and implied herein will be more readily understood upon consideration of the following detailed description of the invention, taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

[0031] FIG. 1 is a schematic diagram that shows three zones: a first "communication zone" (e.g. "Bluetooth range"), a second "authorization zone," and a third "payment zone." The payment zone (that can't be zero) is smaller than or equal to (overlapping completely) the authorization zone.

[0032] FIG. 2 is a schematic diagram that shows the three zone of FIG. 1 with multiple users therein, the mobile-device-to-machine payment systems providing for managing and resolving multiple users.

[0033] FIG. 3 is a table that illustrates the hands-free credit or alert user principle.

[0034] FIG. 4 is a flow chart showing the logging RSSI at User Input.

[0035] FIG. 5 is a block schematic that shows elements of the system including, but not limited to, the adapter module, the machine, the mobile device, and exemplary servers, as well as communications therebetween.

[0036] FIG. 6 is a block schematic that shows there are three areas of encryption used (each is bi-directional) between the adapter module, the machine, the mobile device, and/or exemplary servers.

[0037] FIG. 7 is a block diagram that communications, messaging, vending sequence, and purchase flow between the adapter module, the mobile device, and a system management server.

[0038] FIG. 8A is a timing schematic diagram that shows additional elements and features of the system including, but not limited to, communications medium, messaging, vending sequence, and purchase flow, when the user enters the communication zone (Bluetooth Range).

[0039] FIG. 8B is a timing schematic diagram that shows additional elements and features of the system including, but not limited to, communications medium, messaging, vending sequence, and purchase flow, when the user enters the Authorization Zone.

[0040] FIG. 8C is a timing schematic diagram that shows additional elements and features of the system including, but not limited to, communications medium, messaging, vending sequence, and purchase flow, when the user enters the Payment Zone and, in particular, detailing the hands-free mode alternative and the swipe mode alternative.

[0041] FIG. 8D is a timing schematic diagram that shows additional elements and features of the system including, but not limited to, communications medium, messaging, vending sequence, and purchase flow, in a vending transaction including a loop for multiple transactions.

[0042] FIG. 8E is a timing schematic diagram that shows additional elements and features of the system including, but not limited to, communications medium, messaging, vending sequence, and purchase flow, in the Login mode.

[0043] FIG. 8F is a timing schematic diagram that shows additional elements and features of the system including, but not limited to, communications medium, messaging, vending sequence, and purchase flow, during Module bootup.

[0044] FIG. 8G is a timing schematic diagram that shows additional elements and features of the system including, but not limited to, communications medium, messaging, vending sequence, and purchase flow, during Account Check/Update.

[0045] FIGS. 9A - 9E are flow charts that show exemplary steps and features of the system including, but not limited to, communications, messaging, vending sequence, and purchase flow.

[0046] FIGS. 10A - 10D show an exemplary mobile device with a graphical representation of an exemplary mobile application shown thereon, the mobile application being used as part of the mobile-device-to-machine payment systems.

[0047] FIG. 11 is a perspective view of the exemplary first preferred in-line dongle adapter module.

[0048] FIG. 12 is a front plan view of the in-line dongle adapter module of FIG. 11.

[0049] FIG. 13 is a back plan view of the in-line dongle adapter module of FIG. 11.

[0049.1] FIG. 14 is a side view of the in-line dongle adapter module of FIG. 11 in accordance with some implementations.

[0050] FIG. 15 is a first end view of a connector receptacle of the in-line dongle adapter module of FIG. 11.

[0051] FIG. 16 is a second end view of a connector receptacle of the in-line dongle adapter module of FIG 11.

[0052] FIG. 17 is a perspective view taken from the first end of the in-line dongle adapter module of FIG. 11, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for environmental purposes.

[0053] FIG. 18 is a perspective view taken from the second end of the in-line dongle adapter module of FIG. 11, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for environmental purposes.

[0054] FIG. 19 is a perspective view of the in-line dongle adapter module of FIG. 11 within a vending machine.

[0055] FIG. 20 is a perspective view of the exemplary second preferred in-line dongle adapter module.

[0056] FIG. 21 is a front plan view of the in-line dongle adapter module of FIG. 20.

[0057] FIG. 22 is a back plan view of the in-line dongle adapter module of FIG. 20.

[0058] FIG. 23 is a first side view of the in-line dongle adapter module of FIG. 20, the second side being a mirror image of that shown.

[0059] FIG. 24 is a first end view of a connector receptacle of the in-line dongle adapter module of FIG. 20.

[0060] FIG. 25 is a second end view of a connector receptacle of the in-line dongle adapter module of FIG 20.

[0061] FIG. 26 is a perspective view taken from the first end of the in-line dongle adapter module of FIG. 20, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for environmental purposes.

[0062] FIG. 27 is a perspective view taken from the second end of the in-line dongle adapter module of FIG. 20, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for environmental purposes.

[0063] FIG. 28 is a perspective view of the in-line dongle adapter module of FIG. 20 within a vending machine.

[0064] FIG. 29 is a perspective view of the exemplary third preferred in-line dongle adapter module with a gap indicating the in-line dongle adapter module can be of any length.

[0065] FIG. 30 is a front plan view of the in-line dongle adapter module of FIG. 29.

[0066] FIG. 31 is a back plan view of the in-line dongle adapter module of FIG. 29.

[0067] FIG. 32 is a first side view of the in-line dongle adapter module of FIG. 29, the second side being a mirror image of that shown.

[0068] FIG. 33 is a first end view of a connector receptacle of the in-line dongle adapter module of FIG. 29.

[0069] FIG. 34 is a second end view of a connector receptacle of the in-line dongle adapter module of FIG. 29.

[0070] FIG. 35 is a perspective view taken from the first end of the in-line dongle adapter module of FIG. 29, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for environmental purposes.

[0071] FIG. 36 is a perspective view taken from the second end of the in-line dongle adapter module of FIG. 29, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for environmental purposes.

[0072] FIG. 37 is a perspective view of the in-line dongle adapter module of FIG. 29 within a vending machine.

[0073] FIG. 38 is a perspective view of the exemplary fourth preferred in-line dongle adapter module with two vertical gaps indicating the in-line dongle adapter module can be of any width.

[0074] FIG. 39 is a front plan view of the in-line dongle adapter module of FIG. 38.

[0075] FIG. 40 is a back plan view of the in-line dongle adapter module of FIG. 38.

[0076] FIG. 41 is a first side view of the in-line dongle adapter module of FIG. 38, the second side being a mirror image of that shown.

[0077] FIG. 42 is a first end view of a connector receptacle of the in-line dongle adapter module of FIG. 38.

[0078] FIG. 43 is a second end view of a connector receptacle of the in-line dongle adapter module of FIG 38.

[0079] FIG. 44 is a perspective view taken from the first end of the in-line dongle adapter module of FIG. 38, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for environmental purposes.

[0080] FIG. 45 is a perspective view taken from the second end of the in-line dongle adapter module of FIG. 38, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for environmental purposes.

[0081] FIG. 46 is a perspective view of the in-line dongle adapter module of FIG. 38 within a vending machine.

[0082] FIG. 47 is a perspective view of the exemplary fifth preferred in-line dongle adapter module and, specifically, the longitudinal center portion thereof, the dashed line depiction of the sides indicating the sides of the in-line dongle adapter module can be of any shape or curvature.

[0083] FIG. 48 is a front plan view of the in-line dongle adapter module of FIG. 47.

[0084] FIG. 49 is a back plan view of the in-line dongle adapter module of FIG. 47.

[0084.1] FIG. 50 is a side view of the in-line dongle adapter module of FIG. 47 in accordance with some implementations.

[0085] FIG. 51 is a first end view of a connector receptacle of the in-line dongle adapter module of FIG. 47.

[0086] FIG. 52 is a second end view of a connector receptacle of the in-line dongle adapter module of FIG 47.

[0087] FIG. 53 is a perspective view taken from the first end of the in-line dongle adapter module of FIG. 47, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for environmental purposes.

[0088] FIG. 54 is a perspective view taken from the second end of the in-line dongle adapter module of FIG. 47, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for environmental purposes.

[0089] FIG. 55 is a perspective view of the in-line dongle adapter module of FIG. 47 within a vending machine.

[0090] FIG. 56 is a block diagram of an exemplary adapter module.

[0091] FIG. 57 is a block diagram of an exemplary mobile device.

[0092] FIG. 58 is a block diagram of an exemplary server.

DETAILED DESCRIPTION OF THE INVENTION

[0093] Disclosed herein are mobile-device-to-machine payment systems and, more specifically, mobile-device-to-machine payment systems over a non-persistent network connection. The mobile-device-to-machine payment systems disclosed herein focus on the unattended retail space (e.g. a payment accepting unit 120 or machine 120). More specifically, mobile-device-to-machine payment systems disclosed herein allow a user (having a mobile device 150 with a mobile application 140 thereon) to make a cashless purchase from a payment accepting unit 120 (having an adapter module 100 associated therewith).

[0094] The mobile-device-to-machine payment systems described herein can be implemented with one or more of the following features: easy installation feature, a non-persistent network connection feature; a manual (swipe to pay) mode feature; a hands-free mode feature; and a multiple vending transactions (multi-vend) feature.

[0095] Easy Installation: Installation is very easy, requires no tools, requires no configuration, and takes as little as 30 seconds. This is accomplished by using an adapter

module 100 such as an in-line dongle (a hardware device with software thereon) design for in-line insertion within a multi-drop bus (MDB) of a payment accepting unit (e.g. a vending machine). Installation is as simple as "powering down" (turning off) the machine 120, identifying the "wire" that connects with a payment receiving mechanism (e.g. the coin mechanism), disconnecting the wire (so that there are two loose ends, such as a male connection end or adapter of an MDB and a female connection end or adapter of an MDB), plugging (inserting) the adapter module 100 in serial ("in-line") with the wire (for example, connecting the MDB female adapter to a male adapter of the adapter module 100 and connecting the MDB male adapter to a female adapter of the adapter module 100), tucking the wire and the installed adapter module 100 back into position, and "powering up" (turning on) the machine 120. Most vending machines made since 1995 have this industry standard MDB technology that would allow this easy 30-second installation. On machines without MDB technology, the adapter module 100 can be configured or designed to work with other serial protocols or activate a switch. In essence the adapter module 100 simulates establishing payment on payment accepting unit 120 in much the same manner as other alternative forms of payment (e.g. cash).

[0096] Non-persistent Network Connection: Although payment accepting units (or "machines") that accept only cash (e.g. paper currency and coins) may not require a connection (persistent or non-persistent) to a network, traditional payment accepting units that accept cashless payments (e.g. credit cards, debit cards, and alternative mobile device payment methods using, for example, smart phones) require a persistent connection to a network (wired or wireless) to facilitate the cashless payments. In other words, without a persistent (ongoing or accessible on demand) network connection, traditional payment accepting units cannot accept cashless payments. Most traditional payment accepting units that accept cashless payments include the technology to accomplish this persistent network connection that allows them to connect to a remote server. If the network connection to a traditional machine is temporarily interrupted, cashless payments will be temporarily unavailable. If the machine is located in a location where no signal is available, cashless payments will not be possible. The Whigham reference, the Offer reference, and the Belfer reference disclose alternative payment accepting units that accept cashless payments by using the user's cellular phone to allow the user to manually input coding to a remote server and, thereby act as an on-demand bridge network connection. These references, however, require significant user interaction with the cellular telephone to effectuate the transaction. In

addition to using a mobile device 150 as an intermediary between the payment accepting units 120 and the server 130, mobile-device-to-machine payment systems described herein minimize (manual mode) or eliminate (hands-free mode) user interaction with the mobile device 150. Further, some mobile-device-to-machine payment systems described herein facilitate the acceptance of cashless payments without requiring any network connection near the payment accepting unit 120. Mobile-device-to-machine payment systems described herein that are located in a remote location where no signal is available, therefore, can accept cashless payments.

[0097] Manual (Swipe to Pay) Mode: Using a "swipe to pay" feature (or just "swipe") refers to a user's action implemented on his mobile device 150 in which he quickly brushes his finger (or other pre-determined interaction) on the mobile device's touch screen 152 (or other input device associated with the mobile device 150). From the user's perspective, when the user is within range, a pre-installed mobile application 140 automatically connects to the payment accepting unit 120 (e.g. a vending machine). The mobile application 140 might display (on the touch screen 152) a prepaid balance that the user "swipes" to transfer payment to the payment accepting unit 120. The user could observe the transferred funds on the touch screen 152 of the mobile device 150 and/or on the display 122, 124 of the payment accepting unit 120. The transaction is completed just as if cash was inserted in the machine 120 with the user inputting his selection on the payment accepting unit 120 and the payment accepting unit 120 dispensing the product or service. After the selection is made, the change is returned to the mobile device 150 and this may be shown on the touch screen 152 of the mobile device 150.

[0098] Hands-Free Mode: A "hands-free pay" feature (or just "hands-free") would most likely be used with "favorite" payment accepting units 120 (e.g. a vending machine at work or school). From the user's perspective, he would approach the favorite payment accepting unit 120 and notice that the display 122, 124 of the payment accepting unit 120 showed funds available, he would select the product or service using the payment accepting unit's input mechanisms (e.g. buttons 126 or a touch screen display 124 shown in FIG. 19), and he would retrieve his dispensed services or products. It would be that simple. More specifically, when the user is within range, a pre-installed mobile application 140 automatically connects to the payment accepting unit 120 (e.g. a vending machine). The user may leave the mobile device 150 in a pocket, purse, briefcase, backpack, or other carrier. As the user approaches the payment accepting unit 120 and is in approximately "arms-length"

distance (e.g. 3 to 5 feet), the user could observe the transferred funds on the display 122, 124 of the payment accepting unit 120. The transaction is completed just as if cash was inserted in the machine 120 with the user inputting his selection on the payment accepting unit 120 and the payment accepting unit 120 dispensing the product or service. After the selection is made, the change is returned to the mobile device 150. FIG. 3 details when the hands-free mode would be available.

[0099] Multiple Vending Transactions (Multi-Vend): Both the "swipe to pay" feature and the "hands-free pay" feature could be used multiple times in sequence (implemented, for example, as a loop) so that a user may make multiple purchases. After making his first selection and receiving his product (or service), the user would observe that additional funds were available on the display 122, 124 on the payment accepting unit 120. He could make another selection (or multiple selections) and receive additional product(s) (or service(s)). More specifically, the display 122, 124 may reset as if the transaction is complete, but then, because the user is still standing in range, the mobile application 140 would send another credit to the payment accepting unit 120, allowing for a second purchase. When the walks away, the system clears (e.g. returns unused funds to the mobile application 140 on the mobile device 150.

[00100] The features described above, alone or in combination with other features described herein will revolutionize the hundred billion dollar automated retail industry. The exemplary hardware is very low cost and there are no reoccurring fees because no cellular connection is required on the machine 120. Using the mobile-device-to-machine payment systems described herein, operators can increase frequency of visits and items sold with each visit.

[00101] Mobile-device-to-machine payment systems described herein may be implemented as an apparatus and/or method for enabling payments to a machine 120 via a mobile device 150. Exemplary mobile-device-to-machine payment systems may be better understood with reference to the drawings, but the shown mobile-device-to-machine payment systems are not intended to be of a limiting nature.

Definitions

[00102] Before describing the mobile-device-to-machine payment systems and the figures, some of the terminology should be clarified. Please note that the terms and phrases may have additional definitions and/or examples throughout the specification. Where

otherwise not specifically defined, words, phrases, and acronyms are given their ordinary meaning in the art. The following paragraphs provide some of the definitions for terms and phrases used herein.

- Adapter Module 100: As shown in FIGS. 1 and 2, the adapter module 100 is a physical device that is installed in a machine 120 (a payment accepting unit 120). The shown exemplary adapter module 100 is an in-line dongle (a hardware device with software thereon) device that may be inserted in-line within a multi-drop bus (MDB) of a machine 120. The adapter module 100 bridges the communication between the machine 120 and a mobile device 150. Although described as a unique component, it should be noted that the adapter module 100 could be implemented as a plurality of devices or integrated into other devices (e.g. components of a machine 120). In its unique component form, the adapter module 100 can be easily inserted into a machine 120 so that the machine 120 is able to perform new features with the assistance of the adapter module 100. FIG. 56 shows exemplary components associated with the adapter module 100. The shown example may be divided into multiple distinct components that are associated with each other or the example may be incorporated into or drawn from other technology (e.g. a computer or a payment accepting unit) as long as the components are associated with each other.

- Mobile Device 150 and Application 140 (also referred to as a "mobile application," "mobile app," or "app"): In general, a mobile device 150 may be a user's personal mobile device 150. The mobile device 150 (with a mobile application 140 thereon) acts as a communication bridge between the adapter module 100 (associated with a payment accepting unit 120) and the server 130. The mobile device 150 and application 140, however, are not "trusted" in that the communications (transmissions) it passes are encrypted. Encrypted (secured) communications are undecipherable (unencryptable, unreadable, and/or unuseable) by the mobile device 150. This keeps the passed communications secured and safe from hacking. Exemplary mobile devices include, but are not limited to smart phones, tablet or laptop computers, or personal digital assistants (PDAs), smart cards, or other technology (e.g. a hardware-software combination) known or yet to be discovered that has

structure and/or capabilities similar to the mobile devices described herein. The mobile device 150 preferably has an application 140 (app 140) running on it. The term "app" is used broadly to include any software program(s) capable of implementing the features described herein. FIGS. 10A-10D show exemplary mobile devices 150 with associated apps 140 associated therewith. It should be noted that the phrase "mobile device" can be assumed to include the relevant app unless specifically stated otherwise. Similarly, it should be noted that an "app" can be assumed to be running on an associated mobile device unless specifically stated otherwise. FIG. 57 shows exemplary components associated with the mobile device 150. The shown example may be divided into multiple distinct components that are associated with each other or the example may be incorporated into or drawn from other technology (e.g. the cell phone itself) as long as the components are associated with each other.

- Payment Accepting Unit 120 (or Machine 120): A payment accepting unit 120 (or machine 120) is equipment that requires payment for the dispensing of an product and/or service. Payment accepting units 120 may be vending machines, parking meters, toll booths, laundromat washers and dryers, arcade games, kiosks, photo booths, toll booths, transit ticket dispensing machines, and other known or yet to be discovered payment accepting units 120. Some payment accepting units 120 can accept cashless payments (payments other than cash (paper currency and coins)) by accepting payment from, for example, credit cards, debit cards, and mobile devices.
- Network Connections: For purposes of this discussion, a persistent network connection is a wired or wireless communications connection that is ongoing (e.g. a dedicated connection, a dedicated online connection, and/or a hardwired connection) or accessible on demand (e.g. the ability for the machine to make a temporary connection to a server or the ability for the user to contact a server from his mobile device). Typically the persistent network connection has been conducted over "long-range communication technology" (e.g. hardwired, telephone network technology, cellular technology, WiFi technology, wide area network (WAN), local area network (LAN), or any wired or wireless communication technology over the internet that is known or

yet to be discovered). Traditionally, machines that accept payment other than cash require a persistent (ongoing or accessible on demand) connection to a network to facilitate payment. This is true for machines that accept, for example, credit cards and debit cards. The payment accepting units 120 described herein do not require a traditional persistent network connection. The user's mobile device 150 acts as a communication bridge between the adapter module 100 and the server 130. Communications between user mobile devices 150 and the servers (e.g. a system management server 130 and/or a funding source server 160) take place using long-range communication technology. Communications between user mobile devices 150 and the adapter module 100 of the payment accepting unit 120 take place using "short-range communication technology" (e.g. Bluetooth (e.g. Bluetooth 4.0, Bluetooth Smart, Bluetooth LE (Low Energy), near-field communication, Ultra Wideband (UWB), RFID, infrared wireless, induction wireless, or any wired or wireless technology that could be used to communicate a small distance (e.g. approximately a hundred feet or closer) that is known or yet to be discovered). Neither the adapter module 100 nor the payment accepting unit 120, therefore require a traditional persistent long-range wireless network connection. The exemplary communications technology shown in the figures may be replaced with alternative like communications technology and, therefore, specific shown communications technologies are not meant to be limiting. For example WiFi technology could be replaced with another long-range communication technology.

- Server: A server is the host processing server that may be operated by the company running the system. For each user, the server 130 preferably maintains at least one "virtual wallet" having at least one "balance" (which can be $0) of designated funds for which the server 130 keeps an accounting. The balance may represent, for example, "cash" or it may be a "promotional value" that represents funds that may be spent under certain circumstances. If these funds begin to be depleted, the user may be notified (e.g. via the application 140 on the mobile device 150) that additional funds need to be designated and/or transferred. Alternatively, funds from other sources (e.g. the funding source server 160) may be automatically transferred to restore a

predetermined balance. The balance may also be increased based on a promotion (e.g. points earned or coupons). As shown in FIG. 58, the server includes appropriate processors 950, memory 960 (which would keep an accounting of the user's balance in a manner similar to a gift card), and communication systems 970. As shown, the communications unit 970 of the server 130 includes long-range communication technology (e.g. cellular technology and WiFi mechanisms). The server 130 also includes a security unit 955 for encrypting and decrypting messages. The server 130 receives an AuthRequest from the adapter module 100 (via a mobile device 150) and, if funds are available, returns the AuthGrant for funds. FIG. 58 shows exemplary components associated with the server 130. The shown example may be divided into multiple distinct components that are associated with each other or the example may be incorporated into or drawn from other technology (e.g. a computer or a main frame) as long as the components are associated with each other.

- Advertise Presence: Each adapter module 100 advertises its presence by broadcasting signals (advertising broadcast signals) to mobile devices in the zones 102, 104, 016. Each adapter module 100 can listen to other adapter modules' advertisements

- Received Signal Strength Indicator (RSSI): The adapter module 100 may have a self-calibrating signal strength to determine zone thresholds (e.g. a payment zone threshold). At the time the user selects an item (product or service) from the payment accepting unit 120, the Received Signal Strength Indicator (RSSI) is logged. At this moment, it is presumed the user is within "arms-length" (which may be a predetermined length approximating the distance of a user standing in front of a machine for the purpose of making a purchase) from the payment accepting unit 120. Mathematical computation (In-Range Heuristics) is conducted to derive the optimal RSSI threshold at which point payment should be triggered by an application 140 on a mobile device 150. The threshold may be payment accepting unit specific and can vary over a period of time. This optimal zone threshold is preferably reported to the mobile device 150 during an initial handshake.

- In-Range Heuristics: Mathematical computation that determines the RSSI threshold to determine when a user is in the authorization zone 104 and/or payment zone 102. This computation can take into consideration numerous historical data points as well as transaction specific information such as which mobile device 150 is being used, payment accepting unit type, among other factors. Preferably the RSSI is logged while the user is making his selection (this is the one time in the entire process that the user definitely will be "in range" (e.g. they will be arm's length from the machine 120 because they are physically interacting with the machine 120). The type of user mobile device 150, accelerometer data (e.g. is the user moving or stationary), and/or other information may also be logged while the user is making his selection. The adapter module 100 can give a reference RSSI for the payment zone 102 for the machine 120, and the application 140 can make a +/- adjustment based on the specific mobile device 150 on which it is installed. Over a period of time, the system continues to improve itself based on additional data points.

- Authorization Request (AuthRequest): When a user enters the authorization zone 104, the mobile device 150 notifies the adapter module 100 and the adapter module 100 sends the secured authorization request (e.g. the encrypted authorization request) as a "message" (also referred to as a communication or transmissions) to the server 130 via the mobile device 150. Encryption may be performed by a security unit 755 (security technology that may be associated with the processing unit 750 and/or the memory 760). Significantly, the AuthRequest is a request for authorization of funds, not a request for authorization of a transaction. The purpose of the funds is irrelevant to the server 30.

- Authorization Grant Token (AuthGrant): This is a "message" (also referred to as a communication or transmissions) encrypted by the security unit 955 (security technology) of the server 130 with the unique private key for the adapter module 100. The secured authorization grant (e.g. the encrypted authorization grant) is passed from the server 130 (via the mobile device 150) to the adapter module 100 in the form of a message. The mobile device 150, however, is not able to decrypt and read the message. The authorization grant is in response to the authorization request. The amount of the funds granted

by the AuthGrant may be determined by factors including, but not limited to, the amount of funds available (or, if funds are not available, a mini-loan could be granted), a pre-authorized amount (e.g. set by the server, set by the user during set-up, set by the funding source, or a standard amount), limited by time (e.g. only a certain amount per hour, or a predetermined amount at specific times of the day), limited to the maximum amount of an item on the machine (or enough for two or three items in the machine), or one or more of these and other factors. Significantly, the AuthGrant makes the funds available, but does not authorize a transaction. The AuthGrant may have an associated expiration period in that it may expire if it is not used in a pre-determined time period. The length of time before the AuthGrant expires may be determined by factors including, but not limited to, the trustworthiness of the user (e.g. the user has a long history with the system or some known provider (e.g. credit card provider, bank, or credit union), the user has a good credit rating, or the user has a large wallet balance), a pre-authorized time period (e.g. set by the server, set by the user during set-up, set by the funding source, or a standard time period), limited by time (e.g. predetermined time periods at specific times of the day such as longer times during breakfast, lunch, and dinner), limited by the machine or the products or services sold in the machine, limited by the number of other users near the machine (e.g. if it is a crowded machine, the AuthGrant may expire faster), or one or more of these and other factors. The AuthGrant remains valid until it expires or some other event occurs to end its validity (e.g. the user cancels it). This means that under normal circumstances the mobile device 150 will hold the AuthGrant authorizing use of funds for a pre-determined time period that will allow the user sufficient time to make a purchase. The authorized amount may be considered to be the "wallet balance" that is held in a virtual "wallet."

- Synchronization: Time may be synchronized to the adapter module 100 from the server 130. The server 130 sends time information with encrypted messages and the adapter module 100 uses the time encoded in the messages for synchronization.
- The mobile-device-to-machine payment systems and components thereof may have associated hardware, software, and/or firmware (a variation, subset, or

hybrid of hardware and/or software). The term "hardware" includes at least one "processing unit," "processor," "computer," "programmable apparatus," and/or other known or yet to be discovered technology capable of executing instructions or steps (shown as processing unit 750 in FIG. 56, processing unit 850 in FIG. 57, and processing unit 950 in FIG. 58). The term "software" includes at least one "program," "subprogram," "series of instructions," or other known or yet to be discovered hardware instructions or hardware-readable program code. Software may be loaded onto hardware (or firmware) to produce a "machine," such that the software executes on the hardware to create structures for implementing the functions described herein. Further, the software may be loaded onto the hardware (or firmware) so as to direct the mobile-device-to-machine payment systems (and components thereof) to function in a particular manner described herein or to perform a series of operational steps as described herein. "Hardware" such as the adapter module 100, mobile device 150, and payment accepting unit 120 may have software (e.g. programs and apps) loaded thereon. The phrase "loaded onto the hardware" also includes being loaded into memory (shown as memory 760 in FIG. 56, memory 860 in FIG. 57, and memory 960 in FIG. 58) associated with or accessible by the hardware. The term "memory" is defined to include any type of hardware (or other technology) -readable media (also referred to as computer-readable storage medium) including, but not limited to, attached storage media (e.g. hard disk drives, network disk drives, servers), internal storage media (e.g. RAM, ROM, EPROM, FLASH-EPROM, or any other memory chip or cartridge), removable storage media (e.g. CDs, DVDs, flash drives, memory cards, floppy disks, flexible disks), firmware, and/or other known or yet to be discovered storage media. Depending on its purpose, the memory may be transitory and/or non-transitory. Appropriate "messages," "communications," "signals," and/or "transmissions" (that includes various types of information and/or instructions including, but not limited to, data, commands, bits, symbols, voltages, currents, electromagnetic waves, magnetic fields or particles, optical fields or particles, and/or any combination thereof) over appropriate "communication paths," "transmission paths," and other means for signal transmission including any type of connection between two elements on the system (the system including, for example, the adapter

module 100, mobile device 150, payment accepting unit 120, hardware systems and subsystems, and memory) would be used as appropriate to facilitate controls and communications.

- It should be noted that the terms "programs" and "subprograms" are defined as a series of instructions that may be implemented as software (i.e. computer program instructions or computer-readable program code) that may be loaded onto a computer to produce a "machine," such that the instructions that execute on the computer create structures for implementing the functions described herein or shown in the figures. Further, these programs and subprograms may be loaded onto a computer so that they can direct the computer to function in a particular manner, such that the instructions produce an article of manufacture including instruction structures that implement the function specified in the flow chart block or blocks. The programs and subprograms may also be loaded onto a computer to cause a series of operational steps to be performed on or by the computer to produce a computer implemented process such that the instructions that execute on the computer provide steps for implementing the functions specified in the flow chart block or blocks. The phrase "loaded onto a computer" also includes being loaded into the memory of the computer or a memory associated with or accessible by the computer. Separate, albeit interacting, programs and subprograms may be associated with the adapter modules 100, the server 130, and the mobile device 150 (including the mobile application 140) and these programs and subprograms may be divided into smaller subprograms to perform specific functions.

- The terms "messages," "communications," "signals," and/or "transmissions" include various types of information and/or instructions including, but not limited to, data, commands, bits, symbols, voltages, currents, electromagnetic waves, magnetic fields or particles, optical fields or particles, and/or any combination thereof. Appropriate technology may be used to implement the "communications," "signals," and/or "transmissions" including, for example, transmitters, receivers, and transceivers. "Communications," "signals," and/or "transmissions" described herein would use appropriate technology for their intended purpose. For example, hard-wired communications (e.g. wired serial

communications) would use technology appropriate for hard-wired communications, short-range communications (e.g. Bluetooth) would use technology appropriate for close communications, and long-range communications (e.g. WiFi or Cellular) would use technology appropriate for remote communications over a distance. Appropriate security (e.g. SSL or TLS) for each type of communication is included herein. Security units 755 and 955 include technology for securing messages. The security technology may be, for example, encryption/decryption technology (e.g. software or hardware). Although encryption/decryption is discussed primarily as being performed using a unique private key, alternative strategies include, but are not limited to encryption/decryption performed using public/private keys, or other encryption/decryption strategies known or yet to be discovered. Appropriate input mechanisms and/or output mechanisms, even if not specifically described, are considered to be part of the technology described herein. The exemplary communications unit 770 (shown in FIG. 56) of the adapter module 100 is shown as including appropriate input and output mechanisms 772, 774 that may be implemented in association (e.g. directly or indirectly in functional communication) with male and female adapters 720, 730 of the adapter module 100. The exemplary communications unit 870 (shown in FIG. 57) of the mobile device 150 includes mechanisms for both long-range communications (shown as Cellular and/or WiFi mechanisms 872) for communicating with the server 130 and short-range communications (shown as Bluetooth mechanisms 876) for communicating with the adapter module 100.

- When used in relation to "communications," "signals," and/or "transmissions," the terms "provide" and "providing" (and variations thereof) are meant to include standard means of provision including "transmit" and "transmitting," but can also be used for non-traditional provisions as long as the "communications," "signals," and/or "transmissions" are "received" (that can also mean obtained). The terms "transmit" and "transmitting" (and variations thereof) are meant to include standard means of transmission, but can also be used for non-traditional transmissions as long as the "communications," "signals," and/or "transmissions" are "sent." The terms

"receive" and "receiving" (and variations thereof) are meant to include standard means of reception, but can also be used for non-traditional methods of obtaining as long as the "communications," "signals," and/or "transmissions" are "obtained."

- The term "associated" is defined to mean integral or original, retrofitted, attached, connected (including functionally connected), positioned near, and/or accessible by. For example, if the user interface (e.g. a traditional display 122 (FIG. 19), a touch screen display 124 (FIG. 19), a key pad 126 (FIG. 19), buttons 126 (FIG. 19, shown as part of the key pad 126), a keyboard (not shown), and/or other input or output mechanism) is associated with a payment accepting unit 120, the user interface may be original to the payment accepting unit 120, retrofitted into the payment accepting unit 120, attached to the payment accepting unit 120, and/or a nearby the payment accepting unit 120. Similarly, adapter modules 100 may be associated with payment accepting units 120 in that the adapter modules 100 may be original to the payment accepting unit 120, retrofitted into the payment accepting unit 120, attached to the payment accepting unit 120, and/or a nearby the payment accepting unit 120.
- It should be noted that relative terms are meant to help in the understanding of the technology and are not meant to limit the scope of the invention. Similarly, unless specifically stated otherwise, the terms used for labels (e.g. "first," "second," and "third") are meant solely for purposes of designation and not for order or limitation. The term "short" in the phrase "short-range" (in addition to having technology specific meanings) is relative to the term "long" in the phrase "long-range."
- The terms "may," "might," "can," and "could" are used to indicate alternatives and optional features and only should be construed as a limitation if specifically included in the claims.
- It should be noted that, unless otherwise specified, the term "or" is used in its nonexclusive form (e.g. "A or B" includes A, B, A and B, or any combination thereof, but it would not have to include all of these possibilities). It should be noted that, unless otherwise specified, "and/or" is used similarly (e.g. "A

and/or B" includes A, B, A and B, or any combination thereof, but it would not have to include all of these possibilities). It should be noted that, unless otherwise specified, the terms "includes" and "has" mean "comprises" (e.g. a device that includes, has, or comprises A and B contains A and B, but optionally may contain C or additional components other than A and B). It should be noted that, unless otherwise specified, the singular forms "a," "an," and "the" refer to one or more than one, unless the context clearly dictates otherwise.

System Overview

[00103] FIGS. 5, 6, and 7 together show exemplary major components of the mobile-device-to-machine payment system and the interactions therebetwen.

[00104] As shown, the adapter module 100 functionally connected bi-directionally to the payment accepting unit 120 via a wired serial connection such that no security is necessary. The adapter module 100 is also functionally connected bi-directionally to the mobile device 150 (and its installed mobile application 140) via short-range communication technology (e.g. a Bluetooth connection). Because the mobile device 150 is not a "trusted" link (e.g. it could be hacked by a user), only secured communications (transmissions) are passed between the adapter module 100 and the mobile device 150. This keeps the passed communications secured and safe from hacking. The mobile device 150 (and its installed mobile application 140) is also functionally connected bi-directionally to a system management server 130 and/or a funding source server 160 via long-range communication technology (e.g. WiFi or Cellular connection) that preferably has appropriate security (e.g. SSL security). Security between the mobile device 150 and the system management server 130 has the advantage of protecting communications from the mobile device 150 to the system management server 130 that may include sensitive data and may not be encrypted. The system management server 130 and the funding source server 160 may be connected via a wired Internet connection with SSL security. The system management server 130 may be connected via a wired Internet connection with SSL security to an operators' server 170. Although not necessary to implement a purchase transaction, for other purposes (e.g. inventory), the operators' server 170 may be connected to the payment accepting unit 120 using a handheld computer sync or a cellular connection.

[00105] Also, a unique private key may be used to securely transmit encrypted messages between the adapter module 100 and the system management server 130 (although the encrypted transmissions would most likely be routed through the mobile device 150). The server 130 stores a private key for each adapter module 100, and this key is only known to the adapter module 100 and the server 130. No intermediary is privy to this key (especially not the mobile device 150). When the adapter module 100 and server 130 communicate messages (e.g. AuthRequest and AuthGrant), the security unit 755 of the adapter module 100 encrypts the message with its private key and passes the message to the mobile device 150. The mobile device 150 (which preferably cannot decrypt the message) passes the encrypted message to the server 130. The server 130 is able to decrypt the message using the security unit 955 of the adapter module 100 and the unique private key. The security unit 955 of the server 130 uses this same unique private key to encrypt messages to the adapter module 100 and sends the message to the mobile device 150 to relay to the adapter module 100 that is able to decrypt the message using the security unit 755 of the adapter module 100 and the unique private key.

[00106] FIG. 7 shows specific exemplary communications and messaging with an exemplary vending sequence (the numbers to the left of the communications and messaging) between the adapter module 100, the mobile device 150, and the system management server 130. These communications are discussed in more detail in the discussion pertaining to the timing schematics (FIGS. 8A-8G) and the flow charts (FIGS. 9A-9E).

[00107] It should be noted that FIGS. 5, 6, and 7 are meant to be exemplary and to help in the understanding of the mobile-device-to-machine payment system. For example, the shown long-range communications technology may be replaced with alternative long-range communications technology known or yet to be discovered, the shown short-range communication technology may be replaced with alternative short-range communication technology known or yet to be discovered, and the shown security may be replaced with alternative security known or yet to be discovered. The shown connections are meant to be exemplary in that, for example, there may be intermediaries that are not shown. The shown components have been simplified in that, for example, only one mobile device 150 (or machine 120, adapter module 100, or server 130) is shown where many may be included. Finally, the order of the steps may be changed and some steps may be eliminated.

Adapter Module

[00108] FIGS. 11-55 show exemplary adapter modules 100a-100e (referred to generally as adapter modules 100). These are relatively low cost hardware that are pre-configured to work with industry standard a multi-drop bus (MDB). On machines without MDB technology, the adapter module 100 can be configured or designed to work with other serial protocols or activate a switch. In essence the adapter module 100 simulates establishing payment on payment accepting unit 120 in much the same manner as other alternative forms of payment (e.g. cash).

[00109] The shown exemplary adapter modules 100 are preferably designed to be used as an in-line dongle for in-line insertion within, for example, a MDB of a machine 120. The wire used in MDB technology uses male and female connection ends or adapters to allow the attachment of peripherals. In the case of a vending machine, the wire with the connection ends or adapters would be present to allow the attachment of a payment receiving mechanism (e.g. a coin mechanism). The MDB male and female adapters 700, 710 may be separated (as shown in FIGS. 17, 18, 26, 27, 35, 36, 44, 45, 53, and 54). The adapter modules 100 have male and female adapters 720, 730. The adapter module may be plugged (inserted) in serial ("in-line") with the wire. For example, the MDB female adapter 710 may be connected to the male adapter 720 of the adapter module 100 and the MDB male adapter 700 may be connected to the female adapter 730 of the adapter module 100. The resulting in-line configuration is shown in FIGS. 19, 28, 37, 46, and 55. It should be noted that the adapter modules 100 are designed to allow pass-through communications so that if the mobile-device-to-machine payment systems is not enabled (e.g. for a particular purchase or simply turned off) the MDB functions as though the adapter module 100 is not there and the machine 120 can function normally.

Hands-Free

[00110] Summarily, if it is available, a hands-free mode, from the user's perspective, would allow the user to approach a favorite payment accepting unit 120 and notice that the display (e.g. the displays 122 or 124 shown in FIG. 19) associated with the payment accepting unit 120 shows funds available (e.g. the wallet balance), he would select the product or service using input mechanisms (e.g. buttons 126 or a touch screen display 124 shown in FIG. 19) associated with the payment accepting unit 120, and he would retrieve his dispensed services or products.

[00111] During an initial handshake with the mobile device 150 (when the user is within range), the adapter module 100 reports to the mobile device 150 whether or not hands-free mode is available. If it is available, the installed mobile application 140 automatically connects to the payment accepting unit 120 without the user having to interact with the mobile device 150. The user observes that funds are available on the display 122, 124 of the payment accepting unit 120 and completes the purchase transaction as if cash was inserted in the machine 120 by inputting his selection on the payment accepting unit 120. The payment accepting unit 120 dispenses the product or service. After the selection is made, the change is returned to the mobile device 150.

[00112] Whether hands-free payment is available is determined by factors including, but not limited to whether if other mobile devices 150 are in range, if other adapter modules 100 are in range, if there are any alerts, if the payment trigger threshold is having wide variances and so deemed unstable, or if the payment accepting unit operator (e.g. a vending machine operator) has opted to disable hands-free mode for the payment accepting unit 120. In the latter instance, operators can disable via a maintenance mobile device 150, as well as through the operators' server 170 and/or the system management server 130.

[00113] FIG. 3 is a table that showing exemplary considerations, conditions, or factors that may be used to determine whether the hands-free pay feature is available. Starting at the "Favorite?" column, this indicates whether the payment accepting unit 120 is a favorite machine. Preferably the hands-free pay feature is only available for use with "favorite" payment accepting units 120 (e.g. a vending machine at work or school). The "Alert" column has to do with whether there is some reason (e.g. there are too many users in range) that the hands-free pay feature should not work and, if there is such a reason, the user will be notified (alerted) and may be able to use the manual mode to resolve the alert and/or complete the transaction. FIG. 3 shows situations in which a user is or is not able to make hands-free purchases from a machine 120 using a mobile application 140 on his mobile device 150. It should be noted that the shown interface is meant to be exemplary. For example, some of the features could be automated or pre-selected. (It should be noted that the left hand column, the "Tab" column, relates to whether the selected tab on the mobile application 140 is "all" or "favorite." FIGS. 10A-10D all show these tabs. Unlike the other columns in FIG. 3, this column has more to do with the functionality and view of the application 140 than specifically with the hands-free feature. The tabs would allow a user to select whether he wanted to be alerted when he was in range of all payment accepting units 120 or just

"favorite" payment accepting units 120 and the application 140 would show the appropriate view.)

[00114] Balance Display: An optional feature of the mobile-device-to-machine payment system that is particularly helpful in the hands-free mode (although it may be available in the manual mode and/or in a multiple-vend scenarios) is when the user's mobile device 150 sends "credit" to the payment accepting unit 120 (either via hands-free payment or through a manual swipe), the wallet balance is sent to the payment accepting unit 120 that is then displayed to the user on a display 122, 124 of the machine 120. This is particularly beneficial during hands-free mode when the user does not retrieve the mobile device 150 and, therefore, may not know the balance. Also, in a multiple-vend scenario the user would not have to calculate a remaining balance.

[00115] An exemplary hands-free and multiple-vend scenario with a balance display might be as follows: The user has $5.00 in his virtual wallet as that is the amount that has been authorized (the AuthGrant being stored on the mobile device 150). He walks up to the payment accepting unit 120 and $5.00 is displayed on the display 122, 124 of the payment accepting unit 120 since hands-free mode was enabled and credit was sent (e.g. via short-range communication technology) to the payment accepting unit 120. The user makes a selection of $1.50 by interacting (e.g. pressing buttons) with the machine 120. The item (product or service) is dispensed and the "change" is "returned" (e.g. via short-range communication technology) to the virtual wallet. But since user is still standing in the payment zone 102, the remaining wallet balance of $3.50 is sent to the payment accepting unit 120 and displayed so that the user can now see he has a $3.50 balance. (It should be noted that the authorized funds may remain on the machine 120 and not be transferred back to the mobile device 150 between transactions.) The user decides to purchase a $1.50 item, and the transaction is completed as usual (e.g. by interacting with the machine 120). Now the user is still standing in the payment zone 102 and he sees the wallet balance of $2.00 on the display 122, 124 of the payment accepting unit 120. Deciding he does not wish to purchase anything else, the user walks away. As he walks out of the payment zone 102, the credit is cleared from the machine 120. But he is left with the knowledge that his wallet balance is $2.00 even though he never touched the mobile device 150. Communications between the payment accepting unit 120 and the adapter module 100 (via the mobile device 150) handle the accounting incidental to the transaction. The remaining balance ($2.00) is technically

stored on the server 130, and may be reflected on the application 140 on the mobile device 150.

Multiple Distinct Zones

[00116] As shown in FIGS. 1 and 2, the functions performed by the adapter module 100 can be divided into distinct zones: a first "communication zone" (e.g. "Bluetooth range" 106), a second "authorization zone" 104, and a third "payment zone" 102. The payment zone102 (that can not be zero) is smaller than or equal to (overlapping completely) the authorization zone 104. (Put another way, the payment zone 102 is within or coextensive with the authorization zone 104.) The payment zone 102 is a subset of the authorization zone 104 with a ratio of the payment zone 102 to the authorization zone 104 ranging from 0.01:1 to 1:1. It is not necessarily a fixed ratio and can vary between different payment accepting units 120, different mobile devices 150, different users, and over time. While the zones 102, 104, 106 are depicted as having a uniform shape, the zones may not necessarily be uniform (or constant over time) in that the shape can vary. For example, the shape of the Bluetooth range 106 may vary depending on environmental conditions such as obstacles in the room and payment accepting unit 120 door/wall materials.

[00117] Bluetooth Range 106: The outermost range is the Bluetooth range 106. This is the area in which the adapter module 100 is able to broadcast its presence. In most situations, the Bluetooth range 106 is a passive range in that no actual data is exchanged between the mobile device 150 and the adapter module 100. While in the Bluetooth range 106, the mobile device 150 monitors the RSSI (Received Signal Strength Indicator).

[00118] Authorization Zone 104: The middle region is the authorization zone 104. This is a computed area based on the RSSI. As mentioned, the mobile device 150 monitors the RSSI while it is in the Bluetooth range 106. When the RSSI reaches a certain predetermined threshold based on In-Range Heuristics, the mobile device 150 can be considered to be in the authorization zone 104. In the authorization zone 104 the mobile device 150 establishes a connection to the adapter module 100 (e.g. a Bluetooth connection (FIG. 5) with SSL protection (FIG. 6)) and informs the adapter module 100 of its presence. After a successful handshake with the adapter module 100, the mobile device 150 registers the adapter module 100 and the adapter module 100 requests an authorization to the server 130 via the mobile devices' network connection (e.g. a WiFi or cellular connection (FIG. 5) with SSL protection (FIG. 6)). It is important to note the mobile device 150 and the adapter

module 100 have a non-exclusive relationship at this point. The adapter module 100 may collect registrations for all mobile devices 150 that are within the authorization zone 104.

[00119] An authorization occurs in preparation for when the user enters the payment zone 102. An authorization expires in a set period of time (for example, five minutes), so if the mobile device 150 is still in the authorization zone 104 at the time of expiration, the adapter module 100 submits for and receives another authorization. This will continue for a set number of times (for example, the limit may be three times to limit cases of numerous authorizations for a mobile device that may remain in the authorization zone 104 for an extended period of time without completing a transaction). Should authorization fail (for instance if the limit had been reached) prior to the user entering the payment zone 102, the adapter module 100 will request authorization when the mobile device 150 enters the payment zone 102 (which adds a few seconds to the experience).

[00120] Payment Zone 102: As a user enters the payment zone 102, the mobile device 150 establishes exclusive control of the adapter module 100. Once established, any other user in the payment zone 102 is put into a "waiting" status.

[00121] In the payment zone 102, the payment can be triggered automatically if the system has and is in hands-free mode. In such instances, the mobile device 150 is running the app 140 in background mode and will send credit to the payment accepting unit 120 without any explicit user interaction. The user completes the transaction on the payment accepting unit 120 in much the same manner as if cash had been inserted into the payment accepting unit 120 to establish credit. After the user completes the transaction (that may include one or more purchases), details of the transaction are preferably returned to the mobile device 150 and server 130 in separate messages. The message to the server 130 is preferably encrypted with the adapter module's 100 private key (FIG. 6) to ensure data integrity. As shown in FIG. 7, the "private key" coded message (Encrypted VendDetails) is preferably sent via the mobile device 150. The message to the mobile device 150 may be sent solely for the purpose of closing the transaction. The transaction history and balance are updated server-side via the encrypted message sent to the server 130.

[00122] The other mode of operation is manual mode. In manual mode, the user launches the mobile device 150 and is able to swipe to send payment to the payment accepting unit 120. The user can also swipe back to cancel the payment. Like in hands-free mode, the purchase transaction is completed on the payment accepting unit 120 in the same

manner as if cash were inserted into the payment accepting unit 120. The mobile device 150 is only used to send payment. Selection is made directly on the payment accepting unit 120.

[00123] Self-Calibrating Zone Threshold: A key, but optional feature, of the system is a self-calibrating payment zone RSSI threshold. Because RSSI can vary machine to machine, environment to environment, and device to device, having a fixed threshold at which payment is triggered can be problematic. The approach suggested herein is the creation of a self-calibrating threshold. When the user is interacting with the payment accepting unit 120 (such as when he makes his selection on the payment accepting unit 120), the payment accepting unit 120 notifies the adapter module 100 and the adapter module 100 logs the conditions such as RSSI, type of user mobile device 150, accelerometer data, and other information. It is at this point that it can be ascertained safely that the user is within arms-length from the payment accepting unit 120 (by necessity the user is arms-length because he is making some physical interaction with the payment accepting unit 120). This is the only point in the entire transaction in which it can be certain that the user is within arms-length from the payment accepting unit 120.

[00124] FIG. 4 shows a simplified set of exemplary steps involved when users enter the payment zone 102. Specifically, FIG. 4 shows that credit is established 200 (this may have been done in the authorization zone 104, but if not it would be handled in the payment zone 102), that the user makes a selection using the machine 202, that the machine notifies the adapter module of the selection 204, that the adapter module (optionally) logs the RSSI 206, and that the purchase process(es) continues 208. Using the historically logged RSSI data, the adapter module 100 calculates one of several "average" RSSI using various mathematical models. This "average" could be a traditional average, a moving average, a weighted average, a median, or other similar summary function. The adapter module 100 could pre-process the historical data before running the function, such as to eliminate top and bottom data points, suspect data points, etc.

[00125] Optionally, during the handshake between the mobile device 150 and the adapter module 100, the information transmitted to the adapter module 100 may include, for example, the model of the mobile device 150. Using the received information pertaining to the mobile device models, the adapter module 100 can create multiple payment thresholds, one for each mobile device model. This allows for variances that may be inherent in different types of Bluetooth radios. An alternative to this method is for the adapter module 100 to broadcast a baseline payment zone threshold, and the mobile device 150 can use an offset

from this baseline based on its specific model type. The payment zone thresholds (or baseline offsets) can be unique to specific types of mobile devices (e.g. by manufacturer, operating system, or component parts), models of mobile devices, or individual mobile devices (unique to each user).

[00126] In a typical scenario in which the payment zone threshold has been calibrated, the adapter module 100 advertises its presence along with the threshold at which it considers any mobile device 150 to be in the authorization zone 104. This is a one-way communication from adapter module 100 to mobile device 150. Once the mobile device 150 enters the authorization zone 104, there is a handshake that is established between the adapter module 100 and the mobile device 150. During this handshake, the mobile device 150 can share its model information with the adapter module 100, and the adapter module 100 can return the payment zone 102 threshold for that specific model.

[00127] Optionally, in addition to calibrating the payment zone threshold, the adapter module 100 can apply the self-calibrating model to the authorization zone 104 to calibrate the authorization zone threshold. As with the payment zone thresholds, the authorization zone thresholds can be unique to specific types of mobile devices, models of mobile devices, or individual mobile devices. In this scenario, the adapter module 100 would broadcast multiple thresholds by device type and the mobile device 150 would determine which threshold to apply (or alternatively broadcast a baseline and the mobile device 150 uses an offset based on its device model). Even in this scenario, the authorization zone 104 is a one-way communication.

[00128] Optionally, along with the threshold that is calculated (in the payment and/or the authorization zone(s)), a safety margin can be added to minimize scenarios in which a user is within range, but the mobile-device-to-machine payment systems do not recognize it because the threshold may not have been reached. For example, if the calculated RSSI for an iPhone 5 on machine 4567 is -68db, the mobile-device-to-machine payment systems may add a safety margin of -5db, and establish the threshold at -73db. So when a user's phone is communicating with the adapter module 100 at an RSSI of -73db or better, the mobile-device-to-machine payment systems will allow the mobile device 150 to credit the payment accepting unit 120. The safety margin can be set on the server 130 and downloaded to the adapter module 100, or set on the mobile device 150, or set on the adapter module 100 itself.

[00129] Optionally, in the payment zone threshold, the mobile device 150 can use other data to determine when to cancel the exclusive control of the payment accepting unit 120, to identify when the user is moving out of the payment zone 102. External data could include accelerometer data from the mobile device 150. Using that data, the mobile device 150 can determine whether the user is standing relatively still in front of the payment accepting unit 120, or if the user is in motion – effectively walking away from the payment accepting unit 120.

Signal Unavailability Adaptation

[00130] The mobile-device-to-machine payment systems described herein use a mobile device's 150 short-range communication technology (shown as Bluetooth mechanisms 876 in FIG. 57) and a mobile device's 150 long-range communications technology (shown as Cellular and/or WiFi mechanisms 872 in FIG. 57). The short-range communication technology 876 communicates with the adapter module's 100 short-range communication technology (shown as Bluetooth mechanisms 776 in FIG. 56). The long-range communications technology 872 communicates with the server's 130 communication technology (not shown). The mobile device 150 (with a mobile application 140 thereon) acts as a communication bridge between the adapter module 100 (associated with a payment accepting unit 120) and the server 130. This process is described herein and works properly if there is cellular or WiFi coverage within the payment zone 102.

[00131] One option if there is no cellular or WiFi coverage within the payment zone 102 is to determine whether there is cellular or WiFi coverage within the authorization zone 104 or the Bluetooth range 106. If there is, then the sizes of the zones 102, 104, 106 could be adapted and the timing could be adapted. For example, if the mobile devices 150 detected problems with the cellular or WiFi coverage within the payment zone 102, the user could carry his mobile device 150 into the other zones (or the mobile device 150 could use short-range communication technology to communicate with other mobile devices 150 within the authorization zone 104 or the Bluetooth range 106) to determine whether the zones have cellular or WiFi coverage. If they do have coverage, communication between the mobile device 150 and the server 130 can be advanced (conducted earlier when the mobile device 150 is further from the machine 120) or delayed (conducted later when the mobile device 150 is further from the machine 120). This can be thought of as changing the size or shapes of the zones 102, 104, 106. The timing would also have to be adjusted so that the authorization of funds (AuthGrant) does not expire before the user has a chance to make a purchase. It also

means that balance updates to the server 130 may happen after the user has moved away from the machine 120 and has cellular or WiFi coverage again.

[00132] Another option if there is no cellular or WiFi coverage within any of the zones 102, 104, 106 is for the user to obtain authorization while outside of the zones in a place with cellular or WiFi coverage. This may occur, for example, if a user knows that he will be going to a place with a payment accepting unit 120 equipped with an adapter module 100 (perhaps to a favorite payment accepting unit 120) that does not have (or rarely has) cellular or WiFi coverage. A user may also use the mobile application 140 to query payment accepting units 120 in a given range (e.g. within 50 miles) or at a given location (e.g. at a campground or in a particular remote city) to determine whether there is cellular or WiFi coverage within the zones 102, 104, 106. The user can then obtain pre-authorization from the server 130 using the mobile application 140. Again, the timing would also have to be adjusted so that the authorization of funds (AuthGrant) does not expire before the user has a chance to make a purchase. It also means that balance updates to the server 130 may happen after the user has moved away from the machine 120 and has cellular or WiFi coverage again. A mobile-device-to-machine payment system having the ability to implement this option would be able to accept cashless payments without requiring any network connection near the payment accepting unit 120. Mobile-device-to-machine payment systems described herein that are located in a remote location where no signal is available, therefore, can accept cashless payments.

[00133] As an example of a situation in which there might be no cellular or WiFi coverage within any of the zones 102, 104, 106 of a particular payment accepting unit 120, the user (a teenager) may be traveling to a remote location to attend summer camp where there is no cellular or WiFi coverage. The camp may have several payment accepting units 120 (e.g. a machine that creates a dedicated "hot spot" that requires payment for use, vending machines, or machines for renting equipment (e.g. bikes, kayaks, or basket balls)). The camp facility might notify parents that the mobile-device-to-machine payment system is available. The parents, while at home, could obtain authorization for a particular amount (that could be doled out a certain amount per day or limited to type of machine or location) to be authorized and "loaded" into the user's mobile device 150 and specify that the authorization will not expire for a certain period or until a certain date. Thereafter, while at camp, the user could use the mobile application 140 on his mobile device 150 in a manner similar to those discussed elsewhere herein. Short-range communications may be used for communications

between the adapter modules 100 (associated with the machines 120) and users' mobile devices 150.

[00134] One subtle but powerful component of the systems described herein is that they require internet network connection only in the authorization zone 104 and only for the time period required to send the AuthRequest and receive the AuthGrant. Once a valid AuthGrant is received by the mobile device 150, an internet network connection is not required by either the mobile device 150 or the adapter module 100 in the payment zone 102 as long as the AuthGrant is valid (unexpired). This mechanism allows the system to seamlessly handle authenticated transactions in (temporary) offline mode, with the deferred acknowledgement and transaction messages performing the bookkeeping and cleanup when network connection is regained. The alternatives described above provide a unique way to artificially extend the authorization zone to include any location where the mobile device 150 can communicate with the server 130.

Multiple User Resolution

[00135] As shown in FIG. 2, in likely practical scenarios, there will be multiple users in the zones 102, 104, 106. As shown, users 1, 2, and 3 are in the payment zone 102 near the machine 120, users 5 and 6 are shown as positioned between the authorization zone 104 and the Bluetooth range 106, users 4 and 7 are in the Bluetooth range 106, user 10 is positioned on the edge of the Bluetooth range 106, and users 8 and 9 are positioned outside of Bluetooth range 106. The mobile-device-to-machine payment systems provide for managing, and resolving issues pertaining to multiple users.

[00136] Users 4 and 7 are within the Bluetooth range 106 and user 10 is either entering or leaving the Bluetooth range 106. Within the Bluetooth range 106 the users' mobile devices 150 are able to see the adapter module's 100 advertisement. In this zone, the mobile device 150 preferably does not initiate a connection. The adapter module 100 is preferably unaware of the users in the Bluetooth range 106. All the adapter module 100 is doing is advertising its presence to any multitude of users that may be in Bluetooth range 106.

[00137] The adapter module 100 begins to log users as the users (and their respective mobile devices 150) enter the authorization zone 104 (shown in FIG. 2 as users 5 and 6). At this point, there is a non-exclusive connection initiated by the mobile device 150 to the adapter module 100. It does a handshake (e.g. to exchange information needed to obtain authorization and, optionally, to log information needed for a self-calibrating authorization

zone threshold) and the mobile device 150 contacts the server 130 for an authorization (e.g. sending an AuthRequest and receiving an AuthGrant). The adapter module 100 registers all mobile devices 150 that have requested and received AuthGrants. The adapter module 100 continues communicating with any other mobile device 150 that enters the authorization zone 104. After initial contact, the adapter module 100 may provide the mobile device 150 with a deferral delay of when to check back in with the adapter module 100 allowing opportunity for other mobile devices 150 to communicate with the adapter module 100.

[00138] If there is only one user in the payment zone 102, a purchase transaction may be performed. If there are multiple users in the payment zone 102, the mobile-device-to-machine payment system must handle the situation.

[00139] One optional exemplary solution for handling the situation of the multiple users in the payment zone 102 is queuing users in the payment zone 102. Once any mobile device 150 enters the payment zone 102, it establishes exclusivity to a particular mobile device 150 (first come first serve). Technically, however, the adapter module 100 is not establishing an exclusive connection to the mobile device 150. The adapter module 100 can still perform a round-robin poll and communicate with and advertise to other mobile devices 150. Instead, the adapter module 100 establishes a queue prioritized by RSSI and time (e.g. who was first and whether the authorization has expired) and it notifies (e.g. alerts) other mobile devices 150 to wait. The earliest valid (unexpired) authorization takes precedence when there is any tie in the RSSI. Otherwise, for example, the strongest average RSSI takes priority. Preferably the queue is not a static measure of the RSSI but an averaged measure over the period of time in the queue. This compensates for a scenario in which a user may be walking around in the queue and then shows up at the payment accepting unit 120 just as the previous user is finishing. If another user was also in the payment zone 102 and stood there the entire time, but may have newer authorization, he could win out.

[00140] Anytime that the adapter module 100 cannot determine exactly which user is in the payment zone 102 in front of the payment accepting unit 120, the adapter module 100 will disable hands-free payment. The mobile device 150 will send an alert to the user and he can use swipe to pay (manual mode). All users in payment zone 102 will show "Connected" and the first to swipe payment to the payment accepting unit 120 then locks out other users.

Multiple Module Resolution

[00141] In the scenario where there are multiple modules present, determining which payment accepting unit 120 a user is in front of can be a challenge. The mobile-device-to-machine payment systems described herein allow for adapter modules 100 to communicate to other adapter modules 100 in range via Bluetooth. Each user receives authorization grants for specific payment accepting units 120. This means if there are multiple adapter modules 100 within the same authorization zone 104, there will be multiple authorization grants for the user. When the user enters the payment zone 102, it can be difficult to differentiate which payment accepting unit 120 the user is in front of if the payment zones 102 overlap.

[00142] To solve this problem, when the user enters the payment zone 102, the adapter modules 100 communicate with each other to determine the RSSI for the particular user (based on the signal from his mobile device 150) to triangulate which adapter module 100 (and the associated payment accepting unit 120) is closer to the user. Optionally, the inter-module communications can restrict the user to establishing an exclusive connection with only one payment accepting unit 120.

[00143] Optionally, when the user connects to a payment accepting unit 120, the mobile device 150 can send a communication to the payment accepting unit 120 for momentary display to the user on the display 122, 124 of the payment accepting unit 120. For example, the mobile device 150 can send a communication (e.g. "connected" or "Fred's Mobile Device Connected") to the payment accepting unit's display 122, 124 for a predetermined period of time (e.g. 1-3 seconds) so when the user is in payment zone 102, it is clear which payment accepting unit 120 the user is connected to prior to making a purchase (either in hands-free or manual mode).

[00144] In addition, when the user is in manual mode, the mobile device 150 can display (e.g. on the touch screen 152 as shown in FIGS. 10A-10D) a visual indication of the payment accepting unit 120 (e.g. a picture and/or a payment accepting unit ID of the payment accepting unit 120) for visual confirmation. If the user is in manual mode, the user can manually change the payment accepting unit 120.

Descriptive Scenario

[00145] FIG. 7, FIGS. 8A-8G, and 9A-E (as well as other figures) can be used to understand a detailed exemplary scenario of the mobile-device-to-machine payment systems described herein. An exemplary flow of communications and steps are loosely described

below with reference to these (and other figures). It should be noted that alternative scenarios could include, for example, a modified order of the steps performed.

[00146] Prior to vending transactions, a user downloads a mobile app 140 onto his mobile device 150, creates an account, and configures a funding source via, for example, a funding source server 160. A funding source may be, for example, a debit card, a credit card, campus cards, rewards points, bank accounts, payment services (e.g. PayPal®) or other payment option or combination of payment options known or yet to be discovered. The funding sources may be traditional and/or nontraditional payment sources that are integrated into the ecosystem described herein and then used indirectly as a source of funds. Funds from the funding source are preferably held on the server 130 such that when an AuthRequest is received by the server 130, the server 130 can send an AuthGrant authorizing funds for a purchase.

[00147] The user can specify one or more "favorite" adapter module(s) 100 (that has a one-to-one relationship to the payment accepting unit 120) that he may visit regularly, such as a vending machine at school or work. Favorite adapter modules 100 appear on a pre-filtered list and allow for additional rich features such as hands-free payment.

[00148] The payment accepting unit 120 may be equipped with an adapter module 100 that is constantly advertising its availability via Bluetooth (or other "signals," "communications," and/or "transmissions"). This ongoing advertising and scanning for adapter modules is shown in FIG. 8A. As shown, the mobile device 150 is continuously scanning for any adapter module 100 within Bluetooth (or other "signal," "communication," and/or "transmission") range. When the user is within range of that adapter module 100, the mobile device 150 tracks and monitors the signal strength until a predetermined "authorization zone" threshold is achieved.

[00149] FIGS. 8B and 9A generally show that when the authorization zone threshold is reached, the mobile device 150 enters the authorization zone (block 302) and registers the adapter module 100. The mobile device 150 connects to the server 130 (block 304). The app 140 on the mobile device 150 creates a request for authorization (AuthRequest) and passes the AuthRequest to the server 130 using appropriate communication technology (e.g. cellular or WiFi) (block 306). The server 130 responds with an authorization grant (AuthGrant) encrypted with the specific adapter module's private key (block 306). This authorization token may minimally include the Userl D, Apparatusl D (for the adapter module 100),

authorization amount, and expiration time. The mobile device 150 receives the AuthGrant from the server 130, and retains it until the mobile device 150 is ready to issue payment to an adapter module 100. The mobile device 150 collects all pending AuthGrants that may be one or more depending on how many adapter modules 100 are in-range. Unused AuthGrants that expire are purged from the mobile device 150 and the server 130. It is important to note that the mobile device 150 is unable to read the AuthGrant because it is encrypted with the adapter module's unique private key that is only known to server 130 and adapter module 100. This provides a preferred key element of security in the system as the adapter module 100 only trusts AuthGrants that are issued by the server, and the AuthGrants cannot be read or modified by the mobile device 150 or any other party in between the server and the adapter module 100. Additional mobile devices 150 may enter the authorization zone 104 (block 308).

[00150] As the user approaches a specific adapter module 100, the user enters the payment zone 102 and an event threshold is triggered based on heuristics performed by the mobile device 150. Blocks 310 and 312 show the loop steps of waiting for a mobile device 150 from the authorization zone 104 to enter the payment zone 102. If the user leaves the authorization zone 104 without entering the payment zone 102, the adapter module 100 returns to advertising its presence (block 300).

[00151] FIGS. 8C and 9B generally show the user entering the payment zone. The mobile device 150 verifies that it has an unexpired and valid AuthGrant. If the AuthGrant is not good, it may be requested again, repeating the Auth Request process (block 315). If the AuthGrant is good, the mobile device 150 sends the valid AuthGrant (including the wallet balance (block 322)) to the adapter module 100 to initiate a transaction. The mobile device 150 may issue the AuthGrant automatically without specific user interaction if the hands-free mode is supported (and the device is a favorite (block 318), there is only one device in the payment zone 102 (block 318), and (optionally) there is only one user in the authorization zone 104 (block 320). If any of these factors are not present, the mobile device 150 will prompt and/or wait for the user to begin the transaction manually (block 324).

[00152] FIGS. 8D, 9C, and 9D generally show the transaction process. As shown in FIG. 9C, the adapter module 100 runs through a series of questions to determine if there are any issues that would prevent vending including: has the user canceled in-app? (block 326), has the user walked away? (block 328), is the coin return pressed? (block 330), has more than a predetermined period of time elapsed? (block 332). If the answer to any of these questions

is "yes," the transaction does not proceed. If the answers to all of these questions is "no," the user makes a selection (block 334) on the payment accepting unit 120 in the same or similar manner as compared to if cash or credit were presented to the payment accepting unit 120. If the machine 120 is able to vend (block 336), it attempts to release the product. If the vend fails (block 338) it is reported by the machine (block 340) and a credit is returned to the virtual wallet (block 342). If the vend is successful (block 338) it is reported by the machine (block 344). Put another way, after the transaction is complete, the adapter module 100 returns to the mobile device 150 the details of the transaction as well as an encrypted packet containing the vend details to be sent to the server 130 via the mobile device 150. Optionally, the adapter module 100 can pass additional information not directly related to the transaction such as payment accepting unit health, sales data, error codes, etc.

[00153] FIGS. 8D and 9E generally show the multi-vend function. If the machine has enabled multi-vend capabilities (block 350) and the multi-vend limit has not been reached, the process returns to the question of whether the user is in the payment zone (block 310 of FIG. 9A). If the machine does not have enabled multi-vend capabilities (block 350) or the multi-vend limit has been reached, the wallet is decremented by the vend amount(s) and "change" is returned to the virtual wallet (block 354) and the process ends (block 356).

[00154] FIG. 8E is a timing schematic showing an exemplary Login process. FIG. 8F is a timing schematic showing an exemplary bootup process. FIG. 8G is a timing schematic showing an exemplary Account Check/Update process.

[00155] Several of the figures are flow charts (e.g. FIGS. 9A-9E) illustrating methods and systems. It will be understood that each block of these flow charts, components of all or some of the blocks of these flow charts, and/or combinations of blocks in these flow charts, may be implemented by software (e.g. coding, software, computer program instructions, software programs, subprograms, or other series of computer-executable or processor-executable instructions), by hardware (e.g. processors, memory), by firmware, and/or a combination of these forms. As an example, in the case of software, computer program instructions (computer-readable program code) may be loaded onto a computer to produce a machine, such that the instructions that execute on the computer create structures for implementing the functions specified in the flow chart block or blocks. These computer program instructions may also be stored in a memory that can direct a computer to function in a particular manner, such that the instructions stored in the memory produce an article of manufacture including instruction structures that implement the function specified in the flow

chart block or blocks. The computer program instructions may also be loaded onto a computer to cause a series of operational steps to be performed on or by the computer to produce a computer implemented process such that the instructions that execute on the computer provide steps for implementing the functions specified in the flow chart block or blocks. Accordingly, blocks of the flow charts support combinations of steps, structures, and/or modules for performing the specified functions. It will also be understood that each block of the flow charts, and combinations of blocks in the flow charts, may be divided and/or joined with other blocks of the flow charts without affecting the scope of the invention. This may result, for example, in computer-readable program code being stored in whole on a single memory, or various components of computer-readable program code being stored on more than one memory.

Distinction From Known Systems

[00156] Many of the known systems and methods require that the payment accepting unit be persistently (continuously) connected to and/or connectable on demand to some sort of remote server in order to function. As an example, the Carlson reference describes a system and a method for using a portable consumer device. Described embodiments include a consumer using the portable consumer device to dial a number to purchase an item (product or service) in a vending machine, to send an SMS to purchase an item in a vending machine, or to use a mobile wallet to purchase an item in a vending machine. It is mentioned in one embodiment that the consumer may launch an application in the portable consumer device or, alternatively, the portable consumer device may automatically detect the vending machine and prompt the consumer to enter information associated with the vending machine. It should be noted, however, that even when there is automatic detection, the user is prompted to enter information (e.g. a machine alias, payment information, or a PIN) and it can be inferred that this is entered on the portable consumer device. Once connected to a payment processing network, the authorization process begins using a payment processing network and/or payment server. Significantly, all of the embodiments described in the Carlson reference specify that the payment server sends an authorization response message to the vending machine. This means that, unlike the mobile-device-to-machine payment systems described herein, a persistent network connection is required for the Carlson system to function. Other references that disclose systems that require a persistent network connection include the Khan reference (the MicroAdapter having the persistent connection), the Garibaldi reference, and the Weiner reference.

[00157] Many of the known systems and methods require the user to significantly interact with their mobile devices. As an example, the Whigham reference is directed to a system that eliminates the need for currency for a vending machine and also eliminates the need for a dedicated online connection between the vending machine and the issuer of a credit card or a debit card. Instead the Whigham system and method allows a consumer to purchase a product from an automatic vending machine by using the consumer's cellular telephone, personal digital assistant (P DA), or similar wireless communication device as a link between the provider of the products in the vending machine and the vending machine. The Whigham reference, however, sets forth a system and method requires significant interaction between the consumer and his telephone including dialing a telephone number to a server (that, in turn, provides a vend code to the consumer), requesting a specific product (e.g. by dialing additional digits, although this step is optional if a unique number was dialed for a specific product), and transmitting a vend code to the vending machine. (Other references that disclose systems that require user interaction with the phone include the Offer reference, the Khan reference, the Belfer reference, and the Carlson reference.) In addition to other differences, some of the mobile-device-to-machine payment systems described herein do not require the user to interact with his mobile device at all, which can be contrasted to known systems and methods that require the consumer to, for example, dial a telephone number, enter a machine identification, and/or enter a product identifier using the mobile device to purchase a product.

[00158] The known systems and methods that use a cellular telephone to facilitate cashless transactions at a vending machine use the cellular telephone to authorize a particular transaction. For example, once the user knows what he wants from a vending machine, he can dial a server and receive authorization to make a specific purchase. Sometimes this includes dialing additional numbers on the cellular telephone to specify a particular product. The mobile-device-to-machine payment systems described herein take a completely different approach. The mobile-device-to-machine payment systems described herein are not specifically interested in the details of the transaction to authorize the transaction. Instead, the mobile-device-to-machine payment systems function more like a gift card, a credit card, or a debit card in that they allow the user to have funds to make a purchase. When a user is in range, the adapter module 100 (via a mobile device 150) sends an AuthRequest to the server 130 to preemptively obtain authorization to make funds available. The server 130 returns the AuthGrant for funds to the adapter module 100 (via a mobile device 150) so that

the user may use the funds to make a purchase. The AuthGrant may remain valid until it expires. This gives the user significantly more flexibility than known systems and methods.

Miscellaneous

[00159] It is to be understood that the inventions, examples, and embodiments described herein are not limited to particularly exemplified materials, methods, and/or structures. It is to be understood that the inventions, examples, and embodiments described herein are to be considered preferred inventions, examples, and embodiments whether specifically identified as such or not.

[00160] All references (including, but not limited to, foreign and/or domestic publications, patents, and patent applications) cited herein, whether supra or infra, are hereby incorporated by reference in their entirety.

[00161] The terms and expressions that have been employed in the foregoing specification are used as terms of description and not of limitation, and are not intended to exclude equivalents of the features shown and described. While the above is a complete description of selected embodiments of the present invention, it is possible to practice the invention using various alternatives, modifications, adaptations, variations, and/or combinations and their equivalents. It will be appreciated by those of ordinary skill in the art that any arrangement that is calculated to achieve the same purpose may be substituted for the specific embodiment shown. It is also to be understood that the following claims are intended to cover all of the generic and specific features of the invention herein described and all statements of the scope of the invention that, as a matter of language, might be said to fall therebetween.

WHAT IS CLAIMED IS:

1. A method of payment processing, comprising:

at a device with one or more processors, memory, and two or more communication capabilities:

obtaining, from a payment module, an authorization request via a first communication capability;

sending, to a server, the authorization request via a second communication capability distinct from the first communication capability;

in response to sending the authorization request, obtaining, from the server, authorization information via the second communication capability;

after obtaining the authorization information, detecting a trigger condition to perform a transaction with a payment accepting unit associated with the payment module; and

in response to detecting the trigger condition, sending, to the payment module, at least a portion of the authorization information via the first communication capability.

2. The method of claim 1, wherein the first communication capability corresponds to a short-range communication protocol and the second communication capability corresponds to a long-range communication protocol.

3. The method of claim 1, further comprising:

obtaining, from the payment module, advertised information indicating the payment module's presence via the first communication capability that at least includes authorization zone threshold criterion.; and

after obtaining the advertised information, initiating a handshake process with the payment module, wherein the handshake process includes:

sending, to the payment module, device information at least including user identification information corresponding to the user of the device via the first communication capability; and

receiving, from the payment module, payment module information, wherein the payment module information at least includes an identifier corresponding to the payment module.

4. The method of claim 3, further comprising:

prior to obtaining the authorization request:

in accordance with a determination that the authorization zone threshold criterion is satisfied, sending notification information to the payment module via the first communication capability, wherein the notification information indicates that the authorization zone threshold criterion is satisfied;

wherein the device obtains the authorization request in response to sending the notification information.

5. The method of claim 3, wherein the payment module information further includes an indication that hands-free mode is available and payment zone threshold criterion.

6. The method of claim 5, wherein the device information further includes device identification information corresponding to a model type of the device; and

wherein the payment zone threshold criterion is based at least in part on the device identification information.

7. The method of claim 5, wherein detecting the trigger condition comprises:

determining whether the payment zone threshold criterion is satisfied; and

in accordance with a determination that the payment zone threshold criterion is satisfied, detecting the trigger condition without interaction from a user of the device.

8. The method of claim 1, wherein detecting the trigger condition comprises:

detecting a user input from a user of the device; and

in response to detecting the user input, detecting the trigger condition to perform a transaction with the payment accepting unit.

9. The method of claim 1, further comprising:

in response to obtaining the authorization information, presenting a notification to the user of the device that a connection has been established with the payment module.

10. The method of claim 9, wherein the notification further indicates an authorized amount for the transaction.

11. The method of claim 1, wherein the authorization information includes an identifier corresponding to the payment module, an identifier corresponding to the user of the device,

an authorized amount, an authorization grant token, and an expiration period for the authorization grant token.

12. The method of claim 11, wherein at least a portion of the authorization request and the authorization grant token are encrypted with a unique encryption key corresponding to the payment module.

13. A device, comprising:

two or more communication capabilities;

one or more processors; and

memory storing one or more programs to be executed by the one or more processors, the one or more programs comprising instructions for:

obtaining, from a payment module, an authorization request via a first communication capability;

sending, to a server, the authorization request via a second communication capability distinct from the first communication capability;

in response to sending the authorization request, obtaining, from the server, authorization information via the second communication capability;

after obtaining the authorization information, detecting a trigger condition to perform a transaction with a payment accepting unit associated with the payment module; and

in response to detecting the trigger condition, sending, to the payment module, at least a portion of the authorization information via the first communication capability.

14. The device of claim 13, wherein the first communication capability corresponds to a short-range communication protocol and the second communication capability corresponds to a long-range communication protocol.

15. The device of claim 13, wherein the one or more programs further comprise instructions for:

obtaining, from the payment module, advertised information indicating the payment module's presence via the first communication capability that at least includes authorization zone threshold criterion; and

after obtaining the advertised information, initiating a handshake process with the payment module, wherein the handshake process includes:

sending, to the payment module, device information at least including user identification information corresponding to the user of the device via the first communication capability; and

receiving, from the payment module, payment module information, wherein the payment module information at least includes an identifier corresponding to the payment module.

16. The device of claim 15, wherein the one or more programs further comprise instructions for:

prior to obtaining the authorization request:

in accordance with a determination that the authorization zone threshold criterion is satisfied, sending notification information to the payment module via the first communication capability, wherein the notification information indicates that the authorization zone threshold criterion is satisfied;

wherein the device obtains the authorization request in response to sending the notification information.

17. The device of claim 15, wherein the payment module information further includes an indication that hands-free mode is available and payment zone threshold criterion.

18. The device of claim 17, wherein the device information further includes device identification information corresponding to a model type of the device; and

wherein the payment zone threshold criterion is based at least in part on the device identification information.

19. The device of claim 17, wherein detecting the trigger condition comprises:

determining whether the payment zone threshold criterion is satisfied; and

in accordance with a determination that the payment zone threshold criterion is satisfied, detecting the trigger condition without interaction from a user of the device.

20. The device of claim 13, wherein detecting the trigger condition comprises:

detecting a user input from a user of the device; and

in response to detecting the user input, detecting the trigger condition to perform a transaction with the payment accepting unit.

21. A non-transitory computer readable storage medium storing one or more programs, the one or more programs comprising instructions, which, when executed by a device with one or more processors and two or more communication capabilities, cause the device to perform operations comprising:

obtaining, from a payment module, an authorization request via a first communication capability;

sending, to a server, the authorization request via a second communication capability distinct from the first communication capability;

in response to sending the authorization request, obtaining, from the server, authorization information via the second communication capability;

after obtaining the authorization information, detecting a trigger condition to perform a transaction with a payment accepting unit associated with the payment module; and

in response to detecting the trigger condition, sending, to the payment module, at least a portion of the authorization information via the first communication capability.

22. The non-transitory computer readable storage medium of claim 21, wherein the first communication capability corresponds to a short-range communication protocol and the second communication capability corresponds to a long-range communication protocol.

23. The non-transitory computer readable storage medium of claim 21, wherein the instructions cause the device to perform operations further comprising:

obtaining, from the payment module, advertised information indicating the payment module's presence via the first communication capability that at least includes authorization zone threshold criterion; and

after obtaining the advertised information, initiating a handshake process with the payment module, wherein the handshake process includes:

sending, to the payment module, device information at least including user identification information corresponding to the user of the device via the first communication capability; and

receiving, from the payment module, payment module information, wherein the payment module information at least includes an identifier corresponding to the payment module.

24. The non-transitory computer readable storage medium of claim 23, wherein the instructions cause the device to perform operations further comprising:

prior to obtaining the authorization request:

in accordance with a determination that the authorization zone threshold criterion is satisfied, sending notification information to the payment module via the first communication capability, wherein the notification information indicates that the authorization zone threshold criterion is satisfied;

wherein the device obtains the authorization request in response to sending the notification information.

25. The non-transitory computer readable storage medium of claim 23, wherein the payment module information further includes an indication that hands-free mode is available and payment zone threshold criterion.

26. The non-transitory computer readable storage medium of claim 25, wherein the device information further includes device identification information corresponding to a model type of the device; and

wherein the payment zone threshold criterion is based at least in part on the device identification information.

27. The non-transitory computer readable storage medium of claim 25, wherein detecting the trigger condition comprises:

determining whether the payment zone threshold criterion is satisfied; and

in accordance with a determination that the payment zone threshold criterion is satisfied, detecting the trigger condition without interaction from a user of the device.

28. The non-transitory computer readable storage medium of claim 21, wherein detecting the trigger condition comprises:

detecting a user input from a user of the device; and

in response to detecting the user input, detecting the trigger condition to perform a transaction with the payment accepting unit.

METHOD AND SYSTEM FOR PERFORMING MOBILE DEVICE-TO-MACHINE PAYMENTS

ABSTRACT OF THE DISCLOSURE

A device with one or more processors, memory, and two or more communication capabilities obtains, from a payment module, an authorization request via a first communication capability (e.g., Bluetooth). The device sends, to a server, the authorization request via a second communication capability distinct from the first communication capability (e.g., cellular or WiFi technology). In response to sending the authorization request, the device obtains, from the server, authorization information via the second communication capability. After obtaining the authorization information, the device detects a trigger condition to perform a transaction with a payment accepting unit associated with the payment module. In response to detecting the trigger condition, the device sends, to the payment module, at least a portion of the authorization information via the first communication capability.

METHOD AND SYSTEM FOR PERFORMING MOBILE DEVICE-TO-MACHINE PAYMENTS

PRIORITY CLAIM

[0001] The present application is an continuation of U.S. Patent Application Number 14/214,644, filed March 14, 2014, which claims priority to U.S. Provisional Patent Application Number 61/917,936, filed December 18, 2013, and is a continuation-in-part of U.S. Design Patent Application Number 29/477,025, filed December 18, 2013. The present application is based on and claims priority from these applications, the disclosures of which are hereby expressly incorporated herein by reference.

BACKGROUND OF THE INVENTION

[0002] Disclosed herein are mobile-device-to-machine payment systems and, more specifically, mobile-device-to-machine payment systems over a non-persistent network connection and featuring hands-free and manual modes.

[0003] Vending machines (or "automatic retailing" machines), in the broadest sense, have been around for thousands of years. The first simple mechanical coin operated vending machines were introduced in the 1880s. Modern vending machines stock many different types of products including, but not limited to drinks (e.g. water, juice, coffee, and soda) and edible food products/items (e.g. snacks, candy, fruit, and frozen meals), as well as a wide variety of non-food items. In this fast paced world, vending machines are ubiquitous.

[0004] Vending machines are one type of "payment accepting unit" (payment accepting units are also referred to herein generically as "machines"). A payment accepting unit (or machine) is equipment that requires payment for the dispensing of products and/or services. In addition to vending machines, payment accepting units can also be other machines that require payment for the dispensing of a product and/or services including, but not limited to parking meters, toll booths, laundromat washers and dryers, arcade games, kiosks, photo booths, toll booths, transit ticket dispensing machines, and other known or yet to be discovered payment accepting units.

[0005] In using a payment accepting unit, a user will (1) approach the payment accepting unit, (2) determine from the face of the payment accepting unit the product (or service) he desires, (3) insert payment (e.g. coins, bills, or payment cards), and (4) input his

selection into the payment accepting unit using a user interface (e.g. a series of buttons, a key pad, touch screen, or other input mechanism using, for example, the column and row at which a product is located). Based on the user's inputted selection, technology within the payment accepting unit provides the desired product (or service) to the user.

[0006] As the number of people with internet-connected mobile devices proliferates, so does the variety of uses for such devices. Mobile payment is a logical extension.

[0007] There is a large development effort around bringing mobile payment to the retail sector in an effort to not only provide options to the user, but also increased convenience.

[0008] In recent years, many improvements to modern vending machines have been suggested. Many of the innovations relate to means for communicating with the vending machine. Some of these communication innovations are detailed in U.S. Patent No. 6,584,309 to Whigham (the "Whigham reference"), U.S. Patent No. 7,085,556 to Offer (the "Offer reference"), U.S. Patent No. 7,127,236 to Khan et al. (the "Khan reference"), U.S. Patent No. 7,721,958 to Belfer et al. (the "Belfer reference"), U.S. Patent No. 8,396,589 to Katzenstein Garibaldi et al. (the "Garibaldi reference"), U.S. Patent No. 8,489,140 to Weiner et al. (the "Weiner reference"), and International Publication No. WO/2008/083025 to Carlson (the "Carlson reference").

[0009] The Whigham reference is directed to a system and method for purchasing a product from an automatic vending machine by means of a consumer's cellular telephone. The consumer requests a product available from the vending machine by dialing a specified telephone number that connects the consumer's cellular telephone to a server operated by a billing agency. The server recognizes the request for the product, creates a transaction record, and communicates a vend code to the consumer. Upon receiving the vend code from the server, the consumer transmits the vend code to the vending machine. The vend code may be an RF code, an audible tone code, or a manual code. Upon receipt of the vend code from the consumer, the vending machine dispenses the requested product.

[0010] The Offer reference is directed to a vending machine that is designed to communicate with a cellular phone such that it dispenses a product when it receives information indicating that the product has been selected. The Offer reference teaches permitting the cashless utilization of a vending machines via a communications service, such as a cellular telephone. A response to a signal from the cellular telephone from

[0011] the vending machine that indicates that a connection has been established between the vending machine and the cellular phone may be a visual indication that is displayed on the cellular telephone. The vending machine outputs the cost of the product and that cost is debited from an account to pay for the product.

[0012] The Khan reference describes a point of sale MicroAdapter device that enables payment transactions to be effected through a purchaser's personal trusted device (e.g. the user selecting the micropayment application on his personal trusted device and confirming or cancelling the purchase thereon) without relying upon tokens or prepayment cards. In one embodiment, the MicroAdapter includes a transceiver configured to receive a purchase signal from the personal trusted device including order and payment information. In response, the MicroAdapter communicates via wireless telephony with a transaction authorizer to receive authorization for effectuating the purchase transaction. The MicroAdapter can effectuate micropayment transactions authorized by a Billing On Behalf of Others program administered through a wireless carrier/ISP or third party.

[0013] The Belfer reference is directed to a system wherein a vending machine has an audio code collector and a code validator that is adapted to receive audio tones from a mobile device. The audio tones include authentication codes and dispense codes to control dispensing of product from the vending machine. To start the transaction, the consumer dials a unique set of symbols and digits to route the call to a verification server. The symbols and digits may correspond to a unique vending machine identification number and product identification numbers.

[0014] The Garibaldi reference is directed to an electronic device for the sale of intangible products through vending machines that include interfaces to communicate with external peripherals through the MDB protocol, the RS232 standard, and the DEX protocol, an interface to communicate with users, a communications system that enables it to act as part of a network and communicate with a central system, and a controller, that articulates the communication among the above-mentioned components, so as to enable a central system to perform diverse actions on a vending machine.

[0015] The Weiner reference is directed to a system and method for providing product or service with a cellular telephone. The problem identified in the Weiner reference is that mobile communication devices are long-range electronic devices designed to be used for long-range communications. Eschewing the use of near- field communication because it

requires special design or modification of the mobile station (e.g. the vending machine), the Weiner reference teaches a mobile communication device identifier, consisting of: a shielding defining a coverage area, the shielding arranged to reduce radio signals originating externally of the coverage area to be less than a pre-determined signal strength; an antenna associated within the defined coverage area; a transceiver coupled to the antenna, the transceiver communicating with a mobile station inserted within the defined coverage area utilizing a signal strength greater than the pre-determined signal strength; and a service control unit responsive to the transceiver, the service control unit responsive to the communication to output a signal indicative of an authorization to provide a product or service.

[0016] The Carlson reference is directed to a system and a method for using a portable consumer device such as a mobile phone for payments and the like. One embodiment of the Carlson system is directed to a method that includes the steps of receiving a payment request message (that includes a request to pay for a product from a vending machine) from a portable consumer device operated by a consumer, sending an authorization response message back to the vending machine wherein the vending machine subsequently prompts the consumer to enter a selection if the authorization response message indicates that the consumer is authorized to make a purchase, and receiving an acknowledgement message from the vending machine that the product was purchased. The step of "sending an authorization response message back to the vending machine" is performed by a remote payment server and would require a persistent network connection.

BRIEF SUMMARY OF THE INVENTION

[0017] Disclosed herein are mobile-device-to-machine payment systems and, more specifically, mobile-device-to-machine payment systems over a non-persistent network connection and featuring hands-free and manual modes.

[0018] Described herein is a mobile-device-to-machine payment system for facilitating a cashless transaction for purchase of at least one product or service by a user from a payment accepting unit that preferably has input mechanisms. The user has a mobile device that has both short-range communication technology and long-range communication technology. The payment accepting unit is capable of dispensing at least one product or service. The system includes an adapter module and a server. The adapter module is associated with the payment accepting unit and has short-range communication technology

for communicating with the short-range communication technology of the mobile device. The server has long-range communication technology for communicating with the long-range communication technology of the mobile device. The adapter module is for sending an authorization request for funds to the mobile device using short-range communication technology. The mobile device then forwards the authorization request for funds to the server using long-range communication technology. The server is for sending an authorization grant for funds to the mobile device using long-range communication technology. The mobile device the forwards the authorization grant for funds to the adapter module using short-range communication technology. The payment accepting unit dispenses the at least one product or service in response to receiving user input to the payment accepting unit input mechanism if the adapter module has received the authorization grant.

[0019] The adapter module may have security technology and the server may have security technology. The authorization request may be secured by the adapter module security technology to create a secured authorization request. The authorization grant may be secured by the server security technology to create a secured authorization grant. The secured authorization request and the secured authorization grant are preferably undecipherable to the mobile device.

[0020] The adapter module and the server may share a unique private key. The adapter module may have encryption/decryption technology and the server may have encryption/decryption technology. The authorization request may be encrypted by the adapter module encryption/decryption technology using the unique private key to create an encrypted authorization request. The encrypted authorization request may be decrypted by the server encryption/decryption technology using the unique private key. The authorization grant may be encrypted by the server encryption/decryption technology using the unique private key to create an encrypted authorization grant. The encrypted authorization grant may be decrypted by the adapter module encryption/decryption technology using the unique private key. The encrypted authorization request and the encrypted authorization grant are preferably undecipherable to the mobile device.

[0021] The adapter module is preferably surrounded by two zones, a payment zone and an authorization zone, wherein the payment zone is within the authorization zone. The adapter module sends the authorization request when the mobile device is within the authorization zone. The mobile device forwards the authorization grant for funds to the adapter module when the mobile device is within the payment zone. A third zone possible

zone is a communication zone, the authorization zone being within the communication zone. The mobile device preferably receives advertising broadcast signals from the adapter module within the communication zone.

[0022] The system may have a hands-free mode in which the payment accepting unit dispenses the at least one product or service without the user interacting with the mobile device. A display of the payment accepting unit may be used for displaying funds available based on information from the authorization grant. The input mechanisms of the payment accepting unit may be used for receiving user selection input when the user interacts with the input mechanisms to select the at least one product or service to be dispensed.

[0023] The adapter module may be an in-line dongle for in-line insertion within a multi-drop bus of the payment accepting unit. Further, the payment accepting unit may have a multi-drop bus to a payment receiving mechanism. The multi-drop bus may have a male adapter and a female adapter. The adapter module may have a male adapter and a female adapter. The adapter module is preferably insertable in serial with the multi-drop bus by connecting the male adapter of the adapter module to the female adapter of the multi-drop bus and by connecting the female adapter of the adapter module to the male adapter of the multi-drop bus.

[0024] Also described herein is a method for using a mobile-device-to-machine payment system for facilitating a cashless transaction for purchase of at least one product or service by a user from a payment accepting unit may have input mechanisms. The user may have a mobile device having both short-range communication technology and long-range communication technology. The payment accepting unit is preferably capable of dispensing at least one product or service. The method includes the steps of: (a) sending an authorization request for funds to the mobile device using short-range communication technology of an adapter module associated with the payment accepting unit; (b) receiving the authorization request for funds from the short-range communication technology of the adapter module at the short-range communication technology of the mobile device; (c) forwarding the authorization request for funds to a server using the long-range communication technology of the mobile device; (d) receiving the authorization request for funds from the long-range communication technology of the mobile device at long-range communication technology of the server; (e) sending an authorization grant for funds to the mobile device using the long-range communication technology of the server; (f) receiving the authorization grant for funds from long-range communication technology of the server at the

long-range communication technology of the mobile device; (g) forwarding the authorization grant for funds to the adapter module using the short-range communication technology of the mobile device; and (h) receiving the authorization grant for funds from the short-range communication technology of the mobile device at short-range communication technology of the adapter module. At least one product or service may then be dispensed from the payment accepting unit in response to receiving user input to the payment accepting unit input mechanism if the adapter module has received the authorization grant.

[0025] The method may include the steps of securing the authorization request using security technology associated with the adapter module to create a secured authorization request, securing the authorization grant using security technology associated with the server to create a secured authorization grant, and the secured authorization request and the secured authorization grant are preferably undecipherable to the mobile device.

[0026] The method may include the steps of (a) sharing a unique private key between the adapter module and the server, (b) encrypting using the unique private key the authorization request using encryption/decryption technology associated with the adapter module to create an encrypted authorization request, (c) decrypting using the unique private key the encrypted authorization request using encryption/decryption technology associated with the server, (d) encrypting using the unique private key the authorization grant using the encryption/decryption technology associated with the server to create an encrypted authorization grant, (e) decrypting using the unique private key the encrypted authorization grant using encryption/decryption technology associated with the adapter module, and (e) the encrypted authorization request and the encrypted authorization grant are preferably undecipherable to the mobile device.

[0027] The method may include the steps of (a) surrounding the adapter module with two zones, a payment zone and an authorization zone, wherein the payment zone is within the authorization zone, (b) the adapter module sending the authorization request when the mobile device is within the authorization zone; and (c) the mobile device forwarding the authorization grant for funds to the adapter module when the mobile device is within the payment zone. The adapter module may also include a third zone, a communication zone, wherein the authorization zone is within the communication zone. The mobile device receives advertising broadcast signals from the adapter module within the communication zone.

[0028] The method may have a hands-free mode in which the payment accepting unit dispenses the at least one product or service without the user interacting with the mobile device. The method may further include the steps of (a) displaying funds available on a display of the payment accepting unit, the funds available may be based on information from the authorization grant; and (b) receiving user selection input when the user interacts with input mechanisms of the payment accepting unit to select the at least one product or service to be dispensed.

[0029] The method may include the step of inserting the adapter module as an in-line dongle for in-line insertion within a multi-drop bus of the payment accepting unit. The method may include the step of inserting the adapter module in serial with the multi-drop bus by connecting a male adapter of the adapter module to a female adapter of the multi-drop bus and by connecting a female adapter of the adapter module to a male adapter of the multi-drop bus.

[0030] The subject matter described herein is particularly pointed out and distinctly claimed in the concluding portion of this specification. Objectives, features, combinations, and advantages described and implied herein will be more readily understood upon consideration of the following detailed description of the invention, taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

[0031] FIG. 1 is a schematic diagram that shows three zones: a first "communication zone" (e.g. "Bluetooth range"), a second "authorization zone," and a third "payment zone." The payment zone (that can't be zero) is smaller than or equal to (overlapping completely) the authorization zone.

[0032] FIG. 2 is a schematic diagram that shows the three zone of FIG. 1 with multiple users therein, the mobile-device-to-machine payment systems providing for managing and resolving multiple users.

[0033] FIG. 3 is a table that illustrates the hands-free credit or alert user principle.

[0034] FIG. 4 is a flow chart showing the logging RSSI at User Input.

[0035] FIG. 5 is a block schematic that shows elements of the system including, but not limited to, the adapter module, the machine, the mobile device, and exemplary servers, as well as communications therebetween.

[0036] FIG. 6 is a block schematic that shows there are three areas of encryption used (each is bi-directional) between the adapter module, the machine, the mobile device, and/or exemplary servers.

[0037] FIG. 7 is a block diagram that communications, messaging, vending sequence, and purchase flow between the adapter module, the mobile device, and a system management server.

[0038] FIG. 8A is a timing schematic diagram that shows additional elements and features of the system including, but not limited to, communications medium, messaging, vending sequence, and purchase flow, when the user enters the communication zone (Bluetooth Range).

[0039] FIG. 8B is a timing schematic diagram that shows additional elements and features of the system including, but not limited to, communications medium, messaging, vending sequence, and purchase flow, when the user enters the Authorization Zone.

[0040] FIG. 8C is a timing schematic diagram that shows additional elements and features of the system including, but not limited to, communications medium, messaging, vending sequence, and purchase flow, when the user enters the Payment Zone and, in particular, detailing the hands-free mode alternative and the swipe mode alternative.

[0041] FIG. 8D is a timing schematic diagram that shows additional elements and features of the system including, but not limited to, communications medium, messaging, vending sequence, and purchase flow, in a vending transaction including a loop for multiple transactions.

[0042] FIG. 8E is a timing schematic diagram that shows additional elements and features of the system including, but not limited to, communications medium, messaging, vending sequence, and purchase flow, in the Login mode.

[0043] FIG. 8F is a timing schematic diagram that shows additional elements and features of the system including, but not limited to, communications medium, messaging, vending sequence, and purchase flow, during Module bootup.

[0044] FIG. 8G is a timing schematic diagram that shows additional elements and features of the system including, but not limited to, communications medium, messaging, vending sequence, and purchase flow, during Account Check/Update.

[0045] FIGS. 9A - 9E are flow charts that show exemplary steps and features of the system including, but not limited to, communications, messaging, vending sequence, and purchase flow.

[0046] FIGS. 10A - 10D show an exemplary mobile device with a graphical representation of an exemplary mobile application shown thereon, the mobile application being used as part of the mobile-device-to-machine payment systems.

[0047] FIG. 11 is a perspective view of the exemplary first preferred in-line dongle adapter module.

[0048] FIG. 12 is a front plan view of the in-line dongle adapter module of FIG. 11.

[0049] FIG. 13 is a back plan view of the in-line dongle adapter module of FIG. 11.

[0049.1] FIG. 14 is a side view of the in-line dongle adapter module of FIG. 11 in accordance with some implementations.

[0050] FIG. 15 is a first end view of a connector receptacle of the in-line dongle adapter module of FIG. 11.

[0051] FIG. 16 is a second end view of a connector receptacle of the in-line dongle adapter module of FIG 11.

[0052] FIG. 17 is a perspective view taken from the first end of the in-line dongle adapter module of FIG. 11, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for environmental purposes.

[0053] FIG. 18 is a perspective view taken from the second end of the in-line dongle adapter module of FIG. 11, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for environmental purposes.

[0054] FIG. 19 is a perspective view of the in-line dongle adapter module of FIG. 11 within a vending machine.

[0055] FIG. 20 is a perspective view of the exemplary second preferred in-line dongle adapter module.

[0056] FIG. 21 is a front plan view of the in-line dongle adapter module of FIG. 20.

[0057] FIG. 22 is a back plan view of the in-line dongle adapter module of FIG. 20.

[0058] FIG. 23 is a first side view of the in-line dongle adapter module of FIG. 20, the second side being a mirror image of that shown.

[0059] FIG. 24 is a first end view of a connector receptacle of the in-line dongle adapter module of FIG. 20.

[0060] FIG. 25 is a second end view of a connector receptacle of the in-line dongle adapter module of FIG 20.

[0061] FIG. 26 is a perspective view taken from the first end of the in-line dongle adapter module of FIG. 20, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for environmental purposes.

[0062] FIG. 27 is a perspective view taken from the second end of the in-line dongle adapter module of FIG. 20, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for environmental purposes.

[0063] FIG. 28 is a perspective view of the in-line dongle adapter module of FIG. 20 within a vending machine.

[0064] FIG. 29 is a perspective view of the exemplary third preferred in-line dongle adapter module with a gap indicating the in-line dongle adapter module can be of any length.

[0065] FIG. 30 is a front plan view of the in-line dongle adapter module of FIG. 29.

[0066] FIG. 31 is a back plan view of the in-line dongle adapter module of FIG. 29.

[0067] FIG. 32 is a first side view of the in-line dongle adapter module of FIG. 29, the second side being a mirror image of that shown.

[0068] FIG. 33 is a first end view of a connector receptacle of the in-line dongle adapter module of FIG. 29.

[0069] FIG. 34 is a second end view of a connector receptacle of the in-line dongle adapter module of FIG. 29.

[0070] FIG. 35 is a perspective view taken from the first end of the in-line dongle adapter module of FIG. 29, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for environmental purposes.

[0071] FIG. 36 is a perspective view taken from the second end of the in-line dongle adapter module of FIG. 29, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for environmental purposes.

[0072] FIG. 37 is a perspective view of the in-line dongle adapter module of FIG. 29 within a vending machine.

[0073] FIG. 38 is a perspective view of the exemplary fourth preferred in-line dongle adapter module with two vertical gaps indicating the in-line dongle adapter module can be of any width.

[0074] FIG. 39 is a front plan view of the in-line dongle adapter module of FIG. 38.

[0075] FIG. 40 is a back plan view of the in-line dongle adapter module of FIG. 38.

[0076] FIG. 41 is a first side view of the in-line dongle adapter module of FIG. 38, the second side being a mirror image of that shown.

[0077] FIG. 42 is a first end view of a connector receptacle of the in-line dongle adapter module of FIG. 38.

[0078] FIG. 43 is a second end view of a connector receptacle of the in-line dongle adapter module of FIG 38.

[0079] FIG. 44 is a perspective view taken from the first end of the in-line dongle adapter module of FIG. 38, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for environmental purposes.

[0080] FIG. 45 is a perspective view taken from the second end of the in-line dongle adapter module of FIG. 38, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for environmental purposes.

[0081] FIG. 46 is a perspective view of the in-line dongle adapter module of FIG. 38 within a vending machine.

[0082] FIG. 47 is a perspective view of the exemplary fifth preferred in-line dongle adapter module and, specifically, the longitudinal center portion thereof, the dashed line depiction of the sides indicating the sides of the in-line dongle adapter module can be of any shape or curvature.

[0083] FIG. 48 is a front plan view of the in-line dongle adapter module of FIG. 47.

[0084] FIG. 49 is a back plan view of the in-line dongle adapter module of FIG. 47.

[0084.1] FIG. 50 is a side view of the in-line dongle adapter module of FIG. 47 in accordance with some implementations.

[0085] FIG. 51 is a first end view of a connector receptacle of the in-line dongle adapter module of FIG. 47.

[0086] FIG. 52 is a second end view of a connector receptacle of the in-line dongle adapter module of FIG 47.

[0087] FIG. 53 is a perspective view taken from the first end of the in-line dongle adapter module of FIG. 47, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for environmental purposes.

[0088] FIG. 54 is a perspective view taken from the second end of the in-line dongle adapter module of FIG. 47, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for environmental purposes.

[0089] FIG. 55 is a perspective view of the in-line dongle adapter module of FIG. 47 within a vending machine.

[0090] FIG. 56 is a block diagram of an exemplary adapter module.

[0091] FIG. 57 is a block diagram of an exemplary mobile device.

[0092] FIG. 58 is a block diagram of an exemplary server.

DETAILED DESCRIPTION OF THE INVENTION

[0093] Disclosed herein are mobile-device-to-machine payment systems and, more specifically, mobile-device-to-machine payment systems over a non-persistent network connection. The mobile-device-to-machine payment systems disclosed herein focus on the unattended retail space (e.g. a payment accepting unit 120 or machine 120). More specifically, mobile-device-to-machine payment systems disclosed herein allow a user (having a mobile device 150 with a mobile application 140 thereon) to make a cashless purchase from a payment accepting unit 120 (having an adapter module 100 associated therewith).

[0094] The mobile-device-to-machine payment systems described herein can be implemented with one or more of the following features: easy installation feature, a non-persistent network connection feature; a manual (swipe to pay) mode feature; a hands-free mode feature; and a multiple vending transactions (multi-vend) feature.

[0095] Easy Installation: Installation is very easy, requires no tools, requires no configuration, and takes as little as 30 seconds. This is accomplished by using an adapter

module 100 such as an in-line dongle (a hardware device with software thereon) design for in-line insertion within a multi-drop bus (MDB) of a payment accepting unit (e.g. a vending machine). Installation is as simple as "powering down" (turning off) the machine 120, identifying the "wire" that connects with a payment receiving mechanism (e.g. the coin mechanism), disconnecting the wire (so that there are two loose ends, such as a male connection end or adapter of an MDB and a female connection end or adapter of an MDB), plugging (inserting) the adapter module 100 in serial ("in-line") with the wire (for example, connecting the MDB female adapter to a male adapter of the adapter module 100 and connecting the MDB male adapter to a female adapter of the adapter module 100), tucking the wire and the installed adapter module 100 back into position, and "powering up" (turning on) the machine 120. Most vending machines made since 1995 have this industry standard MDB technology that would allow this easy 30-second installation. On machines without MDB technology, the adapter module 100 can be configured or designed to work with other serial protocols or activate a switch. In essence the adapter module 100 simulates establishing payment on payment accepting unit 120 in much the same manner as other alternative forms of payment (e.g. cash).

[0096] Non-persistent Network Connection: Although payment accepting units (or "machines") that accept only cash (e.g. paper currency and coins) may not require a connection (persistent or non-persistent) to a network, traditional payment accepting units that accept cashless payments (e.g. credit cards, debit cards, and alternative mobile device payment methods using, for example, smart phones) require a persistent connection to a network (wired or wireless) to facilitate the cashless payments. In other words, without a persistent (ongoing or accessible on demand) network connection, traditional payment accepting units cannot accept cashless payments. Most traditional payment accepting units that accept cashless payments include the technology to accomplish this persistent network connection that allows them to connect to a remote server. If the network connection to a traditional machine is temporarily interrupted, cashless payments will be temporarily unavailable. If the machine is located in a location where no signal is available, cashless payments will not be possible. The Whigham reference, the Offer reference, and the Belfer reference disclose alternative payment accepting units that accept cashless payments by using the user's cellular phone to allow the user to manually input coding to a remote server and, thereby act as an on-demand bridge network connection. These references, however, require significant user interaction with the cellular telephone to effectuate the transaction. In

addition to using a mobile device 150 as an intermediary between the payment accepting units 120 and the server 130, mobile-device-to-machine payment systems described herein minimize (manual mode) or eliminate (hands-free mode) user interaction with the mobile device 150. Further, some mobile-device-to-machine payment systems described herein facilitate the acceptance of cashless payments without requiring any network connection near the payment accepting unit 120. Mobile-device-to-machine payment systems described herein that are located in a remote location where no signal is available, therefore, can accept cashless payments.

[0097] Manual (Swipe to Pay) Mode: Using a "swipe to pay" feature (or just "swipe") refers to a user's action implemented on his mobile device 150 in which he quickly brushes his finger (or other pre-determined interaction) on the mobile device's touch screen 152 (or other input device associated with the mobile device 150). From the user's perspective, when the user is within range, a pre-installed mobile application 140 automatically connects to the payment accepting unit 120 (e.g. a vending machine). The mobile application 140 might display (on the touch screen 152) a prepaid balance that the user "swipes" to transfer payment to the payment accepting unit 120. The user could observe the transferred funds on the touch screen 152 of the mobile device 150 and/or on the display 122, 124 of the payment accepting unit 120. The transaction is completed just as if cash was inserted in the machine 120 with the user inputting his selection on the payment accepting unit 120 and the payment accepting unit 120 dispensing the product or service. After the selection is made, the change is returned to the mobile device 150 and this may be shown on the touch screen 152 of the mobile device 150.

[0098] Hands-Free Mode: A "hands-free pay" feature (or just "hands-free") would most likely be used with "favorite" payment accepting units 120 (e.g. a vending machine at work or school). From the user's perspective, he would approach the favorite payment accepting unit 120 and notice that the display 122, 124 of the payment accepting unit 120 showed funds available, he would select the product or service using the payment accepting unit's input mechanisms (e.g. buttons 126 or a touch screen display 124 shown in FIG. 19), and he would retrieve his dispensed services or products. It would be that simple. More specifically, when the user is within range, a pre-installed mobile application 140 automatically connects to the payment accepting unit 120 (e.g. a vending machine). The user may leave the mobile device 150 in a pocket, purse, briefcase, backpack, or other carrier. As the user approaches the payment accepting unit 120 and is in approximately "arms-length"

distance (e.g. 3 to 5 feet), the user could observe the transferred funds on the display 122, 124 of the payment accepting unit 120. The transaction is completed just as if cash was inserted in the machine 120 with the user inputting his selection on the payment accepting unit 120 and the payment accepting unit 120 dispensing the product or service. After the selection is made, the change is returned to the mobile device 150. FIG. 3 details when the hands-free mode would be available.

[0099] Multiple Vending Transactions (Multi-Vend): Both the "swipe to pay" feature and the "hands-free pay" feature could be used multiple times in sequence (implemented, for example, as a loop) so that a user may make multiple purchases. After making his first selection and receiving his product (or service), the user would observe that additional funds were available on the display 122, 124 on the payment accepting unit 120. He could make another selection (or multiple selections) and receive additional product(s) (or service(s)). More specifically, the display 122, 124 may reset as if the transaction is complete, but then, because the user is still standing in range, the mobile application 140 would send another credit to the payment accepting unit 120, allowing for a second purchase. When the walks away, the system clears (e.g. returns unused funds to the mobile application 140 on the mobile device 150.

[00100] The features described above, alone or in combination with other features described herein will revolutionize the hundred billion dollar automated retail industry. The exemplary hardware is very low cost and there are no reoccurring fees because no cellular connection is required on the machine 120. Using the mobile-device-to-machine payment systems described herein, operators can increase frequency of visits and items sold with each visit.

[00101] Mobile-device-to-machine payment systems described herein may be implemented as an apparatus and/or method for enabling payments to a machine 120 via a mobile device 150. Exemplary mobile-device-to-machine payment systems may be better understood with reference to the drawings, but the shown mobile-device-to-machine payment systems are not intended to be of a limiting nature.

Definitions

[00102] Before describing the mobile-device-to-machine payment systems and the figures, some of the terminology should be clarified. Please note that the terms and phrases may have additional definitions and/or examples throughout the specification. Where

otherwise not specifically defined, words, phrases, and acronyms are given their ordinary meaning in the art. The following paragraphs provide some of the definitions for terms and phrases used herein.

- Adapter Module 100: As shown in FIGS. 1 and 2, the adapter module 100 is a physical device that is installed in a machine 120 (a payment accepting unit 120). The shown exemplary adapter module 100 is an in-line dongle (a hardware device with software thereon) device that may be inserted in-line within a multi-drop bus (MDB) of a machine 120. The adapter module 100 bridges the communication between the machine 120 and a mobile device 150. Although described as a unique component, it should be noted that the adapter module 100 could be implemented as a plurality of devices or integrated into other devices (e.g. components of a machine 120). In its unique component form, the adapter module 100 can be easily inserted into a machine 120 so that the machine 120 is able to perform new features with the assistance of the adapter module 100. FIG. 56 shows exemplary components associated with the adapter module 100. The shown example may be divided into multiple distinct components that are associated with each other or the example may be incorporated into or drawn from other technology (e.g. a computer or a payment accepting unit) as long as the components are associated with each other.

- Mobile Device 150 and Application 140 (also referred to as a "mobile application," "mobile app," or "app"): In general, a mobile device 150 may be a user's personal mobile device 150. The mobile device 150 (with a mobile application 140 thereon) acts as a communication bridge between the adapter module 100 (associated with a payment accepting unit 120) and the server 130. The mobile device 150 and application 140, however, are not "trusted" in that the communications (transmissions) it passes are encrypted. Encrypted (secured) communications are undecipherable (unencryptable, unreadable, and/or unuseable) by the mobile device 150. This keeps the passed communications secured and safe from hacking. Exemplary mobile devices include, but are not limited to smart phones, tablet or laptop computers, or personal digital assistants (PDAs), smart cards, or other technology (e.g. a hardware-software combination) known or yet to be discovered that has

structure and/or capabilities similar to the mobile devices described herein. The mobile device 150 preferably has an application 140 (app 140) running on it. The term "app" is used broadly to include any software program(s) capable of implementing the features described herein. FIGS. 10A-10D show exemplary mobile devices 150 with associated apps 140 associated therewith. It should be noted that the phrase "mobile device" can be assumed to include the relevant app unless specifically stated otherwise. Similarly, it should be noted that an "app" can be assumed to be running on an associated mobile device unless specifically stated otherwise. FIG. 57 shows exemplary components associated with the mobile device 150. The shown example may be divided into multiple distinct components that are associated with each other or the example may be incorporated into or drawn from other technology (e.g. the cell phone itself) as long as the components are associated with each other.

- Payment Accepting Unit 120 (or Machine 120): A payment accepting unit 120 (or machine 120) is equipment that requires payment for the dispensing of an product and/or service. Payment accepting units 120 may be vending machines, parking meters, toll booths, laundromat washers and dryers, arcade games, kiosks, photo booths, toll booths, transit ticket dispensing machines, and other known or yet to be discovered payment accepting units 120. Some payment accepting units 120 can accept cashless payments (payments other than cash (paper currency and coins)) by accepting payment from, for example, credit cards, debit cards, and mobile devices.
- Network Connections: For purposes of this discussion, a persistent network connection is a wired or wireless communications connection that is ongoing (e.g. a dedicated connection, a dedicated online connection, and/or a hardwired connection) or accessible on demand (e.g. the ability for the machine to make a temporary connection to a server or the ability for the user to contact a server from his mobile device). Typically the persistent network connection has been conducted over "long-range communication technology" (e.g. hardwired, telephone network technology, cellular technology, WiFi technology, wide area network (WAN), local area network (LAN), or any wired or wireless communication technology over the internet that is known or

yet to be discovered). Traditionally, machines that accept payment other than cash require a persistent (ongoing or accessible on demand) connection to a network to facilitate payment. This is true for machines that accept, for example, credit cards and debit cards. The payment accepting units 120 described herein do not require a traditional persistent network connection. The user's mobile device 150 acts as a communication bridge between the adapter module 100 and the server 130. Communications between user mobile devices 150 and the servers (e.g. a system management server 130 and/or a funding source server 160) take place using long-range communication technology. Communications between user mobile devices 150 and the adapter module 100 of the payment accepting unit 120 take place using "short-range communication technology" (e.g. Bluetooth (e.g. Bluetooth 4.0, Bluetooth Smart, Bluetooth LE (Low Energy), near-field communication, Ultra Wideband (UWB), RFID, infrared wireless, induction wireless, or any wired or wireless technology that could be used to communicate a small distance (e.g. approximately a hundred feet or closer) that is known or yet to be discovered). Neither the adapter module 100 nor the payment accepting unit 120, therefore require a traditional persistent long-range wireless network connection. The exemplary communications technology shown in the figures may be replaced with alternative like communications technology and, therefore, specific shown communications technologies are not meant to be limiting. For example WiFi technology could be replaced with another long-range communication technology.

- Server: A server is the host processing server that may be operated by the company running the system. For each user, the server 130 preferably maintains at least one "virtual wallet" having at least one "balance" (which can be $0) of designated funds for which the server 130 keeps an accounting. The balance may represent, for example, "cash" or it may be a "promotional value" that represents funds that may be spent under certain circumstances. If these funds begin to be depleted, the user may be notified (e.g. via the application 140 on the mobile device 150) that additional funds need to be designated and/or transferred. Alternatively, funds from other sources (e.g. the funding source server 160) may be automatically transferred to restore a

predetermined balance. The balance may also be increased based on a promotion (e.g. points earned or coupons). As shown in FIG. 58, the server includes appropriate processors 950, memory 960 (which would keep an accounting of the user's balance in a manner similar to a gift card), and communication systems 970. As shown, the communications unit 970 of the server 130 includes long-range communication technology (e.g. cellular technology and WiFi mechanisms). The server 130 also includes a security unit 955 for encrypting and decrypting messages. The server 130 receives an AuthRequest from the adapter module 100 (via a mobile device 150) and, if funds are available, returns the AuthGrant for funds. FIG. 58 shows exemplary components associated with the server 130. The shown example may be divided into multiple distinct components that are associated with each other or the example may be incorporated into or drawn from other technology (e.g. a computer or a main frame) as long as the components are associated with each other.

- Advertise Presence: Each adapter module 100 advertises its presence by broadcasting signals (advertising broadcast signals) to mobile devices in the zones 102, 104, 016. Each adapter module 100 can listen to other adapter modules' advertisements

- Received Signal Strength Indicator (RSSI): The adapter module 100 may have a self-calibrating signal strength to determine zone thresholds (e.g. a payment zone threshold). At the time the user selects an item (product or service) from the payment accepting unit 120, the Received Signal Strength Indicator (RSSI) is logged. At this moment, it is presumed the user is within "arms-length" (which may be a predetermined length approximating the distance of a user standing in front of a machine for the purpose of making a purchase) from the payment accepting unit 120. Mathematical computation (In-Range Heuristics) is conducted to derive the optimal RSSI threshold at which point payment should be triggered by an application 140 on a mobile device 150. The threshold may be payment accepting unit specific and can vary over a period of time. This optimal zone threshold is preferably reported to the mobile device 150 during an initial handshake.

- In-Range Heuristics: Mathematical computation that determines the RSSI threshold to determine when a user is in the authorization zone 104 and/or payment zone 102. This computation can take into consideration numerous historical data points as well as transaction specific information such as which mobile device 150 is being used, payment accepting unit type, among other factors. Preferably the RSSI is logged while the user is making his selection (this is the one time in the entire process that the user definitely will be "in range" (e.g. they will be arm's length from the machine 120 because they are physically interacting with the machine 120). The type of user mobile device 150, accelerometer data (e.g. is the user moving or stationary), and/or other information may also be logged while the user is making his selection. The adapter module 100 can give a reference RSSI for the payment zone 102 for the machine 120, and the application 140 can make a +/- adjustment based on the specific mobile device 150 on which it is installed. Over a period of time, the system continues to improve itself based on additional data points.

- Authorization Request (AuthRequest): When a user enters the authorization zone 104, the mobile device 150 notifies the adapter module 100 and the adapter module 100 sends the secured authorization request (e.g. the encrypted authorization request) as a "message" (also referred to as a communication or transmissions) to the server 130 via the mobile device 150. Encryption may be performed by a security unit 755 (security technology that may be associated with the processing unit 750 and/or the memory 760). Significantly, the AuthRequest is a request for authorization of funds, not a request for authorization of a transaction. The purpose of the funds is irrelevant to the server 30.

- Authorization Grant Token (AuthGrant): This is a "message" (also referred to as a communication or transmissions) encrypted by the security unit 955 (security technology) of the server 130 with the unique private key for the adapter module 100. The secured authorization grant (e.g. the encrypted authorization grant) is passed from the server 130 (via the mobile device 150) to the adapter module 100 in the form of a message. The mobile device 150, however, is not able to decrypt and read the message. The authorization grant is in response to the authorization request. The amount of the funds granted

by the AuthGrant may be determined by factors including, but not limited to, the amount of funds available (or, if funds are not available, a mini-loan could be granted), a pre-authorized amount (e.g. set by the server, set by the user during set-up, set by the funding source, or a standard amount), limited by time (e.g. only a certain amount per hour, or a predetermined amount at specific times of the day), limited to the maximum amount of an item on the machine (or enough for two or three items in the machine), or one or more of these and other factors. Significantly, the AuthGrant makes the funds available, but does not authorize a transaction. The AuthGrant may have an associated expiration period in that it may expire if it is not used in a pre-determined time period. The length of time before the AuthGrant expires may be determined by factors including, but not limited to, the trustworthiness of the user (e.g. the user has a long history with the system or some known provider (e.g. credit card provider, bank, or credit union), the user has a good credit rating, or the user has a large wallet balance), a pre-authorized time period (e.g. set by the server, set by the user during set-up, set by the funding source, or a standard time period), limited by time (e.g. predetermined time periods at specific times of the day such as longer times during breakfast, lunch, and dinner), limited by the machine or the products or services sold in the machine, limited by the number of other users near the machine (e.g. if it is a crowded machine, the AuthGrant may expire faster), or one or more of these and other factors. The AuthGrant remains valid until it expires or some other event occurs to end its validity (e.g. the user cancels it). This means that under normal circumstances the mobile device 150 will hold the AuthGrant authorizing use of funds for a pre-determined time period that will allow the user sufficient time to make a purchase. The authorized amount may be considered to be the "wallet balance" that is held in a virtual "wallet."

- Synchronization: Time may be synchronized to the adapter module 100 from the server 130. The server 130 sends time information with encrypted messages and the adapter module 100 uses the time encoded in the messages for synchronization.
- The mobile-device-to-machine payment systems and components thereof may have associated hardware, software, and/or firmware (a variation, subset, or

hybrid of hardware and/or software). The term "hardware" includes at least one "processing unit," "processor," "computer," "programmable apparatus," and/or other known or yet to be discovered technology capable of executing instructions or steps (shown as processing unit 750 in FIG. 56, processing unit 850 in FIG. 57, and processing unit 950 in FIG. 58). The term "software" includes at least one "program," "subprogram," "series of instructions," or other known or yet to be discovered hardware instructions or hardware-readable program code. Software may be loaded onto hardware (or firmware) to produce a "machine," such that the software executes on the hardware to create structures for implementing the functions described herein. Further, the software may be loaded onto the hardware (or firmware) so as to direct the mobile-device-to-machine payment systems (and components thereof) to function in a particular manner described herein or to perform a series of operational steps as described herein. "Hardware" such as the adapter module 100, mobile device 150, and payment accepting unit 120 may have software (e.g. programs and apps) loaded thereon. The phrase "loaded onto the hardware" also includes being loaded into memory (shown as memory 760 in FIG. 56, memory 860 in FIG. 57, and memory 960 in FIG. 58) associated with or accessible by the hardware. The term "memory" is defined to include any type of hardware (or other technology) -readable media (also referred to as computer-readable storage medium) including, but not limited to, attached storage media (e.g. hard disk drives, network disk drives, servers), internal storage media (e.g. RAM, ROM, EPROM, FLASH-EPROM, or any other memory chip or cartridge), removable storage media (e.g. CDs, DVDs, flash drives, memory cards, floppy disks, flexible disks), firmware, and/or other known or yet to be discovered storage media. Depending on its purpose, the memory may be transitory and/or non-transitory. Appropriate "messages," "communications," "signals," and/or "transmissions" (that includes various types of information and/or instructions including, but not limited to, data, commands, bits, symbols, voltages, currents, electromagnetic waves, magnetic fields or particles, optical fields or particles, and/or any combination thereof) over appropriate "communication paths," "transmission paths," and other means for signal transmission including any type of connection between two elements on the system (the system including, for example, the adapter

module 100, mobile device 150, payment accepting unit 120, hardware systems and subsystems, and memory) would be used as appropriate to facilitate controls and communications.

- It should be noted that the terms "programs" and "subprograms" are defined as a series of instructions that may be implemented as software (i.e. computer program instructions or computer-readable program code) that may be loaded onto a computer to produce a "machine," such that the instructions that execute on the computer create structures for implementing the functions described herein or shown in the figures. Further, these programs and subprograms may be loaded onto a computer so that they can direct the computer to function in a particular manner, such that the instructions produce an article of manufacture including instruction structures that implement the function specified in the flow chart block or blocks. The programs and subprograms may also be loaded onto a computer to cause a series of operational steps to be performed on or by the computer to produce a computer implemented process such that the instructions that execute on the computer provide steps for implementing the functions specified in the flow chart block or blocks. The phrase "loaded onto a computer" also includes being loaded into the memory of the computer or a memory associated with or accessible by the computer. Separate, albeit interacting, programs and subprograms may be associated with the adapter modules 100, the server 130, and the mobile device 150 (including the mobile application 140) and these programs and subprograms may be divided into smaller subprograms to perform specific functions.

- The terms "messages," "communications," "signals," and/or "transmissions" include various types of information and/or instructions including, but not limited to, data, commands, bits, symbols, voltages, currents, electromagnetic waves, magnetic fields or particles, optical fields or particles, and/or any combination thereof. Appropriate technology may be used to implement the "communications," "signals," and/or "transmissions" including, for example, transmitters, receivers, and transceivers. "Communications," "signals," and/or "transmissions" described herein would use appropriate technology for their intended purpose. For example, hard-wired communications (e.g. wired serial

communications) would use technology appropriate for hard-wired communications, short-range communications (e.g. Bluetooth) would use technology appropriate for close communications, and long-range communications (e.g. WiFi or Cellular) would use technology appropriate for remote communications over a distance. Appropriate security (e.g. SSL or TLS) for each type of communication is included herein. Security units 755 and 955 include technology for securing messages. The security technology may be, for example, encryption/decryption technology (e.g. software or hardware). Although encryption/decryption is discussed primarily as being performed using a unique private key, alternative strategies include, but are not limited to encryption/decryption performed using public/private keys, or other encryption/decryption strategies known or yet to be discovered. Appropriate input mechanisms and/or output mechanisms, even if not specifically described, are considered to be part of the technology described herein. The exemplary communications unit 770 (shown in FIG. 56) of the adapter module 100 is shown as including appropriate input and output mechanisms 772, 774 that may be implemented in association (e.g. directly or indirectly in functional communication) with male and female adapters 720, 730 of the adapter module 100. The exemplary communications unit 870 (shown in FIG. 57) of the mobile device 150 includes mechanisms for both long-range communications (shown as Cellular and/or WiFi mechanisms 872) for communicating with the server 130 and short-range communications (shown as Bluetooth mechanisms 876) for communicating with the adapter module 100.

- When used in relation to "communications," "signals," and/or "transmissions," the terms "provide" and "providing" (and variations thereof) are meant to include standard means of provision including "transmit" and "transmitting," but can also be used for non-traditional provisions as long as the "communications," "signals," and/or "transmissions" are "received" (that can also mean obtained). The terms "transmit" and "transmitting" (and variations thereof) are meant to include standard means of transmission, but can also be used for non-traditional transmissions as long as the "communications," "signals," and/or "transmissions" are "sent." The terms

"receive" and "receiving" (and variations thereof) are meant to include standard means of reception, but can also be used for non-traditional methods of obtaining as long as the "communications," "signals," and/or "transmissions" are "obtained."

- The term "associated" is defined to mean integral or original, retrofitted, attached, connected (including functionally connected), positioned near, and/or accessible by. For example, if the user interface (e.g. a traditional display 122 (FIG. 19), a touch screen display 124 (FIG. 19), a key pad 126 (FIG. 19), buttons 126 (FIG. 19, shown as part of the key pad 126), a keyboard (not shown), and/or other input or output mechanism) is associated with a payment accepting unit 120, the user interface may be original to the payment accepting unit 120, retrofitted into the payment accepting unit 120, attached to the payment accepting unit 120, and/or a nearby the payment accepting unit 120. Similarly, adapter modules 100 may be associated with payment accepting units 120 in that the adapter modules 100 may be original to the payment accepting unit 120, retrofitted into the payment accepting unit 120, attached to the payment accepting unit 120, and/or a nearby the payment accepting unit 120.
- It should be noted that relative terms are meant to help in the understanding of the technology and are not meant to limit the scope of the invention. Similarly, unless specifically stated otherwise, the terms used for labels (e.g. "first," "second," and "third") are meant solely for purposes of designation and not for order or limitation. The term "short" in the phrase "short-range" (in addition to having technology specific meanings) is relative to the term "long" in the phrase "long-range."
- The terms "may," "might," "can," and "could" are used to indicate alternatives and optional features and only should be construed as a limitation if specifically included in the claims.
- It should be noted that, unless otherwise specified, the term "or" is used in its nonexclusive form (e.g. "A or B" includes A, B, A and B, or any combination thereof, but it would not have to include all of these possibilities). It should be noted that, unless otherwise specified, "and/or" is used similarly (e.g. "A

and/or B" includes A, B, A and B, or any combination thereof, but it would not have to include all of these possibilities). It should be noted that, unless otherwise specified, the terms "includes" and "has" mean "comprises" (e.g. a device that includes, has, or comprises A and B contains A and B, but optionally may contain C or additional components other than A and B). It should be noted that, unless otherwise specified, the singular forms "a," "an," and "the" refer to one or more than one, unless the context clearly dictates otherwise.

System Overview

[00103] FIGS. 5, 6, and 7 together show exemplary major components of the mobile-device-to-machine payment system and the interactions therebetwen.

[00104] As shown, the adapter module 100 functionally connected bi-directionally to the payment accepting unit 120 via a wired serial connection such that no security is necessary. The adapter module 100 is also functionally connected bi-directionally to the mobile device 150 (and its installed mobile application 140) via short-range communication technology (e.g. a Bluetooth connection). Because the mobile device 150 is not a "trusted" link (e.g. it could be hacked by a user), only secured communications (transmissions) are passed between the adapter module 100 and the mobile device 150. This keeps the passed communications secured and safe from hacking. The mobile device 150 (and its installed mobile application 140) is also functionally connected bi-directionally to a system management server 130 and/or a funding source server 160 via long-range communication technology (e.g. WiFi or Cellular connection) that preferably has appropriate security (e.g. SSL security). Security between the mobile device 150 and the system management server 130 has the advantage of protecting communications from the mobile device 150 to the system management server 130 that may include sensitive data and may not be encrypted. The system management server 130 and the funding source server 160 may be connected via a wired Internet connection with SSL security. The system management server 130 may be connected via a wired Internet connection with SSL security to an operators' server 170. Although not necessary to implement a purchase transaction, for other purposes (e.g. inventory), the operators' server 170 may be connected to the payment accepting unit 120 using a handheld computer sync or a cellular connection.

[00105] Also, a unique private key may be used to securely transmit encrypted messages between the adapter module 100 and the system management server 130 (although the encrypted transmissions would most likely be routed through the mobile device 150). The server 130 stores a private key for each adapter module 100, and this key is only known to the adapter module 100 and the server 130. No intermediary is privy to this key (especially not the mobile device 150). When the adapter module 100 and server 130 communicate messages (e.g. AuthRequest and AuthGrant), the security unit 755 of the adapter module 100 encrypts the message with its private key and passes the message to the mobile device 150. The mobile device 150 (which preferably cannot decrypt the message) passes the encrypted message to the server 130. The server 130 is able to decrypt the message using the security unit 955 of the adapter module 100 and the unique private key. The security unit 955 of the server 130 uses this same unique private key to encrypt messages to the adapter module 100 and sends the message to the mobile device 150 to relay to the adapter module 100 that is able to decrypt the message using the security unit 755 of the adapter module 100 and the unique private key.

[00106] FIG. 7 shows specific exemplary communications and messaging with an exemplary vending sequence (the numbers to the left of the communications and messaging) between the adapter module 100, the mobile device 150, and the system management server 130. These communications are discussed in more detail in the discussion pertaining to the timing schematics (FIGS. 8A-8G) and the flow charts (FIGS. 9A-9E).

[00107] It should be noted that FIGS. 5, 6, and 7 are meant to be exemplary and to help in the understanding of the mobile-device-to-machine payment system. For example, the shown long-range communications technology may be replaced with alternative long-range communications technology known or yet to be discovered, the shown short-range communication technology may be replaced with alternative short-range communication technology known or yet to be discovered, and the shown security may be replaced with alternative security known or yet to be discovered. The shown connections are meant to be exemplary in that, for example, there may be intermediaries that are not shown. The shown components have been simplified in that, for example, only one mobile device 150 (or machine 120, adapter module 100, or server 130) is shown where many may be included. Finally, the order of the steps may be changed and some steps may be eliminated.

Adapter Module

[00108] FIGS. 11-55 show exemplary adapter modules 100a-100e (referred to generally as adapter modules 100). These are relatively low cost hardware that are pre-configured to work with industry standard a multi-drop bus (MDB). On machines without MDB technology, the adapter module 100 can be configured or designed to work with other serial protocols or activate a switch. In essence the adapter module 100 simulates establishing payment on payment accepting unit 120 in much the same manner as other alternative forms of payment (e.g. cash).

[00109] The shown exemplary adapter modules 100 are preferably designed to be used as an in-line dongle for in-line insertion within, for example, a MDB of a machine 120. The wire used in MDB technology uses male and female connection ends or adapters to allow the attachment of peripherals. In the case of a vending machine, the wire with the connection ends or adapters would be present to allow the attachment of a payment receiving mechanism (e.g. a coin mechanism). The MDB male and female adapters 700, 710 may be separated (as shown in FIGS. 17, 18, 26, 27, 35, 36, 44, 45, 53, and 54). The adapter modules 100 have male and female adapters 720, 730. The adapter module may be plugged (inserted) in serial ("in-line") with the wire. For example, the MDB female adapter 710 may be connected to the male adapter 720 of the adapter module 100 and the MDB male adapter 700 may be connected to the female adapter 730 of the adapter module 100. The resulting in-line configuration is shown in FIGS. 19, 28, 37, 46, and 55. It should be noted that the adapter modules 100 are designed to allow pass-through communications so that if the mobile-device-to-machine payment systems is not enabled (e.g. for a particular purchase or simply turned off) the MDB functions as though the adapter module 100 is not there and the machine 120 can function normally.

Hands-Free

[00110] Summarily, if it is available, a hands-free mode, from the user's perspective, would allow the user to approach a favorite payment accepting unit 120 and notice that the display (e.g. the displays 122 or 124 shown in FIG. 19) associated with the payment accepting unit 120 shows funds available (e.g. the wallet balance), he would select the product or service using input mechanisms (e.g. buttons 126 or a touch screen display 124 shown in FIG. 19) associated with the payment accepting unit 120, and he would retrieve his dispensed services or products.

[00111] During an initial handshake with the mobile device 150 (when the user is within range), the adapter module 100 reports to the mobile device 150 whether or not hands-free mode is available. If it is available, the installed mobile application 140 automatically connects to the payment accepting unit 120 without the user having to interact with the mobile device 150. The user observes that funds are available on the display 122, 124 of the payment accepting unit 120 and completes the purchase transaction as if cash was inserted in the machine 120 by inputting his selection on the payment accepting unit 120. The payment accepting unit 120 dispenses the product or service. After the selection is made, the change is returned to the mobile device 150.

[00112] Whether hands-free payment is available is determined by factors including, but not limited to whether if other mobile devices 150 are in range, if other adapter modules 100 are in range, if there are any alerts, if the payment trigger threshold is having wide variances and so deemed unstable, or if the payment accepting unit operator (e.g. a vending machine operator) has opted to disable hands-free mode for the payment accepting unit 120. In the latter instance, operators can disable via a maintenance mobile device 150, as well as through the operators' server 170 and/or the system management server 130.

[00113] FIG. 3 is a table that showing exemplary considerations, conditions, or factors that may be used to determine whether the hands-free pay feature is available. Starting at the "Favorite?" column, this indicates whether the payment accepting unit 120 is a favorite machine. Preferably the hands-free pay feature is only available for use with "favorite" payment accepting units 120 (e.g. a vending machine at work or school). The "Alert" column has to do with whether there is some reason (e.g. there are too many users in range) that the hands-free pay feature should not work and, if there is such a reason, the user will be notified (alerted) and may be able to use the manual mode to resolve the alert and/or complete the transaction. FIG. 3 shows situations in which a user is or is not able to make hands-free purchases from a machine 120 using a mobile application 140 on his mobile device 150. It should be noted that the shown interface is meant to be exemplary. For example, some of the features could be automated or pre-selected. (It should be noted that the left hand column, the "Tab" column, relates to whether the selected tab on the mobile application 140 is "all" or "favorite." FIGS. 10A-10D all show these tabs. Unlike the other columns in FIG. 3, this column has more to do with the functionality and view of the application 140 than specifically with the hands-free feature. The tabs would allow a user to select whether he wanted to be alerted when he was in range of all payment accepting units 120 or just

"favorite" payment accepting units 120 and the application 140 would show the appropriate view.)

[00114] Balance Display: An optional feature of the mobile-device-to-machine payment system that is particularly helpful in the hands-free mode (although it may be available in the manual mode and/or in a multiple-vend scenarios) is when the user's mobile device 150 sends "credit" to the payment accepting unit 120 (either via hands-free payment or through a manual swipe), the wallet balance is sent to the payment accepting unit 120 that is then displayed to the user on a display 122, 124 of the machine 120. This is particularly beneficial during hands-free mode when the user does not retrieve the mobile device 150 and, therefore, may not know the balance. Also, in a multiple-vend scenario the user would not have to calculate a remaining balance.

[00115] An exemplary hands-free and multiple-vend scenario with a balance display might be as follows: The user has $5.00 in his virtual wallet as that is the amount that has been authorized (the AuthGrant being stored on the mobile device 150). He walks up to the payment accepting unit 120 and $5.00 is displayed on the display 122, 124 of the payment accepting unit 120 since hands-free mode was enabled and credit was sent (e.g. via short-range communication technology) to the payment accepting unit 120. The user makes a selection of $1.50 by interacting (e.g. pressing buttons) with the machine 120. The item (product or service) is dispensed and the "change" is "returned" (e.g. via short-range communication technology) to the virtual wallet. But since user is still standing in the payment zone 102, the remaining wallet balance of $3.50 is sent to the payment accepting unit 120 and displayed so that the user can now see he has a $3.50 balance. (It should be noted that the authorized funds may remain on the machine 120 and not be transferred back to the mobile device 150 between transactions.) The user decides to purchase a $1.50 item, and the transaction is completed as usual (e.g. by interacting with the machine 120). Now the user is still standing in the payment zone 102 and he sees the wallet balance of $2.00 on the display 122, 124 of the payment accepting unit 120. Deciding he does not wish to purchase anything else, the user walks away. As he walks out of the payment zone 102, the credit is cleared from the machine 120. But he is left with the knowledge that his wallet balance is $2.00 even though he never touched the mobile device 150. Communications between the payment accepting unit 120 and the adapter module 100 (via the mobile device 150) handle the accounting incidental to the transaction. The remaining balance ($2.00) is technically

stored on the server 130, and may be reflected on the application 140 on the mobile device 150.

Multiple Distinct Zones

[00116] As shown in FIGS. 1 and 2, the functions performed by the adapter module 100 can be divided into distinct zones: a first "communication zone" (e.g. "Bluetooth range" 106), a second "authorization zone" 104, and a third "payment zone" 102. The payment zone102 (that can not be zero) is smaller than or equal to (overlapping completely) the authorization zone 104. (Put another way, the payment zone 102 is within or coextensive with the authorization zone 104.) The payment zone 102 is a subset of the authorization zone 104 with a ratio of the payment zone 102 to the authorization zone 104 ranging from 0.01:1 to 1:1. It is not necessarily a fixed ratio and can vary between different payment accepting units 120, different mobile devices 150, different users, and over time. While the zones 102, 104, 106 are depicted as having a uniform shape, the zones may not necessarily be uniform (or constant over time) in that the shape can vary. For example, the shape of the Bluetooth range 106 may vary depending on environmental conditions such as obstacles in the room and payment accepting unit 120 door/wall materials.

[00117] Bluetooth Range 106: The outermost range is the Bluetooth range 106. This is the area in which the adapter module 100 is able to broadcast its presence. In most situations, the Bluetooth range 106 is a passive range in that no actual data is exchanged between the mobile device 150 and the adapter module 100. While in the Bluetooth range 106, the mobile device 150 monitors the RSSI (Received Signal Strength Indicator).

[00118] Authorization Zone 104: The middle region is the authorization zone 104. This is a computed area based on the RSSI. As mentioned, the mobile device 150 monitors the RSSI while it is in the Bluetooth range 106. When the RSSI reaches a certain predetermined threshold based on In-Range Heuristics, the mobile device 150 can be considered to be in the authorization zone 104. In the authorization zone 104 the mobile device 150 establishes a connection to the adapter module 100 (e.g. a Bluetooth connection (FIG. 5) with SSL protection (FIG. 6)) and informs the adapter module 100 of its presence. After a successful handshake with the adapter module 100, the mobile device 150 registers the adapter module 100 and the adapter module 100 requests an authorization to the server 130 via the mobile devices' network connection (e.g. a WiFi or cellular connection (FIG. 5) with SSL protection (FIG. 6)). It is important to note the mobile device 150 and the adapter

module 100 have a non-exclusive relationship at this point. The adapter module 100 may collect registrations for all mobile devices 150 that are within the authorization zone 104.

[00119] An authorization occurs in preparation for when the user enters the payment zone 102. An authorization expires in a set period of time (for example, five minutes), so if the mobile device 150 is still in the authorization zone 104 at the time of expiration, the adapter module 100 submits for and receives another authorization. This will continue for a set number of times (for example, the limit may be three times to limit cases of numerous authorizations for a mobile device that may remain in the authorization zone 104 for an extended period of time without completing a transaction). Should authorization fail (for instance if the limit had been reached) prior to the user entering the payment zone 102, the adapter module 100 will request authorization when the mobile device 150 enters the payment zone 102 (which adds a few seconds to the experience).

[00120] Payment Zone 102: As a user enters the payment zone 102, the mobile device 150 establishes exclusive control of the adapter module 100. Once established, any other user in the payment zone 102 is put into a "waiting" status.

[00121] In the payment zone 102, the payment can be triggered automatically if the system has and is in hands-free mode. In such instances, the mobile device 150 is running the app 140 in background mode and will send credit to the payment accepting unit 120 without any explicit user interaction. The user completes the transaction on the payment accepting unit 120 in much the same manner as if cash had been inserted into the payment accepting unit 120 to establish credit. After the user completes the transaction (that may include one or more purchases), details of the transaction are preferably returned to the mobile device 150 and server 130 in separate messages. The message to the server 130 is preferably encrypted with the adapter module's 100 private key (FIG. 6) to ensure data integrity. As shown in FIG. 7, the "private key" coded message (Encrypted VendDetails) is preferably sent via the mobile device 150. The message to the mobile device 150 may be sent solely for the purpose of closing the transaction. The transaction history and balance are updated server-side via the encrypted message sent to the server 130.

[00122] The other mode of operation is manual mode. In manual mode, the user launches the mobile device 150 and is able to swipe to send payment to the payment accepting unit 120. The user can also swipe back to cancel the payment. Like in hands-free mode, the purchase transaction is completed on the payment accepting unit 120 in the same

manner as if cash were inserted into the payment accepting unit 120. The mobile device 150 is only used to send payment. Selection is made directly on the payment accepting unit 120.

[00123] Self-Calibrating Zone Threshold: A key, but optional feature, of the system is a self-calibrating payment zone RSSI threshold. Because RSSI can vary machine to machine, environment to environment, and device to device, having a fixed threshold at which payment is triggered can be problematic. The approach suggested herein is the creation of a self-calibrating threshold. When the user is interacting with the payment accepting unit 120 (such as when he makes his selection on the payment accepting unit 120), the payment accepting unit 120 notifies the adapter module 100 and the adapter module 100 logs the conditions such as RSSI, type of user mobile device 150, accelerometer data, and other information. It is at this point that it can be ascertained safely that the user is within arms-length from the payment accepting unit 120 (by necessity the user is arms-length because he is making some physical interaction with the payment accepting unit 120). This is the only point in the entire transaction in which it can be certain that the user is within arms-length from the payment accepting unit 120.

[00124] FIG. 4 shows a simplified set of exemplary steps involved when users enter the payment zone 102. Specifically, FIG. 4 shows that credit is established 200 (this may have been done in the authorization zone 104, but if not it would be handled in the payment zone 102), that the user makes a selection using the machine 202, that the machine notifies the adapter module of the selection 204, that the adapter module (optionally) logs the RSSI 206, and that the purchase process(es) continues 208. Using the historically logged RSSI data, the adapter module 100 calculates one of several "average" RSSI using various mathematical models. This "average" could be a traditional average, a moving average, a weighted average, a median, or other similar summary function. The adapter module 100 could pre-process the historical data before running the function, such as to eliminate top and bottom data points, suspect data points, etc.

[00125] Optionally, during the handshake between the mobile device 150 and the adapter module 100, the information transmitted to the adapter module 100 may include, for example, the model of the mobile device 150. Using the received information pertaining to the mobile device models, the adapter module 100 can create multiple payment thresholds, one for each mobile device model. This allows for variances that may be inherent in different types of Bluetooth radios. An alternative to this method is for the adapter module 100 to broadcast a baseline payment zone threshold, and the mobile device 150 can use an offset

from this baseline based on its specific model type. The payment zone thresholds (or baseline offsets) can be unique to specific types of mobile devices (e.g. by manufacturer, operating system, or component parts), models of mobile devices, or individual mobile devices (unique to each user).

[00126] In a typical scenario in which the payment zone threshold has been calibrated, the adapter module 100 advertises its presence along with the threshold at which it considers any mobile device 150 to be in the authorization zone 104. This is a one-way communication from adapter module 100 to mobile device 150. Once the mobile device 150 enters the authorization zone 104, there is a handshake that is established between the adapter module 100 and the mobile device 150. During this handshake, the mobile device 150 can share its model information with the adapter module 100, and the adapter module 100 can return the payment zone 102 threshold for that specific model.

[00127] Optionally, in addition to calibrating the payment zone threshold, the adapter module 100 can apply the self-calibrating model to the authorization zone 104 to calibrate the authorization zone threshold. As with the payment zone thresholds, the authorization zone thresholds can be unique to specific types of mobile devices, models of mobile devices, or individual mobile devices. In this scenario, the adapter module 100 would broadcast multiple thresholds by device type and the mobile device 150 would determine which threshold to apply (or alternatively broadcast a baseline and the mobile device 150 uses an offset based on its device model). Even in this scenario, the authorization zone 104 is a one-way communication.

[00128] Optionally, along with the threshold that is calculated (in the payment and/or the authorization zone(s)), a safety margin can be added to minimize scenarios in which a user is within range, but the mobile-device-to-machine payment systems do not recognize it because the threshold may not have been reached. For example, if the calculated RSSI for an iPhone 5 on machine 4567 is -68db, the mobile-device-to-machine payment systems may add a safety margin of -5db, and establish the threshold at -73db. So when a user's phone is communicating with the adapter module 100 at an RSSI of -73db or better, the mobile-device-to-machine payment systems will allow the mobile device 150 to credit the payment accepting unit 120. The safety margin can be set on the server 130 and downloaded to the adapter module 100, or set on the mobile device 150, or set on the adapter module 100 itself.

[00129] Optionally, in the payment zone threshold, the mobile device 150 can use other data to determine when to cancel the exclusive control of the payment accepting unit 120, to identify when the user is moving out of the payment zone 102. External data could include accelerometer data from the mobile device 150. Using that data, the mobile device 150 can determine whether the user is standing relatively still in front of the payment accepting unit 120, or if the user is in motion – effectively walking away from the payment accepting unit 120.

Signal Unavailability Adaptation

[00130] The mobile-device-to-machine payment systems described herein use a mobile device's 150 short-range communication technology (shown as Bluetooth mechanisms 876 in FIG. 57) and a mobile device's 150 long-range communications technology (shown as Cellular and/or WiFi mechanisms 872 in FIG. 57). The short-range communication technology 876 communicates with the adapter module's 100 short-range communication technology (shown as Bluetooth mechanisms 776 in FIG. 56). The long-range communications technology 872 communicates with the server's 130 communication technology (not shown). The mobile device 150 (with a mobile application 140 thereon) acts as a communication bridge between the adapter module 100 (associated with a payment accepting unit 120) and the server 130. This process is described herein and works properly if there is cellular or WiFi coverage within the payment zone 102.

[00131] One option if there is no cellular or WiFi coverage within the payment zone 102 is to determine whether there is cellular or WiFi coverage within the authorization zone 104 or the Bluetooth range 106. If there is, then the sizes of the zones 102, 104, 106 could be adapted and the timing could be adapted. For example, if the mobile devices 150 detected problems with the cellular or WiFi coverage within the payment zone 102, the user could carry his mobile device 150 into the other zones (or the mobile device 150 could use short-range communication technology to communicate with other mobile devices 150 within the authorization zone 104 or the Bluetooth range 106) to determine whether the zones have cellular or WiFi coverage. If they do have coverage, communication between the mobile device 150 and the server 130 can be advanced (conducted earlier when the mobile device 150 is further from the machine 120) or delayed (conducted later when the mobile device 150 is further from the machine 120). This can be thought of as changing the size or shapes of the zones 102, 104, 106. The timing would also have to be adjusted so that the authorization of funds (AuthGrant) does not expire before the user has a chance to make a purchase. It also

means that balance updates to the server 130 may happen after the user has moved away from the machine 120 and has cellular or WiFi coverage again.

[00132] Another option if there is no cellular or WiFi coverage within any of the zones 102, 104, 106 is for the user to obtain authorization while outside of the zones in a place with cellular or WiFi coverage. This may occur, for example, if a user knows that he will be going to a place with a payment accepting unit 120 equipped with an adapter module 100 (perhaps to a favorite payment accepting unit 120) that does not have (or rarely has) cellular or WiFi coverage. A user may also use the mobile application 140 to query payment accepting units 120 in a given range (e.g. within 50 miles) or at a given location (e.g. at a campground or in a particular remote city) to determine whether there is cellular or WiFi coverage within the zones 102, 104, 106. The user can then obtain pre-authorization from the server 130 using the mobile application 140. Again, the timing would also have to be adjusted so that the authorization of funds (AuthGrant) does not expire before the user has a chance to make a purchase. It also means that balance updates to the server 130 may happen after the user has moved away from the machine 120 and has cellular or WiFi coverage again. A mobile-device-to-machine payment system having the ability to implement this option would be able to accept cashless payments without requiring any network connection near the payment accepting unit 120. Mobile-device-to-machine payment systems described herein that are located in a remote location where no signal is available, therefore, can accept cashless payments.

[00133] As an example of a situation in which there might be no cellular or WiFi coverage within any of the zones 102, 104, 106 of a particular payment accepting unit 120, the user (a teenager) may be traveling to a remote location to attend summer camp where there is no cellular or WiFi coverage. The camp may have several payment accepting units 120 (e.g. a machine that creates a dedicated "hot spot" that requires payment for use, vending machines, or machines for renting equipment (e.g. bikes, kayaks, or basket balls)). The camp facility might notify parents that the mobile-device-to-machine payment system is available. The parents, while at home, could obtain authorization for a particular amount (that could be doled out a certain amount per day or limited to type of machine or location) to be authorized and "loaded" into the user's mobile device 150 and specify that the authorization will not expire for a certain period or until a certain date. Thereafter, while at camp, the user could use the mobile application 140 on his mobile device 150 in a manner similar to those discussed elsewhere herein. Short-range communications may be used for communications

between the adapter modules 100 (associated with the machines 120) and users' mobile devices 150.

[00134] One subtle but powerful component of the systems described herein is that they require internet network connection only in the authorization zone 104 and only for the time period required to send the AuthRequest and receive the AuthGrant. Once a valid AuthGrant is received by the mobile device 150, an internet network connection is not required by either the mobile device 150 or the adapter module 100 in the payment zone 102 as long as the AuthGrant is valid (unexpired). This mechanism allows the system to seamlessly handle authenticated transactions in (temporary) offline mode, with the deferred acknowledgement and transaction messages performing the bookkeeping and cleanup when network connection is regained. The alternatives described above provide a unique way to artificially extend the authorization zone to include any location where the mobile device 150 can communicate with the server 130.

Multiple User Resolution

[00135] As shown in FIG. 2, in likely practical scenarios, there will be multiple users in the zones 102, 104, 106. As shown, users 1, 2, and 3 are in the payment zone 102 near the machine 120, users 5 and 6 are shown as positioned between the authorization zone 104 and the Bluetooth range 106, users 4 and 7 are in the Bluetooth range 106, user 10 is positioned on the edge of the Bluetooth range 106, and users 8 and 9 are positioned outside of Bluetooth range 106. The mobile-device-to-machine payment systems provide for managing, and resolving issues pertaining to multiple users.

[00136] Users 4 and 7 are within the Bluetooth range 106 and user 10 is either entering or leaving the Bluetooth range 106. Within the Bluetooth range 106 the users' mobile devices 150 are able to see the adapter module's 100 advertisement. In this zone, the mobile device 150 preferably does not initiate a connection. The adapter module 100 is preferably unaware of the users in the Bluetooth range 106. All the adapter module 100 is doing is advertising its presence to any multitude of users that may be in Bluetooth range 106.

[00137] The adapter module 100 begins to log users as the users (and their respective mobile devices 150) enter the authorization zone 104 (shown in FIG. 2 as users 5 and 6). At this point, there is a non-exclusive connection initiated by the mobile device 150 to the adapter module 100. It does a handshake (e.g. to exchange information needed to obtain authorization and, optionally, to log information needed for a self-calibrating authorization

zone threshold) and the mobile device 150 contacts the server 130 for an authorization (e.g. sending an AuthRequest and receiving an AuthGrant). The adapter module 100 registers all mobile devices 150 that have requested and received AuthGrants. The adapter module 100 continues communicating with any other mobile device 150 that enters the authorization zone 104. After initial contact, the adapter module 100 may provide the mobile device 150 with a deferral delay of when to check back in with the adapter module 100 allowing opportunity for other mobile devices 150 to communicate with the adapter module 100.

[00138] If there is only one user in the payment zone 102, a purchase transaction may be performed. If there are multiple users in the payment zone 102, the mobile-device-to-machine payment system must handle the situation.

[00139] One optional exemplary solution for handling the situation of the multiple users in the payment zone 102 is queuing users in the payment zone 102. Once any mobile device 150 enters the payment zone 102, it establishes exclusivity to a particular mobile device 150 (first come first serve). Technically, however, the adapter module 100 is not establishing an exclusive connection to the mobile device 150. The adapter module 100 can still perform a round-robin poll and communicate with and advertise to other mobile devices 150. Instead, the adapter module 100 establishes a queue prioritized by RSSI and time (e.g. who was first and whether the authorization has expired) and it notifies (e.g. alerts) other mobile devices 150 to wait. The earliest valid (unexpired) authorization takes precedence when there is any tie in the RSSI. Otherwise, for example, the strongest average RSSI takes priority. Preferably the queue is not a static measure of the RSSI but an averaged measure over the period of time in the queue. This compensates for a scenario in which a user may be walking around in the queue and then shows up at the payment accepting unit 120 just as the previous user is finishing. If another user was also in the payment zone 102 and stood there the entire time, but may have newer authorization, he could win out.

[00140] Anytime that the adapter module 100 cannot determine exactly which user is in the payment zone 102 in front of the payment accepting unit 120, the adapter module 100 will disable hands-free payment. The mobile device 150 will send an alert to the user and he can use swipe to pay (manual mode). All users in payment zone 102 will show "Connected" and the first to swipe payment to the payment accepting unit 120 then locks out other users.

Multiple Module Resolution

[00141] In the scenario where there are multiple modules present, determining which payment accepting unit 120 a user is in front of can be a challenge. The mobile-device-to-machine payment systems described herein allow for adapter modules 100 to communicate to other adapter modules 100 in range via Bluetooth. Each user receives authorization grants for specific payment accepting units 120. This means if there are multiple adapter modules 100 within the same authorization zone 104, there will be multiple authorization grants for the user. When the user enters the payment zone 102, it can be difficult to differentiate which payment accepting unit 120 the user is in front of if the payment zones 102 overlap.

[00142] To solve this problem, when the user enters the payment zone 102, the adapter modules 100 communicate with each other to determine the RSSI for the particular user (based on the signal from his mobile device 150) to triangulate which adapter module 100 (and the associated payment accepting unit 120) is closer to the user. Optionally, the inter-module communications can restrict the user to establishing an exclusive connection with only one payment accepting unit 120.

[00143] Optionally, when the user connects to a payment accepting unit 120, the mobile device 150 can send a communication to the payment accepting unit 120 for momentary display to the user on the display 122, 124 of the payment accepting unit 120. For example, the mobile device 150 can send a communication (e.g. "connected" or "Fred's Mobile Device Connected") to the payment accepting unit's display 122, 124 for a predetermined period of time (e.g. 1-3 seconds) so when the user is in payment zone 102, it is clear which payment accepting unit 120 the user is connected to prior to making a purchase (either in hands-free or manual mode).

[00144] In addition, when the user is in manual mode, the mobile device 150 can display (e.g. on the touch screen 152 as shown in FIGS. 10A-10D) a visual indication of the payment accepting unit 120 (e.g. a picture and/or a payment accepting unit ID of the payment accepting unit 120) for visual confirmation. If the user is in manual mode, the user can manually change the payment accepting unit 120.

Descriptive Scenario

[00145] FIG. 7, FIGS. 8A-8G, and 9A-E (as well as other figures) can be used to understand a detailed exemplary scenario of the mobile-device-to-machine payment systems described herein. An exemplary flow of communications and steps are loosely described

below with reference to these (and other figures). It should be noted that alternative scenarios could include, for example, a modified order of the steps performed.

[00146] Prior to vending transactions, a user downloads a mobile app 140 onto his mobile device 150, creates an account, and configures a funding source via, for example, a funding source server 160. A funding source may be, for example, a debit card, a credit card, campus cards, rewards points, bank accounts, payment services (e.g. PayPal®) or other payment option or combination of payment options known or yet to be discovered. The funding sources may be traditional and/or nontraditional payment sources that are integrated into the ecosystem described herein and then used indirectly as a source of funds. Funds from the funding source are preferably held on the server 130 such that when an AuthRequest is received by the server 130, the server 130 can send an AuthGrant authorizing funds for a purchase.

[00147] The user can specify one or more "favorite" adapter module(s) 100 (that has a one-to-one relationship to the payment accepting unit 120) that he may visit regularly, such as a vending machine at school or work. Favorite adapter modules 100 appear on a pre-filtered list and allow for additional rich features such as hands-free payment.

[00148] The payment accepting unit 120 may be equipped with an adapter module 100 that is constantly advertising its availability via Bluetooth (or other "signals," "communications," and/or "transmissions"). This ongoing advertising and scanning for adapter modules is shown in FIG. 8A. As shown, the mobile device 150 is continuously scanning for any adapter module 100 within Bluetooth (or other "signal," "communication," and/or "transmission") range. When the user is within range of that adapter module 100, the mobile device 150 tracks and monitors the signal strength until a predetermined "authorization zone" threshold is achieved.

[00149] FIGS. 8B and 9A generally show that when the authorization zone threshold is reached, the mobile device 150 enters the authorization zone (block 302) and registers the adapter module 100. The mobile device 150 connects to the server 130 (block 304). The app 140 on the mobile device 150 creates a request for authorization (AuthRequest) and passes the AuthRequest to the server 130 using appropriate communication technology (e.g. cellular or WiFi) (block 306). The server 130 responds with an authorization grant (AuthGrant) encrypted with the specific adapter module's private key (block 306). This authorization token may minimally include the Userl D, Apparatusl D (for the adapter module 100),

authorization amount, and expiration time. The mobile device 150 receives the AuthGrant from the server 130, and retains it until the mobile device 150 is ready to issue payment to an adapter module 100. The mobile device 150 collects all pending AuthGrants that may be one or more depending on how many adapter modules 100 are in-range. Unused AuthGrants that expire are purged from the mobile device 150 and the server 130. It is important to note that the mobile device 150 is unable to read the AuthGrant because it is encrypted with the adapter module's unique private key that is only known to server 130 and adapter module 100. This provides a preferred key element of security in the system as the adapter module 100 only trusts AuthGrants that are issued by the server, and the AuthGrants cannot be read or modified by the mobile device 150 or any other party in between the server and the adapter module 100. Additional mobile devices 150 may enter the authorization zone 104 (block 308).

[00150] As the user approaches a specific adapter module 100, the user enters the payment zone 102 and an event threshold is triggered based on heuristics performed by the mobile device 150. Blocks 310 and 312 show the loop steps of waiting for a mobile device 150 from the authorization zone 104 to enter the payment zone 102. If the user leaves the authorization zone 104 without entering the payment zone 102, the adapter module 100 returns to advertising its presence (block 300).

[00151] FIGS. 8C and 9B generally show the user entering the payment zone. The mobile device 150 verifies that it has an unexpired and valid AuthGrant. If the AuthGrant is not good, it may be requested again, repeating the Auth Request process (block 315). If the AuthGrant is good, the mobile device 150 sends the valid AuthGrant (including the wallet balance (block 322)) to the adapter module 100 to initiate a transaction. The mobile device 150 may issue the AuthGrant automatically without specific user interaction if the hands-free mode is supported (and the device is a favorite (block 318), there is only one device in the payment zone 102 (block 318), and (optionally) there is only one user in the authorization zone 104 (block 320). If any of these factors are not present, the mobile device 150 will prompt and/or wait for the user to begin the transaction manually (block 324).

[00152] FIGS. 8D, 9C, and 9D generally show the transaction process. As shown in FIG. 9C, the adapter module 100 runs through a series of questions to determine if there are any issues that would prevent vending including: has the user canceled in-app? (block 326), has the user walked away? (block 328), is the coin return pressed? (block 330), has more than a predetermined period of time elapsed? (block 332). If the answer to any of these questions

is "yes," the transaction does not proceed. If the answers to all of these questions is "no," the user makes a selection (block 334) on the payment accepting unit 120 in the same or similar manner as compared to if cash or credit were presented to the payment accepting unit 120. If the machine 120 is able to vend (block 336), it attempts to release the product. If the vend fails (block 338) it is reported by the machine (block 340) and a credit is returned to the virtual wallet (block 342). If the vend is successful (block 338) it is reported by the machine (block 344). Put another way, after the transaction is complete, the adapter module 100 returns to the mobile device 150 the details of the transaction as well as an encrypted packet containing the vend details to be sent to the server 130 via the mobile device 150. Optionally, the adapter module 100 can pass additional information not directly related to the transaction such as payment accepting unit health, sales data, error codes, etc.

[00153] FIGS. 8D and 9E generally show the multi-vend function. If the machine has enabled multi-vend capabilities (block 350) and the multi-vend limit has not been reached, the process returns to the question of whether the user is in the payment zone (block 310 of FIG. 9A). If the machine does not have enabled multi-vend capabilities (block 350) or the multi-vend limit has been reached, the wallet is decremented by the vend amount(s) and "change" is returned to the virtual wallet (block 354) and the process ends (block 356).

[00154] FIG. 8E is a timing schematic showing an exemplary Login process. FIG. 8F is a timing schematic showing an exemplary bootup process. FIG. 8G is a timing schematic showing an exemplary Account Check/Update process.

[00155] Several of the figures are flow charts (e.g. FIGS. 9A-9E) illustrating methods and systems. It will be understood that each block of these flow charts, components of all or some of the blocks of these flow charts, and/or combinations of blocks in these flow charts, may be implemented by software (e.g. coding, software, computer program instructions, software programs, subprograms, or other series of computer-executable or processor-executable instructions), by hardware (e.g. processors, memory), by firmware, and/or a combination of these forms. As an example, in the case of software, computer program instructions (computer-readable program code) may be loaded onto a computer to produce a machine, such that the instructions that execute on the computer create structures for implementing the functions specified in the flow chart block or blocks. These computer program instructions may also be stored in a memory that can direct a computer to function in a particular manner, such that the instructions stored in the memory produce an article of manufacture including instruction structures that implement the function specified in the flow

chart block or blocks. The computer program instructions may also be loaded onto a computer to cause a series of operational steps to be performed on or by the computer to produce a computer implemented process such that the instructions that execute on the computer provide steps for implementing the functions specified in the flow chart block or blocks. Accordingly, blocks of the flow charts support combinations of steps, structures, and/or modules for performing the specified functions. It will also be understood that each block of the flow charts, and combinations of blocks in the flow charts, may be divided and/or joined with other blocks of the flow charts without affecting the scope of the invention. This may result, for example, in computer-readable program code being stored in whole on a single memory, or various components of computer-readable program code being stored on more than one memory.

Distinction From Known Systems

[00156] Many of the known systems and methods require that the payment accepting unit be persistently (continuously) connected to and/or connectable on demand to some sort of remote server in order to function. As an example, the Carlson reference describes a system and a method for using a portable consumer device. Described embodiments include a consumer using the portable consumer device to dial a number to purchase an item (product or service) in a vending machine, to send an SMS to purchase an item in a vending machine, or to use a mobile wallet to purchase an item in a vending machine. It is mentioned in one embodiment that the consumer may launch an application in the portable consumer device or, alternatively, the portable consumer device may automatically detect the vending machine and prompt the consumer to enter information associated with the vending machine. It should be noted, however, that even when there is automatic detection, the user is prompted to enter information (e.g. a machine alias, payment information, or a PIN) and it can be inferred that this is entered on the portable consumer device. Once connected to a payment processing network, the authorization process begins using a payment processing network and/or payment server. Significantly, all of the embodiments described in the Carlson reference specify that the payment server sends an authorization response message to the vending machine. This means that, unlike the mobile-device-to-machine payment systems described herein, a persistent network connection is required for the Carlson system to function. Other references that disclose systems that require a persistent network connection include the Khan reference (the MicroAdapter having the persistent connection), the Garibaldi reference, and the Weiner reference.

[00157] Many of the known systems and methods require the user to significantly interact with their mobile devices. As an example, the Whigham reference is directed to a system that eliminates the need for currency for a vending machine and also eliminates the need for a dedicated online connection between the vending machine and the issuer of a credit card or a debit card. Instead the Whigham system and method allows a consumer to purchase a product from an automatic vending machine by using the consumer's cellular telephone, personal digital assistant (P DA), or similar wireless communication device as a link between the provider of the products in the vending machine and the vending machine. The Whigham reference, however, sets forth a system and method requires significant interaction between the consumer and his telephone including dialing a telephone number to a server (that, in turn, provides a vend code to the consumer), requesting a specific product (e.g. by dialing additional digits, although this step is optional if a unique number was dialed for a specific product), and transmitting a vend code to the vending machine. (Other references that disclose systems that require user interaction with the phone include the Offer reference, the Khan reference, the Belfer reference, and the Carlson reference.) In addition to other differences, some of the mobile-device-to-machine payment systems described herein do not require the user to interact with his mobile device at all, which can be contrasted to known systems and methods that require the consumer to, for example, dial a telephone number, enter a machine identification, and/or enter a product identifier using the mobile device to purchase a product.

[00158] The known systems and methods that use a cellular telephone to facilitate cashless transactions at a vending machine use the cellular telephone to authorize a particular transaction. For example, once the user knows what he wants from a vending machine, he can dial a server and receive authorization to make a specific purchase. Sometimes this includes dialing additional numbers on the cellular telephone to specify a particular product. The mobile-device-to-machine payment systems described herein take a completely different approach. The mobile-device-to-machine payment systems described herein are not specifically interested in the details of the transaction to authorize the transaction. Instead, the mobile-device-to-machine payment systems function more like a gift card, a credit card, or a debit card in that they allow the user to have funds to make a purchase. When a user is in range, the adapter module 100 (via a mobile device 150) sends an AuthRequest to the server 130 to preemptively obtain authorization to make funds available. The server 130 returns the AuthGrant for funds to the adapter module 100 (via a mobile device 150) so that

the user may use the funds to make a purchase. The AuthGrant may remain valid until it expires. This gives the user significantly more flexibility than known systems and methods.

Miscellaneous

[00159] It is to be understood that the inventions, examples, and embodiments described herein are not limited to particularly exemplified materials, methods, and/or structures. It is to be understood that the inventions, examples, and embodiments described herein are to be considered preferred inventions, examples, and embodiments whether specifically identified as such or not.

[00160] All references (including, but not limited to, foreign and/or domestic publications, patents, and patent applications) cited herein, whether supra or infra, are hereby incorporated by reference in their entirety.

[00161] The terms and expressions that have been employed in the foregoing specification are used as terms of description and not of limitation, and are not intended to exclude equivalents of the features shown and described. While the above is a complete description of selected embodiments of the present invention, it is possible to practice the invention using various alternatives, modifications, adaptations, variations, and/or combinations and their equivalents. It will be appreciated by those of ordinary skill in the art that any arrangement that is calculated to achieve the same purpose may be substituted for the specific embodiment shown. It is also to be understood that the following claims are intended to cover all of the generic and specific features of the invention herein described and all statements of the scope of the invention that, as a matter of language, might be said to fall therebetween.

WHAT IS CLAIMED IS:

1. A method of payment processing, comprising:

at a device with one or more processors, memory, and two or more communication capabilities:

obtaining, from a payment module, an authorization request via a first communication capability;

sending, to a server, the authorization request via a second communication capability distinct from the first communication capability;

in response to sending the authorization request, obtaining, from the server, authorization information via the second communication capability;

after obtaining the authorization information, detecting a trigger condition to perform a transaction with a payment accepting unit associated with the payment module; and

in response to detecting the trigger condition, sending, to the payment module, at least a portion of the authorization information via the first communication capability.

2. The method of claim 1, wherein the first communication capability corresponds to a short-range communication protocol and the second communication capability corresponds to a long-range communication protocol.

3. The method of claim 1, further comprising:

obtaining, from the payment module, advertised information indicating the payment module's presence via the first communication capability that at least includes authorization zone threshold criterion.; and

after obtaining the advertised information, initiating a handshake process with the payment module, wherein the handshake process includes:

sending, to the payment module, device information at least including user identification information corresponding to the user of the device via the first communication capability; and

receiving, from the payment module, payment module information, wherein the payment module information at least includes an identifier corresponding to the payment module.

4. The method of claim 3, further comprising:

prior to obtaining the authorization request:

in accordance with a determination that the authorization zone threshold criterion is satisfied, sending notification information to the payment module via the first communication capability, wherein the notification information indicates that the authorization zone threshold criterion is satisfied;

wherein the device obtains the authorization request in response to sending the notification information.

5. The method of claim 3, wherein the payment module information further includes an indication that hands-free mode is available and payment zone threshold criterion.

6. The method of claim 5, wherein the device information further includes device identification information corresponding to a model type of the device; and

wherein the payment zone threshold criterion is based at least in part on the device identification information.

7. The method of claim 5, wherein detecting the trigger condition comprises:

determining whether the payment zone threshold criterion is satisfied; and

in accordance with a determination that the payment zone threshold criterion is satisfied, detecting the trigger condition without interaction from a user of the device.

8. The method of claim 1, wherein detecting the trigger condition comprises:

detecting a user input from a user of the device; and

in response to detecting the user input, detecting the trigger condition to perform a transaction with the payment accepting unit.

9. The method of claim 1, further comprising:

in response to obtaining the authorization information, presenting a notification to the user of the device that a connection has been established with the payment module.

10. The method of claim 9, wherein the notification further indicates an authorized amount for the transaction.

11. The method of claim 1, wherein the authorization information includes an identifier corresponding to the payment module, an identifier corresponding to the user of the device,

an authorized amount, an authorization grant token, and an expiration period for the authorization grant token.

12. The method of claim 11, wherein at least a portion of the authorization request and the authorization grant token are encrypted with a unique encryption key corresponding to the payment module.

13. A device, comprising:

two or more communication capabilities;

one or more processors; and

memory storing one or more programs to be executed by the one or more processors, the one or more programs comprising instructions for:

obtaining, from a payment module, an authorization request via a first communication capability;

sending, to a server, the authorization request via a second communication capability distinct from the first communication capability;

in response to sending the authorization request, obtaining, from the server, authorization information via the second communication capability;

after obtaining the authorization information, detecting a trigger condition to perform a transaction with a payment accepting unit associated with the payment module; and

in response to detecting the trigger condition, sending, to the payment module, at least a portion of the authorization information via the first communication capability.

14. The device of claim 13, wherein the first communication capability corresponds to a short-range communication protocol and the second communication capability corresponds to a long-range communication protocol.

15. The device of claim 13, wherein the one or more programs further comprise instructions for:

obtaining, from the payment module, advertised information indicating the payment module's presence via the first communication capability that at least includes authorization zone threshold criterion; and

after obtaining the advertised information, initiating a handshake process with the payment module, wherein the handshake process includes:

sending, to the payment module, device information at least including user identification information corresponding to the user of the device via the first communication capability; and

receiving, from the payment module, payment module information, wherein the payment module information at least includes an identifier corresponding to the payment module.

16. The device of claim 15, wherein the one or more programs further comprise instructions for:

prior to obtaining the authorization request:

in accordance with a determination that the authorization zone threshold criterion is satisfied, sending notification information to the payment module via the first communication capability, wherein the notification information indicates that the authorization zone threshold criterion is satisfied;

wherein the device obtains the authorization request in response to sending the notification information.

17. The device of claim 15, wherein the payment module information further includes an indication that hands-free mode is available and payment zone threshold criterion.

18. The device of claim 17, wherein the device information further includes device identification information corresponding to a model type of the device; and

wherein the payment zone threshold criterion is based at least in part on the device identification information.

19. The device of claim 17, wherein detecting the trigger condition comprises:

determining whether the payment zone threshold criterion is satisfied; and

in accordance with a determination that the payment zone threshold criterion is satisfied, detecting the trigger condition without interaction from a user of the device.

20. The device of claim 13, wherein detecting the trigger condition comprises:

detecting a user input from a user of the device; and

in response to detecting the user input, detecting the trigger condition to perform a transaction with the payment accepting unit.

21. A non-transitory computer readable storage medium storing one or more programs, the one or more programs comprising instructions, which, when executed by a device with one or more processors and two or more communication capabilities, cause the device to perform operations comprising:

obtaining, from a payment module, an authorization request via a first communication capability;

sending, to a server, the authorization request via a second communication capability distinct from the first communication capability;

in response to sending the authorization request, obtaining, from the server, authorization information via the second communication capability;

after obtaining the authorization information, detecting a trigger condition to perform a transaction with a payment accepting unit associated with the payment module; and

in response to detecting the trigger condition, sending, to the payment module, at least a portion of the authorization information via the first communication capability.

22. The non-transitory computer readable storage medium of claim 21, wherein the first communication capability corresponds to a short-range communication protocol and the second communication capability corresponds to a long-range communication protocol.

23. The non-transitory computer readable storage medium of claim 21, wherein the instructions cause the device to perform operations further comprising:

obtaining, from the payment module, advertised information indicating the payment module's presence via the first communication capability that at least includes authorization zone threshold criterion; and

after obtaining the advertised information, initiating a handshake process with the payment module, wherein the handshake process includes:

sending, to the payment module, device information at least including user identification information corresponding to the user of the device via the first communication capability; and

receiving, from the payment module, payment module information, wherein the payment module information at least includes an identifier corresponding to the payment module.

24. The non-transitory computer readable storage medium of claim 23, wherein the instructions cause the device to perform operations further comprising:

prior to obtaining the authorization request:

in accordance with a determination that the authorization zone threshold criterion is satisfied, sending notification information to the payment module via the first communication capability, wherein the notification information indicates that the authorization zone threshold criterion is satisfied;

wherein the device obtains the authorization request in response to sending the notification information.

25. The non-transitory computer readable storage medium of claim 23, wherein the payment module information further includes an indication that hands-free mode is available and payment zone threshold criterion.

26. The non-transitory computer readable storage medium of claim 25, wherein the device information further includes device identification information corresponding to a model type of the device; and

wherein the payment zone threshold criterion is based at least in part on the device identification information.

27. The non-transitory computer readable storage medium of claim 25, wherein detecting the trigger condition comprises:

determining whether the payment zone threshold criterion is satisfied; and

in accordance with a determination that the payment zone threshold criterion is satisfied, detecting the trigger condition without interaction from a user of the device.

28. The non-transitory computer readable storage medium of claim 21, wherein detecting the trigger condition comprises:

detecting a user input from a user of the device; and

in response to detecting the user input, detecting the trigger condition to perform a transaction with the payment accepting unit.

METHOD AND SYSTEM FOR PERFORMING MOBILE DEVICE-TO-MACHINE PAYMENTS

ABSTRACT OF THE DISCLOSURE

A device with one or more processors, memory, and two or more communication capabilities obtains, from a payment module, an authorization request via a first communication capability (e.g., Bluetooth). The device sends, to a server, the authorization request via a second communication capability distinct from the first communication capability (e.g., cellular or WiFi technology). In response to sending the authorization request, the device obtains, from the server, authorization information via the second communication capability. After obtaining the authorization information, the device detects a trigger condition to perform a transaction with a payment accepting unit associated with the payment module. In response to detecting the trigger condition, the device sends, to the payment module, at least a portion of the authorization information via the first communication capability.

Electronic Patent Application Fee Transmittal

Application Number:	14335762
Filing Date:	18-Jul-2014
Title of Invention:	Method and System for Performing Mobile Device-To-Machine Payments
First Named Inventor/Applicant Name:	Paresh K. Patel
Filer:	Douglas James Crisman/Sherri Ballbach
Attorney Docket Number:	104402-5002-US

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Late Filing Fee for Oath or Declaration	2051	1	70	70
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
			Total in USD ($)	**70**

Electronic Acknowledgement Receipt

EFS ID:	19966287
Application Number:	14335762
International Application Number:	
Confirmation Number:	6199
Title of Invention:	Method and System for Performing Mobile Device-To-Machine Payments
First Named Inventor/Applicant Name:	Paresh K. Patel
Customer Number:	24341
Filer:	Douglas James Crisman/Sherri Ballbach
Filer Authorized By:	Douglas James Crisman
Attorney Docket Number:	104402-5002-US
Receipt Date:	26-AUG-2014
Filing Date:	18-JUL-2014
Time Stamp:	13:35:33
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$70
RAM confirmation Number	10184
Deposit Account	500310
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

1	Applicant Response to Pre-Exam Formalities Notice	104402-5002-US_ResponseToNoticeOfMissingParts.pdf	1390448 8b5172954e714f75596aeb1b162ad858b4cc2200	no	117
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	29908 bb11d84d8c9d07fdc10d4b776780a00fe3a92e2b	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	1420356	

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.

<u>New Applications Under 35 U.S.C. 111</u>
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.

<u>National Stage of an International Application under 35 U.S.C. 371</u>
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.

<u>New International Application Filed with the USPTO as a Receiving Office</u>
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.

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE UNITED STATES PATENT AND TRADEMARK OFFICE

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

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(c).

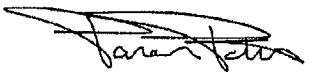
I hereby appoint the practitioners of Morgan, Lewis & Bockius LLP, Customer Number **24341** as attorneys or agents to represent the undersigned and to transact all business before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications and patents assigned only to the undersigned according to the USPTO assignment records or assignment documents attached to this form in accordance with 37 C.F.R. § 3.73(c), said appointment to be to the exclusion of the inventor(s) and their attorney(s) in accordance with the provisions of 37 C.F.R. § 3.71, provided that, if any one of these attorneys ceases being affiliated with the law firm of Morgan, Lewis & Bockius LLP as partner, counsel, or employee, then the appointment of that attorney and all powers derived therefrom shall terminate on the date such attorney ceases being so affiliated.

Assignee Name and Address:

PayRange Inc.
12815 NE Marx Street
Portland, Oregon 97230

SIGNATURE of Assignee of Record

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

Signature			
Name	Paresh K. Patel, PhD, MBA	Date	June 24, 2014
Title	CEO	Telephone	855-856-6398

A copy of this form, together with a statement under 37 C.F.R. § 3.73(c) (Form PTO/SB96 or equivalent) is required to be filed in each application in which this form is used. The statement under 37 C.F.R. § 3.73(c) may be completed by one of the practitioners appointed in this form if the appointed practitioner is authorized to act on behalf of the assignee and must identify the application in which this Power of Attorney is to be filed.

Electronic Acknowledgement Receipt

EFS ID:	19966394
Application Number:	14335762
International Application Number:	
Confirmation Number:	6199
Title of Invention:	Method and System for Performing Mobile Device-To-Machine Payments
First Named Inventor/Applicant Name:	Paresh K. Patel
Customer Number:	24341
Filer:	Douglas James Crisman/Sherri Ballbach
Filer Authorized By:	Douglas James Crisman
Attorney Docket Number:	104402-5002-US
Receipt Date:	26-AUG-2014
Filing Date:	18-JUL-2014
Time Stamp:	13:40:44
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		104402-5002-US_StatementUnder3_73WithPowerOfAttorney.pdf	82726 68c765f2262c0366e98b882cb3f932a655a4df9d	yes	2

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Assignee showing of ownership per 37 CFR 3.73.	1	1
	Power of Attorney	2	2
Warnings:			
Information:			
	Total Files Size (in bytes):	82726	

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.

Electronically filed: August 26, 2014

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application of:	Dr. Paresh K. Patel et al.	Confirmation No.:	6199
Application No.:	14/335,762	Art Unit	2876
Filed:	July 18, 2014	Examiner:	To be assigned
For:	Method and System for Performing Mobile Device-to-Machine Payments	Attorney Docket No.:	104402-5002-US

STATEMENT UNDER 37 C.F.R. § 3.73(c)

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

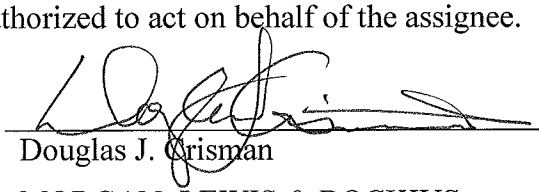
Sir:

PayRange Inc., a Corporation, states that it is the assignee of the entire right, title and interest in the patent application/patent identified above by virtue of 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 on August 14, 2014 at Reel 033538, Frame 0157, or for which a copy thereof is attached.

The undersigned is authorized to act on behalf of the assignee.

Date: August 26, 2014



39,951
Douglas J. Crisman (Reg. No.)

MORGAN, LEWIS & BOCKIUS LLP
2 Palo Alto Square
3000 El Camino Real, Suite 700
Palo Alto, CA 94306
(650) 843-4000

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	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/335,762	07/18/2014	Paresh K. Patel	104402-5002-US

CONFIRMATION NO. 6199

24341
MORGAN, LEWIS & BOCKIUS LLP (PA)
2 PALO ALTO SQUARE
3000 EL CAMINO REAL, SUITE 700
PALO ALTO, CA 94306

FORMALITIES LETTER

OC000000070439925

Date Mailed: 09/02/2014

NOTICE OF INCOMPLETE REPLY (NONPROVISIONAL)

Filing Date Granted

The U.S. Patent and Trademark Office has received your reply on 08/26/2014 to the Notice to File Missing Parts (Notice) mailed 07/31/2014 and it has been entered into the nonprovisional application. The reply, however, does not include the following items required in the Notice. A complete reply must be timely filed to prevent ABANDONMENT of the above-identified application. Replies should be mailed to: Mail Stop Missing Parts, Commissioner for Patents, P.O. Box 1450, Alexandria VA 22313-1450.

Applicant is given **TWO MONTHS** from the date of the Notice to File Missing Parts (Notice) mailed 07/31/2014 within which to file all required items and pay any fees required below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

Items Required to Avoid Abandonment:

The required items noted below SHOULD be filed along with any items required above. The filing date of this nonprovisional application will be the date of receipt of the items required above.

The application is informal since it does not comply with the regulations for the reason(s) indicated below.

The required item(s) identified below must be timely submitted to avoid abandonment:

- Applicant did not provide a statement that the substitute specification contains no new matter.

Applicant is cautioned that correction of the above items may cause the specification and drawings page count to exceed 100 pages. If the specification and drawings exceed 100 pages, applicant will need to submit the required application size fee.

Replies must be received in the USPTO within the set time period or must include a proper Certificate of Mailing or Transmission under 37 CFR 1.8 with a mailing or transmission date within the set time period. For more information and a suggested format, see Form PTO/SB/92 and MPEP 512.

Replies should be mailed to:

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web, including a copy of this Notice and selecting the document description "Applicant response to Pre-Exam Formalities Notice". https://sportal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html

For more information about EFS-Web please call the USPTO Electronic Business Center at **1-866-217-9197** or visit our website at http://www.uspto.gov/ebc.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

/ytbedada/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 14/335,762

APPLICATION AS FILED - PART I

	(Column 1)		(Column 2)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED		NUMBER EXTRA	RATE($)	FEE($)		RATE($)	FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A		N/A	N/A	70		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A		N/A	N/A	300		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A		N/A	N/A	360		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	28	minus 20 =	* 8	x 40 =	320	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3	minus 3 =	*	x 210 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).				0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))					0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL	1050		TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1)		(Column 2)	(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1)		(Column 2)	(Column 3)					
		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

Electronically filed: September 24, 2014

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application of:	Paresh K. Patel et al.	Confirmation No.:	6199
Serial No.:	14/335,762	Art Unit:	2876
Filed:	July 18, 2014	Examiner:	To Be Assigned
For:	*Method and System for Performing Mobile Device-To-Machine Payments*	Attorney Docket No:	104402-5002-US

RESPONSE TO THE NOTICE OF INCOMPLETE REPLY

Mail Stop: MISSING PARTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

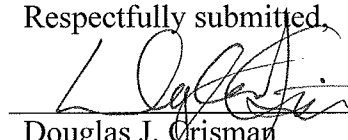
Sir:

In Response to the Notice of Incomplete Reply mailed August 21, 2014, enclosed is the Substitute Specification with Markings as well as a clean version of the Specification. No new matter has been added.

No fee is believed due at this time, but the Commissioner is hereby authorized to charge the required fees or credit any overpayments to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no. 104402-5002-US).

Respectfully submitted,

Date: September 24, 2014



39,951
Douglas J. Crisman (Reg. No.)
MORGAN, LEWIS & BOCKIUS LLP
2 Palo Alto Square
3000 El Camino Real, Suite 700
Palo Alto, CA 94306
(650) 843-4000

METHOD AND SYSTEM FOR PERFORMING MOBILE DEVICE-TO-MACHINE PAYMENTS

PRIORITY CLAIM

[0001] The present application is an continuation of U.S. Patent Application Number 14/214,644, filed March 14, 2014, which claims priority to U.S. Provisional Patent Application Number 61/917,936, filed December 18, 2013, and is a continuation-in-part of U.S. Design Patent Application Number 29/477,025, filed December 18, 2013. The present application is based on and claims priority from these applications, the disclosures of which are hereby expressly incorporated herein by reference.

BACKGROUND OF THE INVENTION

[0002] Disclosed herein are mobile-device-to-machine payment systems and, more specifically, mobile-device-to-machine payment systems over a non-persistent network connection and featuring hands-free and manual modes.

[0003] Vending machines (or "automatic retailing" machines), in the broadest sense, have been around for thousands of years. The first simple mechanical coin operated vending machines were introduced in the 1880s. Modern vending machines stock many different types of products including, but not limited to drinks (e.g. water, juice, coffee, and soda) and edible food products/items (e.g. snacks, candy, fruit, and frozen meals), as well as a wide variety of non-food items. In this fast paced world, vending machines are ubiquitous.

[0004] Vending machines are one type of "payment accepting unit" (payment accepting units are also referred to herein generically as "machines"). A payment accepting unit (or machine) is equipment that requires payment for the dispensing of products and/or services. In addition to vending machines, payment accepting units can also be other machines that require payment for the dispensing of a product and/or services including, but not limited to parking meters, toll booths, laundromat washers and dryers, arcade games, kiosks, photo booths, toll booths, transit ticket dispensing machines, and other known or yet to be discovered payment accepting units.

[0005] In using a payment accepting unit, a user will (1) approach the payment accepting unit, (2) determine from the face of the payment accepting unit the product (or service) he desires, (3) insert payment (e.g. coins, bills, or payment cards), and (4) input his

selection into the payment accepting unit using a user interface (e.g. a series of buttons, a key pad, touch screen, or other input mechanism using, for example, the column and row at which a product is located). Based on the user's inputted selection, technology within the payment accepting unit provides the desired product (or service) to the user.

[0006] As the number of people with internet-connected mobile devices proliferates, so does the variety of uses for such devices. Mobile payment is a logical extension.

[0007] There is a large development effort around bringing mobile payment to the retail sector in an effort to not only provide options to the user, but also increased convenience.

[0008] In recent years, many improvements to modern vending machines have been suggested. Many of the innovations relate to means for communicating with the vending machine. Some of these communication innovations are detailed in U.S. Patent No. 6,584,309 to Whigham (the "Whigham reference"), U.S. Patent No. 7,085,556 to Offer (the "Offer reference"), U.S. Patent No. 7,127,236 to Khan et al. (the "Khan reference"), U.S. Patent No. 7,721,958 to Belfer et al. (the "Belfer reference"), U.S. Patent No. 8,396,589 to Katzenstein Garibaldi et al. (the "Garibaldi reference"), U.S. Patent No. 8,489,140 to Weiner et al. (the "Weiner reference"), and International Publication No. WO/2008/083025 to Carlson (the "Carlson reference").

[0009] The Whigham reference is directed to a system and method for purchasing a product from an automatic vending machine by means of a consumer's cellular telephone. The consumer requests a product available from the vending machine by dialing a specified telephone number that connects the consumer's cellular telephone to a server operated by a billing agency. The server recognizes the request for the product, creates a transaction record, and communicates a vend code to the consumer. Upon receiving the vend code from the server, the consumer transmits the vend code to the vending machine. The vend code may be an RF code, an audible tone code, or a manual code. Upon receipt of the vend code from the consumer, the vending machine dispenses the requested product.

[0010] The Offer reference is directed to a vending machine that is designed to communicate with a cellular phone such that it dispenses a product when it receives information indicating that the product has been selected. The Offer reference teaches permitting the cashless utilization of a vending machines via a communications service, such as a cellular telephone. A response to a signal from the cellular telephone from

[0011] the vending machine that indicates that a connection has been established between the vending machine and the cellular phone may be a visual indication that is displayed on the cellular telephone. The vending machine outputs the cost of the product and that cost is debited from an account to pay for the product.

[0012] The Khan reference describes a point of sale MicroAdapter device that enables payment transactions to be effected through a purchaser's personal trusted device (e.g. the user selecting the micropayment application on his personal trusted device and confirming or cancelling the purchase thereon) without relying upon tokens or prepayment cards. In one embodiment, the MicroAdapter includes a transceiver configured to receive a purchase signal from the personal trusted device including order and payment information. In response, the MicroAdapter communicates via wireless telephony with a transaction authorizer to receive authorization for effectuating the purchase transaction. The MicroAdapter can effectuate micropayment transactions authorized by a Billing On Behalf of Others program administered through a wireless carrier/ISP or third party.

[0013] The Belfer reference is directed to a system wherein a vending machine has an audio code collector and a code validator that is adapted to receive audio tones from a mobile device. The audio tones include authentication codes and dispense codes to control dispensing of product from the vending machine. To start the transaction, the consumer dials a unique set of symbols and digits to route the call to a verification server. The symbols and digits may correspond to a unique vending machine identification number and product identification numbers.

[0014] The Garibaldi reference is directed to an electronic device for the sale of intangible products through vending machines that include interfaces to communicate with external peripherals through the MDB protocol, the RS232 standard, and the DEX protocol, an interface to communicate with users, a communications system that enables it to act as part of a network and communicate with a central system, and a controller, that articulates the communication among the above-mentioned components, so as to enable a central system to perform diverse actions on a vending machine.

[0015] The Weiner reference is directed to a system and method for providing product or service with a cellular telephone. The problem identified in the Weiner reference is that mobile communication devices are long-range electronic devices designed to be used for long-range communications. Eschewing the use of near- field communication because it

requires special design or modification of the mobile station (e.g. the vending machine), the Weiner reference teaches a mobile communication device identifier, consisting of: a shielding defining a coverage area, the shielding arranged to reduce radio signals originating externally of the coverage area to be less than a pre-determined signal strength; an antenna associated within the defined coverage area; a transceiver coupled to the antenna, the transceiver communicating with a mobile station inserted within the defined coverage area utilizing a signal strength greater than the pre-determined signal strength; and a service control unit responsive to the transceiver, the service control unit responsive to the communication to output a signal indicative of an authorization to provide a product or service.

[0016] The Carlson reference is directed to a system and a method for using a portable consumer device such as a mobile phone for payments and the like. One embodiment of the Carlson system is directed to a method that includes the steps of receiving a payment request message (that includes a request to pay for a product from a vending machine) from a portable consumer device operated by a consumer, sending an authorization response message back to the vending machine wherein the vending machine subsequently prompts the consumer to enter a selection if the authorization response message indicates that the consumer is authorized to make a purchase, and receiving an acknowledgement message from the vending machine that the product was purchased. The step of "sending an authorization response message back to the vending machine" is performed by a remote payment server and would require a persistent network connection.

BRIEF SUMMARY OF THE INVENTION

[0017] Disclosed herein are mobile-device-to-machine payment systems and, more specifically, mobile-device-to-machine payment systems over a non-persistent network connection and featuring hands-free and manual modes.

[0018] Described herein is a mobile-device-to-machine payment system for facilitating a cashless transaction for purchase of at least one product or service by a user from a payment accepting unit that preferably has input mechanisms. The user has a mobile device that has both short-range communication technology and long-range communication technology. The payment accepting unit is capable of dispensing at least one product or service. The system includes an adapter module and a server. The adapter module is associated with the payment accepting unit and has short-range communication technology

for communicating with the short-range communication technology of the mobile device. The server has long-range communication technology for communicating with the long-range communication technology of the mobile device. The adapter module is for sending an authorization request for funds to the mobile device using short-range communication technology. The mobile device then forwards the authorization request for funds to the server using long-range communication technology. The server is for sending an authorization grant for funds to the mobile device using long-range communication technology. The mobile device the forwards the authorization grant for funds to the adapter module using short-range communication technology. The payment accepting unit dispenses the at least one product or service in response to receiving user input to the payment accepting unit input mechanism if the adapter module has received the authorization grant.

[0019] The adapter module may have security technology and the server may have security technology. The authorization request may be secured by the adapter module security technology to create a secured authorization request. The authorization grant may be secured by the server security technology to create a secured authorization grant. The secured authorization request and the secured authorization grant are preferably undecipherable to the mobile device.

[0020] The adapter module and the server may share a unique private key. The adapter module may have encryption/decryption technology and the server may have encryption/decryption technology. The authorization request may be encrypted by the adapter module encryption/decryption technology using the unique private key to create an encrypted authorization request. The encrypted authorization request may be decrypted by the server encryption/decryption technology using the unique private key. The authorization grant may be encrypted by the server encryption/decryption technology using the unique private key to create an encrypted authorization grant. The encrypted authorization grant may be decrypted by the adapter module encryption/decryption technology using the unique private key. The encrypted authorization request and the encrypted authorization grant are preferably undecipherable to the mobile device.

[0021] The adapter module is preferably surrounded by two zones, a payment zone and an authorization zone, wherein the payment zone is within the authorization zone. The adapter module sends the authorization request when the mobile device is within the authorization zone. The mobile device forwards the authorization grant for funds to the adapter module when the mobile device is within the payment zone. A third zone possible

zone is a communication zone, the authorization zone being within the communication zone. The mobile device preferably receives advertising broadcast signals from the adapter module within the communication zone.

[0022] The system may have a hands-free mode in which the payment accepting unit dispenses the at least one product or service without the user interacting with the mobile device. A display of the payment accepting unit may be used for displaying funds available based on information from the authorization grant. The input mechanisms of the payment accepting unit may be used for receiving user selection input when the user interacts with the input mechanisms to select the at least one product or service to be dispensed.

[0023] The adapter module may be an in-line dongle for in-line insertion within a multi-drop bus of the payment accepting unit. Further, the payment accepting unit may have a multi-drop bus to a payment receiving mechanism. The multi-drop bus may have a male adapter and a female adapter. The adapter module may have a male adapter and a female adapter. The adapter module is preferably insertable in serial with the multi-drop bus by connecting the male adapter of the adapter module to the female adapter of the multi-drop bus and by connecting the female adapter of the adapter module to the male adapter of the multi-drop bus.

[0024] Also described herein is a method for using a mobile-device-to-machine payment system for facilitating a cashless transaction for purchase of at least one product or service by a user from a payment accepting unit may have input mechanisms. The user may have a mobile device having both short-range communication technology and long-range communication technology. The payment accepting unit is preferably capable of dispensing at least one product or service. The method includes the steps of: (a) sending an authorization request for funds to the mobile device using short-range communication technology of an adapter module associated with the payment accepting unit; (b) receiving the authorization request for funds from the short-range communication technology of the adapter module at the short-range communication technology of the mobile device; (c) forwarding the authorization request for funds to a server using the long-range communication technology of the mobile device; (d) receiving the authorization request for funds from the long-range communication technology of the mobile device at long-range communication technology of the server; (e) sending an authorization grant for funds to the mobile device using the long-range communication technology of the server; (f) receiving the authorization grant for funds from long-range communication technology of the server at the

long-range communication technology of the mobile device; (g) forwarding the authorization grant for funds to the adapter module using the short-range communication technology of the mobile device; and (h) receiving the authorization grant for funds from the short-range communication technology of the mobile device at short-range communication technology of the adapter module. At least one product or service may then be dispensed from the payment accepting unit in response to receiving user input to the payment accepting unit input mechanism if the adapter module has received the authorization grant.

[0025] The method may include the steps of securing the authorization request using security technology associated with the adapter module to create a secured authorization request, securing the authorization grant using security technology associated with the server to create a secured authorization grant, and the secured authorization request and the secured authorization grant are preferably undecipherable to the mobile device.

[0026] The method may include the steps of (a) sharing a unique private key between the adapter module and the server, (b) encrypting using the unique private key the authorization request using encryption/decryption technology associated with the adapter module to create an encrypted authorization request, (c) decrypting using the unique private key the encrypted authorization request using encryption/decryption technology associated with the server, (d) encrypting using the unique private key the authorization grant using the encryption/decryption technology associated with the server to create an encrypted authorization grant, (e) decrypting using the unique private key the encrypted authorization grant using encryption/decryption technology associated with the adapter module, and (e) the encrypted authorization request and the encrypted authorization grant are preferably undecipherable to the mobile device.

[0027] The method may include the steps of (a) surrounding the adapter module with two zones, a payment zone and an authorization zone, wherein the payment zone is within the authorization zone, (b) the adapter module sending the authorization request when the mobile device is within the authorization zone; and (c) the mobile device forwarding the authorization grant for funds to the adapter module when the mobile device is within the payment zone. The adapter module may also include a third zone, a communication zone, wherein the authorization zone is within the communication zone. The mobile device receives advertising broadcast signals from the adapter module within the communication zone.

[0028] The method may have a hands-free mode in which the payment accepting unit dispenses the at least one product or service without the user interacting with the mobile device. The method may further include the steps of (a) displaying funds available on a display of the payment accepting unit, the funds available may be based on information from the authorization grant; and (b) receiving user selection input when the user interacts with input mechanisms of the payment accepting unit to select the at least one product or service to be dispensed.

[0029] The method may include the step of inserting the adapter module as an in-line dongle for in-line insertion within a multi-drop bus of the payment accepting unit. The method may include the step of inserting the adapter module in serial with the multi-drop bus by connecting a male adapter of the adapter module to a female adapter of the multi-drop bus and by connecting a female adapter of the adapter module to a male adapter of the multi-drop bus.

[0030] The subject matter described herein is particularly pointed out and distinctly claimed in the concluding portion of this specification. Objectives, features, combinations, and advantages described and implied herein will be more readily understood upon consideration of the following detailed description of the invention, taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

[0031] FIG. 1 is a schematic diagram that shows three zones: a first "communication zone" (e.g. "Bluetooth range"), a second "authorization zone," and a third "payment zone." The payment zone (that can't be zero) is smaller than or equal to (overlapping completely) the authorization zone.

[0032] FIG. 2 is a schematic diagram that shows the three zone of FIG. 1 with multiple users therein, the mobile-device-to-machine payment systems providing for managing and resolving multiple users.

[0033] FIG. 3 is a table that illustrates the hands-free credit or alert user principle.

[0034] FIG. 4 is a flow chart showing the logging RSSI at User Input.

[0035] FIG. 5 is a block schematic that shows elements of the system including, but not limited to, the adapter module, the machine, the mobile device, and exemplary servers, as well as communications therebetween.

[0036] FIG. 6 is a block schematic that shows there are three areas of encryption used (each is bi-directional) between the adapter module, the machine, the mobile device, and/or exemplary servers.

[0037] FIG. 7 is a block diagram that communications, messaging, vending sequence, and purchase flow between the adapter module, the mobile device, and a system management server.

[0038] FIG. 8A is a timing schematic diagram that shows additional elements and features of the system including, but not limited to, communications medium, messaging, vending sequence, and purchase flow, when the user enters the communication zone (Bluetooth Range).

[0039] FIG. 8B is a timing schematic diagram that shows additional elements and features of the system including, but not limited to, communications medium, messaging, vending sequence, and purchase flow, when the user enters the Authorization Zone.

[0040] FIG. 8C is a timing schematic diagram that shows additional elements and features of the system including, but not limited to, communications medium, messaging, vending sequence, and purchase flow, when the user enters the Payment Zone and, in particular, detailing the hands-free mode alternative and the swipe mode alternative.

[0041] FIG. 8D is a timing schematic diagram that shows additional elements and features of the system including, but not limited to, communications medium, messaging, vending sequence, and purchase flow, in a vending transaction including a loop for multiple transactions.

[0042] FIG. 8E is a timing schematic diagram that shows additional elements and features of the system including, but not limited to, communications medium, messaging, vending sequence, and purchase flow, in the Login mode.

[0043] FIG. 8F is a timing schematic diagram that shows additional elements and features of the system including, but not limited to, communications medium, messaging, vending sequence, and purchase flow, during Module bootup.

[0044] FIG. 8G is a timing schematic diagram that shows additional elements and features of the system including, but not limited to, communications medium, messaging, vending sequence, and purchase flow, during Account Check/Update.

[0045] FIGS. 9A - 9E are flow charts that show exemplary steps and features of the system including, but not limited to, communications, messaging, vending sequence, and purchase flow.

[0046] FIGS. 10A - 10D show an exemplary mobile device with a graphical representation of an exemplary mobile application shown thereon, the mobile application being used as part of the mobile-device-to-machine payment systems.

[0047] FIG. 11 is a perspective view of the exemplary first preferred in-line dongle adapter module.

[0048] FIG. 12 is a front plan view of the in-line dongle adapter module of FIG. 11.

[0049] FIG. 13 is a back plan view of the in-line dongle adapter module of FIG. 11.

[0049.1] FIG. 14 is a side view of the in-line dongle adapter module of FIG. 11 in accordance with some implementations.

[0050] FIG. 15 is a first end view of a connector receptacle of the in-line dongle adapter module of FIG. 11.

[0051] FIG. 16 is a second end view of a connector receptacle of the in-line dongle adapter module of FIG 11.

[0052] FIG. 17 is a perspective view taken from the first end of the in-line dongle adapter module of FIG. 11, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for environmental purposes.

[0053] FIG. 18 is a perspective view taken from the second end of the in-line dongle adapter module of FIG. 11, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for environmental purposes.

[0054] FIG. 19 is a perspective view of the in-line dongle adapter module of FIG. 11 within a vending machine.

[0055] FIG. 20 is a perspective view of the exemplary second preferred in-line dongle adapter module.

[0056] FIG. 21 is a front plan view of the in-line dongle adapter module of FIG. 20.

[0057] FIG. 22 is a back plan view of the in-line dongle adapter module of FIG. 20.

[0058] FIG. 23 is a first side view of the in-line dongle adapter module of FIG. 20, the second side being a mirror image of that shown.

[0059] FIG. 24 is a first end view of a connector receptacle of the in-line dongle adapter module of FIG. 20.

[0060] FIG. 25 is a second end view of a connector receptacle of the in-line dongle adapter module of FIG 20.

[0061] FIG. 26 is a perspective view taken from the first end of the in-line dongle adapter module of FIG. 20, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for environmental purposes.

[0062] FIG. 27 is a perspective view taken from the second end of the in-line dongle adapter module of FIG. 20, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for environmental purposes.

[0063] FIG. 28 is a perspective view of the in-line dongle adapter module of FIG. 20 within a vending machine.

[0064] FIG. 29 is a perspective view of the exemplary third preferred in-line dongle adapter module with a gap indicating the in-line dongle adapter module can be of any length.

[0065] FIG. 30 is a front plan view of the in-line dongle adapter module of FIG. 29.

[0066] FIG. 31 is a back plan view of the in-line dongle adapter module of FIG. 29.

[0067] FIG. 32 is a first side view of the in-line dongle adapter module of FIG. 29, the second side being a mirror image of that shown.

[0068] FIG. 33 is a first end view of a connector receptacle of the in-line dongle adapter module of FIG. 29.

[0069] FIG. 34 is a second end view of a connector receptacle of the in-line dongle adapter module of FIG. 29.

[0070] FIG. 35 is a perspective view taken from the first end of the in-line dongle adapter module of FIG. 29, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for environmental purposes.

[0071] FIG. 36 is a perspective view taken from the second end of the in-line dongle adapter module of FIG. 29, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for environmental purposes.

[0072] FIG. 37 is a perspective view of the in-line dongle adapter module of FIG. 29 within a vending machine.

[0073] FIG. 38 is a perspective view of the exemplary fourth preferred in-line dongle adapter module with two vertical gaps indicating the in-line dongle adapter module can be of any width.

[0074] FIG. 39 is a front plan view of the in-line dongle adapter module of FIG. 38.

[0075] FIG. 40 is a back plan view of the in-line dongle adapter module of FIG. 38.

[0076] FIG. 41 is a first side view of the in-line dongle adapter module of FIG. 38, the second side being a mirror image of that shown.

[0077] FIG. 42 is a first end view of a connector receptacle of the in-line dongle adapter module of FIG. 38.

[0078] FIG. 43 is a second end view of a connector receptacle of the in-line dongle adapter module of FIG 38.

[0079] FIG. 44 is a perspective view taken from the first end of the in-line dongle adapter module of FIG. 38, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for environmental purposes.

[0080] FIG. 45 is a perspective view taken from the second end of the in-line dongle adapter module of FIG. 38, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for environmental purposes.

[0081] FIG. 46 is a perspective view of the in-line dongle adapter module of FIG. 38 within a vending machine.

[0082] FIG. 47 is a perspective view of the exemplary fifth preferred in-line dongle adapter module and, specifically, the longitudinal center portion thereof, the dashed line depiction of the sides indicating the sides of the in-line dongle adapter module can be of any shape or curvature.

[0083] FIG. 48 is a front plan view of the in-line dongle adapter module of FIG. 47.

[0084] FIG. 49 is a back plan view of the in-line dongle adapter module of FIG. 47.

[0084.1] FIG. 50 is a side view of the in-line dongle adapter module of FIG. 47 in accordance with some implementations.

[0085] FIG. 51 is a first end view of a connector receptacle of the in-line dongle adapter module of FIG. 47.

[0086] FIG. 52 is a second end view of a connector receptacle of the in-line dongle adapter module of FIG 47.

[0087] FIG. 53 is a perspective view taken from the first end of the in-line dongle adapter module of FIG. 47, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for environmental purposes.

[0088] FIG. 54 is a perspective view taken from the second end of the in-line dongle adapter module of FIG. 47, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for environmental purposes.

[0089] FIG. 55 is a perspective view of the in-line dongle adapter module of FIG. 47 within a vending machine.

[0090] FIG. 56 is a block diagram of an exemplary adapter module.

[0091] FIG. 57 is a block diagram of an exemplary mobile device.

[0092] FIG. 58 is a block diagram of an exemplary server.

DETAILED DESCRIPTION OF THE INVENTION

[0093] Disclosed herein are mobile-device-to-machine payment systems and, more specifically, mobile-device-to-machine payment systems over a non-persistent network connection. The mobile-device-to-machine payment systems disclosed herein focus on the unattended retail space (e.g. a payment accepting unit 120 or machine 120). More specifically, mobile-device-to-machine payment systems disclosed herein allow a user (having a mobile device 150 with a mobile application 140 thereon) to make a cashless purchase from a payment accepting unit 120 (having an adapter module 100 associated therewith).

[0094] The mobile-device-to-machine payment systems described herein can be implemented with one or more of the following features: easy installation feature, a non-persistent network connection feature; a manual (swipe to pay) mode feature; a hands-free mode feature; and a multiple vending transactions (multi-vend) feature.

[0095] Easy Installation: Installation is very easy, requires no tools, requires no configuration, and takes as little as 30 seconds. This is accomplished by using an adapter

module 100 such as an in-line dongle (a hardware device with software thereon) design for in-line insertion within a multi-drop bus (MDB) of a payment accepting unit (e.g. a vending machine). Installation is as simple as "powering down" (turning off) the machine 120, identifying the "wire" that connects with a payment receiving mechanism (e.g. the coin mechanism), disconnecting the wire (so that there are two loose ends, such as a male connection end or adapter of an MDB and a female connection end or adapter of an MDB), plugging (inserting) the adapter module 100 in serial ("in-line") with the wire (for example, connecting the MDB female adapter to a male adapter of the adapter module 100 and connecting the MDB male adapter to a female adapter of the adapter module 100), tucking the wire and the installed adapter module 100 back into position, and "powering up" (turning on) the machine 120. Most vending machines made since 1995 have this industry standard MDB technology that would allow this easy 30-second installation. On machines without MDB technology, the adapter module 100 can be configured or designed to work with other serial protocols or activate a switch. In essence the adapter module 100 simulates establishing payment on payment accepting unit 120 in much the same manner as other alternative forms of payment (e.g. cash).

[0096] Non-persistent Network Connection: Although payment accepting units (or "machines") that accept only cash (e.g. paper currency and coins) may not require a connection (persistent or non-persistent) to a network, traditional payment accepting units that accept cashless payments (e.g. credit cards, debit cards, and alternative mobile device payment methods using, for example, smart phones) require a persistent connection to a network (wired or wireless) to facilitate the cashless payments. In other words, without a persistent (ongoing or accessible on demand) network connection, traditional payment accepting units cannot accept cashless payments. Most traditional payment accepting units that accept cashless payments include the technology to accomplish this persistent network connection that allows them to connect to a remote server. If the network connection to a traditional machine is temporarily interrupted, cashless payments will be temporarily unavailable. If the machine is located in a location where no signal is available, cashless payments will not be possible. The Whigham reference, the Offer reference, and the Belfer reference disclose alternative payment accepting units that accept cashless payments by using the user's cellular phone to allow the user to manually input coding to a remote server and, thereby act as an on-demand bridge network connection. These references, however, require significant user interaction with the cellular telephone to effectuate the transaction. In

addition to using a mobile device 150 as an intermediary between the payment accepting units 120 and the server 130, mobile-device-to-machine payment systems described herein minimize (manual mode) or eliminate (hands-free mode) user interaction with the mobile device 150. Further, some mobile-device-to-machine payment systems described herein facilitate the acceptance of cashless payments without requiring any network connection near the payment accepting unit 120. Mobile-device-to-machine payment systems described herein that are located in a remote location where no signal is available, therefore, can accept cashless payments.

[0097] Manual (Swipe to Pay) Mode: Using a "swipe to pay" feature (or just "swipe") refers to a user's action implemented on his mobile device 150 in which he quickly brushes his finger (or other pre-determined interaction) on the mobile device's touch screen 152 (or other input device associated with the mobile device 150). From the user's perspective, when the user is within range, a pre-installed mobile application 140 automatically connects to the payment accepting unit 120 (e.g. a vending machine). The mobile application 140 might display (on the touch screen 152) a prepaid balance that the user "swipes" to transfer payment to the payment accepting unit 120. The user could observe the transferred funds on the touch screen 152 of the mobile device 150 and/or on the display 122, 124 of the payment accepting unit 120. The transaction is completed just as if cash was inserted in the machine 120 with the user inputting his selection on the payment accepting unit 120 and the payment accepting unit 120 dispensing the product or service. After the selection is made, the change is returned to the mobile device 150 and this may be shown on the touch screen 152 of the mobile device 150.

[0098] Hands-Free Mode: A "hands-free pay" feature (or just "hands-free") would most likely be used with "favorite" payment accepting units 120 (e.g. a vending machine at work or school). From the user's perspective, he would approach the favorite payment accepting unit 120 and notice that the display 122, 124 of the payment accepting unit 120 showed funds available, he would select the product or service using the payment accepting unit's input mechanisms (e.g. buttons 126 or a touch screen display 124 shown in FIG. 19), and he would retrieve his dispensed services or products. It would be that simple. More specifically, when the user is within range, a pre-installed mobile application 140 automatically connects to the payment accepting unit 120 (e.g. a vending machine). The user may leave the mobile device 150 in a pocket, purse, briefcase, backpack, or other carrier. As the user approaches the payment accepting unit 120 and is in approximately "arms-length"

distance (e.g. 3 to 5 feet), the user could observe the transferred funds on the display 122, 124 of the payment accepting unit 120. The transaction is completed just as if cash was inserted in the machine 120 with the user inputting his selection on the payment accepting unit 120 and the payment accepting unit 120 dispensing the product or service. After the selection is made, the change is returned to the mobile device 150. FIG. 3 details when the hands-free mode would be available.

[0099] Multiple Vending Transactions (Multi-Vend): Both the "swipe to pay" feature and the "hands-free pay" feature could be used multiple times in sequence (implemented, for example, as a loop) so that a user may make multiple purchases. After making his first selection and receiving his product (or service), the user would observe that additional funds were available on the display 122, 124 on the payment accepting unit 120. He could make another selection (or multiple selections) and receive additional product(s) (or service(s)). More specifically, the display 122, 124 may reset as if the transaction is complete, but then, because the user is still standing in range, the mobile application 140 would send another credit to the payment accepting unit 120, allowing for a second purchase. When the walks away, the system clears (e.g. returns unused funds to the mobile application 140 on the mobile device 150.

[00100] The features described above, alone or in combination with other features described herein will revolutionize the hundred billion dollar automated retail industry. The exemplary hardware is very low cost and there are no reoccurring fees because no cellular connection is required on the machine 120. Using the mobile-device-to-machine payment systems described herein, operators can increase frequency of visits and items sold with each visit.

[00101] Mobile-device-to-machine payment systems described herein may be implemented as an apparatus and/or method for enabling payments to a machine 120 via a mobile device 150. Exemplary mobile-device-to-machine payment systems may be better understood with reference to the drawings, but the shown mobile-device-to-machine payment systems are not intended to be of a limiting nature.

Definitions

[00102] Before describing the mobile-device-to-machine payment systems and the figures, some of the terminology should be clarified. Please note that the terms and phrases may have additional definitions and/or examples throughout the specification. Where

otherwise not specifically defined, words, phrases, and acronyms are given their ordinary meaning in the art. The following paragraphs provide some of the definitions for terms and phrases used herein.

- Adapter Module 100: As shown in FIGS. 1 and 2, the adapter module 100 is a physical device that is installed in a machine 120 (a payment accepting unit 120). The shown exemplary adapter module 100 is an in-line dongle (a hardware device with software thereon) device that may be inserted in-line within a multi-drop bus (MDB) of a machine 120. The adapter module 100 bridges the communication between the machine 120 and a mobile device 150. Although described as a unique component, it should be noted that the adapter module 100 could be implemented as a plurality of devices or integrated into other devices (e.g. components of a machine 120). In its unique component form, the adapter module 100 can be easily inserted into a machine 120 so that the machine 120 is able to perform new features with the assistance of the adapter module 100. FIG. 56 shows exemplary components associated with the adapter module 100. The shown example may be divided into multiple distinct components that are associated with each other or the example may be incorporated into or drawn from other technology (e.g. a computer or a payment accepting unit) as long as the components are associated with each other.

- Mobile Device 150 and Application 140 (also referred to as a "mobile application," "mobile app," or "app"): In general, a mobile device 150 may be a user's personal mobile device 150. The mobile device 150 (with a mobile application 140 thereon) acts as a communication bridge between the adapter module 100 (associated with a payment accepting unit 120) and the server 130. The mobile device 150 and application 140, however, are not "trusted" in that the communications (transmissions) it passes are encrypted. Encrypted (secured) communications are undecipherable (unencryptable, unreadable, and/or unuseable) by the mobile device 150. This keeps the passed communications secured and safe from hacking. Exemplary mobile devices include, but are not limited to smart phones, tablet or laptop computers, or personal digital assistants (PDAs), smart cards, or other technology (e.g. a hardware-software combination) known or yet to be discovered that has

structure and/or capabilities similar to the mobile devices described herein. The mobile device 150 preferably has an application 140 (app 140) running on it. The term "app" is used broadly to include any software program(s) capable of implementing the features described herein. FIGS. 10A-10D show exemplary mobile devices 150 with associated apps 140 associated therewith. It should be noted that the phrase "mobile device" can be assumed to include the relevant app unless specifically stated otherwise. Similarly, it should be noted that an "app" can be assumed to be running on an associated mobile device unless specifically stated otherwise. FIG. 57 shows exemplary components associated with the mobile device 150. The shown example may be divided into multiple distinct components that are associated with each other or the example may be incorporated into or drawn from other technology (e.g. the cell phone itself) as long as the components are associated with each other.

- Payment Accepting Unit 120 (or Machine 120): A payment accepting unit 120 (or machine 120) is equipment that requires payment for the dispensing of an product and/or service. Payment accepting units 120 may be vending machines, parking meters, toll booths, laundromat washers and dryers, arcade games, kiosks, photo booths, toll booths, transit ticket dispensing machines, and other known or yet to be discovered payment accepting units 120. Some payment accepting units 120 can accept cashless payments (payments other than cash (paper currency and coins)) by accepting payment from, for example, credit cards, debit cards, and mobile devices.
- Network Connections: For purposes of this discussion, a persistent network connection is a wired or wireless communications connection that is ongoing (e.g. a dedicated connection, a dedicated online connection, and/or a hardwired connection) or accessible on demand (e.g. the ability for the machine to make a temporary connection to a server or the ability for the user to contact a server from his mobile device). Typically the persistent network connection has been conducted over "long-range communication technology" (e.g. hardwired, telephone network technology, cellular technology, WiFi technology, wide area network (WAN), local area network (LAN), or any wired or wireless communication technology over the internet that is known or

yet to be discovered). Traditionally, machines that accept payment other than cash require a persistent (ongoing or accessible on demand) connection to a network to facilitate payment. This is true for machines that accept, for example, credit cards and debit cards. The payment accepting units 120 described herein do not require a traditional persistent network connection. The user's mobile device 150 acts as a communication bridge between the adapter module 100 and the server 130. Communications between user mobile devices 150 and the servers (e.g. a system management server 130 and/or a funding source server 160) take place using long-range communication technology. Communications between user mobile devices 150 and the adapter module 100 of the payment accepting unit 120 take place using "short-range communication technology" (e.g. Bluetooth (e.g. Bluetooth 4.0, Bluetooth Smart, Bluetooth LE (Low Energy), near-field communication, Ultra Wideband (UWB), RFID, infrared wireless, induction wireless, or any wired or wireless technology that could be used to communicate a small distance (e.g. approximately a hundred feet or closer) that is known or yet to be discovered). Neither the adapter module 100 nor the payment accepting unit 120, therefore require a traditional persistent long-range wireless network connection. The exemplary communications technology shown in the figures may be replaced with alternative like communications technology and, therefore, specific shown communications technologies are not meant to be limiting. For example WiFi technology could be replaced with another long-range communication technology.

- Server: A server is the host processing server that may be operated by the company running the system. For each user, the server 130 preferably maintains at least one "virtual wallet" having at least one "balance" (which can be $0) of designated funds for which the server 130 keeps an accounting. The balance may represent, for example, "cash" or it may be a "promotional value" that represents funds that may be spent under certain circumstances. If these funds begin to be depleted, the user may be notified (e.g. via the application 140 on the mobile device 150) that additional funds need to be designated and/or transferred. Alternatively, funds from other sources (e.g. the funding source server 160) may be automatically transferred to restore a

predetermined balance. The balance may also be increased based on a promotion (e.g. points earned or coupons). As shown in FIG. 58, the server includes appropriate processors 950, memory 960 (which would keep an accounting of the user's balance in a manner similar to a gift card), and communication systems 970. As shown, the communications unit 970 of the server 130 includes long-range communication technology (e.g. cellular technology and WiFi mechanisms). The server 130 also includes a security unit 955 for encrypting and decrypting messages. The server 130 receives an AuthRequest from the adapter module 100 (via a mobile device 150) and, if funds are available, returns the AuthGrant for funds. FIG. 58 shows exemplary components associated with the server 130. The shown example may be divided into multiple distinct components that are associated with each other or the example may be incorporated into or drawn from other technology (e.g. a computer or a main frame) as long as the components are associated with each other.

- Advertise Presence: Each adapter module 100 advertises its presence by broadcasting signals (advertising broadcast signals) to mobile devices in the zones 102, 104, 016. Each adapter module 100 can listen to other adapter modules' advertisements

- Received Signal Strength Indicator (RSSI): The adapter module 100 may have a self-calibrating signal strength to determine zone thresholds (e.g. a payment zone threshold). At the time the user selects an item (product or service) from the payment accepting unit 120, the Received Signal Strength Indicator (RSSI) is logged. At this moment, it is presumed the user is within "arms-length" (which may be a predetermined length approximating the distance of a user standing in front of a machine for the purpose of making a purchase) from the payment accepting unit 120. Mathematical computation (In-Range Heuristics) is conducted to derive the optimal RSSI threshold at which point payment should be triggered by an application 140 on a mobile device 150. The threshold may be payment accepting unit specific and can vary over a period of time. This optimal zone threshold is preferably reported to the mobile device 150 during an initial handshake.

- In-Range Heuristics: Mathematical computation that determines the RSSI threshold to determine when a user is in the authorization zone 104 and/or payment zone 102. This computation can take into consideration numerous historical data points as well as transaction specific information such as which mobile device 150 is being used, payment accepting unit type, among other factors. Preferably the RSSI is logged while the user is making his selection (this is the one time in the entire process that the user definitely will be "in range" (e.g. they will be arm's length from the machine 120 because they are physically interacting with the machine 120). The type of user mobile device 150, accelerometer data (e.g. is the user moving or stationary), and/or other information may also be logged while the user is making his selection. The adapter module 100 can give a reference RSSI for the payment zone 102 for the machine 120, and the application 140 can make a +/- adjustment based on the specific mobile device 150 on which it is installed. Over a period of time, the system continues to improve itself based on additional data points.

- Authorization Request (AuthRequest): When a user enters the authorization zone 104, the mobile device 150 notifies the adapter module 100 and the adapter module 100 sends the secured authorization request (e.g. the encrypted authorization request) as a "message" (also referred to as a communication or transmissions) to the server 130 via the mobile device 150. Encryption may be performed by a security unit 755 (security technology that may be associated with the processing unit 750 and/or the memory 760). Significantly, the AuthRequest is a request for authorization of funds, not a request for authorization of a transaction. The purpose of the funds is irrelevant to the server 30.

- Authorization Grant Token (AuthGrant): This is a "message" (also referred to as a communication or transmissions) encrypted by the security unit 955 (security technology) of the server 130 with the unique private key for the adapter module 100. The secured authorization grant (e.g. the encrypted authorization grant) is passed from the server 130 (via the mobile device 150) to the adapter module 100 in the form of a message. The mobile device 150, however, is not able to decrypt and read the message. The authorization grant is in response to the authorization request. The amount of the funds granted

by the AuthGrant may be determined by factors including, but not limited to, the amount of funds available (or, if funds are not available, a mini-loan could be granted), a pre-authorized amount (e.g. set by the server, set by the user during set-up, set by the funding source, or a standard amount), limited by time (e.g. only a certain amount per hour, or a predetermined amount at specific times of the day), limited to the maximum amount of an item on the machine (or enough for two or three items in the machine), or one or more of these and other factors. Significantly, the AuthGrant makes the funds available, but does not authorize a transaction. The AuthGrant may have an associated expiration period in that it may expire if it is not used in a pre-determined time period. The length of time before the AuthGrant expires may be determined by factors including, but not limited to, the trustworthiness of the user (e.g. the user has a long history with the system or some known provider (e.g. credit card provider, bank, or credit union), the user has a good credit rating, or the user has a large wallet balance), a pre-authorized time period (e.g. set by the server, set by the user during set-up, set by the funding source, or a standard time period), limited by time (e.g. predetermined time periods at specific times of the day such as longer times during breakfast, lunch, and dinner), limited by the machine or the products or services sold in the machine, limited by the number of other users near the machine (e.g. if it is a crowded machine, the AuthGrant may expire faster), or one or more of these and other factors. The AuthGrant remains valid until it expires or some other event occurs to end its validity (e.g. the user cancels it). This means that under normal circumstances the mobile device 150 will hold the AuthGrant authorizing use of funds for a pre-determined time period that will allow the user sufficient time to make a purchase. The authorized amount may be considered to be the "wallet balance" that is held in a virtual "wallet."

- Synchronization: Time may be synchronized to the adapter module 100 from the server 130. The server 130 sends time information with encrypted messages and the adapter module 100 uses the time encoded in the messages for synchronization.
- The mobile-device-to-machine payment systems and components thereof may have associated hardware, software, and/or firmware (a variation, subset, or

hybrid of hardware and/or software). The term "hardware" includes at least one "processing unit," "processor," "computer," "programmable apparatus," and/or other known or yet to be discovered technology capable of executing instructions or steps (shown as processing unit 750 in FIG. 56, processing unit 850 in FIG. 57, and processing unit 950 in FIG. 58). The term "software" includes at least one "program," "subprogram," "series of instructions," or other known or yet to be discovered hardware instructions or hardware-readable program code. Software may be loaded onto hardware (or firmware) to produce a "machine," such that the software executes on the hardware to create structures for implementing the functions described herein. Further, the software may be loaded onto the hardware (or firmware) so as to direct the mobile-device-to-machine payment systems (and components thereof) to function in a particular manner described herein or to perform a series of operational steps as described herein. "Hardware" such as the adapter module 100, mobile device 150, and payment accepting unit 120 may have software (e.g. programs and apps) loaded thereon. The phrase "loaded onto the hardware" also includes being loaded into memory (shown as memory 760 in FIG. 56, memory 860 in FIG. 57, and memory 960 in FIG. 58) associated with or accessible by the hardware. The term "memory" is defined to include any type of hardware (or other technology) -readable media (also referred to as computer-readable storage medium) including, but not limited to, attached storage media (e.g. hard disk drives, network disk drives, servers), internal storage media (e.g. RAM, ROM, EPROM, FLASH-EPROM, or any other memory chip or cartridge), removable storage media (e.g. CDs, DVDs, flash drives, memory cards, floppy disks, flexible disks), firmware, and/or other known or yet to be discovered storage media. Depending on its purpose, the memory may be transitory and/or non-transitory. Appropriate "messages," "communications," "signals," and/or "transmissions" (that includes various types of information and/or instructions including, but not limited to, data, commands, bits, symbols, voltages, currents, electromagnetic waves, magnetic fields or particles, optical fields or particles, and/or any combination thereof) over appropriate "communication paths," "transmission paths," and other means for signal transmission including any type of connection between two elements on the system (the system including, for example, the adapter

module 100, mobile device 150, payment accepting unit 120, hardware systems and subsystems, and memory) would be used as appropriate to facilitate controls and communications.

- It should be noted that the terms "programs" and "subprograms" are defined as a series of instructions that may be implemented as software (i.e. computer program instructions or computer-readable program code) that may be loaded onto a computer to produce a "machine," such that the instructions that execute on the computer create structures for implementing the functions described herein or shown in the figures. Further, these programs and subprograms may be loaded onto a computer so that they can direct the computer to function in a particular manner, such that the instructions produce an article of manufacture including instruction structures that implement the function specified in the flow chart block or blocks. The programs and subprograms may also be loaded onto a computer to cause a series of operational steps to be performed on or by the computer to produce a computer implemented process such that the instructions that execute on the computer provide steps for implementing the functions specified in the flow chart block or blocks. The phrase "loaded onto a computer" also includes being loaded into the memory of the computer or a memory associated with or accessible by the computer. Separate, albeit interacting, programs and subprograms may be associated with the adapter modules 100, the server 130, and the mobile device 150 (including the mobile application 140) and these programs and subprograms may be divided into smaller subprograms to perform specific functions.

- The terms "messages," "communications," "signals," and/or "transmissions" include various types of information and/or instructions including, but not limited to, data, commands, bits, symbols, voltages, currents, electromagnetic waves, magnetic fields or particles, optical fields or particles, and/or any combination thereof. Appropriate technology may be used to implement the "communications," "signals," and/or "transmissions" including, for example, transmitters, receivers, and transceivers. "Communications," "signals," and/or "transmissions" described herein would use appropriate technology for their intended purpose. For example, hard-wired communications (e.g. wired serial

communications) would use technology appropriate for hard-wired communications, short-range communications (e.g. Bluetooth) would use technology appropriate for close communications, and long-range communications (e.g. WiFi or Cellular) would use technology appropriate for remote communications over a distance. Appropriate security (e.g. SSL or TLS) for each type of communication is included herein. Security units 755 and 955 include technology for securing messages. The security technology may be, for example, encryption/decryption technology (e.g. software or hardware). Although encryption/decryption is discussed primarily as being performed using a unique private key, alternative strategies include, but are not limited to encryption/decryption performed using public/private keys, or other encryption/decryption strategies known or yet to be discovered. Appropriate input mechanisms and/or output mechanisms, even if not specifically described, are considered to be part of the technology described herein. The exemplary communications unit 770 (shown in FIG. 56) of the adapter module 100 is shown as including appropriate input and output mechanisms 772, 774 that may be implemented in association (e.g. directly or indirectly in functional communication) with male and female adapters 720, 730 of the adapter module 100. The exemplary communications unit 870 (shown in FIG. 57) of the mobile device 150 includes mechanisms for both long-range communications (shown as Cellular and/or WiFi mechanisms 872) for communicating with the server 130 and short-range communications (shown as Bluetooth mechanisms 876) for communicating with the adapter module 100.

- When used in relation to "communications," "signals," and/or "transmissions," the terms "provide" and "providing" (and variations thereof) are meant to include standard means of provision including "transmit" and "transmitting," but can also be used for non-traditional provisions as long as the "communications," "signals," and/or "transmissions" are "received" (that can also mean obtained). The terms "transmit" and "transmitting" (and variations thereof) are meant to include standard means of transmission, but can also be used for non-traditional transmissions as long as the "communications," "signals," and/or "transmissions" are "sent." The terms

"receive" and "receiving" (and variations thereof) are meant to include standard means of reception, but can also be used for non-traditional methods of obtaining as long as the "communications," "signals," and/or "transmissions" are "obtained."

- The term "associated" is defined to mean integral or original, retrofitted, attached, connected (including functionally connected), positioned near, and/or accessible by. For example, if the user interface (e.g. a traditional display 122 (FIG. 19), a touch screen display 124 (FIG. 19), a key pad 126 (FIG. 19), buttons 126 (FIG. 19, shown as part of the key pad 126), a keyboard (not shown), and/or other input or output mechanism) is associated with a payment accepting unit 120, the user interface may be original to the payment accepting unit 120, retrofitted into the payment accepting unit 120, attached to the payment accepting unit 120, and/or a nearby the payment accepting unit 120. Similarly, adapter modules 100 may be associated with payment accepting units 120 in that the adapter modules 100 may be original to the payment accepting unit 120, retrofitted into the payment accepting unit 120, attached to the payment accepting unit 120, and/or a nearby the payment accepting unit 120.
- It should be noted that relative terms are meant to help in the understanding of the technology and are not meant to limit the scope of the invention. Similarly, unless specifically stated otherwise, the terms used for labels (e.g. "first," "second," and "third") are meant solely for purposes of designation and not for order or limitation. The term "short" in the phrase "short-range" (in addition to having technology specific meanings) is relative to the term "long" in the phrase "long-range."
- The terms "may," "might," "can," and "could" are used to indicate alternatives and optional features and only should be construed as a limitation if specifically included in the claims.
- It should be noted that, unless otherwise specified, the term "or" is used in its nonexclusive form (e.g. "A or B" includes A, B, A and B, or any combination thereof, but it would not have to include all of these possibilities). It should be noted that, unless otherwise specified, "and/or" is used similarly (e.g. "A

and/or B" includes A, B, A and B, or any combination thereof, but it would not have to include all of these possibilities). It should be noted that, unless otherwise specified, the terms "includes" and "has" mean "comprises" (e.g. a device that includes, has, or comprises A and B contains A and B, but optionally may contain C or additional components other than A and B). It should be noted that, unless otherwise specified, the singular forms "a," "an," and "the" refer to one or more than one, unless the context clearly dictates otherwise.

System Overview

[00103] FIGS. 5, 6, and 7 together show exemplary major components of the mobile-device-to-machine payment system and the interactions therebetwen.

[00104] As shown, the adapter module 100 functionally connected bi-directionally to the payment accepting unit 120 via a wired serial connection such that no security is necessary. The adapter module 100 is also functionally connected bi-directionally to the mobile device 150 (and its installed mobile application 140) via short-range communication technology (e.g. a Bluetooth connection). Because the mobile device 150 is not a "trusted" link (e.g. it could be hacked by a user), only secured communications (transmissions) are passed between the adapter module 100 and the mobile device 150. This keeps the passed communications secured and safe from hacking. The mobile device 150 (and its installed mobile application 140) is also functionally connected bi-directionally to a system management server 130 and/or a funding source server 160 via long-range communication technology (e.g. WiFi or Cellular connection) that preferably has appropriate security (e.g. SSL security). Security between the mobile device 150 and the system management server 130 has the advantage of protecting communications from the mobile device 150 to the system management server 130 that may include sensitive data and may not be encrypted. The system management server 130 and the funding source server 160 may be connected via a wired Internet connection with SSL security. The system management server 130 may be connected via a wired Internet connection with SSL security to an operators' server 170. Although not necessary to implement a purchase transaction, for other purposes (e.g. inventory), the operators' server 170 may be connected to the payment accepting unit 120 using a handheld computer sync or a cellular connection.

[00105] Also, a unique private key may be used to securely transmit encrypted messages between the adapter module 100 and the system management server 130 (although the encrypted transmissions would most likely be routed through the mobile device 150). The server 130 stores a private key for each adapter module 100, and this key is only known to the adapter module 100 and the server 130. No intermediary is privy to this key (especially not the mobile device 150). When the adapter module 100 and server 130 communicate messages (e.g. AuthRequest and AuthGrant), the security unit 755 of the adapter module 100 encrypts the message with its private key and passes the message to the mobile device 150. The mobile device 150 (which preferably cannot decrypt the message) passes the encrypted message to the server 130. The server 130 is able to decrypt the message using the security unit 955 of the adapter module 100 and the unique private key. The security unit 955 of the server 130 uses this same unique private key to encrypt messages to the adapter module 100 and sends the message to the mobile device 150 to relay to the adapter module 100 that is able to decrypt the message using the security unit 755 of the adapter module 100 and the unique private key.

[00106] FIG. 7 shows specific exemplary communications and messaging with an exemplary vending sequence (the numbers to the left of the communications and messaging) between the adapter module 100, the mobile device 150, and the system management server 130. These communications are discussed in more detail in the discussion pertaining to the timing schematics (FIGS. 8A-8G) and the flow charts (FIGS. 9A-9E).

[00107] It should be noted that FIGS. 5, 6, and 7 are meant to be exemplary and to help in the understanding of the mobile-device-to-machine payment system. For example, the shown long-range communications technology may be replaced with alternative long-range communications technology known or yet to be discovered, the shown short-range communication technology may be replaced with alternative short-range communication technology known or yet to be discovered, and the shown security may be replaced with alternative security known or yet to be discovered. The shown connections are meant to be exemplary in that, for example, there may be intermediaries that are not shown. The shown components have been simplified in that, for example, only one mobile device 150 (or machine 120, adapter module 100, or server 130) is shown where many may be included. Finally, the order of the steps may be changed and some steps may be eliminated.

Adapter Module

[00108] FIGS. 11-55 show exemplary adapter modules 100a-100e (referred to generally as adapter modules 100). These are relatively low cost hardware that are pre-configured to work with industry standard a multi-drop bus (MDB). On machines without MDB technology, the adapter module 100 can be configured or designed to work with other serial protocols or activate a switch. In essence the adapter module 100 simulates establishing payment on payment accepting unit 120 in much the same manner as other alternative forms of payment (e.g. cash).

[00109] The shown exemplary adapter modules 100 are preferably designed to be used as an in-line dongle for in-line insertion within, for example, a MDB of a machine 120. The wire used in MDB technology uses male and female connection ends or adapters to allow the attachment of peripherals. In the case of a vending machine, the wire with the connection ends or adapters would be present to allow the attachment of a payment receiving mechanism (e.g. a coin mechanism). The MDB male and female adapters 700, 710 may be separated (as shown in FIGS. 17, 18, 26, 27, 35, 36, 44, 45, 53, and 54). The adapter modules 100 have male and female adapters 720, 730. The adapter module may be plugged (inserted) in serial ("in-line") with the wire. For example, the MDB female adapter 710 may be connected to the male adapter 720 of the adapter module 100 and the MDB male adapter 700 may be connected to the female adapter 730 of the adapter module 100. The resulting in-line configuration is shown in FIGS. 19, 28, 37, 46, and 55. It should be noted that the adapter modules 100 are designed to allow pass-through communications so that if the mobile-device-to-machine payment systems is not enabled (e.g. for a particular purchase or simply turned off) the MDB functions as though the adapter module 100 is not there and the machine 120 can function normally.

Hands-Free

[00110] Summarily, if it is available, a hands-free mode, from the user's perspective, would allow the user to approach a favorite payment accepting unit 120 and notice that the display (e.g. the displays 122 or 124 shown in FIG. 19) associated with the payment accepting unit 120 shows funds available (e.g. the wallet balance), he would select the product or service using input mechanisms (e.g. buttons 126 or a touch screen display 124 shown in FIG. 19) associated with the payment accepting unit 120, and he would retrieve his dispensed services or products.

[00111] During an initial handshake with the mobile device 150 (when the user is within range), the adapter module 100 reports to the mobile device 150 whether or not hands-free mode is available. If it is available, the installed mobile application 140 automatically connects to the payment accepting unit 120 without the user having to interact with the mobile device 150. The user observes that funds are available on the display 122, 124 of the payment accepting unit 120 and completes the purchase transaction as if cash was inserted in the machine 120 by inputting his selection on the payment accepting unit 120. The payment accepting unit 120 dispenses the product or service. After the selection is made, the change is returned to the mobile device 150.

[00112] Whether hands-free payment is available is determined by factors including, but not limited to whether if other mobile devices 150 are in range, if other adapter modules 100 are in range, if there are any alerts, if the payment trigger threshold is having wide variances and so deemed unstable, or if the payment accepting unit operator (e.g. a vending machine operator) has opted to disable hands-free mode for the payment accepting unit 120. In the latter instance, operators can disable via a maintenance mobile device 150, as well as through the operators' server 170 and/or the system management server 130.

[00113] FIG. 3 is a table that showing exemplary considerations, conditions, or factors that may be used to determine whether the hands-free pay feature is available. Starting at the "Favorite?" column, this indicates whether the payment accepting unit 120 is a favorite machine. Preferably the hands-free pay feature is only available for use with "favorite" payment accepting units 120 (e.g. a vending machine at work or school). The "Alert" column has to do with whether there is some reason (e.g. there are too many users in range) that the hands-free pay feature should not work and, if there is such a reason, the user will be notified (alerted) and may be able to use the manual mode to resolve the alert and/or complete the transaction. FIG. 3 shows situations in which a user is or is not able to make hands-free purchases from a machine 120 using a mobile application 140 on his mobile device 150. It should be noted that the shown interface is meant to be exemplary. For example, some of the features could be automated or pre-selected. (It should be noted that the left hand column, the "Tab" column, relates to whether the selected tab on the mobile application 140 is "all" or "favorite." FIGS. 10A-10D all show these tabs. Unlike the other columns in FIG. 3, this column has more to do with the functionality and view of the application 140 than specifically with the hands-free feature. The tabs would allow a user to select whether he wanted to be alerted when he was in range of all payment accepting units 120 or just

"favorite" payment accepting units 120 and the application 140 would show the appropriate view.)

[00114] Balance Display: An optional feature of the mobile-device-to-machine payment system that is particularly helpful in the hands-free mode (although it may be available in the manual mode and/or in a multiple-vend scenarios) is when the user's mobile device 150 sends "credit" to the payment accepting unit 120 (either via hands-free payment or through a manual swipe), the wallet balance is sent to the payment accepting unit 120 that is then displayed to the user on a display 122, 124 of the machine 120. This is particularly beneficial during hands-free mode when the user does not retrieve the mobile device 150 and, therefore, may not know the balance. Also, in a multiple-vend scenario the user would not have to calculate a remaining balance.

[00115] An exemplary hands-free and multiple-vend scenario with a balance display might be as follows: The user has $5.00 in his virtual wallet as that is the amount that has been authorized (the AuthGrant being stored on the mobile device 150). He walks up to the payment accepting unit 120 and $5.00 is displayed on the display 122, 124 of the payment accepting unit 120 since hands-free mode was enabled and credit was sent (e.g. via short-range communication technology) to the payment accepting unit 120. The user makes a selection of $1.50 by interacting (e.g. pressing buttons) with the machine 120. The item (product or service) is dispensed and the "change" is "returned" (e.g. via short-range communication technology) to the virtual wallet. But since user is still standing in the payment zone 102, the remaining wallet balance of $3.50 is sent to the payment accepting unit 120 and displayed so that the user can now see he has a $3.50 balance. (It should be noted that the authorized funds may remain on the machine 120 and not be transferred back to the mobile device 150 between transactions.) The user decides to purchase a $1.50 item, and the transaction is completed as usual (e.g. by interacting with the machine 120). Now the user is still standing in the payment zone 102 and he sees the wallet balance of $2.00 on the display 122, 124 of the payment accepting unit 120. Deciding he does not wish to purchase anything else, the user walks away. As he walks out of the payment zone 102, the credit is cleared from the machine 120. But he is left with the knowledge that his wallet balance is $2.00 even though he never touched the mobile device 150. Communications between the payment accepting unit 120 and the adapter module 100 (via the mobile device 150) handle the accounting incidental to the transaction. The remaining balance ($2.00) is technically

stored on the server 130, and may be reflected on the application 140 on the mobile device 150.

Multiple Distinct Zones

[00116] As shown in FIGS. 1 and 2, the functions performed by the adapter module 100 can be divided into distinct zones: a first "communication zone" (e.g. "Bluetooth range" 106), a second "authorization zone" 104, and a third "payment zone" 102. The payment zone102 (that can not be zero) is smaller than or equal to (overlapping completely) the authorization zone 104. (Put another way, the payment zone 102 is within or coextensive with the authorization zone 104.) The payment zone 102 is a subset of the authorization zone 104 with a ratio of the payment zone 102 to the authorization zone 104 ranging from 0.01:1 to 1:1. It is not necessarily a fixed ratio and can vary between different payment accepting units 120, different mobile devices 150, different users, and over time. While the zones 102, 104, 106 are depicted as having a uniform shape, the zones may not necessarily be uniform (or constant over time) in that the shape can vary. For example, the shape of the Bluetooth range 106 may vary depending on environmental conditions such as obstacles in the room and payment accepting unit 120 door/wall materials.

[00117] Bluetooth Range 106: The outermost range is the Bluetooth range 106. This is the area in which the adapter module 100 is able to broadcast its presence. In most situations, the Bluetooth range 106 is a passive range in that no actual data is exchanged between the mobile device 150 and the adapter module 100. While in the Bluetooth range 106, the mobile device 150 monitors the RSSI (Received Signal Strength Indicator).

[00118] Authorization Zone 104: The middle region is the authorization zone 104. This is a computed area based on the RSSI. As mentioned, the mobile device 150 monitors the RSSI while it is in the Bluetooth range 106. When the RSSI reaches a certain predetermined threshold based on In-Range Heuristics, the mobile device 150 can be considered to be in the authorization zone 104. In the authorization zone 104 the mobile device 150 establishes a connection to the adapter module 100 (e.g. a Bluetooth connection (FIG. 5) with SSL protection (FIG. 6)) and informs the adapter module 100 of its presence. After a successful handshake with the adapter module 100, the mobile device 150 registers the adapter module 100 and the adapter module 100 requests an authorization to the server 130 via the mobile devices' network connection (e.g. a WiFi or cellular connection (FIG. 5) with SSL protection (FIG. 6)). It is important to note the mobile device 150 and the adapter

module 100 have a non-exclusive relationship at this point. The adapter module 100 may collect registrations for all mobile devices 150 that are within the authorization zone 104.

[00119] An authorization occurs in preparation for when the user enters the payment zone 102. An authorization expires in a set period of time (for example, five minutes), so if the mobile device 150 is still in the authorization zone 104 at the time of expiration, the adapter module 100 submits for and receives another authorization. This will continue for a set number of times (for example, the limit may be three times to limit cases of numerous authorizations for a mobile device that may remain in the authorization zone 104 for an extended period of time without completing a transaction). Should authorization fail (for instance if the limit had been reached) prior to the user entering the payment zone 102, the adapter module 100 will request authorization when the mobile device 150 enters the payment zone 102 (which adds a few seconds to the experience).

[00120] Payment Zone 102: As a user enters the payment zone 102, the mobile device 150 establishes exclusive control of the adapter module 100. Once established, any other user in the payment zone 102 is put into a "waiting" status.

[00121] In the payment zone 102, the payment can be triggered automatically if the system has and is in hands-free mode. In such instances, the mobile device 150 is running the app 140 in background mode and will send credit to the payment accepting unit 120 without any explicit user interaction. The user completes the transaction on the payment accepting unit 120 in much the same manner as if cash had been inserted into the payment accepting unit 120 to establish credit. After the user completes the transaction (that may include one or more purchases), details of the transaction are preferably returned to the mobile device 150 and server 130 in separate messages. The message to the server 130 is preferably encrypted with the adapter module's 100 private key (FIG. 6) to ensure data integrity. As shown in FIG. 7, the "private key" coded message (Encrypted VendDetails) is preferably sent via the mobile device 150. The message to the mobile device 150 may be sent solely for the purpose of closing the transaction. The transaction history and balance are updated server-side via the encrypted message sent to the server 130.

[00122] The other mode of operation is manual mode. In manual mode, the user launches the mobile device 150 and is able to swipe to send payment to the payment accepting unit 120. The user can also swipe back to cancel the payment. Like in hands-free mode, the purchase transaction is completed on the payment accepting unit 120 in the same

manner as if cash were inserted into the payment accepting unit 120. The mobile device 150 is only used to send payment. Selection is made directly on the payment accepting unit 120.

[00123] Self-Calibrating Zone Threshold: A key, but optional feature, of the system is a self-calibrating payment zone RSSI threshold. Because RSSI can vary machine to machine, environment to environment, and device to device, having a fixed threshold at which payment is triggered can be problematic. The approach suggested herein is the creation of a self-calibrating threshold. When the user is interacting with the payment accepting unit 120 (such as when he makes his selection on the payment accepting unit 120), the payment accepting unit 120 notifies the adapter module 100 and the adapter module 100 logs the conditions such as RSSI, type of user mobile device 150, accelerometer data, and other information. It is at this point that it can be ascertained safely that the user is within arms-length from the payment accepting unit 120 (by necessity the user is arms-length because he is making some physical interaction with the payment accepting unit 120). This is the only point in the entire transaction in which it can be certain that the user is within arms-length from the payment accepting unit 120.

[00124] FIG. 4 shows a simplified set of exemplary steps involved when users enter the payment zone 102. Specifically, FIG. 4 shows that credit is established 200 (this may have been done in the authorization zone 104, but if not it would be handled in the payment zone 102), that the user makes a selection using the machine 202, that the machine notifies the adapter module of the selection 204, that the adapter module (optionally) logs the RSSI 206, and that the purchase process(es) continues 208. Using the historically logged RSSI data, the adapter module 100 calculates one of several "average" RSSI using various mathematical models. This "average" could be a traditional average, a moving average, a weighted average, a median, or other similar summary function. The adapter module 100 could pre-process the historical data before running the function, such as to eliminate top and bottom data points, suspect data points, etc.

[00125] Optionally, during the handshake between the mobile device 150 and the adapter module 100, the information transmitted to the adapter module 100 may include, for example, the model of the mobile device 150. Using the received information pertaining to the mobile device models, the adapter module 100 can create multiple payment thresholds, one for each mobile device model. This allows for variances that may be inherent in different types of Bluetooth radios. An alternative to this method is for the adapter module 100 to broadcast a baseline payment zone threshold, and the mobile device 150 can use an offset

from this baseline based on its specific model type. The payment zone thresholds (or baseline offsets) can be unique to specific types of mobile devices (e.g. by manufacturer, operating system, or component parts), models of mobile devices, or individual mobile devices (unique to each user).

[00126] In a typical scenario in which the payment zone threshold has been calibrated, the adapter module 100 advertises its presence along with the threshold at which it considers any mobile device 150 to be in the authorization zone 104. This is a one-way communication from adapter module 100 to mobile device 150. Once the mobile device 150 enters the authorization zone 104, there is a handshake that is established between the adapter module 100 and the mobile device 150. During this handshake, the mobile device 150 can share its model information with the adapter module 100, and the adapter module 100 can return the payment zone 102 threshold for that specific model.

[00127] Optionally, in addition to calibrating the payment zone threshold, the adapter module 100 can apply the self-calibrating model to the authorization zone 104 to calibrate the authorization zone threshold. As with the payment zone thresholds, the authorization zone thresholds can be unique to specific types of mobile devices, models of mobile devices, or individual mobile devices. In this scenario, the adapter module 100 would broadcast multiple thresholds by device type and the mobile device 150 would determine which threshold to apply (or alternatively broadcast a baseline and the mobile device 150 uses an offset based on its device model). Even in this scenario, the authorization zone 104 is a one-way communication.

[00128] Optionally, along with the threshold that is calculated (in the payment and/or the authorization zone(s)), a safety margin can be added to minimize scenarios in which a user is within range, but the mobile-device-to-machine payment systems do not recognize it because the threshold may not have been reached. For example, if the calculated RSSI for an iPhone 5 on machine 4567 is -68db, the mobile-device-to-machine payment systems may add a safety margin of -5db, and establish the threshold at -73db. So when a user's phone is communicating with the adapter module 100 at an RSSI of -73db or better, the mobile-device-to-machine payment systems will allow the mobile device 150 to credit the payment accepting unit 120. The safety margin can be set on the server 130 and downloaded to the adapter module 100, or set on the mobile device 150, or set on the adapter module 100 itself.

[00129] Optionally, in the payment zone threshold, the mobile device 150 can use other data to determine when to cancel the exclusive control of the payment accepting unit 120, to identify when the user is moving out of the payment zone 102. External data could include accelerometer data from the mobile device 150. Using that data, the mobile device 150 can determine whether the user is standing relatively still in front of the payment accepting unit 120, or if the user is in motion – effectively walking away from the payment accepting unit 120.

Signal Unavailability Adaptation

[00130] The mobile-device-to-machine payment systems described herein use a mobile device's 150 short-range communication technology (shown as Bluetooth mechanisms 876 in FIG. 57) and a mobile device's 150 long-range communications technology (shown as Cellular and/or WiFi mechanisms 872 in FIG. 57). The short-range communication technology 876 communicates with the adapter module's 100 short-range communication technology (shown as Bluetooth mechanisms 776 in FIG. 56). The long-range communications technology 872 communicates with the server's 130 communication technology (not shown). The mobile device 150 (with a mobile application 140 thereon) acts as a communication bridge between the adapter module 100 (associated with a payment accepting unit 120) and the server 130. This process is described herein and works properly if there is cellular or WiFi coverage within the payment zone 102.

[00131] One option if there is no cellular or WiFi coverage within the payment zone 102 is to determine whether there is cellular or WiFi coverage within the authorization zone 104 or the Bluetooth range 106. If there is, then the sizes of the zones 102, 104, 106 could be adapted and the timing could be adapted. For example, if the mobile devices 150 detected problems with the cellular or WiFi coverage within the payment zone 102, the user could carry his mobile device 150 into the other zones (or the mobile device 150 could use short-range communication technology to communicate with other mobile devices 150 within the authorization zone 104 or the Bluetooth range 106) to determine whether the zones have cellular or WiFi coverage. If they do have coverage, communication between the mobile device 150 and the server 130 can be advanced (conducted earlier when the mobile device 150 is further from the machine 120) or delayed (conducted later when the mobile device 150 is further from the machine 120). This can be thought of as changing the size or shapes of the zones 102, 104, 106. The timing would also have to be adjusted so that the authorization of funds (AuthGrant) does not expire before the user has a chance to make a purchase. It also

means that balance updates to the server 130 may happen after the user has moved away from the machine 120 and has cellular or WiFi coverage again.

[00132] Another option if there is no cellular or WiFi coverage within any of the zones 102, 104, 106 is for the user to obtain authorization while outside of the zones in a place with cellular or WiFi coverage. This may occur, for example, if a user knows that he will be going to a place with a payment accepting unit 120 equipped with an adapter module 100 (perhaps to a favorite payment accepting unit 120) that does not have (or rarely has) cellular or WiFi coverage. A user may also use the mobile application 140 to query payment accepting units 120 in a given range (e.g. within 50 miles) or at a given location (e.g. at a campground or in a particular remote city) to determine whether there is cellular or WiFi coverage within the zones 102, 104, 106. The user can then obtain pre-authorization from the server 130 using the mobile application 140. Again, the timing would also have to be adjusted so that the authorization of funds (AuthGrant) does not expire before the user has a chance to make a purchase. It also means that balance updates to the server 130 may happen after the user has moved away from the machine 120 and has cellular or WiFi coverage again. A mobile-device-to-machine payment system having the ability to implement this option would be able to accept cashless payments without requiring any network connection near the payment accepting unit 120. Mobile-device-to-machine payment systems described herein that are located in a remote location where no signal is available, therefore, can accept cashless payments.

[00133] As an example of a situation in which there might be no cellular or WiFi coverage within any of the zones 102, 104, 106 of a particular payment accepting unit 120, the user (a teenager) may be traveling to a remote location to attend summer camp where there is no cellular or WiFi coverage. The camp may have several payment accepting units 120 (e.g. a machine that creates a dedicated "hot spot" that requires payment for use, vending machines, or machines for renting equipment (e.g. bikes, kayaks, or basket balls)). The camp facility might notify parents that the mobile-device-to-machine payment system is available. The parents, while at home, could obtain authorization for a particular amount (that could be doled out a certain amount per day or limited to type of machine or location) to be authorized and "loaded" into the user's mobile device 150 and specify that the authorization will not expire for a certain period or until a certain date. Thereafter, while at camp, the user could use the mobile application 140 on his mobile device 150 in a manner similar to those discussed elsewhere herein. Short-range communications may be used for communications

between the adapter modules 100 (associated with the machines 120) and users' mobile devices 150.

[00134] One subtle but powerful component of the systems described herein is that they require internet network connection only in the authorization zone 104 and only for the time period required to send the AuthRequest and receive the AuthGrant. Once a valid AuthGrant is received by the mobile device 150, an internet network connection is not required by either the mobile device 150 or the adapter module 100 in the payment zone 102 as long as the AuthGrant is valid (unexpired). This mechanism allows the system to seamlessly handle authenticated transactions in (temporary) offline mode, with the deferred acknowledgement and transaction messages performing the bookkeeping and cleanup when network connection is regained. The alternatives described above provide a unique way to artificially extend the authorization zone to include any location where the mobile device 150 can communicate with the server 130.

Multiple User Resolution

[00135] As shown in FIG. 2, in likely practical scenarios, there will be multiple users in the zones 102, 104, 106. As shown, users 1, 2, and 3 are in the payment zone 102 near the machine 120, users 5 and 6 are shown as positioned between the authorization zone 104 and the Bluetooth range 106, users 4 and 7 are in the Bluetooth range 106, user 10 is positioned on the edge of the Bluetooth range 106, and users 8 and 9 are positioned outside of Bluetooth range 106. The mobile-device-to-machine payment systems provide for managing, and resolving issues pertaining to multiple users.

[00136] Users 4 and 7 are within the Bluetooth range 106 and user 10 is either entering or leaving the Bluetooth range 106. Within the Bluetooth range 106 the users' mobile devices 150 are able to see the adapter module's 100 advertisement. In this zone, the mobile device 150 preferably does not initiate a connection. The adapter module 100 is preferably unaware of the users in the Bluetooth range 106. All the adapter module 100 is doing is advertising its presence to any multitude of users that may be in Bluetooth range 106.

[00137] The adapter module 100 begins to log users as the users (and their respective mobile devices 150) enter the authorization zone 104 (shown in FIG. 2 as users 5 and 6). At this point, there is a non-exclusive connection initiated by the mobile device 150 to the adapter module 100. It does a handshake (e.g. to exchange information needed to obtain authorization and, optionally, to log information needed for a self-calibrating authorization

zone threshold) and the mobile device 150 contacts the server 130 for an authorization (e.g. sending an AuthRequest and receiving an AuthGrant). The adapter module 100 registers all mobile devices 150 that have requested and received AuthGrants. The adapter module 100 continues communicating with any other mobile device 150 that enters the authorization zone 104. After initial contact, the adapter module 100 may provide the mobile device 150 with a deferral delay of when to check back in with the adapter module 100 allowing opportunity for other mobile devices 150 to communicate with the adapter module 100.

[00138] If there is only one user in the payment zone 102, a purchase transaction may be performed. If there are multiple users in the payment zone 102, the mobile-device-to-machine payment system must handle the situation.

[00139] One optional exemplary solution for handling the situation of the multiple users in the payment zone 102 is queuing users in the payment zone 102. Once any mobile device 150 enters the payment zone 102, it establishes exclusivity to a particular mobile device 150 (first come first serve). Technically, however, the adapter module 100 is not establishing an exclusive connection to the mobile device 150. The adapter module 100 can still perform a round-robin poll and communicate with and advertise to other mobile devices 150. Instead, the adapter module 100 establishes a queue prioritized by RSSI and time (e.g. who was first and whether the authorization has expired) and it notifies (e.g. alerts) other mobile devices 150 to wait. The earliest valid (unexpired) authorization takes precedence when there is any tie in the RSSI. Otherwise, for example, the strongest average RSSI takes priority. Preferably the queue is not a static measure of the RSSI but an averaged measure over the period of time in the queue. This compensates for a scenario in which a user may be walking around in the queue and then shows up at the payment accepting unit 120 just as the previous user is finishing. If another user was also in the payment zone 102 and stood there the entire time, but may have newer authorization, he could win out.

[00140] Anytime that the adapter module 100 cannot determine exactly which user is in the payment zone 102 in front of the payment accepting unit 120, the adapter module 100 will disable hands-free payment. The mobile device 150 will send an alert to the user and he can use swipe to pay (manual mode). All users in payment zone 102 will show "Connected" and the first to swipe payment to the payment accepting unit 120 then locks out other users.

Multiple Module Resolution

[00141] In the scenario where there are multiple modules present, determining which payment accepting unit 120 a user is in front of can be a challenge. The mobile-device-to-machine payment systems described herein allow for adapter modules 100 to communicate to other adapter modules 100 in range via Bluetooth. Each user receives authorization grants for specific payment accepting units 120. This means if there are multiple adapter modules 100 within the same authorization zone 104, there will be multiple authorization grants for the user. When the user enters the payment zone 102, it can be difficult to differentiate which payment accepting unit 120 the user is in front of if the payment zones 102 overlap.

[00142] To solve this problem, when the user enters the payment zone 102, the adapter modules 100 communicate with each other to determine the RSSI for the particular user (based on the signal from his mobile device 150) to triangulate which adapter module 100 (and the associated payment accepting unit 120) is closer to the user. Optionally, the inter-module communications can restrict the user to establishing an exclusive connection with only one payment accepting unit 120.

[00143] Optionally, when the user connects to a payment accepting unit 120, the mobile device 150 can send a communication to the payment accepting unit 120 for momentary display to the user on the display 122, 124 of the payment accepting unit 120. For example, the mobile device 150 can send a communication (e.g. "connected" or "Fred's Mobile Device Connected") to the payment accepting unit's display 122, 124 for a predetermined period of time (e.g. 1-3 seconds) so when the user is in payment zone 102, it is clear which payment accepting unit 120 the user is connected to prior to making a purchase (either in hands-free or manual mode).

[00144] In addition, when the user is in manual mode, the mobile device 150 can display (e.g. on the touch screen 152 as shown in FIGS. 10A-10D) a visual indication of the payment accepting unit 120 (e.g. a picture and/or a payment accepting unit ID of the payment accepting unit 120) for visual confirmation. If the user is in manual mode, the user can manually change the payment accepting unit 120.

Descriptive Scenario

[00145] FIG. 7, FIGS. 8A-8G, and 9A-E (as well as other figures) can be used to understand a detailed exemplary scenario of the mobile-device-to-machine payment systems described herein. An exemplary flow of communications and steps are loosely described

below with reference to these (and other figures). It should be noted that alternative scenarios could include, for example, a modified order of the steps performed.

[00146] Prior to vending transactions, a user downloads a mobile app 140 onto his mobile device 150, creates an account, and configures a funding source via, for example, a funding source server 160. A funding source may be, for example, a debit card, a credit card, campus cards, rewards points, bank accounts, payment services (e.g. PayPal®) or other payment option or combination of payment options known or yet to be discovered. The funding sources may be traditional and/or nontraditional payment sources that are integrated into the ecosystem described herein and then used indirectly as a source of funds. Funds from the funding source are preferably held on the server 130 such that when an AuthRequest is received by the server 130, the server 130 can send an AuthGrant authorizing funds for a purchase.

[00147] The user can specify one or more "favorite" adapter module(s) 100 (that has a one-to-one relationship to the payment accepting unit 120) that he may visit regularly, such as a vending machine at school or work. Favorite adapter modules 100 appear on a pre-filtered list and allow for additional rich features such as hands-free payment.

[00148] The payment accepting unit 120 may be equipped with an adapter module 100 that is constantly advertising its availability via Bluetooth (or other "signals," "communications," and/or "transmissions"). This ongoing advertising and scanning for adapter modules is shown in FIG. 8A. As shown, the mobile device 150 is continuously scanning for any adapter module 100 within Bluetooth (or other "signal," "communication," and/or "transmission") range. When the user is within range of that adapter module 100, the mobile device 150 tracks and monitors the signal strength until a predetermined "authorization zone" threshold is achieved.

[00149] FIGS. 8B and 9A generally show that when the authorization zone threshold is reached, the mobile device 150 enters the authorization zone (block 302) and registers the adapter module 100. The mobile device 150 connects to the server 130 (block 304). The app 140 on the mobile device 150 creates a request for authorization (AuthRequest) and passes the AuthRequest to the server 130 using appropriate communication technology (e.g. cellular or WiFi) (block 306). The server 130 responds with an authorization grant (AuthGrant) encrypted with the specific adapter module's private key (block 306). This authorization token may minimally include the Userl D, Apparatusl D (for the adapter module 100),

authorization amount, and expiration time. The mobile device 150 receives the AuthGrant from the server 130, and retains it until the mobile device 150 is ready to issue payment to an adapter module 100. The mobile device 150 collects all pending AuthGrants that may be one or more depending on how many adapter modules 100 are in-range. Unused AuthGrants that expire are purged from the mobile device 150 and the server 130. It is important to note that the mobile device 150 is unable to read the AuthGrant because it is encrypted with the adapter module's unique private key that is only known to server 130 and adapter module 100. This provides a preferred key element of security in the system as the adapter module 100 only trusts AuthGrants that are issued by the server, and the AuthGrants cannot be read or modified by the mobile device 150 or any other party in between the server and the adapter module 100. Additional mobile devices 150 may enter the authorization zone 104 (block 308).

[00150] As the user approaches a specific adapter module 100, the user enters the payment zone 102 and an event threshold is triggered based on heuristics performed by the mobile device 150. Blocks 310 and 312 show the loop steps of waiting for a mobile device 150 from the authorization zone 104 to enter the payment zone 102. If the user leaves the authorization zone 104 without entering the payment zone 102, the adapter module 100 returns to advertising its presence (block 300).

[00151] FIGS. 8C and 9B generally show the user entering the payment zone. The mobile device 150 verifies that it has an unexpired and valid AuthGrant. If the AuthGrant is not good, it may be requested again, repeating the Auth Request process (block 315). If the AuthGrant is good, the mobile device 150 sends the valid AuthGrant (including the wallet balance (block 322)) to the adapter module 100 to initiate a transaction. The mobile device 150 may issue the AuthGrant automatically without specific user interaction if the hands-free mode is supported (and the device is a favorite (block 318), there is only one device in the payment zone 102 (block 318), and (optionally) there is only one user in the authorization zone 104 (block 320). If any of these factors are not present, the mobile device 150 will prompt and/or wait for the user to begin the transaction manually (block 324).

[00152] FIGS. 8D, 9C, and 9D generally show the transaction process. As shown in FIG. 9C, the adapter module 100 runs through a series of questions to determine if there are any issues that would prevent vending including: has the user canceled in-app? (block 326), has the user walked away? (block 328), is the coin return pressed? (block 330), has more than a predetermined period of time elapsed? (block 332). If the answer to any of these questions

is "yes," the transaction does not proceed. If the answers to all of these questions is "no," the user makes a selection (block 334) on the payment accepting unit 120 in the same or similar manner as compared to if cash or credit were presented to the payment accepting unit 120. If the machine 120 is able to vend (block 336), it attempts to release the product. If the vend fails (block 338) it is reported by the machine (block 340) and a credit is returned to the virtual wallet (block 342). If the vend is successful (block 338) it is reported by the machine (block 344). Put another way, after the transaction is complete, the adapter module 100 returns to the mobile device 150 the details of the transaction as well as an encrypted packet containing the vend details to be sent to the server 130 via the mobile device 150. Optionally, the adapter module 100 can pass additional information not directly related to the transaction such as payment accepting unit health, sales data, error codes, etc.

[00153] FIGS. 8D and 9E generally show the multi-vend function. If the machine has enabled multi-vend capabilities (block 350) and the multi-vend limit has not been reached, the process returns to the question of whether the user is in the payment zone (block 310 of FIG. 9A). If the machine does not have enabled multi-vend capabilities (block 350) or the multi-vend limit has been reached, the wallet is decremented by the vend amount(s) and "change" is returned to the virtual wallet (block 354) and the process ends (block 356).

[00154] FIG. 8E is a timing schematic showing an exemplary Login process. FIG. 8F is a timing schematic showing an exemplary bootup process. FIG. 8G is a timing schematic showing an exemplary Account Check/Update process.

[00155] Several of the figures are flow charts (e.g. FIGS. 9A-9E) illustrating methods and systems. It will be understood that each block of these flow charts, components of all or some of the blocks of these flow charts, and/or combinations of blocks in these flow charts, may be implemented by software (e.g. coding, software, computer program instructions, software programs, subprograms, or other series of computer-executable or processor-executable instructions), by hardware (e.g. processors, memory), by firmware, and/or a combination of these forms. As an example, in the case of software, computer program instructions (computer-readable program code) may be loaded onto a computer to produce a machine, such that the instructions that execute on the computer create structures for implementing the functions specified in the flow chart block or blocks. These computer program instructions may also be stored in a memory that can direct a computer to function in a particular manner, such that the instructions stored in the memory produce an article of manufacture including instruction structures that implement the function specified in the flow

chart block or blocks. The computer program instructions may also be loaded onto a computer to cause a series of operational steps to be performed on or by the computer to produce a computer implemented process such that the instructions that execute on the computer provide steps for implementing the functions specified in the flow chart block or blocks. Accordingly, blocks of the flow charts support combinations of steps, structures, and/or modules for performing the specified functions. It will also be understood that each block of the flow charts, and combinations of blocks in the flow charts, may be divided and/or joined with other blocks of the flow charts without affecting the scope of the invention. This may result, for example, in computer-readable program code being stored in whole on a single memory, or various components of computer-readable program code being stored on more than one memory.

Distinction From Known Systems

[00156] Many of the known systems and methods require that the payment accepting unit be persistently (continuously) connected to and/or connectable on demand to some sort of remote server in order to function. As an example, the Carlson reference describes a system and a method for using a portable consumer device. Described embodiments include a consumer using the portable consumer device to dial a number to purchase an item (product or service) in a vending machine, to send an SMS to purchase an item in a vending machine, or to use a mobile wallet to purchase an item in a vending machine. It is mentioned in one embodiment that the consumer may launch an application in the portable consumer device or, alternatively, the portable consumer device may automatically detect the vending machine and prompt the consumer to enter information associated with the vending machine. It should be noted, however, that even when there is automatic detection, the user is prompted to enter information (e.g. a machine alias, payment information, or a PIN) and it can be inferred that this is entered on the portable consumer device. Once connected to a payment processing network, the authorization process begins using a payment processing network and/or payment server. Significantly, all of the embodiments described in the Carlson reference specify that the payment server sends an authorization response message to the vending machine. This means that, unlike the mobile-device-to-machine payment systems described herein, a persistent network connection is required for the Carlson system to function. Other references that disclose systems that require a persistent network connection include the Khan reference (the MicroAdapter having the persistent connection), the Garibaldi reference, and the Weiner reference.

[00157] Many of the known systems and methods require the user to significantly interact with their mobile devices. As an example, the Whigham reference is directed to a system that eliminates the need for currency for a vending machine and also eliminates the need for a dedicated online connection between the vending machine and the issuer of a credit card or a debit card. Instead the Whigham system and method allows a consumer to purchase a product from an automatic vending machine by using the consumer's cellular telephone, personal digital assistant (P DA), or similar wireless communication device as a link between the provider of the products in the vending machine and the vending machine. The Whigham reference, however, sets forth a system and method requires significant interaction between the consumer and his telephone including dialing a telephone number to a server (that, in turn, provides a vend code to the consumer), requesting a specific product (e.g. by dialing additional digits, although this step is optional if a unique number was dialed for a specific product), and transmitting a vend code to the vending machine. (Other references that disclose systems that require user interaction with the phone include the Offer reference, the Khan reference, the Belfer reference, and the Carlson reference.) In addition to other differences, some of the mobile-device-to-machine payment systems described herein do not require the user to interact with his mobile device at all, which can be contrasted to known systems and methods that require the consumer to, for example, dial a telephone number, enter a machine identification, and/or enter a product identifier using the mobile device to purchase a product.

[00158] The known systems and methods that use a cellular telephone to facilitate cashless transactions at a vending machine use the cellular telephone to authorize a particular transaction. For example, once the user knows what he wants from a vending machine, he can dial a server and receive authorization to make a specific purchase. Sometimes this includes dialing additional numbers on the cellular telephone to specify a particular product. The mobile-device-to-machine payment systems described herein take a completely different approach. The mobile-device-to-machine payment systems described herein are not specifically interested in the details of the transaction to authorize the transaction. Instead, the mobile-device-to-machine payment systems function more like a gift card, a credit card, or a debit card in that they allow the user to have funds to make a purchase. When a user is in range, the adapter module 100 (via a mobile device 150) sends an AuthRequest to the server 130 to preemptively obtain authorization to make funds available. The server 130 returns the AuthGrant for funds to the adapter module 100 (via a mobile device 150) so that

the user may use the funds to make a purchase. The AuthGrant may remain valid until it expires. This gives the user significantly more flexibility than known systems and methods.

Miscellaneous

[00159] It is to be understood that the inventions, examples, and embodiments described herein are not limited to particularly exemplified materials, methods, and/or structures. It is to be understood that the inventions, examples, and embodiments described herein are to be considered preferred inventions, examples, and embodiments whether specifically identified as such or not.

[00160] All references (including, but not limited to, foreign and/or domestic publications, patents, and patent applications) cited herein, whether supra or infra, are hereby incorporated by reference in their entirety.

[00161] The terms and expressions that have been employed in the foregoing specification are used as terms of description and not of limitation, and are not intended to exclude equivalents of the features shown and described. While the above is a complete description of selected embodiments of the present invention, it is possible to practice the invention using various alternatives, modifications, adaptations, variations, and/or combinations and their equivalents. It will be appreciated by those of ordinary skill in the art that any arrangement that is calculated to achieve the same purpose may be substituted for the specific embodiment shown. It is also to be understood that the following claims are intended to cover all of the generic and specific features of the invention herein described and all statements of the scope of the invention that, as a matter of language, might be said to fall therebetween.

WHAT IS CLAIMED IS:

1. A method of payment processing, comprising:

at a device with one or more processors, memory, and two or more communication capabilities:

obtaining, from a payment module, an authorization request via a first communication capability;

sending, to a server, the authorization request via a second communication capability distinct from the first communication capability;

in response to sending the authorization request, obtaining, from the server, authorization information via the second communication capability;

after obtaining the authorization information, detecting a trigger condition to perform a transaction with a payment accepting unit associated with the payment module; and

in response to detecting the trigger condition, sending, to the payment module, at least a portion of the authorization information via the first communication capability.

2. The method of claim 1, wherein the first communication capability corresponds to a short-range communication protocol and the second communication capability corresponds to a long-range communication protocol.

3. The method of claim 1, further comprising:

obtaining, from the payment module, advertised information indicating the payment module's presence via the first communication capability that at least includes authorization zone threshold criterion.; and

after obtaining the advertised information, initiating a handshake process with the payment module, wherein the handshake process includes:

sending, to the payment module, device information at least including user identification information corresponding to the user of the device via the first communication capability; and

receiving, from the payment module, payment module information, wherein the payment module information at least includes an identifier corresponding to the payment module.

4. The method of claim 3, further comprising:

prior to obtaining the authorization request:

in accordance with a determination that the authorization zone threshold criterion is satisfied, sending notification information to the payment module via the first communication capability, wherein the notification information indicates that the authorization zone threshold criterion is satisfied;

wherein the device obtains the authorization request in response to sending the notification information.

5. The method of claim 3, wherein the payment module information further includes an indication that hands-free mode is available and payment zone threshold criterion.

6. The method of claim 5, wherein the device information further includes device identification information corresponding to a model type of the device; and

wherein the payment zone threshold criterion is based at least in part on the device identification information.

7. The method of claim 5, wherein detecting the trigger condition comprises:

determining whether the payment zone threshold criterion is satisfied; and

in accordance with a determination that the payment zone threshold criterion is satisfied, detecting the trigger condition without interaction from a user of the device.

8. The method of claim 1, wherein detecting the trigger condition comprises:

detecting a user input from a user of the device; and

in response to detecting the user input, detecting the trigger condition to perform a transaction with the payment accepting unit.

9. The method of claim 1, further comprising:

in response to obtaining the authorization information, presenting a notification to the user of the device that a connection has been established with the payment module.

10. The method of claim 9, wherein the notification further indicates an authorized amount for the transaction.

11. The method of claim 1, wherein the authorization information includes an identifier corresponding to the payment module, an identifier corresponding to the user of the device,

an authorized amount, an authorization grant token, and an expiration period for the authorization grant token.

12. The method of claim 11, wherein at least a portion of the authorization request and the authorization grant token are encrypted with a unique encryption key corresponding to the payment module.

13. A device, comprising:

two or more communication capabilities;

one or more processors; and

memory storing one or more programs to be executed by the one or more processors, the one or more programs comprising instructions for:

obtaining, from a payment module, an authorization request via a first communication capability;

sending, to a server, the authorization request via a second communication capability distinct from the first communication capability;

in response to sending the authorization request, obtaining, from the server, authorization information via the second communication capability;

after obtaining the authorization information, detecting a trigger condition to perform a transaction with a payment accepting unit associated with the payment module; and

in response to detecting the trigger condition, sending, to the payment module, at least a portion of the authorization information via the first communication capability.

14. The device of claim 13, wherein the first communication capability corresponds to a short-range communication protocol and the second communication capability corresponds to a long-range communication protocol.

15. The device of claim 13, wherein the one or more programs further comprise instructions for:

obtaining, from the payment module, advertised information indicating the payment module's presence via the first communication capability that at least includes authorization zone threshold criterion; and

after obtaining the advertised information, initiating a handshake process with the payment module, wherein the handshake process includes:

sending, to the payment module, device information at least including user identification information corresponding to the user of the device via the first communication capability; and

receiving, from the payment module, payment module information, wherein the payment module information at least includes an identifier corresponding to the payment module.

16. The device of claim 15, wherein the one or more programs further comprise instructions for:

prior to obtaining the authorization request:

in accordance with a determination that the authorization zone threshold criterion is satisfied, sending notification information to the payment module via the first communication capability, wherein the notification information indicates that the authorization zone threshold criterion is satisfied;

wherein the device obtains the authorization request in response to sending the notification information.

17. The device of claim 15, wherein the payment module information further includes an indication that hands-free mode is available and payment zone threshold criterion.

18. The device of claim 17, wherein the device information further includes device identification information corresponding to a model type of the device; and

wherein the payment zone threshold criterion is based at least in part on the device identification information.

19. The device of claim 17, wherein detecting the trigger condition comprises:

determining whether the payment zone threshold criterion is satisfied; and

in accordance with a determination that the payment zone threshold criterion is satisfied, detecting the trigger condition without interaction from a user of the device.

20. The device of claim 13, wherein detecting the trigger condition comprises:

detecting a user input from a user of the device; and

in response to detecting the user input, detecting the trigger condition to perform a transaction with the payment accepting unit.

21. A non-transitory computer readable storage medium storing one or more programs, the one or more programs comprising instructions, which, when executed by a device with one or more processors and two or more communication capabilities, cause the device to perform operations comprising:

obtaining, from a payment module, an authorization request via a first communication capability;

sending, to a server, the authorization request via a second communication capability distinct from the first communication capability;

in response to sending the authorization request, obtaining, from the server, authorization information via the second communication capability;

after obtaining the authorization information, detecting a trigger condition to perform a transaction with a payment accepting unit associated with the payment module; and

in response to detecting the trigger condition, sending, to the payment module, at least a portion of the authorization information via the first communication capability.

22. The non-transitory computer readable storage medium of claim 21, wherein the first communication capability corresponds to a short-range communication protocol and the second communication capability corresponds to a long-range communication protocol.

23. The non-transitory computer readable storage medium of claim 21, wherein the instructions cause the device to perform operations further comprising:

obtaining, from the payment module, advertised information indicating the payment module's presence via the first communication capability that at least includes authorization zone threshold criterion; and

after obtaining the advertised information, initiating a handshake process with the payment module, wherein the handshake process includes:

sending, to the payment module, device information at least including user identification information corresponding to the user of the device via the first communication capability; and

receiving, from the payment module, payment module information, wherein the payment module information at least includes an identifier corresponding to the payment module.

24. The non-transitory computer readable storage medium of claim 23, wherein the instructions cause the device to perform operations further comprising:

prior to obtaining the authorization request:

in accordance with a determination that the authorization zone threshold criterion is satisfied, sending notification information to the payment module via the first communication capability, wherein the notification information indicates that the authorization zone threshold criterion is satisfied;

wherein the device obtains the authorization request in response to sending the notification information.

25. The non-transitory computer readable storage medium of claim 23, wherein the payment module information further includes an indication that hands-free mode is available and payment zone threshold criterion.

26. The non-transitory computer readable storage medium of claim 25, wherein the device information further includes device identification information corresponding to a model type of the device; and

wherein the payment zone threshold criterion is based at least in part on the device identification information.

27. The non-transitory computer readable storage medium of claim 25, wherein detecting the trigger condition comprises:

determining whether the payment zone threshold criterion is satisfied; and

in accordance with a determination that the payment zone threshold criterion is satisfied, detecting the trigger condition without interaction from a user of the device.

28. The non-transitory computer readable storage medium of claim 21, wherein detecting the trigger condition comprises:

detecting a user input from a user of the device; and

in response to detecting the user input, detecting the trigger condition to perform a transaction with the payment accepting unit.

METHOD AND SYSTEM FOR PERFORMING MOBILE DEVICE-TO-MACHINE PAYMENTS

ABSTRACT OF THE DISCLOSURE

A device with one or more processors, memory, and two or more communication capabilities obtains, from a payment module, an authorization request via a first communication capability (e.g., Bluetooth). The device sends, to a server, the authorization request via a second communication capability distinct from the first communication capability (e.g., cellular or WiFi technology). In response to sending the authorization request, the device obtains, from the server, authorization information via the second communication capability. After obtaining the authorization information, the device detects a trigger condition to perform a transaction with a payment accepting unit associated with the payment module. In response to detecting the trigger condition, the device sends, to the payment module, at least a portion of the authorization information via the first communication capability.

METHOD AND SYSTEM FOR PERFORMING MOBILE DEVICE-TO-MACHINE PAYMENTS

PRIORITY CLAIM

[0001] The present application is an continuation of U.S. Patent Application Number 14/214,644, filed March 14, 2014, which claims priority to U.S. Provisional Patent Application Number 61/917,936, filed December 18, 2013, and is a continuation-in-part of U.S. Design Patent Application Number 29/477,025, filed December 18, 2013. The present application is based on and claims priority from these applications, the disclosures of which are hereby expressly incorporated herein by reference.

BACKGROUND OF THE INVENTION

[0002] Disclosed herein are mobile-device-to-machine payment systems and, more specifically, mobile-device-to-machine payment systems over a non-persistent network connection and featuring hands-free and manual modes.

[0003] Vending machines (or "automatic retailing" machines), in the broadest sense, have been around for thousands of years. The first simple mechanical coin operated vending machines were introduced in the 1880s. Modern vending machines stock many different types of products including, but not limited to drinks (e.g. water, juice, coffee, and soda) and edible food products/items (e.g. snacks, candy, fruit, and frozen meals), as well as a wide variety of non-food items. In this fast paced world, vending machines are ubiquitous.

[0004] Vending machines are one type of "payment accepting unit" (payment accepting units are also referred to herein generically as "machines"). A payment accepting unit (or machine) is equipment that requires payment for the dispensing of products and/or services. In addition to vending machines, payment accepting units can also be other machines that require payment for the dispensing of a product and/or services including, but not limited to parking meters, toll booths, laundromat washers and dryers, arcade games, kiosks, photo booths, toll booths, transit ticket dispensing machines, and other known or yet to be discovered payment accepting units.

[0005] In using a payment accepting unit, a user will (1) approach the payment accepting unit, (2) determine from the face of the payment accepting unit the product (or service) he desires, (3) insert payment (e.g. coins, bills, or payment cards), and (4) input his

selection into the payment accepting unit using a user interface (e.g. a series of buttons, a key pad, touch screen, or other input mechanism using, for example, the column and row at which a product is located). Based on the user's inputted selection, technology within the payment accepting unit provides the desired product (or service) to the user.

[0006] As the number of people with internet-connected mobile devices proliferates, so does the variety of uses for such devices. Mobile payment is a logical extension.

[0007] There is a large development effort around bringing mobile payment to the retail sector in an effort to not only provide options to the user, but also increased convenience.

[0008] In recent years, many improvements to modern vending machines have been suggested. Many of the innovations relate to means for communicating with the vending machine. Some of these communication innovations are detailed in U.S. Patent No. 6,584,309 to Whigham (the "Whigham reference"), U.S. Patent No. 7,085,556 to Offer (the "Offer reference"), U.S. Patent No. 7,127,236 to Khan et al. (the "Khan reference"), U.S. Patent No. 7,721,958 to Belfer et al. (the "Belfer reference"), U.S. Patent No. 8,396,589 to Katzenstein Garibaldi et al. (the "Garibaldi reference"), U.S. Patent No. 8,489,140 to Weiner et al. (the "Weiner reference"), and International Publication No. WO/2008/083025 to Carlson (the "Carlson reference").

[0009] The Whigham reference is directed to a system and method for purchasing a product from an automatic vending machine by means of a consumer's cellular telephone. The consumer requests a product available from the vending machine by dialing a specified telephone number that connects the consumer's cellular telephone to a server operated by a billing agency. The server recognizes the request for the product, creates a transaction record, and communicates a vend code to the consumer. Upon receiving the vend code from the server, the consumer transmits the vend code to the vending machine. The vend code may be an RF code, an audible tone code, or a manual code. Upon receipt of the vend code from the consumer, the vending machine dispenses the requested product.

[0010] The Offer reference is directed to a vending machine that is designed to communicate with a cellular phone such that it dispenses a product when it receives information indicating that the product has been selected. The Offer reference teaches permitting the cashless utilization of a vending machines via a communications service, such as a cellular telephone. A response to a signal from the cellular telephone from

[0011] the vending machine that indicates that a connection has been established between the vending machine and the cellular phone may be a visual indication that is displayed on the cellular telephone. The vending machine outputs the cost of the product and that cost is debited from an account to pay for the product.

[0012] The Khan reference describes a point of sale MicroAdapter device that enables payment transactions to be effected through a purchaser's personal trusted device (e.g. the user selecting the micropayment application on his personal trusted device and confirming or cancelling the purchase thereon) without relying upon tokens or prepayment cards. In one embodiment, the MicroAdapter includes a transceiver configured to receive a purchase signal from the personal trusted device including order and payment information. In response, the MicroAdapter communicates via wireless telephony with a transaction authorizer to receive authorization for effectuating the purchase transaction. The MicroAdapter can effectuate micropayment transactions authorized by a Billing On Behalf of Others program administered through a wireless carrier/ISP or third party.

[0013] The Belfer reference is directed to a system wherein a vending machine has an audio code collector and a code validator that is adapted to receive audio tones from a mobile device. The audio tones include authentication codes and dispense codes to control dispensing of product from the vending machine. To start the transaction, the consumer dials a unique set of symbols and digits to route the call to a verification server. The symbols and digits may correspond to a unique vending machine identification number and product identification numbers.

[0014] The Garibaldi reference is directed to an electronic device for the sale of intangible products through vending machines that include interfaces to communicate with external peripherals through the MDB protocol, the RS232 standard, and the DEX protocol, an interface to communicate with users, a communications system that enables it to act as part of a network and communicate with a central system, and a controller, that articulates the communication among the above-mentioned components, so as to enable a central system to perform diverse actions on a vending machine.

[0015] The Weiner reference is directed to a system and method for providing product or service with a cellular telephone. The problem identified in the Weiner reference is that mobile communication devices are long-range electronic devices designed to be used for long-range communications. Eschewing the use of near- field communication because it

requires special design or modification of the mobile station (e.g. the vending machine), the Weiner reference teaches a mobile communication device identifier, consisting of: a shielding defining a coverage area, the shielding arranged to reduce radio signals originating externally of the coverage area to be less than a pre-determined signal strength; an antenna associated within the defined coverage area; a transceiver coupled to the antenna, the transceiver communicating with a mobile station inserted within the defined coverage area utilizing a signal strength greater than the pre-determined signal strength; and a service control unit responsive to the transceiver, the service control unit responsive to the communication to output a signal indicative of an authorization to provide a product or service.

[0016] The Carlson reference is directed to a system and a method for using a portable consumer device such as a mobile phone for payments and the like. One embodiment of the Carlson system is directed to a method that includes the steps of receiving a payment request message (that includes a request to pay for a product from a vending machine) from a portable consumer device operated by a consumer, sending an authorization response message back to the vending machine wherein the vending machine subsequently prompts the consumer to enter a selection if the authorization response message indicates that the consumer is authorized to make a purchase, and receiving an acknowledgement message from the vending machine that the product was purchased. The step of "sending an authorization response message back to the vending machine" is performed by a remote payment server and would require a persistent network connection.

BRIEF SUMMARY OF THE INVENTION

[0017] Disclosed herein are mobile-device-to-machine payment systems and, more specifically, mobile-device-to-machine payment systems over a non-persistent network connection and featuring hands-free and manual modes.

[0018] Described herein is a mobile-device-to-machine payment system for facilitating a cashless transaction for purchase of at least one product or service by a user from a payment accepting unit that preferably has input mechanisms. The user has a mobile device that has both short-range communication technology and long-range communication technology. The payment accepting unit is capable of dispensing at least one product or service. The system includes an adapter module and a server. The adapter module is associated with the payment accepting unit and has short-range communication technology

for communicating with the short-range communication technology of the mobile device. The server has long-range communication technology for communicating with the long-range communication technology of the mobile device. The adapter module is for sending an authorization request for funds to the mobile device using short-range communication technology. The mobile device then forwards the authorization request for funds to the server using long-range communication technology. The server is for sending an authorization grant for funds to the mobile device using long-range communication technology. The mobile device the forwards the authorization grant for funds to the adapter module using short-range communication technology. The payment accepting unit dispenses the at least one product or service in response to receiving user input to the payment accepting unit input mechanism if the adapter module has received the authorization grant.

[0019] The adapter module may have security technology and the server may have security technology. The authorization request may be secured by the adapter module security technology to create a secured authorization request. The authorization grant may be secured by the server security technology to create a secured authorization grant. The secured authorization request and the secured authorization grant are preferably undecipherable to the mobile device.

[0020] The adapter module and the server may share a unique private key. The adapter module may have encryption/decryption technology and the server may have encryption/decryption technology. The authorization request may be encrypted by the adapter module encryption/decryption technology using the unique private key to create an encrypted authorization request. The encrypted authorization request may be decrypted by the server encryption/decryption technology using the unique private key. The authorization grant may be encrypted by the server encryption/decryption technology using the unique private key to create an encrypted authorization grant. The encrypted authorization grant may be decrypted by the adapter module encryption/decryption technology using the unique private key. The encrypted authorization request and the encrypted authorization grant are preferably undecipherable to the mobile device.

[0021] The adapter module is preferably surrounded by two zones, a payment zone and an authorization zone, wherein the payment zone is within the authorization zone. The adapter module sends the authorization request when the mobile device is within the authorization zone. The mobile device forwards the authorization grant for funds to the adapter module when the mobile device is within the payment zone. A third zone possible

zone is a communication zone, the authorization zone being within the communication zone. The mobile device preferably receives advertising broadcast signals from the adapter module within the communication zone.

[0022] The system may have a hands-free mode in which the payment accepting unit dispenses the at least one product or service without the user interacting with the mobile device. A display of the payment accepting unit may be used for displaying funds available based on information from the authorization grant. The input mechanisms of the payment accepting unit may be used for receiving user selection input when the user interacts with the input mechanisms to select the at least one product or service to be dispensed.

[0023] The adapter module may be an in-line dongle for in-line insertion within a multi-drop bus of the payment accepting unit. Further, the payment accepting unit may have a multi-drop bus to a payment receiving mechanism. The multi-drop bus may have a male adapter and a female adapter. The adapter module may have a male adapter and a female adapter. The adapter module is preferably insertable in serial with the multi-drop bus by connecting the male adapter of the adapter module to the female adapter of the multi-drop bus and by connecting the female adapter of the adapter module to the male adapter of the multi-drop bus.

[0024] Also described herein is a method for using a mobile-device-to-machine payment system for facilitating a cashless transaction for purchase of at least one product or service by a user from a payment accepting unit may have input mechanisms. The user may have a mobile device having both short-range communication technology and long-range communication technology. The payment accepting unit is preferably capable of dispensing at least one product or service. The method includes the steps of: (a) sending an authorization request for funds to the mobile device using short-range communication technology of an adapter module associated with the payment accepting unit; (b) receiving the authorization request for funds from the short-range communication technology of the adapter module at the short-range communication technology of the mobile device; (c) forwarding the authorization request for funds to a server using the long-range communication technology of the mobile device; (d) receiving the authorization request for funds from the long-range communication technology of the mobile device at long-range communication technology of the server; (e) sending an authorization grant for funds to the mobile device using the long-range communication technology of the server; (f) receiving the authorization grant for funds from long-range communication technology of the server at the

long-range communication technology of the mobile device; (g) forwarding the authorization grant for funds to the adapter module using the short-range communication technology of the mobile device; and (h) receiving the authorization grant for funds from the short-range communication technology of the mobile device at short-range communication technology of the adapter module. At least one product or service may then be dispensed from the payment accepting unit in response to receiving user input to the payment accepting unit input mechanism if the adapter module has received the authorization grant.

[0025] The method may include the steps of securing the authorization request using security technology associated with the adapter module to create a secured authorization request, securing the authorization grant using security technology associated with the server to create a secured authorization grant, and the secured authorization request and the secured authorization grant are preferably undecipherable to the mobile device.

[0026] The method may include the steps of (a) sharing a unique private key between the adapter module and the server, (b) encrypting using the unique private key the authorization request using encryption/decryption technology associated with the adapter module to create an encrypted authorization request, (c) decrypting using the unique private key the encrypted authorization request using encryption/decryption technology associated with the server, (d) encrypting using the unique private key the authorization grant using the encryption/decryption technology associated with the server to create an encrypted authorization grant, (e) decrypting using the unique private key the encrypted authorization grant using encryption/decryption technology associated with the adapter module, and (e) the encrypted authorization request and the encrypted authorization grant are preferably undecipherable to the mobile device.

[0027] The method may include the steps of (a) surrounding the adapter module with two zones, a payment zone and an authorization zone, wherein the payment zone is within the authorization zone, (b) the adapter module sending the authorization request when the mobile device is within the authorization zone; and (c) the mobile device forwarding the authorization grant for funds to the adapter module when the mobile device is within the payment zone. The adapter module may also include a third zone, a communication zone, wherein the authorization zone is within the communication zone. The mobile device receives advertising broadcast signals from the adapter module within the communication zone.

[0028] The method may have a hands-free mode in which the payment accepting unit dispenses the at least one product or service without the user interacting with the mobile device. The method may further include the steps of (a) displaying funds available on a display of the payment accepting unit, the funds available may be based on information from the authorization grant; and (b) receiving user selection input when the user interacts with input mechanisms of the payment accepting unit to select the at least one product or service to be dispensed.

[0029] The method may include the step of inserting the adapter module as an in-line dongle for in-line insertion within a multi-drop bus of the payment accepting unit. The method may include the step of inserting the adapter module in serial with the multi-drop bus by connecting a male adapter of the adapter module to a female adapter of the multi-drop bus and by connecting a female adapter of the adapter module to a male adapter of the multi-drop bus.

[0030] The subject matter described herein is particularly pointed out and distinctly claimed in the concluding portion of this specification. Objectives, features, combinations, and advantages described and implied herein will be more readily understood upon consideration of the following detailed description of the invention, taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

[0031] FIG. 1 is a schematic diagram that shows three zones: a first "communication zone" (e.g. "Bluetooth range"), a second "authorization zone," and a third "payment zone." The payment zone (that can't be zero) is smaller than or equal to (overlapping completely) the authorization zone.

[0032] FIG. 2 is a schematic diagram that shows the three zone of FIG. 1 with multiple users therein, the mobile-device-to-machine payment systems providing for managing and resolving multiple users.

[0033] FIG. 3 is a table that illustrates the hands-free credit or alert user principle.

[0034] FIG. 4 is a flow chart showing the logging RSSI at User Input.

[0035] FIG. 5 is a block schematic that shows elements of the system including, but not limited to, the adapter module, the machine, the mobile device, and exemplary servers, as well as communications therebetween.

[0036] FIG. 6 is a block schematic that shows there are three areas of encryption used (each is bi-directional) between the adapter module, the machine, the mobile device, and/or exemplary servers.

[0037] FIG. 7 is a block diagram that communications, messaging, vending sequence, and purchase flow between the adapter module, the mobile device, and a system management server.

[0038] FIG. 8A is a timing schematic diagram that shows additional elements and features of the system including, but not limited to, communications medium, messaging, vending sequence, and purchase flow, when the user enters the communication zone (Bluetooth Range).

[0039] FIG. 8B is a timing schematic diagram that shows additional elements and features of the system including, but not limited to, communications medium, messaging, vending sequence, and purchase flow, when the user enters the Authorization Zone.

[0040] FIG. 8C is a timing schematic diagram that shows additional elements and features of the system including, but not limited to, communications medium, messaging, vending sequence, and purchase flow, when the user enters the Payment Zone and, in particular, detailing the hands-free mode alternative and the swipe mode alternative.

[0041] FIG. 8D is a timing schematic diagram that shows additional elements and features of the system including, but not limited to, communications medium, messaging, vending sequence, and purchase flow, in a vending transaction including a loop for multiple transactions.

[0042] FIG. 8E is a timing schematic diagram that shows additional elements and features of the system including, but not limited to, communications medium, messaging, vending sequence, and purchase flow, in the Login mode.

[0043] FIG. 8F is a timing schematic diagram that shows additional elements and features of the system including, but not limited to, communications medium, messaging, vending sequence, and purchase flow, during Module bootup.

[0044] FIG. 8G is a timing schematic diagram that shows additional elements and features of the system including, but not limited to, communications medium, messaging, vending sequence, and purchase flow, during Account Check/Update.

[0045] FIGS. 9A - 9E are flow charts that show exemplary steps and features of the system including, but not limited to, communications, messaging, vending sequence, and purchase flow.

[0046] FIGS. 10A - 10D show an exemplary mobile device with a graphical representation of an exemplary mobile application shown thereon, the mobile application being used as part of the mobile-device-to-machine payment systems.

[0047] FIG. 11 is a perspective view of the exemplary first preferred in-line dongle adapter module.

[0048] FIG. 12 is a front plan view of the in-line dongle adapter module of FIG. 11.

[0049] FIG. 13 is a back plan view of the in-line dongle adapter module of FIG. 11.

[0049.1] FIG. 14 is a side view of the in-line dongle adapter module of FIG. 11 in accordance with some implementations.

[0050] FIG. 15 is a first end view of a connector receptacle of the in-line dongle adapter module of FIG. 11.

[0051] FIG. 16 is a second end view of a connector receptacle of the in-line dongle adapter module of FIG 11.

[0052] FIG. 17 is a perspective view taken from the first end of the in-line dongle adapter module of FIG. 11, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for environmental purposes.

[0053] FIG. 18 is a perspective view taken from the second end of the in-line dongle adapter module of FIG. 11, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for environmental purposes.

[0054] FIG. 19 is a perspective view of the in-line dongle adapter module of FIG. 11 within a vending machine.

[0055] FIG. 20 is a perspective view of the exemplary second preferred in-line dongle adapter module.

[0056] FIG. 21 is a front plan view of the in-line dongle adapter module of FIG. 20.

[0057] FIG. 22 is a back plan view of the in-line dongle adapter module of FIG. 20.

[0058] FIG. 23 is a first side view of the in-line dongle adapter module of FIG. 20, the second side being a mirror image of that shown.

[0059] FIG. 24 is a first end view of a connector receptacle of the in-line dongle adapter module of FIG. 20.

[0060] FIG. 25 is a second end view of a connector receptacle of the in-line dongle adapter module of FIG 20.

[0061] FIG. 26 is a perspective view taken from the first end of the in-line dongle adapter module of FIG. 20, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for environmental purposes.

[0062] FIG. 27 is a perspective view taken from the second end of the in-line dongle adapter module of FIG. 20, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for environmental purposes.

[0063] FIG. 28 is a perspective view of the in-line dongle adapter module of FIG. 20 within a vending machine.

[0064] FIG. 29 is a perspective view of the exemplary third preferred in-line dongle adapter module with a gap indicating the in-line dongle adapter module can be of any length.

[0065] FIG. 30 is a front plan view of the in-line dongle adapter module of FIG. 29.

[0066] FIG. 31 is a back plan view of the in-line dongle adapter module of FIG. 29.

[0067] FIG. 32 is a first side view of the in-line dongle adapter module of FIG. 29, the second side being a mirror image of that shown.

[0068] FIG. 33 is a first end view of a connector receptacle of the in-line dongle adapter module of FIG. 29.

[0069] FIG. 34 is a second end view of a connector receptacle of the in-line dongle adapter module of FIG. 29.

[0070] FIG. 35 is a perspective view taken from the first end of the in-line dongle adapter module of FIG. 29, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for environmental purposes.

[0071] FIG. 36 is a perspective view taken from the second end of the in-line dongle adapter module of FIG. 29, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for environmental purposes.

[0072] FIG. 37 is a perspective view of the in-line dongle adapter module of FIG. 29 within a vending machine.

[0073] FIG. 38 is a perspective view of the exemplary fourth preferred in-line dongle adapter module with two vertical gaps indicating the in-line dongle adapter module can be of any width.

[0074] FIG. 39 is a front plan view of the in-line dongle adapter module of FIG. 38.

[0075] FIG. 40 is a back plan view of the in-line dongle adapter module of FIG. 38.

[0076] FIG. 41 is a first side view of the in-line dongle adapter module of FIG. 38, the second side being a mirror image of that shown.

[0077] FIG. 42 is a first end view of a connector receptacle of the in-line dongle adapter module of FIG. 38.

[0078] FIG. 43 is a second end view of a connector receptacle of the in-line dongle adapter module of FIG 38.

[0079] FIG. 44 is a perspective view taken from the first end of the in-line dongle adapter module of FIG. 38, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for environmental purposes.

[0080] FIG. 45 is a perspective view taken from the second end of the in-line dongle adapter module of FIG. 38, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for environmental purposes.

[0081] FIG. 46 is a perspective view of the in-line dongle adapter module of FIG. 38 within a vending machine.

[0082] FIG. 47 is a perspective view of the exemplary fifth preferred in-line dongle adapter module and, specifically, the longitudinal center portion thereof, the dashed line depiction of the sides indicating the sides of the in-line dongle adapter module can be of any shape or curvature.

[0083] FIG. 48 is a front plan view of the in-line dongle adapter module of FIG. 47.

[0084] FIG. 49 is a back plan view of the in-line dongle adapter module of FIG. 47.

[0084.1] FIG. 50 is a side view of the in-line dongle adapter module of FIG. 47 in accordance with some implementations.

[0085] FIG. 51 is a first end view of a connector receptacle of the in-line dongle adapter module of FIG. 47.

[0086] FIG. 52 is a second end view of a connector receptacle of the in-line dongle adapter module of FIG 47.

[0087] FIG. 53 is a perspective view taken from the first end of the in-line dongle adapter module of FIG. 47, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for environmental purposes.

[0088] FIG. 54 is a perspective view taken from the second end of the in-line dongle adapter module of FIG. 47, the connectors and cables between which the in-line dongle adapter module is inserted being shown in broken lines for environmental purposes.

[0089] FIG. 55 is a perspective view of the in-line dongle adapter module of FIG. 47 within a vending machine.

[0090] FIG. 56 is a block diagram of an exemplary adapter module.

[0091] FIG. 57 is a block diagram of an exemplary mobile device.

[0092] FIG. 58 is a block diagram of an exemplary server.

DETAILED DESCRIPTION OF THE INVENTION

[0093] Disclosed herein are mobile-device-to-machine payment systems and, more specifically, mobile-device-to-machine payment systems over a non-persistent network connection. The mobile-device-to-machine payment systems disclosed herein focus on the unattended retail space (e.g. a payment accepting unit 120 or machine 120). More specifically, mobile-device-to-machine payment systems disclosed herein allow a user (having a mobile device 150 with a mobile application 140 thereon) to make a cashless purchase from a payment accepting unit 120 (having an adapter module 100 associated therewith).

[0094] The mobile-device-to-machine payment systems described herein can be implemented with one or more of the following features: easy installation feature, a non-persistent network connection feature; a manual (swipe to pay) mode feature; a hands-free mode feature; and a multiple vending transactions (multi-vend) feature.

[0095] Easy Installation: Installation is very easy, requires no tools, requires no configuration, and takes as little as 30 seconds. This is accomplished by using an adapter

module 100 such as an in-line dongle (a hardware device with software thereon) design for in-line insertion within a multi-drop bus (MDB) of a payment accepting unit (e.g. a vending machine). Installation is as simple as "powering down" (turning off) the machine 120, identifying the "wire" that connects with a payment receiving mechanism (e.g. the coin mechanism), disconnecting the wire (so that there are two loose ends, such as a male connection end or adapter of an MDB and a female connection end or adapter of an MDB), plugging (inserting) the adapter module 100 in serial ("in-line") with the wire (for example, connecting the MDB female adapter to a male adapter of the adapter module 100 and connecting the MDB male adapter to a female adapter of the adapter module 100), tucking the wire and the installed adapter module 100 back into position, and "powering up" (turning on) the machine 120. Most vending machines made since 1995 have this industry standard MDB technology that would allow this easy 30-second installation. On machines without MDB technology, the adapter module 100 can be configured or designed to work with other serial protocols or activate a switch. In essence the adapter module 100 simulates establishing payment on payment accepting unit 120 in much the same manner as other alternative forms of payment (e.g. cash).

[0096] Non-persistent Network Connection: Although payment accepting units (or "machines") that accept only cash (e.g. paper currency and coins) may not require a connection (persistent or non-persistent) to a network, traditional payment accepting units that accept cashless payments (e.g. credit cards, debit cards, and alternative mobile device payment methods using, for example, smart phones) require a persistent connection to a network (wired or wireless) to facilitate the cashless payments. In other words, without a persistent (ongoing or accessible on demand) network connection, traditional payment accepting units cannot accept cashless payments. Most traditional payment accepting units that accept cashless payments include the technology to accomplish this persistent network connection that allows them to connect to a remote server. If the network connection to a traditional machine is temporarily interrupted, cashless payments will be temporarily unavailable. If the machine is located in a location where no signal is available, cashless payments will not be possible. The Whigham reference, the Offer reference, and the Belfer reference disclose alternative payment accepting units that accept cashless payments by using the user's cellular phone to allow the user to manually input coding to a remote server and, thereby act as an on-demand bridge network connection. These references, however, require significant user interaction with the cellular telephone to effectuate the transaction. In

addition to using a mobile device 150 as an intermediary between the payment accepting units 120 and the server 130, mobile-device-to-machine payment systems described herein minimize (manual mode) or eliminate (hands-free mode) user interaction with the mobile device 150. Further, some mobile-device-to-machine payment systems described herein facilitate the acceptance of cashless payments without requiring any network connection near the payment accepting unit 120. Mobile-device-to-machine payment systems described herein that are located in a remote location where no signal is available, therefore, can accept cashless payments.

[0097] Manual (Swipe to Pay) Mode: Using a "swipe to pay" feature (or just "swipe") refers to a user's action implemented on his mobile device 150 in which he quickly brushes his finger (or other pre-determined interaction) on the mobile device's touch screen 152 (or other input device associated with the mobile device 150). From the user's perspective, when the user is within range, a pre-installed mobile application 140 automatically connects to the payment accepting unit 120 (e.g. a vending machine). The mobile application 140 might display (on the touch screen 152) a prepaid balance that the user "swipes" to transfer payment to the payment accepting unit 120. The user could observe the transferred funds on the touch screen 152 of the mobile device 150 and/or on the display 122, 124 of the payment accepting unit 120. The transaction is completed just as if cash was inserted in the machine 120 with the user inputting his selection on the payment accepting unit 120 and the payment accepting unit 120 dispensing the product or service. After the selection is made, the change is returned to the mobile device 150 and this may be shown on the touch screen 152 of the mobile device 150.

[0098] Hands-Free Mode: A "hands-free pay" feature (or just "hands-free") would most likely be used with "favorite" payment accepting units 120 (e.g. a vending machine at work or school). From the user's perspective, he would approach the favorite payment accepting unit 120 and notice that the display 122, 124 of the payment accepting unit 120 showed funds available, he would select the product or service using the payment accepting unit's input mechanisms (e.g. buttons 126 or a touch screen display 124 shown in FIG. 19), and he would retrieve his dispensed services or products. It would be that simple. More specifically, when the user is within range, a pre-installed mobile application 140 automatically connects to the payment accepting unit 120 (e.g. a vending machine). The user may leave the mobile device 150 in a pocket, purse, briefcase, backpack, or other carrier. As the user approaches the payment accepting unit 120 and is in approximately "arms-length"

distance (e.g. 3 to 5 feet), the user could observe the transferred funds on the display 122, 124 of the payment accepting unit 120. The transaction is completed just as if cash was inserted in the machine 120 with the user inputting his selection on the payment accepting unit 120 and the payment accepting unit 120 dispensing the product or service. After the selection is made, the change is returned to the mobile device 150. FIG. 3 details when the hands-free mode would be available.

[0099] Multiple Vending Transactions (Multi-Vend): Both the "swipe to pay" feature and the "hands-free pay" feature could be used multiple times in sequence (implemented, for example, as a loop) so that a user may make multiple purchases. After making his first selection and receiving his product (or service), the user would observe that additional funds were available on the display 122, 124 on the payment accepting unit 120. He could make another selection (or multiple selections) and receive additional product(s) (or service(s)). More specifically, the display 122, 124 may reset as if the transaction is complete, but then, because the user is still standing in range, the mobile application 140 would send another credit to the payment accepting unit 120, allowing for a second purchase. When the walks away, the system clears (e.g. returns unused funds to the mobile application 140 on the mobile device 150.

[00100] The features described above, alone or in combination with other features described herein will revolutionize the hundred billion dollar automated retail industry. The exemplary hardware is very low cost and there are no reoccurring fees because no cellular connection is required on the machine 120. Using the mobile-device-to-machine payment systems described herein, operators can increase frequency of visits and items sold with each visit.

[00101] Mobile-device-to-machine payment systems described herein may be implemented as an apparatus and/or method for enabling payments to a machine 120 via a mobile device 150. Exemplary mobile-device-to-machine payment systems may be better understood with reference to the drawings, but the shown mobile-device-to-machine payment systems are not intended to be of a limiting nature.

Definitions

[00102] Before describing the mobile-device-to-machine payment systems and the figures, some of the terminology should be clarified. Please note that the terms and phrases may have additional definitions and/or examples throughout the specification. Where

otherwise not specifically defined, words, phrases, and acronyms are given their ordinary meaning in the art. The following paragraphs provide some of the definitions for terms and phrases used herein.

- Adapter Module 100: As shown in FIGS. 1 and 2, the adapter module 100 is a physical device that is installed in a machine 120 (a payment accepting unit 120). The shown exemplary adapter module 100 is an in-line dongle (a hardware device with software thereon) device that may be inserted in-line within a multi-drop bus (MDB) of a machine 120. The adapter module 100 bridges the communication between the machine 120 and a mobile device 150. Although described as a unique component, it should be noted that the adapter module 100 could be implemented as a plurality of devices or integrated into other devices (e.g. components of a machine 120). In its unique component form, the adapter module 100 can be easily inserted into a machine 120 so that the machine 120 is able to perform new features with the assistance of the adapter module 100. FIG. 56 shows exemplary components associated with the adapter module 100. The shown example may be divided into multiple distinct components that are associated with each other or the example may be incorporated into or drawn from other technology (e.g. a computer or a payment accepting unit) as long as the components are associated with each other.

- Mobile Device 150 and Application 140 (also referred to as a "mobile application," "mobile app," or "app"): In general, a mobile device 150 may be a user's personal mobile device 150. The mobile device 150 (with a mobile application 140 thereon) acts as a communication bridge between the adapter module 100 (associated with a payment accepting unit 120) and the server 130. The mobile device 150 and application 140, however, are not "trusted" in that the communications (transmissions) it passes are encrypted. Encrypted (secured) communications are undecipherable (unencryptable, unreadable, and/or unuseable) by the mobile device 150. This keeps the passed communications secured and safe from hacking. Exemplary mobile devices include, but are not limited to smart phones, tablet or laptop computers, or personal digital assistants (PDAs), smart cards, or other technology (e.g. a hardware-software combination) known or yet to be discovered that has

structure and/or capabilities similar to the mobile devices described herein. The mobile device 150 preferably has an application 140 (app 140) running on it. The term "app" is used broadly to include any software program(s) capable of implementing the features described herein. FIGS. 10A-10D show exemplary mobile devices 150 with associated apps 140 associated therewith. It should be noted that the phrase "mobile device" can be assumed to include the relevant app unless specifically stated otherwise. Similarly, it should be noted that an "app" can be assumed to be running on an associated mobile device unless specifically stated otherwise. FIG. 57 shows exemplary components associated with the mobile device 150. The shown example may be divided into multiple distinct components that are associated with each other or the example may be incorporated into or drawn from other technology (e.g. the cell phone itself) as long as the components are associated with each other.

- Payment Accepting Unit 120 (or Machine 120): A payment accepting unit 120 (or machine 120) is equipment that requires payment for the dispensing of an product and/or service. Payment accepting units 120 may be vending machines, parking meters, toll booths, laundromat washers and dryers, arcade games, kiosks, photo booths, toll booths, transit ticket dispensing machines, and other known or yet to be discovered payment accepting units 120. Some payment accepting units 120 can accept cashless payments (payments other than cash (paper currency and coins)) by accepting payment from, for example, credit cards, debit cards, and mobile devices.
- Network Connections: For purposes of this discussion, a persistent network connection is a wired or wireless communications connection that is ongoing (e.g. a dedicated connection, a dedicated online connection, and/or a hardwired connection) or accessible on demand (e.g. the ability for the machine to make a temporary connection to a server or the ability for the user to contact a server from his mobile device). Typically the persistent network connection has been conducted over "long-range communication technology" (e.g. hardwired, telephone network technology, cellular technology, WiFi technology, wide area network (WAN), local area network (LAN), or any wired or wireless communication technology over the internet that is known or

yet to be discovered). Traditionally, machines that accept payment other than cash require a persistent (ongoing or accessible on demand) connection to a network to facilitate payment. This is true for machines that accept, for example, credit cards and debit cards. The payment accepting units 120 described herein do not require a traditional persistent network connection. The user's mobile device 150 acts as a communication bridge between the adapter module 100 and the server 130. Communications between user mobile devices 150 and the servers (e.g. a system management server 130 and/or a funding source server 160) take place using long-range communication technology. Communications between user mobile devices 150 and the adapter module 100 of the payment accepting unit 120 take place using "short-range communication technology" (e.g. Bluetooth (e.g. Bluetooth 4.0, Bluetooth Smart, Bluetooth LE (Low Energy), near-field communication, Ultra Wideband (UWB), RFID, infrared wireless, induction wireless, or any wired or wireless technology that could be used to communicate a small distance (e.g. approximately a hundred feet or closer) that is known or yet to be discovered). Neither the adapter module 100 nor the payment accepting unit 120, therefore require a traditional persistent long-range wireless network connection. The exemplary communications technology shown in the figures may be replaced with alternative like communications technology and, therefore, specific shown communications technologies are not meant to be limiting. For example WiFi technology could be replaced with another long-range communication technology.

- Server: A server is the host processing server that may be operated by the company running the system. For each user, the server 130 preferably maintains at least one "virtual wallet" having at least one "balance" (which can be $0) of designated funds for which the server 130 keeps an accounting. The balance may represent, for example, "cash" or it may be a "promotional value" that represents funds that may be spent under certain circumstances. If these funds begin to be depleted, the user may be notified (e.g. via the application 140 on the mobile device 150) that additional funds need to be designated and/or transferred. Alternatively, funds from other sources (e.g. the funding source server 160) may be automatically transferred to restore a

predetermined balance. The balance may also be increased based on a promotion (e.g. points earned or coupons). As shown in FIG. 58, the server includes appropriate processors 950, memory 960 (which would keep an accounting of the user's balance in a manner similar to a gift card), and communication systems 970. As shown, the communications unit 970 of the server 130 includes long-range communication technology (e.g. cellular technology and WiFi mechanisms). The server 130 also includes a security unit 955 for encrypting and decrypting messages. The server 130 receives an AuthRequest from the adapter module 100 (via a mobile device 150) and, if funds are available, returns the AuthGrant for funds. FIG. 58 shows exemplary components associated with the server 130. The shown example may be divided into multiple distinct components that are associated with each other or the example may be incorporated into or drawn from other technology (e.g. a computer or a main frame) as long as the components are associated with each other.

- Advertise Presence: Each adapter module 100 advertises its presence by broadcasting signals (advertising broadcast signals) to mobile devices in the zones 102, 104, 016. Each adapter module 100 can listen to other adapter modules' advertisements

- Received Signal Strength Indicator (RSSI): The adapter module 100 may have a self-calibrating signal strength to determine zone thresholds (e.g. a payment zone threshold). At the time the user selects an item (product or service) from the payment accepting unit 120, the Received Signal Strength Indicator (RSSI) is logged. At this moment, it is presumed the user is within "arms-length" (which may be a predetermined length approximating the distance of a user standing in front of a machine for the purpose of making a purchase) from the payment accepting unit 120. Mathematical computation (In-Range Heuristics) is conducted to derive the optimal RSSI threshold at which point payment should be triggered by an application 140 on a mobile device 150. The threshold may be payment accepting unit specific and can vary over a period of time. This optimal zone threshold is preferably reported to the mobile device 150 during an initial handshake.

- In-Range Heuristics: Mathematical computation that determines the RSSI threshold to determine when a user is in the authorization zone 104 and/or payment zone 102. This computation can take into consideration numerous historical data points as well as transaction specific information such as which mobile device 150 is being used, payment accepting unit type, among other factors. Preferably the RSSI is logged while the user is making his selection (this is the one time in the entire process that the user definitely will be "in range" (e.g. they will be arm's length from the machine 120 because they are physically interacting with the machine 120). The type of user mobile device 150, accelerometer data (e.g. is the user moving or stationary), and/or other information may also be logged while the user is making his selection. The adapter module 100 can give a reference RSSI for the payment zone 102 for the machine 120, and the application 140 can make a +/- adjustment based on the specific mobile device 150 on which it is installed. Over a period of time, the system continues to improve itself based on additional data points.

- Authorization Request (AuthRequest): When a user enters the authorization zone 104, the mobile device 150 notifies the adapter module 100 and the adapter module 100 sends the secured authorization request (e.g. the encrypted authorization request) as a "message" (also referred to as a communication or transmissions) to the server 130 via the mobile device 150. Encryption may be performed by a security unit 755 (security technology that may be associated with the processing unit 750 and/or the memory 760). Significantly, the AuthRequest is a request for authorization of funds, not a request for authorization of a transaction. The purpose of the funds is irrelevant to the server 30.

- Authorization Grant Token (AuthGrant): This is a "message" (also referred to as a communication or transmissions) encrypted by the security unit 955 (security technology) of the server 130 with the unique private key for the adapter module 100. The secured authorization grant (e.g. the encrypted authorization grant) is passed from the server 130 (via the mobile device 150) to the adapter module 100 in the form of a message. The mobile device 150, however, is not able to decrypt and read the message. The authorization grant is in response to the authorization request. The amount of the funds granted

by the AuthGrant may be determined by factors including, but not limited to, the amount of funds available (or, if funds are not available, a mini-loan could be granted), a pre-authorized amount (e.g. set by the server, set by the user during set-up, set by the funding source, or a standard amount), limited by time (e.g. only a certain amount per hour, or a predetermined amount at specific times of the day), limited to the maximum amount of an item on the machine (or enough for two or three items in the machine), or one or more of these and other factors. Significantly, the AuthGrant makes the funds available, but does not authorize a transaction. The AuthGrant may have an associated expiration period in that it may expire if it is not used in a pre-determined time period. The length of time before the AuthGrant expires may be determined by factors including, but not limited to, the trustworthiness of the user (e.g. the user has a long history with the system or some known provider (e.g. credit card provider, bank, or credit union), the user has a good credit rating, or the user has a large wallet balance), a pre-authorized time period (e.g. set by the server, set by the user during set-up, set by the funding source, or a standard time period), limited by time (e.g. predetermined time periods at specific times of the day such as longer times during breakfast, lunch, and dinner), limited by the machine or the products or services sold in the machine, limited by the number of other users near the machine (e.g. if it is a crowded machine, the AuthGrant may expire faster), or one or more of these and other factors. The AuthGrant remains valid until it expires or some other event occurs to end its validity (e.g. the user cancels it). This means that under normal circumstances the mobile device 150 will hold the AuthGrant authorizing use of funds for a pre-determined time period that will allow the user sufficient time to make a purchase. The authorized amount may be considered to be the "wallet balance" that is held in a virtual "wallet."

- Synchronization: Time may be synchronized to the adapter module 100 from the server 130. The server 130 sends time information with encrypted messages and the adapter module 100 uses the time encoded in the messages for synchronization.
- The mobile-device-to-machine payment systems and components thereof may have associated hardware, software, and/or firmware (a variation, subset, or

hybrid of hardware and/or software). The term "hardware" includes at least one "processing unit," "processor," "computer," "programmable apparatus," and/or other known or yet to be discovered technology capable of executing instructions or steps (shown as processing unit 750 in FIG. 56, processing unit 850 in FIG. 57, and processing unit 950 in FIG. 58). The term "software" includes at least one "program," "subprogram," "series of instructions," or other known or yet to be discovered hardware instructions or hardware-readable program code. Software may be loaded onto hardware (or firmware) to produce a "machine," such that the software executes on the hardware to create structures for implementing the functions described herein. Further, the software may be loaded onto the hardware (or firmware) so as to direct the mobile-device-to-machine payment systems (and components thereof) to function in a particular manner described herein or to perform a series of operational steps as described herein. "Hardware" such as the adapter module 100, mobile device 150, and payment accepting unit 120 may have software (e.g. programs and apps) loaded thereon. The phrase "loaded onto the hardware" also includes being loaded into memory (shown as memory 760 in FIG. 56, memory 860 in FIG. 57, and memory 960 in FIG. 58) associated with or accessible by the hardware. The term "memory" is defined to include any type of hardware (or other technology) -readable media (also referred to as computer-readable storage medium) including, but not limited to, attached storage media (e.g. hard disk drives, network disk drives, servers), internal storage media (e.g. RAM, ROM, EPROM, FLASH-EPROM, or any other memory chip or cartridge), removable storage media (e.g. CDs, DVDs, flash drives, memory cards, floppy disks, flexible disks), firmware, and/or other known or yet to be discovered storage media. Depending on its purpose, the memory may be transitory and/or non-transitory. Appropriate "messages," "communications," "signals," and/or "transmissions" (that includes various types of information and/or instructions including, but not limited to, data, commands, bits, symbols, voltages, currents, electromagnetic waves, magnetic fields or particles, optical fields or particles, and/or any combination thereof) over appropriate "communication paths," "transmission paths," and other means for signal transmission including any type of connection between two elements on the system (the system including, for example, the adapter

module 100, mobile device 150, payment accepting unit 120, hardware systems and subsystems, and memory) would be used as appropriate to facilitate controls and communications.

- It should be noted that the terms "programs" and "subprograms" are defined as a series of instructions that may be implemented as software (i.e. computer program instructions or computer-readable program code) that may be loaded onto a computer to produce a "machine," such that the instructions that execute on the computer create structures for implementing the functions described herein or shown in the figures. Further, these programs and subprograms may be loaded onto a computer so that they can direct the computer to function in a particular manner, such that the instructions produce an article of manufacture including instruction structures that implement the function specified in the flow chart block or blocks. The programs and subprograms may also be loaded onto a computer to cause a series of operational steps to be performed on or by the computer to produce a computer implemented process such that the instructions that execute on the computer provide steps for implementing the functions specified in the flow chart block or blocks. The phrase "loaded onto a computer" also includes being loaded into the memory of the computer or a memory associated with or accessible by the computer. Separate, albeit interacting, programs and subprograms may be associated with the adapter modules 100, the server 130, and the mobile device 150 (including the mobile application 140) and these programs and subprograms may be divided into smaller subprograms to perform specific functions.

- The terms "messages," "communications," "signals," and/or "transmissions" include various types of information and/or instructions including, but not limited to, data, commands, bits, symbols, voltages, currents, electromagnetic waves, magnetic fields or particles, optical fields or particles, and/or any combination thereof. Appropriate technology may be used to implement the "communications," "signals," and/or "transmissions" including, for example, transmitters, receivers, and transceivers. "Communications," "signals," and/or "transmissions" described herein would use appropriate technology for their intended purpose. For example, hard-wired communications (e.g. wired serial

communications) would use technology appropriate for hard-wired communications, short-range communications (e.g. Bluetooth) would use technology appropriate for close communications, and long-range communications (e.g. WiFi or Cellular) would use technology appropriate for remote communications over a distance. Appropriate security (e.g. SSL or TLS) for each type of communication is included herein. Security units 755 and 955 include technology for securing messages. The security technology may be, for example, encryption/decryption technology (e.g. software or hardware). Although encryption/decryption is discussed primarily as being performed using a unique private key, alternative strategies include, but are not limited to encryption/decryption performed using public/private keys, or other encryption/decryption strategies known or yet to be discovered. Appropriate input mechanisms and/or output mechanisms, even if not specifically described, are considered to be part of the technology described herein. The exemplary communications unit 770 (shown in FIG. 56) of the adapter module 100 is shown as including appropriate input and output mechanisms 772, 774 that may be implemented in association (e.g. directly or indirectly in functional communication) with male and female adapters 720, 730 of the adapter module 100. The exemplary communications unit 870 (shown in FIG. 57) of the mobile device 150 includes mechanisms for both long-range communications (shown as Cellular and/or WiFi mechanisms 872) for communicating with the server 130 and short-range communications (shown as Bluetooth mechanisms 876) for communicating with the adapter module 100.

- When used in relation to "communications," "signals," and/or "transmissions," the terms "provide" and "providing" (and variations thereof) are meant to include standard means of provision including "transmit" and "transmitting," but can also be used for non-traditional provisions as long as the "communications," "signals," and/or "transmissions" are "received" (that can also mean obtained). The terms "transmit" and "transmitting" (and variations thereof) are meant to include standard means of transmission, but can also be used for non-traditional transmissions as long as the "communications," "signals," and/or "transmissions" are "sent." The terms

"receive" and "receiving" (and variations thereof) are meant to include standard means of reception, but can also be used for non-traditional methods of obtaining as long as the "communications," "signals," and/or "transmissions" are "obtained."

- The term "associated" is defined to mean integral or original, retrofitted, attached, connected (including functionally connected), positioned near, and/or accessible by. For example, if the user interface (e.g. a traditional display 122 (FIG. 19), a touch screen display 124 (FIG. 19), a key pad 126 (FIG. 19), buttons 126 (FIG. 19, shown as part of the key pad 126), a keyboard (not shown), and/or other input or output mechanism) is associated with a payment accepting unit 120, the user interface may be original to the payment accepting unit 120, retrofitted into the payment accepting unit 120, attached to the payment accepting unit 120, and/or a nearby the payment accepting unit 120. Similarly, adapter modules 100 may be associated with payment accepting units 120 in that the adapter modules 100 may be original to the payment accepting unit 120, retrofitted into the payment accepting unit 120, attached to the payment accepting unit 120, and/or a nearby the payment accepting unit 120.
- It should be noted that relative terms are meant to help in the understanding of the technology and are not meant to limit the scope of the invention. Similarly, unless specifically stated otherwise, the terms used for labels (e.g. "first," "second," and "third") are meant solely for purposes of designation and not for order or limitation. The term "short" in the phrase "short-range" (in addition to having technology specific meanings) is relative to the term "long" in the phrase "long-range."
- The terms "may," "might," "can," and "could" are used to indicate alternatives and optional features and only should be construed as a limitation if specifically included in the claims.
- It should be noted that, unless otherwise specified, the term "or" is used in its nonexclusive form (e.g. "A or B" includes A, B, A and B, or any combination thereof, but it would not have to include all of these possibilities). It should be noted that, unless otherwise specified, "and/or" is used similarly (e.g. "A

and/or B" includes A, B, A and B, or any combination thereof, but it would not have to include all of these possibilities). It should be noted that, unless otherwise specified, the terms "includes" and "has" mean "comprises" (e.g. a device that includes, has, or comprises A and B contains A and B, but optionally may contain C or additional components other than A and B). It should be noted that, unless otherwise specified, the singular forms "a," "an," and "the" refer to one or more than one, unless the context clearly dictates otherwise.

System Overview

[00103] FIGS. 5, 6, and 7 together show exemplary major components of the mobile-device-to-machine payment system and the interactions therebetwen.

[00104] As shown, the adapter module 100 functionally connected bi-directionally to the payment accepting unit 120 via a wired serial connection such that no security is necessary. The adapter module 100 is also functionally connected bi-directionally to the mobile device 150 (and its installed mobile application 140) via short-range communication technology (e.g. a Bluetooth connection). Because the mobile device 150 is not a "trusted" link (e.g. it could be hacked by a user), only secured communications (transmissions) are passed between the adapter module 100 and the mobile device 150. This keeps the passed communications secured and safe from hacking. The mobile device 150 (and its installed mobile application 140) is also functionally connected bi-directionally to a system management server 130 and/or a funding source server 160 via long-range communication technology (e.g. WiFi or Cellular connection) that preferably has appropriate security (e.g. SSL security). Security between the mobile device 150 and the system management server 130 has the advantage of protecting communications from the mobile device 150 to the system management server 130 that may include sensitive data and may not be encrypted. The system management server 130 and the funding source server 160 may be connected via a wired Internet connection with SSL security. The system management server 130 may be connected via a wired Internet connection with SSL security to an operators' server 170. Although not necessary to implement a purchase transaction, for other purposes (e.g. inventory), the operators' server 170 may be connected to the payment accepting unit 120 using a handheld computer sync or a cellular connection.

[00105] Also, a unique private key may be used to securely transmit encrypted messages between the adapter module 100 and the system management server 130 (although the encrypted transmissions would most likely be routed through the mobile device 150). The server 130 stores a private key for each adapter module 100, and this key is only known to the adapter module 100 and the server 130. No intermediary is privy to this key (especially not the mobile device 150). When the adapter module 100 and server 130 communicate messages (e.g. AuthRequest and AuthGrant), the security unit 755 of the adapter module 100 encrypts the message with its private key and passes the message to the mobile device 150. The mobile device 150 (which preferably cannot decrypt the message) passes the encrypted message to the server 130. The server 130 is able to decrypt the message using the security unit 955 of the adapter module 100 and the unique private key. The security unit 955 of the server 130 uses this same unique private key to encrypt messages to the adapter module 100 and sends the message to the mobile device 150 to relay to the adapter module 100 that is able to decrypt the message using the security unit 755 of the adapter module 100 and the unique private key.

[00106] FIG. 7 shows specific exemplary communications and messaging with an exemplary vending sequence (the numbers to the left of the communications and messaging) between the adapter module 100, the mobile device 150, and the system management server 130. These communications are discussed in more detail in the discussion pertaining to the timing schematics (FIGS. 8A-8G) and the flow charts (FIGS. 9A-9E).

[00107] It should be noted that FIGS. 5, 6, and 7 are meant to be exemplary and to help in the understanding of the mobile-device-to-machine payment system. For example, the shown long-range communications technology may be replaced with alternative long-range communications technology known or yet to be discovered, the shown short-range communication technology may be replaced with alternative short-range communication technology known or yet to be discovered, and the shown security may be replaced with alternative security known or yet to be discovered. The shown connections are meant to be exemplary in that, for example, there may be intermediaries that are not shown. The shown components have been simplified in that, for example, only one mobile device 150 (or machine 120, adapter module 100, or server 130) is shown where many may be included. Finally, the order of the steps may be changed and some steps may be eliminated.

Adapter Module

[00108] FIGS. 11-55 show exemplary adapter modules 100a-100e (referred to generally as adapter modules 100). These are relatively low cost hardware that are pre-configured to work with industry standard a multi-drop bus (MDB). On machines without MDB technology, the adapter module 100 can be configured or designed to work with other serial protocols or activate a switch. In essence the adapter module 100 simulates establishing payment on payment accepting unit 120 in much the same manner as other alternative forms of payment (e.g. cash).

[00109] The shown exemplary adapter modules 100 are preferably designed to be used as an in-line dongle for in-line insertion within, for example, a MDB of a machine 120. The wire used in MDB technology uses male and female connection ends or adapters to allow the attachment of peripherals. In the case of a vending machine, the wire with the connection ends or adapters would be present to allow the attachment of a payment receiving mechanism (e.g. a coin mechanism). The MDB male and female adapters 700, 710 may be separated (as shown in FIGS. 17, 18, 26, 27, 35, 36, 44, 45, 53, and 54). The adapter modules 100 have male and female adapters 720, 730. The adapter module may be plugged (inserted) in serial ("in-line") with the wire. For example, the MDB female adapter 710 may be connected to the male adapter 720 of the adapter module 100 and the MDB male adapter 700 may be connected to the female adapter 730 of the adapter module 100. The resulting in-line configuration is shown in FIGS. 19, 28, 37, 46, and 55. It should be noted that the adapter modules 100 are designed to allow pass-through communications so that if the mobile-device-to-machine payment systems is not enabled (e.g. for a particular purchase or simply turned off) the MDB functions as though the adapter module 100 is not there and the machine 120 can function normally.

Hands-Free

[00110] Summarily, if it is available, a hands-free mode, from the user's perspective, would allow the user to approach a favorite payment accepting unit 120 and notice that the display (e.g. the displays 122 or 124 shown in FIG. 19) associated with the payment accepting unit 120 shows funds available (e.g. the wallet balance), he would select the product or service using input mechanisms (e.g. buttons 126 or a touch screen display 124 shown in FIG. 19) associated with the payment accepting unit 120, and he would retrieve his dispensed services or products.

[00111] During an initial handshake with the mobile device 150 (when the user is within range), the adapter module 100 reports to the mobile device 150 whether or not hands-free mode is available. If it is available, the installed mobile application 140 automatically connects to the payment accepting unit 120 without the user having to interact with the mobile device 150. The user observes that funds are available on the display 122, 124 of the payment accepting unit 120 and completes the purchase transaction as if cash was inserted in the machine 120 by inputting his selection on the payment accepting unit 120. The payment accepting unit 120 dispenses the product or service. After the selection is made, the change is returned to the mobile device 150.

[00112] Whether hands-free payment is available is determined by factors including, but not limited to whether if other mobile devices 150 are in range, if other adapter modules 100 are in range, if there are any alerts, if the payment trigger threshold is having wide variances and so deemed unstable, or if the payment accepting unit operator (e.g. a vending machine operator) has opted to disable hands-free mode for the payment accepting unit 120. In the latter instance, operators can disable via a maintenance mobile device 150, as well as through the operators' server 170 and/or the system management server 130.

[00113] FIG. 3 is a table that showing exemplary considerations, conditions, or factors that may be used to determine whether the hands-free pay feature is available. Starting at the "Favorite?" column, this indicates whether the payment accepting unit 120 is a favorite machine. Preferably the hands-free pay feature is only available for use with "favorite" payment accepting units 120 (e.g. a vending machine at work or school). The "Alert" column has to do with whether there is some reason (e.g. there are too many users in range) that the hands-free pay feature should not work and, if there is such a reason, the user will be notified (alerted) and may be able to use the manual mode to resolve the alert and/or complete the transaction. FIG. 3 shows situations in which a user is or is not able to make hands-free purchases from a machine 120 using a mobile application 140 on his mobile device 150. It should be noted that the shown interface is meant to be exemplary. For example, some of the features could be automated or pre-selected. (It should be noted that the left hand column, the "Tab" column, relates to whether the selected tab on the mobile application 140 is "all" or "favorite." FIGS. 10A-10D all show these tabs. Unlike the other columns in FIG. 3, this column has more to do with the functionality and view of the application 140 than specifically with the hands-free feature. The tabs would allow a user to select whether he wanted to be alerted when he was in range of all payment accepting units 120 or just

"favorite" payment accepting units 120 and the application 140 would show the appropriate view.)

[00114] Balance Display: An optional feature of the mobile-device-to-machine payment system that is particularly helpful in the hands-free mode (although it may be available in the manual mode and/or in a multiple-vend scenarios) is when the user's mobile device 150 sends "credit" to the payment accepting unit 120 (either via hands-free payment or through a manual swipe), the wallet balance is sent to the payment accepting unit 120 that is then displayed to the user on a display 122, 124 of the machine 120. This is particularly beneficial during hands-free mode when the user does not retrieve the mobile device 150 and, therefore, may not know the balance. Also, in a multiple-vend scenario the user would not have to calculate a remaining balance.

[00115] An exemplary hands-free and multiple-vend scenario with a balance display might be as follows: The user has $5.00 in his virtual wallet as that is the amount that has been authorized (the AuthGrant being stored on the mobile device 150). He walks up to the payment accepting unit 120 and $5.00 is displayed on the display 122, 124 of the payment accepting unit 120 since hands-free mode was enabled and credit was sent (e.g. via short-range communication technology) to the payment accepting unit 120. The user makes a selection of $1.50 by interacting (e.g. pressing buttons) with the machine 120. The item (product or service) is dispensed and the "change" is "returned" (e.g. via short-range communication technology) to the virtual wallet. But since user is still standing in the payment zone 102, the remaining wallet balance of $3.50 is sent to the payment accepting unit 120 and displayed so that the user can now see he has a $3.50 balance. (It should be noted that the authorized funds may remain on the machine 120 and not be transferred back to the mobile device 150 between transactions.) The user decides to purchase a $1.50 item, and the transaction is completed as usual (e.g. by interacting with the machine 120). Now the user is still standing in the payment zone 102 and he sees the wallet balance of $2.00 on the display 122, 124 of the payment accepting unit 120. Deciding he does not wish to purchase anything else, the user walks away. As he walks out of the payment zone 102, the credit is cleared from the machine 120. But he is left with the knowledge that his wallet balance is $2.00 even though he never touched the mobile device 150. Communications between the payment accepting unit 120 and the adapter module 100 (via the mobile device 150) handle the accounting incidental to the transaction. The remaining balance ($2.00) is technically

stored on the server 130, and may be reflected on the application 140 on the mobile device 150.

Multiple Distinct Zones

[00116] As shown in FIGS. 1 and 2, the functions performed by the adapter module 100 can be divided into distinct zones: a first "communication zone" (e.g. "Bluetooth range" 106), a second "authorization zone" 104, and a third "payment zone" 102. The payment zone102 (that can not be zero) is smaller than or equal to (overlapping completely) the authorization zone 104. (Put another way, the payment zone 102 is within or coextensive with the authorization zone 104.) The payment zone 102 is a subset of the authorization zone 104 with a ratio of the payment zone 102 to the authorization zone 104 ranging from 0.01:1 to 1:1. It is not necessarily a fixed ratio and can vary between different payment accepting units 120, different mobile devices 150, different users, and over time. While the zones 102, 104, 106 are depicted as having a uniform shape, the zones may not necessarily be uniform (or constant over time) in that the shape can vary. For example, the shape of the Bluetooth range 106 may vary depending on environmental conditions such as obstacles in the room and payment accepting unit 120 door/wall materials.

[00117] Bluetooth Range 106: The outermost range is the Bluetooth range 106. This is the area in which the adapter module 100 is able to broadcast its presence. In most situations, the Bluetooth range 106 is a passive range in that no actual data is exchanged between the mobile device 150 and the adapter module 100. While in the Bluetooth range 106, the mobile device 150 monitors the RSSI (Received Signal Strength Indicator).

[00118] Authorization Zone 104: The middle region is the authorization zone 104. This is a computed area based on the RSSI. As mentioned, the mobile device 150 monitors the RSSI while it is in the Bluetooth range 106. When the RSSI reaches a certain predetermined threshold based on In-Range Heuristics, the mobile device 150 can be considered to be in the authorization zone 104. In the authorization zone 104 the mobile device 150 establishes a connection to the adapter module 100 (e.g. a Bluetooth connection (FIG. 5) with SSL protection (FIG. 6)) and informs the adapter module 100 of its presence. After a successful handshake with the adapter module 100, the mobile device 150 registers the adapter module 100 and the adapter module 100 requests an authorization to the server 130 via the mobile devices' network connection (e.g. a WiFi or cellular connection (FIG. 5) with SSL protection (FIG. 6)). It is important to note the mobile device 150 and the adapter

module 100 have a non-exclusive relationship at this point. The adapter module 100 may collect registrations for all mobile devices 150 that are within the authorization zone 104.

[00119] An authorization occurs in preparation for when the user enters the payment zone 102. An authorization expires in a set period of time (for example, five minutes), so if the mobile device 150 is still in the authorization zone 104 at the time of expiration, the adapter module 100 submits for and receives another authorization. This will continue for a set number of times (for example, the limit may be three times to limit cases of numerous authorizations for a mobile device that may remain in the authorization zone 104 for an extended period of time without completing a transaction). Should authorization fail (for instance if the limit had been reached) prior to the user entering the payment zone 102, the adapter module 100 will request authorization when the mobile device 150 enters the payment zone 102 (which adds a few seconds to the experience).

[00120] Payment Zone 102: As a user enters the payment zone 102, the mobile device 150 establishes exclusive control of the adapter module 100. Once established, any other user in the payment zone 102 is put into a "waiting" status.

[00121] In the payment zone 102, the payment can be triggered automatically if the system has and is in hands-free mode. In such instances, the mobile device 150 is running the app 140 in background mode and will send credit to the payment accepting unit 120 without any explicit user interaction. The user completes the transaction on the payment accepting unit 120 in much the same manner as if cash had been inserted into the payment accepting unit 120 to establish credit. After the user completes the transaction (that may include one or more purchases), details of the transaction are preferably returned to the mobile device 150 and server 130 in separate messages. The message to the server 130 is preferably encrypted with the adapter module's 100 private key (FIG. 6) to ensure data integrity. As shown in FIG. 7, the "private key" coded message (Encrypted VendDetails) is preferably sent via the mobile device 150. The message to the mobile device 150 may be sent solely for the purpose of closing the transaction. The transaction history and balance are updated server-side via the encrypted message sent to the server 130.

[00122] The other mode of operation is manual mode. In manual mode, the user launches the mobile device 150 and is able to swipe to send payment to the payment accepting unit 120. The user can also swipe back to cancel the payment. Like in hands-free mode, the purchase transaction is completed on the payment accepting unit 120 in the same

manner as if cash were inserted into the payment accepting unit 120. The mobile device 150 is only used to send payment. Selection is made directly on the payment accepting unit 120.

[00123] Self-Calibrating Zone Threshold: A key, but optional feature, of the system is a self-calibrating payment zone RSSI threshold. Because RSSI can vary machine to machine, environment to environment, and device to device, having a fixed threshold at which payment is triggered can be problematic. The approach suggested herein is the creation of a self-calibrating threshold. When the user is interacting with the payment accepting unit 120 (such as when he makes his selection on the payment accepting unit 120), the payment accepting unit 120 notifies the adapter module 100 and the adapter module 100 logs the conditions such as RSSI, type of user mobile device 150, accelerometer data, and other information. It is at this point that it can be ascertained safely that the user is within arms-length from the payment accepting unit 120 (by necessity the user is arms-length because he is making some physical interaction with the payment accepting unit 120). This is the only point in the entire transaction in which it can be certain that the user is within arms-length from the payment accepting unit 120.

[00124] FIG. 4 shows a simplified set of exemplary steps involved when users enter the payment zone 102. Specifically, FIG. 4 shows that credit is established 200 (this may have been done in the authorization zone 104, but if not it would be handled in the payment zone 102), that the user makes a selection using the machine 202, that the machine notifies the adapter module of the selection 204, that the adapter module (optionally) logs the RSSI 206, and that the purchase process(es) continues 208. Using the historically logged RSSI data, the adapter module 100 calculates one of several "average" RSSI using various mathematical models. This "average" could be a traditional average, a moving average, a weighted average, a median, or other similar summary function. The adapter module 100 could pre-process the historical data before running the function, such as to eliminate top and bottom data points, suspect data points, etc.

[00125] Optionally, during the handshake between the mobile device 150 and the adapter module 100, the information transmitted to the adapter module 100 may include, for example, the model of the mobile device 150. Using the received information pertaining to the mobile device models, the adapter module 100 can create multiple payment thresholds, one for each mobile device model. This allows for variances that may be inherent in different types of Bluetooth radios. An alternative to this method is for the adapter module 100 to broadcast a baseline payment zone threshold, and the mobile device 150 can use an offset

from this baseline based on its specific model type. The payment zone thresholds (or baseline offsets) can be unique to specific types of mobile devices (e.g. by manufacturer, operating system, or component parts), models of mobile devices, or individual mobile devices (unique to each user).

[00126] In a typical scenario in which the payment zone threshold has been calibrated, the adapter module 100 advertises its presence along with the threshold at which it considers any mobile device 150 to be in the authorization zone 104. This is a one-way communication from adapter module 100 to mobile device 150. Once the mobile device 150 enters the authorization zone 104, there is a handshake that is established between the adapter module 100 and the mobile device 150. During this handshake, the mobile device 150 can share its model information with the adapter module 100, and the adapter module 100 can return the payment zone 102 threshold for that specific model.

[00127] Optionally, in addition to calibrating the payment zone threshold, the adapter module 100 can apply the self-calibrating model to the authorization zone 104 to calibrate the authorization zone threshold. As with the payment zone thresholds, the authorization zone thresholds can be unique to specific types of mobile devices, models of mobile devices, or individual mobile devices. In this scenario, the adapter module 100 would broadcast multiple thresholds by device type and the mobile device 150 would determine which threshold to apply (or alternatively broadcast a baseline and the mobile device 150 uses an offset based on its device model). Even in this scenario, the authorization zone 104 is a one-way communication.

[00128] Optionally, along with the threshold that is calculated (in the payment and/or the authorization zone(s)), a safety margin can be added to minimize scenarios in which a user is within range, but the mobile-device-to-machine payment systems do not recognize it because the threshold may not have been reached. For example, if the calculated RSSI for an iPhone 5 on machine 4567 is -68db, the mobile-device-to-machine payment systems may add a safety margin of -5db, and establish the threshold at -73db. So when a user's phone is communicating with the adapter module 100 at an RSSI of -73db or better, the mobile-device-to-machine payment systems will allow the mobile device 150 to credit the payment accepting unit 120. The safety margin can be set on the server 130 and downloaded to the adapter module 100, or set on the mobile device 150, or set on the adapter module 100 itself.

[00129] Optionally, in the payment zone threshold, the mobile device 150 can use other data to determine when to cancel the exclusive control of the payment accepting unit 120, to identify when the user is moving out of the payment zone 102. External data could include accelerometer data from the mobile device 150. Using that data, the mobile device 150 can determine whether the user is standing relatively still in front of the payment accepting unit 120, or if the user is in motion – effectively walking away from the payment accepting unit 120.

Signal Unavailability Adaptation

[00130] The mobile-device-to-machine payment systems described herein use a mobile device's 150 short-range communication technology (shown as Bluetooth mechanisms 876 in FIG. 57) and a mobile device's 150 long-range communications technology (shown as Cellular and/or WiFi mechanisms 872 in FIG. 57). The short-range communication technology 876 communicates with the adapter module's 100 short-range communication technology (shown as Bluetooth mechanisms 776 in FIG. 56). The long-range communications technology 872 communicates with the server's 130 communication technology (not shown). The mobile device 150 (with a mobile application 140 thereon) acts as a communication bridge between the adapter module 100 (associated with a payment accepting unit 120) and the server 130. This process is described herein and works properly if there is cellular or WiFi coverage within the payment zone 102.

[00131] One option if there is no cellular or WiFi coverage within the payment zone 102 is to determine whether there is cellular or WiFi coverage within the authorization zone 104 or the Bluetooth range 106. If there is, then the sizes of the zones 102, 104, 106 could be adapted and the timing could be adapted. For example, if the mobile devices 150 detected problems with the cellular or WiFi coverage within the payment zone 102, the user could carry his mobile device 150 into the other zones (or the mobile device 150 could use short-range communication technology to communicate with other mobile devices 150 within the authorization zone 104 or the Bluetooth range 106) to determine whether the zones have cellular or WiFi coverage. If they do have coverage, communication between the mobile device 150 and the server 130 can be advanced (conducted earlier when the mobile device 150 is further from the machine 120) or delayed (conducted later when the mobile device 150 is further from the machine 120). This can be thought of as changing the size or shapes of the zones 102, 104, 106. The timing would also have to be adjusted so that the authorization of funds (AuthGrant) does not expire before the user has a chance to make a purchase. It also

means that balance updates to the server 130 may happen after the user has moved away from the machine 120 and has cellular or WiFi coverage again.

[00132] Another option if there is no cellular or WiFi coverage within any of the zones 102, 104, 106 is for the user to obtain authorization while outside of the zones in a place with cellular or WiFi coverage. This may occur, for example, if a user knows that he will be going to a place with a payment accepting unit 120 equipped with an adapter module 100 (perhaps to a favorite payment accepting unit 120) that does not have (or rarely has) cellular or WiFi coverage. A user may also use the mobile application 140 to query payment accepting units 120 in a given range (e.g. within 50 miles) or at a given location (e.g. at a campground or in a particular remote city) to determine whether there is cellular or WiFi coverage within the zones 102, 104, 106. The user can then obtain pre-authorization from the server 130 using the mobile application 140. Again, the timing would also have to be adjusted so that the authorization of funds (AuthGrant) does not expire before the user has a chance to make a purchase. It also means that balance updates to the server 130 may happen after the user has moved away from the machine 120 and has cellular or WiFi coverage again. A mobile-device-to-machine payment system having the ability to implement this option would be able to accept cashless payments without requiring any network connection near the payment accepting unit 120. Mobile-device-to-machine payment systems described herein that are located in a remote location where no signal is available, therefore, can accept cashless payments.

[00133] As an example of a situation in which there might be no cellular or WiFi coverage within any of the zones 102, 104, 106 of a particular payment accepting unit 120, the user (a teenager) may be traveling to a remote location to attend summer camp where there is no cellular or WiFi coverage. The camp may have several payment accepting units 120 (e.g. a machine that creates a dedicated "hot spot" that requires payment for use, vending machines, or machines for renting equipment (e.g. bikes, kayaks, or basket balls)). The camp facility might notify parents that the mobile-device-to-machine payment system is available. The parents, while at home, could obtain authorization for a particular amount (that could be doled out a certain amount per day or limited to type of machine or location) to be authorized and "loaded" into the user's mobile device 150 and specify that the authorization will not expire for a certain period or until a certain date. Thereafter, while at camp, the user could use the mobile application 140 on his mobile device 150 in a manner similar to those discussed elsewhere herein. Short-range communications may be used for communications

between the adapter modules 100 (associated with the machines 120) and users' mobile devices 150.

[00134] One subtle but powerful component of the systems described herein is that they require internet network connection only in the authorization zone 104 and only for the time period required to send the AuthRequest and receive the AuthGrant. Once a valid AuthGrant is received by the mobile device 150, an internet network connection is not required by either the mobile device 150 or the adapter module 100 in the payment zone 102 as long as the AuthGrant is valid (unexpired). This mechanism allows the system to seamlessly handle authenticated transactions in (temporary) offline mode, with the deferred acknowledgement and transaction messages performing the bookkeeping and cleanup when network connection is regained. The alternatives described above provide a unique way to artificially extend the authorization zone to include any location where the mobile device 150 can communicate with the server 130.

Multiple User Resolution

[00135] As shown in FIG. 2, in likely practical scenarios, there will be multiple users in the zones 102, 104, 106. As shown, users 1, 2, and 3 are in the payment zone 102 near the machine 120, users 5 and 6 are shown as positioned between the authorization zone 104 and the Bluetooth range 106, users 4 and 7 are in the Bluetooth range 106, user 10 is positioned on the edge of the Bluetooth range 106, and users 8 and 9 are positioned outside of Bluetooth range 106. The mobile-device-to-machine payment systems provide for managing, and resolving issues pertaining to multiple users.

[00136] Users 4 and 7 are within the Bluetooth range 106 and user 10 is either entering or leaving the Bluetooth range 106. Within the Bluetooth range 106 the users' mobile devices 150 are able to see the adapter module's 100 advertisement. In this zone, the mobile device 150 preferably does not initiate a connection. The adapter module 100 is preferably unaware of the users in the Bluetooth range 106. All the adapter module 100 is doing is advertising its presence to any multitude of users that may be in Bluetooth range 106.

[00137] The adapter module 100 begins to log users as the users (and their respective mobile devices 150) enter the authorization zone 104 (shown in FIG. 2 as users 5 and 6). At this point, there is a non-exclusive connection initiated by the mobile device 150 to the adapter module 100. It does a handshake (e.g. to exchange information needed to obtain authorization and, optionally, to log information needed for a self-calibrating authorization

zone threshold) and the mobile device 150 contacts the server 130 for an authorization (e.g. sending an AuthRequest and receiving an AuthGrant). The adapter module 100 registers all mobile devices 150 that have requested and received AuthGrants. The adapter module 100 continues communicating with any other mobile device 150 that enters the authorization zone 104. After initial contact, the adapter module 100 may provide the mobile device 150 with a deferral delay of when to check back in with the adapter module 100 allowing opportunity for other mobile devices 150 to communicate with the adapter module 100.

[00138] If there is only one user in the payment zone 102, a purchase transaction may be performed. If there are multiple users in the payment zone 102, the mobile-device-to-machine payment system must handle the situation.

[00139] One optional exemplary solution for handling the situation of the multiple users in the payment zone 102 is queuing users in the payment zone 102. Once any mobile device 150 enters the payment zone 102, it establishes exclusivity to a particular mobile device 150 (first come first serve). Technically, however, the adapter module 100 is not establishing an exclusive connection to the mobile device 150. The adapter module 100 can still perform a round-robin poll and communicate with and advertise to other mobile devices 150. Instead, the adapter module 100 establishes a queue prioritized by RSSI and time (e.g. who was first and whether the authorization has expired) and it notifies (e.g. alerts) other mobile devices 150 to wait. The earliest valid (unexpired) authorization takes precedence when there is any tie in the RSSI. Otherwise, for example, the strongest average RSSI takes priority. Preferably the queue is not a static measure of the RSSI but an averaged measure over the period of time in the queue. This compensates for a scenario in which a user may be walking around in the queue and then shows up at the payment accepting unit 120 just as the previous user is finishing. If another user was also in the payment zone 102 and stood there the entire time, but may have newer authorization, he could win out.

[00140] Anytime that the adapter module 100 cannot determine exactly which user is in the payment zone 102 in front of the payment accepting unit 120, the adapter module 100 will disable hands-free payment. The mobile device 150 will send an alert to the user and he can use swipe to pay (manual mode). All users in payment zone 102 will show "Connected" and the first to swipe payment to the payment accepting unit 120 then locks out other users.

Multiple Module Resolution

[00141] In the scenario where there are multiple modules present, determining which payment accepting unit 120 a user is in front of can be a challenge. The mobile-device-to-machine payment systems described herein allow for adapter modules 100 to communicate to other adapter modules 100 in range via Bluetooth. Each user receives authorization grants for specific payment accepting units 120. This means if there are multiple adapter modules 100 within the same authorization zone 104, there will be multiple authorization grants for the user. When the user enters the payment zone 102, it can be difficult to differentiate which payment accepting unit 120 the user is in front of if the payment zones 102 overlap.

[00142] To solve this problem, when the user enters the payment zone 102, the adapter modules 100 communicate with each other to determine the RSSI for the particular user (based on the signal from his mobile device 150) to triangulate which adapter module 100 (and the associated payment accepting unit 120) is closer to the user. Optionally, the inter-module communications can restrict the user to establishing an exclusive connection with only one payment accepting unit 120.

[00143] Optionally, when the user connects to a payment accepting unit 120, the mobile device 150 can send a communication to the payment accepting unit 120 for momentary display to the user on the display 122, 124 of the payment accepting unit 120. For example, the mobile device 150 can send a communication (e.g. "connected" or "Fred's Mobile Device Connected") to the payment accepting unit's display 122, 124 for a predetermined period of time (e.g. 1-3 seconds) so when the user is in payment zone 102, it is clear which payment accepting unit 120 the user is connected to prior to making a purchase (either in hands-free or manual mode).

[00144] In addition, when the user is in manual mode, the mobile device 150 can display (e.g. on the touch screen 152 as shown in FIGS. 10A-10D) a visual indication of the payment accepting unit 120 (e.g. a picture and/or a payment accepting unit ID of the payment accepting unit 120) for visual confirmation. If the user is in manual mode, the user can manually change the payment accepting unit 120.

Descriptive Scenario

[00145] FIG. 7, FIGS. 8A-8G, and 9A-E (as well as other figures) can be used to understand a detailed exemplary scenario of the mobile-device-to-machine payment systems described herein. An exemplary flow of communications and steps are loosely described

below with reference to these (and other figures). It should be noted that alternative scenarios could include, for example, a modified order of the steps performed.

[00146] Prior to vending transactions, a user downloads a mobile app 140 onto his mobile device 150, creates an account, and configures a funding source via, for example, a funding source server 160. A funding source may be, for example, a debit card, a credit card, campus cards, rewards points, bank accounts, payment services (e.g. PayPal®) or other payment option or combination of payment options known or yet to be discovered. The funding sources may be traditional and/or nontraditional payment sources that are integrated into the ecosystem described herein and then used indirectly as a source of funds. Funds from the funding source are preferably held on the server 130 such that when an AuthRequest is received by the server 130, the server 130 can send an AuthGrant authorizing funds for a purchase.

[00147] The user can specify one or more "favorite" adapter module(s) 100 (that has a one-to-one relationship to the payment accepting unit 120) that he may visit regularly, such as a vending machine at school or work. Favorite adapter modules 100 appear on a pre-filtered list and allow for additional rich features such as hands-free payment.

[00148] The payment accepting unit 120 may be equipped with an adapter module 100 that is constantly advertising its availability via Bluetooth (or other "signals," "communications," and/or "transmissions"). This ongoing advertising and scanning for adapter modules is shown in FIG. 8A. As shown, the mobile device 150 is continuously scanning for any adapter module 100 within Bluetooth (or other "signal," "communication," and/or "transmission") range. When the user is within range of that adapter module 100, the mobile device 150 tracks and monitors the signal strength until a predetermined "authorization zone" threshold is achieved.

[00149] FIGS. 8B and 9A generally show that when the authorization zone threshold is reached, the mobile device 150 enters the authorization zone (block 302) and registers the adapter module 100. The mobile device 150 connects to the server 130 (block 304). The app 140 on the mobile device 150 creates a request for authorization (AuthRequest) and passes the AuthRequest to the server 130 using appropriate communication technology (e.g. cellular or WiFi) (block 306). The server 130 responds with an authorization grant (AuthGrant) encrypted with the specific adapter module's private key (block 306). This authorization token may minimally include the Userl D, Apparatusl D (for the adapter module 100),

authorization amount, and expiration time. The mobile device 150 receives the AuthGrant from the server 130, and retains it until the mobile device 150 is ready to issue payment to an adapter module 100. The mobile device 150 collects all pending AuthGrants that may be one or more depending on how many adapter modules 100 are in-range. Unused AuthGrants that expire are purged from the mobile device 150 and the server 130. It is important to note that the mobile device 150 is unable to read the AuthGrant because it is encrypted with the adapter module's unique private key that is only known to server 130 and adapter module 100. This provides a preferred key element of security in the system as the adapter module 100 only trusts AuthGrants that are issued by the server, and the AuthGrants cannot be read or modified by the mobile device 150 or any other party in between the server and the adapter module 100. Additional mobile devices 150 may enter the authorization zone 104 (block 308).

[00150] As the user approaches a specific adapter module 100, the user enters the payment zone 102 and an event threshold is triggered based on heuristics performed by the mobile device 150. Blocks 310 and 312 show the loop steps of waiting for a mobile device 150 from the authorization zone 104 to enter the payment zone 102. If the user leaves the authorization zone 104 without entering the payment zone 102, the adapter module 100 returns to advertising its presence (block 300).

[00151] FIGS. 8C and 9B generally show the user entering the payment zone. The mobile device 150 verifies that it has an unexpired and valid AuthGrant. If the AuthGrant is not good, it may be requested again, repeating the Auth Request process (block 315). If the AuthGrant is good, the mobile device 150 sends the valid AuthGrant (including the wallet balance (block 322)) to the adapter module 100 to initiate a transaction. The mobile device 150 may issue the AuthGrant automatically without specific user interaction if the hands-free mode is supported (and the device is a favorite (block 318), there is only one device in the payment zone 102 (block 318), and (optionally) there is only one user in the authorization zone 104 (block 320). If any of these factors are not present, the mobile device 150 will prompt and/or wait for the user to begin the transaction manually (block 324).

[00152] FIGS. 8D, 9C, and 9D generally show the transaction process. As shown in FIG. 9C, the adapter module 100 runs through a series of questions to determine if there are any issues that would prevent vending including: has the user canceled in-app? (block 326), has the user walked away? (block 328), is the coin return pressed? (block 330), has more than a predetermined period of time elapsed? (block 332). If the answer to any of these questions

is "yes," the transaction does not proceed. If the answers to all of these questions is "no," the user makes a selection (block 334) on the payment accepting unit 120 in the same or similar manner as compared to if cash or credit were presented to the payment accepting unit 120. If the machine 120 is able to vend (block 336), it attempts to release the product. If the vend fails (block 338) it is reported by the machine (block 340) and a credit is returned to the virtual wallet (block 342). If the vend is successful (block 338) it is reported by the machine (block 344). Put another way, after the transaction is complete, the adapter module 100 returns to the mobile device 150 the details of the transaction as well as an encrypted packet containing the vend details to be sent to the server 130 via the mobile device 150. Optionally, the adapter module 100 can pass additional information not directly related to the transaction such as payment accepting unit health, sales data, error codes, etc.

[00153] FIGS. 8D and 9E generally show the multi-vend function. If the machine has enabled multi-vend capabilities (block 350) and the multi-vend limit has not been reached, the process returns to the question of whether the user is in the payment zone (block 310 of FIG. 9A). If the machine does not have enabled multi-vend capabilities (block 350) or the multi-vend limit has been reached, the wallet is decremented by the vend amount(s) and "change" is returned to the virtual wallet (block 354) and the process ends (block 356).

[00154] FIG. 8E is a timing schematic showing an exemplary Login process. FIG. 8F is a timing schematic showing an exemplary bootup process. FIG. 8G is a timing schematic showing an exemplary Account Check/Update process.

[00155] Several of the figures are flow charts (e.g. FIGS. 9A-9E) illustrating methods and systems. It will be understood that each block of these flow charts, components of all or some of the blocks of these flow charts, and/or combinations of blocks in these flow charts, may be implemented by software (e.g. coding, software, computer program instructions, software programs, subprograms, or other series of computer-executable or processor-executable instructions), by hardware (e.g. processors, memory), by firmware, and/or a combination of these forms. As an example, in the case of software, computer program instructions (computer-readable program code) may be loaded onto a computer to produce a machine, such that the instructions that execute on the computer create structures for implementing the functions specified in the flow chart block or blocks. These computer program instructions may also be stored in a memory that can direct a computer to function in a particular manner, such that the instructions stored in the memory produce an article of manufacture including instruction structures that implement the function specified in the flow

chart block or blocks. The computer program instructions may also be loaded onto a computer to cause a series of operational steps to be performed on or by the computer to produce a computer implemented process such that the instructions that execute on the computer provide steps for implementing the functions specified in the flow chart block or blocks. Accordingly, blocks of the flow charts support combinations of steps, structures, and/or modules for performing the specified functions. It will also be understood that each block of the flow charts, and combinations of blocks in the flow charts, may be divided and/or joined with other blocks of the flow charts without affecting the scope of the invention. This may result, for example, in computer-readable program code being stored in whole on a single memory, or various components of computer-readable program code being stored on more than one memory.

Distinction From Known Systems

[00156] Many of the known systems and methods require that the payment accepting unit be persistently (continuously) connected to and/or connectable on demand to some sort of remote server in order to function. As an example, the Carlson reference describes a system and a method for using a portable consumer device. Described embodiments include a consumer using the portable consumer device to dial a number to purchase an item (product or service) in a vending machine, to send an SMS to purchase an item in a vending machine, or to use a mobile wallet to purchase an item in a vending machine. It is mentioned in one embodiment that the consumer may launch an application in the portable consumer device or, alternatively, the portable consumer device may automatically detect the vending machine and prompt the consumer to enter information associated with the vending machine. It should be noted, however, that even when there is automatic detection, the user is prompted to enter information (e.g. a machine alias, payment information, or a PIN) and it can be inferred that this is entered on the portable consumer device. Once connected to a payment processing network, the authorization process begins using a payment processing network and/or payment server. Significantly, all of the embodiments described in the Carlson reference specify that the payment server sends an authorization response message to the vending machine. This means that, unlike the mobile-device-to-machine payment systems described herein, a persistent network connection is required for the Carlson system to function. Other references that disclose systems that require a persistent network connection include the Khan reference (the MicroAdapter having the persistent connection), the Garibaldi reference, and the Weiner reference.

[00157] Many of the known systems and methods require the user to significantly interact with their mobile devices. As an example, the Whigham reference is directed to a system that eliminates the need for currency for a vending machine and also eliminates the need for a dedicated online connection between the vending machine and the issuer of a credit card or a debit card. Instead the Whigham system and method allows a consumer to purchase a product from an automatic vending machine by using the consumer's cellular telephone, personal digital assistant (P DA), or similar wireless communication device as a link between the provider of the products in the vending machine and the vending machine. The Whigham reference, however, sets forth a system and method requires significant interaction between the consumer and his telephone including dialing a telephone number to a server (that, in turn, provides a vend code to the consumer), requesting a specific product (e.g. by dialing additional digits, although this step is optional if a unique number was dialed for a specific product), and transmitting a vend code to the vending machine. (Other references that disclose systems that require user interaction with the phone include the Offer reference, the Khan reference, the Belfer reference, and the Carlson reference.) In addition to other differences, some of the mobile-device-to-machine payment systems described herein do not require the user to interact with his mobile device at all, which can be contrasted to known systems and methods that require the consumer to, for example, dial a telephone number, enter a machine identification, and/or enter a product identifier using the mobile device to purchase a product.

[00158] The known systems and methods that use a cellular telephone to facilitate cashless transactions at a vending machine use the cellular telephone to authorize a particular transaction. For example, once the user knows what he wants from a vending machine, he can dial a server and receive authorization to make a specific purchase. Sometimes this includes dialing additional numbers on the cellular telephone to specify a particular product. The mobile-device-to-machine payment systems described herein take a completely different approach. The mobile-device-to-machine payment systems described herein are not specifically interested in the details of the transaction to authorize the transaction. Instead, the mobile-device-to-machine payment systems function more like a gift card, a credit card, or a debit card in that they allow the user to have funds to make a purchase. When a user is in range, the adapter module 100 (via a mobile device 150) sends an AuthRequest to the server 130 to preemptively obtain authorization to make funds available. The server 130 returns the AuthGrant for funds to the adapter module 100 (via a mobile device 150) so that

the user may use the funds to make a purchase. The AuthGrant may remain valid until it expires. This gives the user significantly more flexibility than known systems and methods.

Miscellaneous

[00159] It is to be understood that the inventions, examples, and embodiments described herein are not limited to particularly exemplified materials, methods, and/or structures. It is to be understood that the inventions, examples, and embodiments described herein are to be considered preferred inventions, examples, and embodiments whether specifically identified as such or not.

[00160] All references (including, but not limited to, foreign and/or domestic publications, patents, and patent applications) cited herein, whether supra or infra, are hereby incorporated by reference in their entirety.

[00161] The terms and expressions that have been employed in the foregoing specification are used as terms of description and not of limitation, and are not intended to exclude equivalents of the features shown and described. While the above is a complete description of selected embodiments of the present invention, it is possible to practice the invention using various alternatives, modifications, adaptations, variations, and/or combinations and their equivalents. It will be appreciated by those of ordinary skill in the art that any arrangement that is calculated to achieve the same purpose may be substituted for the specific embodiment shown. It is also to be understood that the following claims are intended to cover all of the generic and specific features of the invention herein described and all statements of the scope of the invention that, as a matter of language, might be said to fall therebetween.

WHAT IS CLAIMED IS:

1. A method of payment processing, comprising:

at a device with one or more processors, memory, and two or more communication capabilities:

obtaining, from a payment module, an authorization request via a first communication capability;

sending, to a server, the authorization request via a second communication capability distinct from the first communication capability;

in response to sending the authorization request, obtaining, from the server, authorization information via the second communication capability;

after obtaining the authorization information, detecting a trigger condition to perform a transaction with a payment accepting unit associated with the payment module; and

in response to detecting the trigger condition, sending, to the payment module, at least a portion of the authorization information via the first communication capability.

2. The method of claim 1, wherein the first communication capability corresponds to a short-range communication protocol and the second communication capability corresponds to a long-range communication protocol.

3. The method of claim 1, further comprising:

obtaining, from the payment module, advertised information indicating the payment module's presence via the first communication capability that at least includes authorization zone threshold criterion.; and

after obtaining the advertised information, initiating a handshake process with the payment module, wherein the handshake process includes:

sending, to the payment module, device information at least including user identification information corresponding to the user of the device via the first communication capability; and

receiving, from the payment module, payment module information, wherein the payment module information at least includes an identifier corresponding to the payment module.

4. The method of claim 3, further comprising:

prior to obtaining the authorization request:

in accordance with a determination that the authorization zone threshold criterion is satisfied, sending notification information to the payment module via the first communication capability, wherein the notification information indicates that the authorization zone threshold criterion is satisfied;

wherein the device obtains the authorization request in response to sending the notification information.

5. The method of claim 3, wherein the payment module information further includes an indication that hands-free mode is available and payment zone threshold criterion.

6. The method of claim 5, wherein the device information further includes device identification information corresponding to a model type of the device; and

wherein the payment zone threshold criterion is based at least in part on the device identification information.

7. The method of claim 5, wherein detecting the trigger condition comprises:

determining whether the payment zone threshold criterion is satisfied; and

in accordance with a determination that the payment zone threshold criterion is satisfied, detecting the trigger condition without interaction from a user of the device.

8. The method of claim 1, wherein detecting the trigger condition comprises:

detecting a user input from a user of the device; and

in response to detecting the user input, detecting the trigger condition to perform a transaction with the payment accepting unit.

9. The method of claim 1, further comprising:

in response to obtaining the authorization information, presenting a notification to the user of the device that a connection has been established with the payment module.

10. The method of claim 9, wherein the notification further indicates an authorized amount for the transaction.

11. The method of claim 1, wherein the authorization information includes an identifier corresponding to the payment module, an identifier corresponding to the user of the device,

an authorized amount, an authorization grant token, and an expiration period for the authorization grant token.

12. The method of claim 11, wherein at least a portion of the authorization request and the authorization grant token are encrypted with a unique encryption key corresponding to the payment module.

13. A device, comprising:

two or more communication capabilities;

one or more processors; and

memory storing one or more programs to be executed by the one or more processors, the one or more programs comprising instructions for:

obtaining, from a payment module, an authorization request via a first communication capability;

sending, to a server, the authorization request via a second communication capability distinct from the first communication capability;

in response to sending the authorization request, obtaining, from the server, authorization information via the second communication capability;

after obtaining the authorization information, detecting a trigger condition to perform a transaction with a payment accepting unit associated with the payment module; and

in response to detecting the trigger condition, sending, to the payment module, at least a portion of the authorization information via the first communication capability.

14. The device of claim 13, wherein the first communication capability corresponds to a short-range communication protocol and the second communication capability corresponds to a long-range communication protocol.

15. The device of claim 13, wherein the one or more programs further comprise instructions for:

obtaining, from the payment module, advertised information indicating the payment module's presence via the first communication capability that at least includes authorization zone threshold criterion; and

after obtaining the advertised information, initiating a handshake process with the payment module, wherein the handshake process includes:

sending, to the payment module, device information at least including user identification information corresponding to the user of the device via the first communication capability; and

receiving, from the payment module, payment module information, wherein the payment module information at least includes an identifier corresponding to the payment module.

16. The device of claim 15, wherein the one or more programs further comprise instructions for:

prior to obtaining the authorization request:

in accordance with a determination that the authorization zone threshold criterion is satisfied, sending notification information to the payment module via the first communication capability, wherein the notification information indicates that the authorization zone threshold criterion is satisfied;

wherein the device obtains the authorization request in response to sending the notification information.

17. The device of claim 15, wherein the payment module information further includes an indication that hands-free mode is available and payment zone threshold criterion.

18. The device of claim 17, wherein the device information further includes device identification information corresponding to a model type of the device; and

wherein the payment zone threshold criterion is based at least in part on the device identification information.

19. The device of claim 17, wherein detecting the trigger condition comprises:

determining whether the payment zone threshold criterion is satisfied; and

in accordance with a determination that the payment zone threshold criterion is satisfied, detecting the trigger condition without interaction from a user of the device.

20. The device of claim 13, wherein detecting the trigger condition comprises:

detecting a user input from a user of the device; and

in response to detecting the user input, detecting the trigger condition to perform a transaction with the payment accepting unit.

21. A non-transitory computer readable storage medium storing one or more programs, the one or more programs comprising instructions, which, when executed by a device with one or more processors and two or more communication capabilities, cause the device to perform operations comprising:

obtaining, from a payment module, an authorization request via a first communication capability;

sending, to a server, the authorization request via a second communication capability distinct from the first communication capability;

in response to sending the authorization request, obtaining, from the server, authorization information via the second communication capability;

after obtaining the authorization information, detecting a trigger condition to perform a transaction with a payment accepting unit associated with the payment module; and

in response to detecting the trigger condition, sending, to the payment module, at least a portion of the authorization information via the first communication capability.

22. The non-transitory computer readable storage medium of claim 21, wherein the first communication capability corresponds to a short-range communication protocol and the second communication capability corresponds to a long-range communication protocol.

23. The non-transitory computer readable storage medium of claim 21, wherein the instructions cause the device to perform operations further comprising:

obtaining, from the payment module, advertised information indicating the payment module's presence via the first communication capability that at least includes authorization zone threshold criterion; and

after obtaining the advertised information, initiating a handshake process with the payment module, wherein the handshake process includes:

sending, to the payment module, device information at least including user identification information corresponding to the user of the device via the first communication capability; and

receiving, from the payment module, payment module information, wherein the payment module information at least includes an identifier corresponding to the payment module.

24. The non-transitory computer readable storage medium of claim 23, wherein the instructions cause the device to perform operations further comprising:

prior to obtaining the authorization request:

in accordance with a determination that the authorization zone threshold criterion is satisfied, sending notification information to the payment module via the first communication capability, wherein the notification information indicates that the authorization zone threshold criterion is satisfied;

wherein the device obtains the authorization request in response to sending the notification information.

25. The non-transitory computer readable storage medium of claim 23, wherein the payment module information further includes an indication that hands-free mode is available and payment zone threshold criterion.

26. The non-transitory computer readable storage medium of claim 25, wherein the device information further includes device identification information corresponding to a model type of the device; and

wherein the payment zone threshold criterion is based at least in part on the device identification information.

27. The non-transitory computer readable storage medium of claim 25, wherein detecting the trigger condition comprises:

determining whether the payment zone threshold criterion is satisfied; and

in accordance with a determination that the payment zone threshold criterion is satisfied, detecting the trigger condition without interaction from a user of the device.

28. The non-transitory computer readable storage medium of claim 21, wherein detecting the trigger condition comprises:

detecting a user input from a user of the device; and

in response to detecting the user input, detecting the trigger condition to perform a transaction with the payment accepting unit.

METHOD AND SYSTEM FOR PERFORMING MOBILE DEVICE-TO-MACHINE PAYMENTS

ABSTRACT OF THE DISCLOSURE

A device with one or more processors, memory, and two or more communication capabilities obtains, from a payment module, an authorization request via a first communication capability (e.g., Bluetooth). The device sends, to a server, the authorization request via a second communication capability distinct from the first communication capability (e.g., cellular or WiFi technology). In response to sending the authorization request, the device obtains, from the server, authorization information via the second communication capability. After obtaining the authorization information, the device detects a trigger condition to perform a transaction with a payment accepting unit associated with the payment module. In response to detecting the trigger condition, the device sends, to the payment module, at least a portion of the authorization information via the first communication capability.

Electronic Acknowledgement Receipt

EFS ID:	20236056
Application Number:	14335762
International Application Number:	
Confirmation Number:	6199
Title of Invention:	Method and System for Performing Mobile Device-To-Machine Payments
First Named Inventor/Applicant Name:	Paresh K. Patel
Customer Number:	24341
Filer:	Douglas James Crisman/Sherri Ballbach
Filer Authorized By:	Douglas James Crisman
Attorney Docket Number:	104402-5002-US
Receipt Date:	24-SEP-2014
Filing Date:	18-JUL-2014
Time Stamp:	17:44:35
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	Miscellaneous Incoming Letter	104402-5002-US_ResponseToNoticeOfIncompleteReply.pdf	736584 887f76024d6cd3d8abc621d2951ab8d80e551273	no	107

Warnings:	
Information:	

Total Files Size (in bytes):	736584

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.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 14/335,762

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	70		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	300		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	360		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	28 minus 20 =	* 8	x 40 =	320	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*	x 210 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	1050		TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

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
14/335,762	07/18/2014	2876	1120	104402-5002-US	28	3

CONFIRMATION NO. 6199

UPDATED FILING RECEIPT

24341
MORGAN, LEWIS & BOCKIUS LLP (PA)
2 PALO ALTO SQUARE
3000 EL CAMINO REAL, SUITE 700
PALO ALTO, CA 94306

OC000000071021516

Date Mailed: 10/01/2014

Receipt is acknowledged of this non-provisional 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 APPLICANT, 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 Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections 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**

Inventor(s)

Paresh K. Patel, Portland, OR;
Chau M. Doan, Beaverton, OR;

Applicant(s)

Paresh K. Patel, Portland, OR;
Chau M. Doan, Beaverton, OR;

Power of Attorney: None

Domestic Applications for which benefit is claimed - None.
A proper domestic benefit claim must be provided in an Application Data Sheet in order to constitute a claim for domestic benefit. See 37 CFR 1.76 and 1.78.

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.

If Required, Foreign Filing License Granted: 07/29/2014

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 14/335,762**

Projected Publication Date: 01/21/2016

Non-Publication Request: No

Early Publication Request: No
** **SMALL ENTITY** **

Title

Method and System for Performing Mobile Device-To-Machine Payments

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

Electronically filed: October 14, 2014

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application of:	Paresh K. Patel et al.	Confirmation No.:	6199
Serial No.:	14/335,762	Art Unit:	2876
Filed:	July 18, 2014	Examiner:	To Be Assigned
For:	*Method and System for Performing Mobile Device-To-Machine Payments*	Attorney Docket No:	104402-5002-US

SUPPLEMENTAL APPLICATION DATA SHEET

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

Sir:

Please find attached a Supplemental Application Data Sheet with the Domestic Benefit/National Stage Information properly underlined. Please send us an updated filing receipt that lists the priority claim information.

No fee is believed due at this time, but the Commissioner is hereby authorized to charge the required fees or credit any overpayments to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no. 104402-5002-US).

Respectfully submitted,

Date: October 14, 2014

39,951
Douglas J. Crisman (Reg. No.)
MORGAN, LEWIS & BOCKIUS LLP
2 Palo Alto Square
3000 El Camino Real, Suite 700
Palo Alto, CA 94306
(650) 843-4000

PTO/AIA/14 (11-13)
Approved for use through 01/31/2014. OMB 0651-0032
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.

SUPPLEMENTAL **Application Data Sheet 37 CFR 1.76**	Attorney Docket Number	104402-5002-US
	Application Number	
Title of Invention	Method and System for Performing Mobile Device-To-Machine Payments	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
Dr.	Paresh	K.	Patel	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Portland	State/Province	OR	Country of Residence	US

Mailing Address of Inventor:

Address 1	12815 NE Marx Street		
Address 2			
City	Portland	**State/Province**	OR
Postal Code	97230	**Country**	US

Inventor 2 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Chau	M.	Doan	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Beaverton	State/Province	OR	Country of Residence	US

Mailing Address of Inventor:

Address 1	12815 NE Marx Street		
Address 2			
City	Portland	**State/Province**	OR
Postal Code	97230	**Country**	US

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

PTO/AIA/14 (11-13)
Approved for use through 01/31/2014. OMB 0651-0032
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.

SUPPLEMENTAL **Application Data Sheet 37 CFR 1.76**	Attorney Docket Number	104402-5002-US
	Application Number	
Title of Invention	Method and System for Performing Mobile Device-To-Machine Payments	

☐ **An Address is being provided for the correspondence Information of this application.**			
Customer Number	24341		
Email Address		Add Email	Remove Email

Application Information:

Title of the Invention	Method and System for Performing Mobile Device-To-Machine Payments		
Attorney Docket Number	104402-5002-US	**Small Entity Status Claimed**	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	44	**Suggested Figure for Publication (if any)**	

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)
☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	24341		

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) 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.
When referring to the current application, please leave the application number blank.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Continuation of	14/214644	2014-03-14
Prior Application Status	Pending		Remove

PTO/AIA/14 (11-13)
Approved for use through 01/31/2014. OMB 0651-0032
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.

SUPPLEMENTAL **Application Data Sheet 37 CFR 1.76**	Attorney Docket Number	104402-5002-US
	Application Number	
Title of Invention	Method and System for Performing Mobile Device-To-Machine Payments	

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
14/214644	Claims benefit of provisional	61/917936	2013-12-18
Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
14/214644	Continuation in part of	29/477025	2013-12-18

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button.

Foreign Priority Information:

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(d). When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX)[i] the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(h)(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).

Remove

Application Number	Country[i]	Filing Date (YYYY-MM-DD)	Access Code[i] (if applicable)

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button.

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Authorization to Permit Access:

☐ Authorization to Permit Access to the Instant Application by the Participating Offices

PTO/AIA/14 (11-13)
Approved for use through 01/31/2014. OMB 0651-0032
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.

SUPPLEMENTAL **Application Data Sheet 37 CFR 1.76**	Attorney Docket Number	104402-5002-US
	Application Number	
Title of Invention	Method and System for Performing Mobile Device-To-Machine Payments	

If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the instant patent application is filed access to the instant patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the instant patent application is filed to have access to the instant patent application.

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the instant patent application with respect to: 1) the instant patent application-as-filed; 2) any foreign application to which the instant patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the instant patent application; and 3) any U.S. application-as-filed from which benefit is sought in the instant patent application.

In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date o f filing this Authorization.

Applicant 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.

Applicant 1

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. 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. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

◯ Assignee	◯ Legal Representative under 35 U.S.C. 117	◯ Joint Inventor
◯ Person to whom the inventor is obligated to assign.	◯ Person who shows sufficient proprietary interest	

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 :

If the Applicant is an Organization check here. ☒

Organization Name	PayRange Inc.

Mailing Address Information For Applicant:

Address 1	12815 NE Marx Street		
Address 2			
City	Portland	**State/Province**	OR
Country	US	Postal Code	97230
Phone Number		Fax Number	

PTO/AIA/14 (11-13)
Approved for use through 01/31/2014. OMB 0651-0032
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.

SUPPLEMENTAL **Application Data Sheet 37 CFR 1.76**	Attorney Docket Number	104402-5002-US
	Application Number	
Title of Invention	Method and System for Performing Mobile Device-To-Machine Payments	

Email Address	

Additional Applicant Data may be generated within this form by selecting the Add button.

Assignee Information including Non-Applicant Assignee Information:

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

Assignee 1

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication . An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

If the Assignee or Non-Applicant Assignee is an Organization check here. ☐

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information For Assignee including Non-Applicant Assignee:

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

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button.

Signature:

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

Signature				Date (YYYY-MM-DD)	2014-10-14
First Name	Douglas J.	Last Name	Crisman	Registration Number	39951

Additional Signature may be generated within this form by selecting the Add button.

PTO/AIA/14 (11-13)
Approved for use through 01/31/2014. OMB 0651-0032
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.

SUPPLEMENTAL **Application Data Sheet 37 CFR 1.76**	Attorney Docket Number	104402-5002-US
	Application Number	
Title of Invention	Method and System for Performing Mobile Device-To-Machine Payments	

This collection of information is required by 37 CFR 1.76. 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 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet 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 records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent C o o p eration 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.

Electronic Acknowledgement Receipt

EFS ID:	20415696
Application Number:	14335762
International Application Number:	
Confirmation Number:	6199
Title of Invention:	Method and System for Performing Mobile Device-To-Machine Payments
First Named Inventor/Applicant Name:	Paresh K. Patel
Customer Number:	24341
Filer:	Douglas James Crisman/Linda Quintana
Filer Authorized By:	Douglas James Crisman
Attorney Docket Number:	104402-5002-US
Receipt Date:	14-OCT-2014
Filing Date:	18-JUL-2014
Time Stamp:	19:54:56
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		104402-5002-US_SupplementalADS.pdf	505035 d2704602bb7e804e14b3a0cc4d4d627d051 14c93	yes	8

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Transmittal Letter	1	1
	Application Data Sheet	2	8
Warnings:			
Information:			
	Total Files Size (in bytes):	505035	

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

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

MAILED
OCT 30 2014
OFFICE OF PETITIONS

MORGAN, LEWIS & BOCKIUS LLP (PA)
2 PALO ALTO SQUARE
3000 EL CAMINO REAL, SUITE 700
PALO ALTO CA 94306

Doc Code: TRACK1.GRANT

Decision Granting Request for Prioritized Examination (Track I or After RCE)	Application No.: 14/335,762

1. THE REQUEST FILED 7/18/14 IS **GRANTED**.

The above-identified application has met the requirements for prioritized examination

A. ☒ for an original nonprovisional application (Track I).
B. ☐ for an application undergoing continued examination (RCE).

2. **The above-identified application will undergo prioritized examination.** The application will be accorded special status throughout its entire course of prosecution until one of the following occurs:

A. filing a **petition for extension of time** to extend the time period for filing a reply;
B. filing an **amendment to amend the application to contain more than four independent claims, more than thirty total claims**, or a multiple dependent claim;
C. filing a **request for continued examination**;
D. filing a notice of appeal;
E. filing a request for suspension of action;
F. mailing of a notice of allowance;
G. mailing of a final Office action;
H. completion of examination as defined in 37 CFR 41.102; or
I. abandonment of the application.

Telephone inquiries with regard to this decision should be directed to Terri Johnson at 571-272-2991. In his/her absence, calls may be directed to Brian Brown at 571-272-5338.

/Terri Johnson/ — Paralegal Specialist

[*Signature*] — (Title)

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.
14/335,762	07/18/2014	Paresh K. Patel	104402-5002-US	6199

24341 7590 12/10/2014

MORGAN, LEWIS & BOCKIUS LLP (PA)
2 PALO ALTO SQUARE
3000 EL CAMINO REAL, SUITE 700
PALO ALTO, CA 94306

EXAMINER
NIGH, JAMES D

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
12/10/2014	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

padocketingdepartment@morganlewis.com
vskliba@morganlewis.com

Office Action Summary	Application No. 14/335,762	Applicant(s) PATEL ET AL.	
	Examiner JAMES D. NIGH	Art Unit 3685	AIA (First Inventor to File) Status Yes

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 July 2014*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ 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.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) *1-28* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-28* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, 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.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ 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)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

Priority

CONTINUATION

2. This application is a continuation application of U.S. application no. 14/214,644 filed on 14 March 2014, now U.S. Patent 8,856,045 ("Parent Application"). See MPEP §201.07. In accordance with MPEP §609.02 *A.* 2 and MPEP §2001.06(b) (last paragraph), the Examiner has reviewed and considered the prior art cited in the Parent Application. Also in accordance with MPEP §2001.06(b) (last paragraph), all documents cited or considered 'of record' in the Parent Application are now considered cited or 'of record' in this application. Additionally, Applicant(s) are reminded that a listing of the information cited or 'of record' in the Parent Application need not be resubmitted in this application unless Applicants desire the information to be printed on a patent issuing from this application. See MPEP §609.02 *A.* 2. Finally, Applicants are reminded that the prosecution history of the Parent Application is relevant in this application. See *e.g., Microsoft Corp. v. Multi-Tech Sys., Inc.*, 357 F.3d 1340, 1350, 69 USPQ2d 1815, 1823 (Fed. Cir. 2004) (holding that statements made in prosecution of one patent are relevant to the scope of all sibling patents).

3. Applicant's claim for the benefit of U.S. provisional patent application 61/917,936 filed 18 December 2013 under 35 U.S.C. 119(e) is acknowledged.

Continuation-In-Part

4. This application is a continuation-in-part ("CIP") application of U.S. application no. 29/477,025 filed on 18 December 2013 ("Parent Application"). See MPEP §201.08. In accordance with MPEP §609.02 *A.* 2 and MPEP §2001.06(b) (last paragraph), the Examiner has reviewed and considered the prior art cited in the Parent Application. Also in accordance with MPEP §2001.06(b) (last paragraph), all documents cited or considered 'of record' in the Parent Application are now considered cited or 'of record' in this application. Additionally, Applicant(s) are reminded that a listing of the information cited or 'of record' in the Parent Application need not be resubmitted in this application unless Applicants desire the information to be printed on a patent issuing from this application. See MPEP §609.02 *A.* 2. Finally, Applicants are reminded that the prosecution history of the Parent Application is relevant in this application. See *e.g., Microsoft Corp. v. Multi-Tech Sys., Inc.*, 357 F.3d 1340, 1350, 69 USPQ2d 1815, 1823 (Fed. Cir. 2004) (holding that statements made in prosecution of one patent are relevant to the scope of all sibling patents).

Claim Rejections - 35 USC § 101

5. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

6. Claims 1-28 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter because the claims as a whole,

considering all claim elements both individually and in combination, do not amount to significantly more than an abstract idea.

7. Claims 1-12 are directed towards the abstract idea of payment authorization which is an old and well known fundamental economic practice. The additional elements or combination of elements in claims 1-12 other than the abstract idea per se amount to no more than mere instructions to implement the idea on a computer. Viewed as a whole, these additional claim elements do not provide meaningful limitations to transform the abstract idea into a patent eligible application of the abstract idea such that claims 1-12 amount to significantly more than the abstract idea itself. Therefore, claims 1-12 are rejected under 35 U.S.C. 101 as being directed to non-statutory subject matter.

8. Claims 13-20 are directed towards the abstract idea of payment authorization which is an old and well known fundamental economic practice. The additional elements or combination of elements in claims 13-20 other than the abstract idea per se amount to no more than recitation of generic computer structure that serves to perform generic computer functions that are well-understood, routine, and conventional activities previously known to the industry. Viewed as a whole, these additional claim elements do not provide meaningful limitations to transform the abstract idea into a patent eligible application of the abstract idea such that claims 13-20 amount to significantly more than the abstract idea itself. Therefore, claims 13-20 are rejected under 35 U.S.C. 101 as being directed to non-statutory subject matter.

9. Claims 21-28 are directed towards the abstract idea of payment authorization which is an old and well known fundamental economic practice. The additional elements or combination of elements in claims 21-28 other than the abstract idea per se amount to no more than mere instructions to implement the idea on a computer. Viewed as a whole, these additional claim elements do not provide meaningful limitations to transform the abstract idea into a patent eligible application of the abstract idea such that claims 21-28 amount to significantly more than the abstract idea itself. Therefore, claims 21-28 are rejected under 35 U.S.C. 101 as being directed to non-statutory subject matter.

Conclusion

Please note:

A recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claim.

Applicant(s) are reminded that optional or conditional elements do not narrow the claims because they can always be omitted. See *e.g.* MPEP § 2103 I C: "Language that suggests or makes optional but does not require steps to be performed or does not limit a claim to a particular structure does not limit the scope of a claim or claim limitation. [Emphasis in original.]"; and *In re Johnston,* 435 F.3d 1381, 77 USPQ2d 1788, 1790 (Fed. Cir. 2006) ("As a matter of linguistic precision, optional elements do not narrow the claim because they can always be omitted.").

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JAMES D. NIGH whose telephone number is (571)270-5486. The examiner can normally be reached on Monday-Friday 9:00 - 5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Calvin L. Hewitt II can be reached on 571-272-6709. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/JAMES D NIGH/
Primary Examiner, Art Unit 3685

Notice of References Cited	Application/Control No. 14/335,762	Applicant(s)/Patent Under Reexamination PATEL ET AL.	
	Examiner JAMES D. NIGH	Art Unit 3685	Page 1 of 3

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-5,844,808 A	12-1998	Konsmo et al.	700/244
*	B	US-6,462,644 B1	10-2002	Howell et al.	340/5.92
*	C	US-6,584,309 B1	06-2003	Whigham, Roger Chris	455/414.1
*	D	US-2004/0049454 A1	03-2004	Kanno et al.	705/039
*	E	US-7,085,556 B2	08-2006	Offer, Gero	455/414.1
*	F	US-7,127,236 B2	10-2006	Khan et al.	455/414.1
*	G	US-2008/0033880 A1	02-2008	Fiebiger et al.	705/044
*	H	US-2008/0154735 A1	06-2008	Carlson, Mark	705/16
*	I	US-2008/0154727 A1	06-2008	Carlson, Mark	705/14
*	J	US-2008/0183480 A1	07-2008	Carlson et al.	705/1
*	K	US-2008/0167991 A1	07-2008	Carlson et al.	705/50
*	L	US-2008/0201226 A1	08-2008	Carlson et al.	705/14
*	M	US-2008/0255947 A1	10-2008	Friedman, Brian	705/14

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Notice of References Cited	Application/Control No. 14/335,762	Applicant(s)/Patent Under Reexamination PATEL ET AL.	
	Examiner JAMES D. NIGH	Art Unit 3685	Page 2 of 3

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2009/0119190 A1	05-2009	Realini, Carol	705/30
*	B	US-7,721,958 B2	05-2010	Belfer et al.	235/381
*	C	US-7,848,980 B2	12-2010	Carlson, Mark	705/35
*	D	US-2011/0153436 A1	06-2011	Krampe, Richard L.	705/16
*	E	US-2011/0153442 A1	06-2011	Krampe, Richard L.	705/21
*	F	US-2011/0251910 A1	10-2011	Dimmick, James	705/17
*	G	US-2012/0011024 A1	01-2012	Dorsey et al.	705/26.41
*	H	US-2012/0078735 A1	03-2012	Bauer et al.	705/16
*	I	US-2012/0231844 A1	09-2012	Coppinger, Paul D.	455/558
*	J	US-D669,899 S	10-2012	Cheng, Jung-Ching	D14/435.1
*	K	US-2012/0303528 A1	11-2012	Weiner et al.	705/44
*	L	US-2013/0030931 A1	01-2013	Moshfeghi, Mehran	705/16
*	M	US-8,346,670 B2	01-2013	Hasson et al.	705/75

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Notice of References Cited	Application/Control No. 14/335,762	Applicant(s)/Patent Under Reexamination PATEL ET AL.	
	Examiner JAMES D. NIGH	Art Unit 3685	Page 3 of 3

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-8,356,754 B2	01-2013	Johnson et al.	235/472.01
*	B	US-8,376,227 B2	02-2013	Hammad et al.	235/384
*	C	US-8,396,589 B2	03-2013	Katzenstein Garibaldi et al.	700/232
*	D	US-8,489,140 B2	07-2013	Weiner et al.	455/550.1
*	E	US-8,517,766 B2	08-2013	Golko et al.	439/607.41
*	F	US-2013/0267121 A1	10-2013	Hsu, Ching-Jen	439/625
*	G	US-8,596,528 B2	12-2013	Fernandes et al.	235/380
*	H	US-8,615,445 B2	12-2013	Dorsey et al.	705/26.1
*	I	US-2014/0040028 A1	02-2014	King et al.	705/14.53
*	J	US-2014/0040117 A1	02-2014	Jain, Deepak	705/39
*	K	US-8,769,643 B1	07-2014	Ben Ayed, Mourad	726/5
*	L	US-8,838,481 B2	09-2014	Moshfeghi, Mehran	705/16
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

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

BIB DATA SHEET

CONFIRMATION NO. 6199

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
14/335,762	07/18/2014	705	3685	104402-5002-US

APPLICANTS

INVENTORS

Paresh K. Patel, Portland, OR;
Chau M. Doan, Beaverton, OR;

**** CONTINUING DATA ***************************

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED **** ** SMALL ENTITY **
07/29/2014

Foreign Priority claimed ☐ Yes ☑ No 35 USC 119(a-d) conditions met ☐ Yes ☑ No Verified and Acknowledged /JAMES D NIGH/ Examiner's Signature	☐ Met after Allowance Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		OR	44	28	3

ADDRESS

MORGAN, LEWIS & BOCKIUS LLP (PA)
2 PALO ALTO SQUARE
3000 EL CAMINO REAL, SUITE 700
PALO ALTO, CA 94306
UNITED STATES

TITLE

Method and System for Performing Mobile Device-To-Machine Payments

FILING FEE RECEIVED		
1120	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	229	(SMS near5 payment) (payment near5 processor)	US-PGPUB; USPAT	AND	ON	2014/12/03 15:33
S2	224	(SMS near5 payment) (payment near5 processor) @ad<="20140314"	US-PGPUB; USPAT	AND	ON	2014/12/03 15:33
S3	12	(SMS near5 payment near5 authoriz$6) (payment near5 processor) @ad<="20140314"	US-PGPUB; USPAT	AND	ON	2014/12/03 15:34
S4	2047	square.as. @ad<="20140314"	US-PGPUB; USPAT	AND	ON	2014/12/04 11:34
S5	81	square.as. @ad<="20140314" payment	US-PGPUB; USPAT	AND	ON	2014/12/04 11:34
S6	61	square.as. @ad<="20140314" payment wifi	US-PGPUB; USPAT	AND	ON	2014/12/04 13:09
S7	22	square.as. @ad<="20140314" payment wifi gateway	US-PGPUB; USPAT	AND	ON	2014/12/04 13:10
S8	1	("20120011024").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2014/12/04 14:12
S9	6939	(authoriz$8 near5 request) ((purchase or transaction) near10 (payment or debit or funds)) ((send or transmit) near10 authoriz$8)	US-PGPUB; USPAT	AND	ON	2014/12/04 14:15
S10	239	(authoriz$8 near5 request) ((purchase or transaction) near10 (payment or debit or funds)) ((send or transmit) near10 authoriz$8) (authoriz$8 near20 (zone or proximity))	US-PGPUB; USPAT	AND	ON	2014/12/04 14:17
S11	20	(authoriz$8 near5 request) ((purchase or transaction) near10 (payment or debit or funds)) ((send or transmit) near10 authoriz$8) RSSI	US-PGPUB; USPAT	AND	ON	2014/12/04 14:27
S12	1	("20130030931").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2014/12/04 15:27
S13	4167	(payment near3 gateway)	US-PGPUB; USPAT	AND	ON	2014/12/05 10:57
S14	2189	(payment near3 gateway) (request near3 authoriz$8)	US-PGPUB; USPAT	AND	ON	2014/12/05 10:57

S15	820	(payment near3 gateway) (request near3 authoriz$8) (authoriz$8 near5 (response or obtain$5))	US-PGPUB; USPAT	AND	ON	2014/12/05 10:58
S16	23	(payment near3 gateway) ((request near3 authoriz$8) near10 (bluetooth or wifi or NFC)) (authoriz$8 near5 (response or obtain$5))	US-PGPUB; USPAT	AND	ON	2014/12/05 11:00

EAST Search History (Interference)

< This search history is empty>

12/ 5/ 2014 1:40:29 PM
C:\ Users\ jnigh\ Documents\ EAST\ Workspaces\ 14335762.wsp

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	229	(SMS near5 payment) (payment near5 processor)	US-PGPUB; USPAT	AND	ON	2014/12/03 15:33
S2	224	(SMS near5 payment) (payment near5 processor) @ad<="20140314"	US-PGPUB; USPAT	AND	ON	2014/12/03 15:33
S3	12	(SMS near5 payment near5 authoriz$6) (payment near5 processor) @ad<="20140314"	US-PGPUB; USPAT	AND	ON	2014/12/03 15:34
S4	2047	square.as. @ad<="20140314"	US-PGPUB; USPAT	AND	ON	2014/12/04 11:34
S5	81	square.as. @ad<="20140314" payment	US-PGPUB; USPAT	AND	ON	2014/12/04 11:34
S6	61	square.as. @ad<="20140314" payment wifi	US-PGPUB; USPAT	AND	ON	2014/12/04 13:09
S7	22	square.as. @ad<="20140314" payment wifi gateway	US-PGPUB; USPAT	AND	ON	2014/12/04 13:10
S8	1	("20120011024").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2014/12/04 14:12
S9	6939	(authoriz$8 near5 request) ((purchase or transaction) near10 (payment or debit or funds)) ((send or transmit) near10 authoriz$8)	US-PGPUB; USPAT	AND	ON	2014/12/04 14:15
S10	239	(authoriz$8 near5 request) ((purchase or transaction) near10 (payment or debit or funds)) ((send or transmit) near10 authoriz$8) (authoriz$8 near20 (zone or proximity))	US-PGPUB; USPAT	AND	ON	2014/12/04 14:17
S11	20	(authoriz$8 near5 request) ((purchase or transaction) near10 (payment or debit or funds)) ((send or transmit) near10 authoriz$8) RSSI	US-PGPUB; USPAT	AND	ON	2014/12/04 14:27
S12	1	("20130030931").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2014/12/04 15:27
S13	4167	(payment near3 gateway)	US-PGPUB; USPAT	AND	ON	2014/12/05 10:57
S14	2189	(payment near3 gateway) (request near3 authoriz$8)	US-PGPUB; USPAT	AND	ON	2014/12/05 10:57
S15	820	(payment near3 gateway) (request near3	US-	AND	ON	2014/12/05

		authoriz$8) (authoriz$8 near5 (response or obtain$5))	PGPUB; USPAT			10:58
S16	23	(payment near3 gateway) ((request near3 authoriz$8) near10 (bluetooth or wifi or NFC)) (authoriz$8 near5 (response or obtain$5))	US-PGPUB; USPAT	AND	ON	2014/12/05 11:00
S17	36	("20080167991" | "7127236" | "7721958" | "20080255947" | "20090119190" | "20110040686" | "20080154735" | "20080201226" | "6584309" | "7848980" | "7848980" | "20110153442" | "20080183480" | "20130267121" | "20080033880" | "20120303528" | "8645971" | "20110251910" | "8376227" | "6462644" | "8396589" | "8489140" | "8517766" | "D669899" | "20040049454" | "20120078735" | "20120231844" | "20140040028" | "20080154727" | "20110040686" | "5844808" | "20140040117" | "8356754" | "8396589" | "8596528" | "20110153436" | "7085556" | "20090327089" | "8346670").PN.	US-PGPUB; USPAT	AND	ON	2014/12/05 13:41

EAST Search History (Interference)

< This search history is empty>

12/ 5/ 2014 1:46:51 PM
C:\ Users\ jnigh\ Documents\ EAST\ Workspaces\ 14335762.wsp

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14335762	PATEL ET AL.
	Examiner	Art Unit
	JAMES D NIGH	3685

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES		
Search Notes	Date	Examiner
EAST Text Search	12/04/2014	JDN

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

	/JAMES D NIGH/ Primary Examiner.Art Unit 3685

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.
14/335,762	07/18/2014	Paresh K. Patel	104402-5002-US	6199

24341 7590 01/07/2015

MORGAN, LEWIS & BOCKIUS LLP (PA)
2 PALO ALTO SQUARE
3000 EL CAMINO REAL, SUITE 700
PALO ALTO, CA 94306

EXAMINER
NIGH, JAMES D

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
01/07/2015	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

padocketingdepartment@morganlewis.com
vskliba@morganlewis.com

Applicant-Initiated Interview Summary	Application No.	Applicant(s)	
	14/335,762	PATEL ET AL.	
	Examiner	Art Unit	
	JAMES D. NIGH	3685	

All participants (applicant, applicant's representative, PTO personnel):

(1) *JAMES D. NIGH*. (3)_____.

(2) *Douglas J. Grisman (Reg. No. 39,951)*. (4)_____.

Date of Interview: *30 December 2014*.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☒ No.
If Yes, brief description: _____.

Issues Discussed ☒101 ☐112 ☐102 ☐103 ☒Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *1-28*.

Identification of prior art discussed: *N/A*.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Applicant requested clarification on the Office Action mailed 10 December 2014. Examiner indicated that like the parent application 14/214644 which was also examined by this Examiner no prior art read on claims 1-28, therefore the only rejection applicable to the claims was the section 101 rejection indicated in the Office Action and that the claims would otherwise be allowable if the 101 rejection is overcome..

Applicant recordation instructions: The formal written reply to the last Office action must include the substance of the interview. (See MPEP section 713.04). If a reply to the last Office action has already been filed, applicant is given a non-extendable period of the longer of one month or thirty days from this interview date, or the mailing date of this interview summary form, whichever is later, to file a statement of the substance of the interview

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/JAMES D NIGH/ Primary Examiner, Art Unit 3685	

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews
Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.
All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:
- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:
1) A brief description of the nature of any exhibit shown or any demonstration conducted,
2) an identification of the claims discussed,
3) an identification of the specific prior art discussed,
4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
5) a brief identification of the general thrust of the principal arguments presented to the examiner,
   (The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
6) a general indication of any other pertinent matters discussed, and
7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

INFORMATION DISCLOSURE CITATION Substitute for Form 1449-PTO				*Electronically filed January 15, 2015*	
				Application Number	*14/335,762*
				Filing Date	*July 18, 2014*
				First Named Inventor	*Paresh K. Patel*
				Art Unit	*3685*
				Examiner Name	*Nigh, James D*
Sheet	1	of	3	Attorney Docket Number	*104402-5002-US*

PATENT DOCUMENTS					
Examiner Initials	Cite No.[1]	Document Number Number - Kind Code[2]	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		D669,899 S	10-30-2012	Cheng S	
		5,844,808	12-01-1998	Konsmo, et al.	
		5,892,900	04-06-1999	Ginter et al.	
		6,462,644 B1	10-08-2002	Howell, et al.	
		6,584,309 B1	06-24-2003	Whigham	
		7,085,556 B2	08-01-2006	Offer	
		7,127,236 B2	10-24-2006	Khan, et al.	
		7,721,958 B2	05-25-2010	Belfer, et al.	
		7,848,980 B2	12-07-2010	Carlson	
		8,346,670 B2	01-01-2013	Hasson et al.	
		8,356,754 B2	01-22-2013	Johnson et al.	
		8,376,227 B2	02-19-2013	Hammad et al.	
		8,396,589 B2	03-12-2013	Katzenstein Garibaldi et al.	
		8,412,626 B2	04-02-2013	Hirson et al.	
		8,489,140 B2	07-16-2013	Weiner et al.	
		8,517,766 B2	08-27-2013	Golko et al.	
		8,548,426 B2	10-01-2013	Smith	
		8,583,496 B2	11-12-2013	Yoo et al.	
		8,596,528 B2	12-03-2013	Fernandes et al.	
		8,615,445 B2	12-24-2013	Dorsey et al.	
		8,645,971 B2	02-04-2014	Carlson et al.	
		8,700,530 B2	04-15-2014	Smith	
		8,769,643 B1	07-01-2014	Ben Ayed	
		8,838,481 B2	09-16-2014	Moshfeghi	
		8,856,045 B1	10-07-2014	Patel et al.	
		2003/0158891 A1	08-21-2003	Lei et al.	
		2004/0049454 A1	03-11-2004	Kanno et al.	
		2007/0187491 A1	08-16-2007	Godwin et al.	
		2008/0033880 A1	02-07-2008	Fiebiger et al.	
		2008/0154727 A1	06-26-2008	Carlson	
		2008/0154735 A1	06-26-2008	Carlson	
		2008/0167991 A1	07-10-2008	Carlson et al.	
		2008/0183480 A1	07-31-2008	Carlson et al.	
		2008/0201226 A1	08-21-2008	Carlson et al.	
		2008/0208762 A1	08-28-2008	Arthur et al.	
		2008/0255947 A1	10-16-2008	Friedman	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kind Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

INFORMATION DISCLOSURE CITATION Substitute for Form 1449-PTO				*Electronically filed January 15, 2015*	
				Application Number	*14/335,762*
				Filing Date	*July 18, 2014*
				First Named Inventor	*Paresh K. Patel*
				Art Unit	*3685*
				Examiner Name	*Nigh, James D*
Sheet	2	of	3	Attorney Docket Number	*104402-5002-US*

		2009/0037284 A1	02-05-2009	Lewis et al.	
		2009/0119190 A1	05-07-2009	Realini	
		2009/0327089 A1	12-31-2009	Kanno et al.	
		2011/0040686 A1	02-17-2011	Carlson	
		2011/0153436 A1	06-23-2011	Krampe	
		2011/0153442 A1	06-23-2011	Krampe	
		2011/0251910 A1	10-13-2011	Dimmick	
		2012/0011024 A1	01-12-2012	Dorsey et al.	
		2012/0036045 A1	02-09-2012	Lowe et al.	
		2012/0078735 A1	03-29-2012	Bauer et al.	
		2012/0197740 A1	08-02-2012	Grigg et al.	
		2012/0231844 A1	09-13-2012	Coppinger	
		2012/0246074 A1	09-27-2012	Annamalai et al.	
		2012/0290472 A1	11-15-2012	Mullen et al.	
		2012/0030831 A1	02-02-2012	Moshfeghi	
		2012/0303528 A1	11-29-2012	Weiner et al.	
		2013/0030831 A1	01-31-2013	Moshfeghi	
		2013/0085835 A1	04-04-2013	Horowitz	
		2013/0117738 A1	05-09-2013	Livingston et al.	
		2013/0124289 A1	05-16-2013	Fisher	
		2013/0166448 A1	06-27-2013	Narayanan	
		2013/0217333 A1	08-22-2013	Sprigg et al.	
		2013/0246171 A1	09-19-2013	Carapelli	
		2013/0246364 A1	09-19-2013	Bhavith	
		2013/0267176 A1	10-10-2013	Hertel et al.	
		2013/0267121 A1	10-10-2013	Hsu	
		2013/0311379 A1	11-21-2013	Smith	
		2013/0311382 A1	11-21-2013	Fosmark et al.	
		2014/0019367 A1	01-16-2014	Khan et al.	
		2014/0040028 A1	02-06-2014	King et al.	
		2014/0040117 A1	02-06-2014	Jain	
		2014/0074723 A1	03-13-2014	Kamat	
		2014/0100977 A1	04-10-2014	Davis	
		2014/0180852 A1	06-26-2014	Kamat	
		2014/0201066 A1	07-17-2014	Roux et al.	
		2014/0249995 A1	09-04-2014	Ogilvy	

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite	Foreign Patent Document	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines,	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kind Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

INFORMATION DISCLOSURE CITATION Substitute for Form 1449-PTO				*Electronically filed January 15, 2015*	
				Application Number	*14/335,762*
				Filing Date	*July 18, 2014*
				First Named Inventor	*Paresh K. Patel*
				Art Unit	*3685*
				Examiner Name	*Nigh, James D*
Sheet	3	of	3	Attorney Docket Number	*104402-5002-US*

	No.	Country Code[3] – Number[4] - Kind Code[5] *(if known*	MM-DD-YYYY		Where Relevant Passages or Relevant Figures Appear	
		WO2008/083022 A1	07-10-2008	Visa USA Inc		
		WO2008/083025 A2	07-10-2008	Visa USA Inc		
		WO2008/083078 A2	07-10-2008	Visa USA Inc		
		WO2008/083089 A1	07-10-2008	Visa USA Inc		
		WO2008/083105 A2	07-10-2008	Visa USA Inc		
		WO2008/083115 A1	07-10-2008	Visa USA Inc		
		WO2008/083119 A1	07-10-2008	Visa USA Inc		
		WO2013/177416 A2	11-28-2013	Bush et al.		

NON PATENT LITERATURE DOCUMENTS

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, page(s), volume-issue number(s), publisher, city and/or country where published
		Bing, Bing Images Search: "dongle", http://www.bing.com/images/search?q=dongle&FORM+HDRSC2, December 5, 2013, 2 pgs,
		Google, Chromecast, htttp://www.google.com/intl/devices/chromecast/, December 12, 2013, 4 pgs.
		Madlmayr et al., "Near Field Communication Based Mobile Payment System," Austrian Research Funding Agency, Project 811408, 6 March 2008, 13 pgs.
		Patel, Office Action Serial No. 14/321,733, dated 21AUG2014, 9 pgs.
		Patel, Office Action Serial No. 14/320,534, dated 29OCT2014, 18 pgs.
		Patel, Final Office Action Serial No. 14/321,733, dated 14NOV2014, 11 pgs.
		Patel, Office Action Serial No. 14/321,717, dated 19DEC2014, 16 pgs.
		Patel, Office Action Serial No. 14/456,683, dated 02JAN2015, 10 pgs.
		Patel, Office Action Serial No. 14/458,199, dated 05JAN2015, 7 pgs.
		Provisional patent application 60/871,898, VALUE BASED OFFERS, inventor Mark Carlson, filed December 26, 2006. US Patent and Trademark Office, 169 pgs.

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kind Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Electronic Patent Application Fee Transmittal

Application Number:	14335762
Filing Date:	18-Jul-2014
Title of Invention:	Method and System for Performing Mobile Device-To-Machine Payments
First Named Inventor/Applicant Name:	Paresh K. Patel
Filer:	Douglas James Crisman/Edith Fuentes
Attorney Docket Number:	104402-5002-US

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:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	2806	1	90	90
		Total in USD ($)		**90**

Electronic Acknowledgement Receipt

EFS ID:	21225486
Application Number:	14335762
International Application Number:	
Confirmation Number:	6199
Title of Invention:	Method and System for Performing Mobile Device-To-Machine Payments
First Named Inventor/Applicant Name:	Paresh K. Patel
Customer Number:	24341
Filer:	Douglas James Crisman/Edith Fuentes
Filer Authorized By:	Douglas James Crisman
Attorney Docket Number:	104402-5002-US
Receipt Date:	15-JAN-2015
Filing Date:	18-JUL-2014
Time Stamp:	20:27:09
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$90
RAM confirmation Number	6799
Deposit Account	500310
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Foreign Reference	WO2008083022A1.pdf	1021047 36a80f9b2769c55d0fa15898fe4ebfe6c46e2301	no	27
Warnings:					
Information:					
2	Foreign Reference	WO2008083025A2.pdf	1158552 0e4145612c6d5d4e8ab13c7a0dcd69f5166bd2b9	no	30
Warnings:					
Information:					
3	Foreign Reference	WO2008083078A2.pdf	1337432 795ec351bffa27eeee0579c4fe548d81d67fabfe	no	31
Warnings:					
Information:					
4	Foreign Reference	WO2008083089A1.pdf	1310686 74cf8bc96a89b02f4066ea41492a94742fe7222f	no	31
Warnings:					
Information:					
5	Foreign Reference	WO2008083105A2.pdf	1311326 04064d013b3c0b5c8c250ba52cb7a10638551fe1	no	35
Warnings:					
Information:					
6	Foreign Reference	WO2008083115A1.pdf	1255117 c3f1b03738aca13010aa68433af2ad7b2a299e8e	no	35
Warnings:					
Information:					
7	Foreign Reference	WO2008083119A1.pdf	1287261 b068e1256801af3a9c58acaa63a0da9db116da6f	no	26
Warnings:					
Information:					

8	Foreign Reference	WO2013177416A2.pdf	3616295 f7ad29a646cddb95b31f0318ab93280897524afb	no	95
Warnings:					
Information:					
9	Non Patent Literature	Bing_Bing-Images-Search-Dongle.pdf	225377 4afed984a5581c0630637ee4f2962cb337d4e544	no	2
Warnings:					
Information:					
10	Non Patent Literature	Google_Chromecast.pdf	402631 f1d8193731d34bf9a335085067a2004e599ea82a	no	4
Warnings:					
Information:					
11	Non Patent Literature	Madlmayr_Near-Field-Communication-Based-Mobile.pdf	642775 ed138d7aba53f73a6799bdb89d3802d03ebf97c8	no	13
Warnings:					
Information:					
12	Other Reference-Patent/App/Search documents	Patel_Office-Action-14321733_082114.pdf	357879 97c5ff498bfcd84e1f79a678b6deb9213d3c3c57	no	9
Warnings:					
Information:					
13	Other Reference-Patent/App/Search documents	Patel_Office-Action-14320534_102914.pdf	628294 82b6389f86dba714b29c5c7329301fda7fddfbf9	no	18
Warnings:					
Information:					
14	Other Reference-Patent/App/Search documents	Patel_Final-Office-Action-14321733_111414.pdf	412699 f88f982609eeb3abd144a0dec1e9cf6d312673a6	no	11
Warnings:					
Information:					
15	Other Reference-Patent/App/Search documents	Patel_Office-Action-14321717_121914.pdf	578543 f9c3810dc6ab21110856adfb17117731bd1cb2e8	no	16
Warnings:					
Information:					
16	Other Reference-Patent/App/Search documents	Patel_Office-Action-14456683_010215.pdf	335617 dd2962c3ce06f3f56869652924a9c35b55eff7a1	no	10
Warnings:					
Information:					

17	Non Patent Literature	Patel_Office-Action-14458199_010515.pdf	270996 ad090c8ef10339b8e429795a8d2a2843f1c246af	no	7
Warnings:					
Information:					
18	Other Reference-Patent/App/Search documents	Provisional-Patent-Application-60871898-Mark-Carlson_122606.pdf	7517788 7d99b22320948335733a7c8c30b5dcbac7a88ff6	no	169
Warnings:					
Information:					
19		104402-5002US_IDS.pdf	405766 27f7ce7683bd762c85cc1a4f0ce088bf6bc76f07	yes	7

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Transmittal Letter	1	4
	Information Disclosure Statement (IDS) Form (SB08)	5	7

Warnings:					
Information:					
20	Fee Worksheet (SB06)	fee-info.pdf	30180 04f4202c69492ad1970455b5c458d4c4bd8ad481	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	24106261		

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.

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 July 2008 (10.07.2008)

PCT

(10) International Publication Number
WO 2008/083022 A1

(51) International Patent Classification:
G06Q 40/00 (2006.01)

(21) International Application Number:
PCT/US2007/088289

(22) International Filing Date:
20 December 2007 (20.12.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/871,898 26 December 2006 (26.12.2006) US
11/767,033 22 June 2007 (22.06.2007) US

(71) Applicants *(for all designated States except US)*: **VISA U.S.A. INC.** [US/US]; P.O. Box 8999, MS M3-2B, San Francisco, CA 94128 (US). **VISA INTERNATIONAL SERVICE ASSOCIATION** [US/US]; 900 Metro Center Boulevard, Foster City, CA 94404 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **CARLSON, Mark** [US/US]; 153 Miramontes Avenue, Half Moon Bay, CA 94019 (US).

(74) Agents: **JEWIK, Patrick, R.** et al.; Townsend and Townsend and Crew LLP, Two Embarcadero Center, 8th Floor, San Francisco, CA 94111 (US).

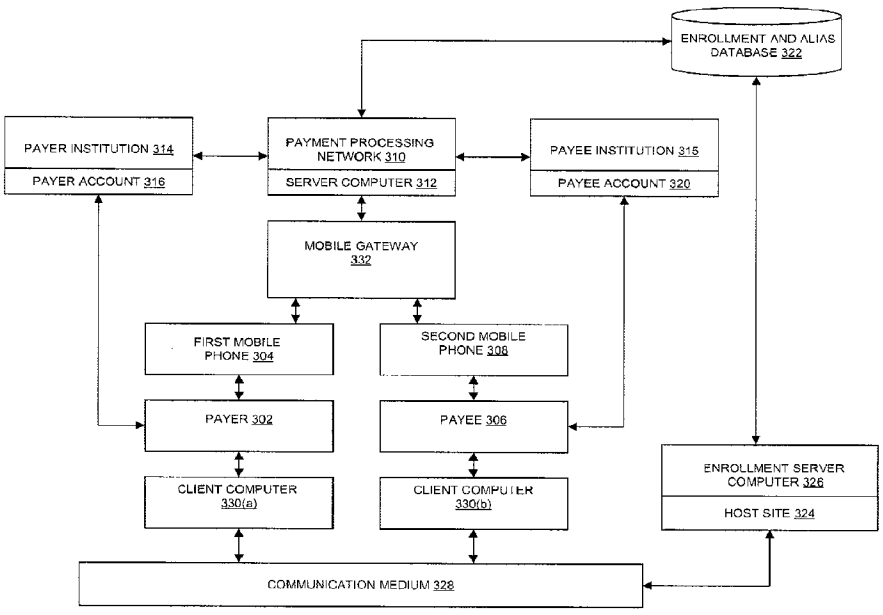
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN,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



(57) Abstract: Methods and systems are disclosed for allowing financial transactions to be conducted using mobile phones. A payer initiates a transaction by sending a payment request message from a mobile phone which specifies the payee and amount to be paid. Payees are identified by unique aliases, which are maintained in a database. Methods for assembling the enrollment and alias database are included.

WO 2008/083022 A1

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

MOBILE PAYMENT SYSTEM AND METHOD USING ALIAS

CROSS-REFERENCES TO RELATED APPLICATIONS

[0001] This patent application is a non-provisional of and claims priority to U.S. provisional patent application no. 60/871,898, filed on December 26, 2006, which is herein incorporated by reference in its entirety for all purposes.

BACKGROUND

[0002] The use of mobile phones to conduct financial transactions is growing in popularity. Various means of using mobile phones to conduct financial transactions have been tried. The most common involves sending a payment to a payee using the payee's cellular phone number as an identifier. This approach gives rise certain difficulties, however. First, the payee must have a cellular phone which is capable of receiving the payments. Second, the payer must know the payee's phone number. As cellular phone numbers tend to change frequently, a payer must make certain that the phone number being used is current. Otherwise, the payer runs the risk of sending a payment to an unintended third party, who has been assigned the intended payee's old phone number. Further, in some cases, the payee and payee may not wish to reveal personal information such as their cellular phone numbers to each other. Accordingly, there is a need for a new method of conducting financial transactions using phones.

[0003] Embodiments of the invention address these and other problems.

BRIEF SUMMARY

[0004] Embodiments of the invention are directed to methods and systems for allowing payments to be made using mobile phones.

[0005] One embodiment of the invention is directed to a method. The method comprises receiving a payment request message from a mobile phone operated by a payer, wherein the payment request message includes a request to pay a payee a predetermined amount of money, and wherein the payment request message

comprises a personal alias uniquely associated with the payee and a transaction amount. The payment request message is analyzed to determine if the payer is authorized to pay the payee. A payment notification message is sent to the payee indicating that a payment from the payer to the payee has been made.

[0006] Another embodiment of the invention is directed to a method. The method comprises receiving a payment request message from a payer, the payment request message comprising an amount of money to be paid to a payee and an alias associated with the payee, where the payment request message is sent by the payer via a mobile phone operated by the payer. An authentication request message is sent to the mobile phone in response to the message. An authentication token is received from the payer in response to sending the authentication request message. The authentication token is sent by the payer using the mobile phone, and the authentication token that is associated with the payer is verified. If the authentication token is verified as being associated with the payer, a payment for the amount of money to the payee using the alias is initiated.

[0007] Another embodiment of the invention is directed to a method. The method comprises receiving a registration request from a payee to create an alias uniquely associated with that payee, where the request specifies the alias requested. The payee operates a mobile phone and can receive or make payments using the alias and mobile phone. The alias is compared with other previously registered aliases associated with other payees. If the requested alias has not already been associated with another payee, the alias associated with the payee is registered.

[0008] Other embodiments of the invention are directed to systems, computer readable media, and devices adapted to implement the above methods.

[0009] These and other embodiments of the invention are described in further detail below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] FIG. 1 shows a block diagram of a system according to an embodiment of invention.

[0011] FIG. 2 shows a block diagram of components in a computer.

[0012] FIG. 3 shows a block diagram of components in a mobile phone.

[0013] FIG. 4 shows a flowchart illustrating an alias registration process.

[0014] FIG. 5 shows information that can be provided when registering aliases.

[0015] FIG. 6 shows a flowchart illustrating a payment method according to an embodiment of the invention.

DETAILED DESCRIPTION

[0016] Embodiments of the invention are directed to making person-to-person (P2P) and/or person-to-business (P2B) payments, using mobile phones. In embodiments of the invention, a payer may send a payment request message to a payment processing network. The payment request message identifies the desired payee using an alias, which is uniquely associated with the payee. The payment processing network may then determine who the payee is using an enrollment and alias database, and may forward the payment request message to a payer institution. The payer institution may be a payer bank and the payer may have a payer account associated with it. The payer institution may thereafter analyze the payment request message and may authorize or not authorize the transaction depending on whether the payer has sufficient credit and/or funds in the payer's account. If the payment request is approved by the payer institution, the payer institution may thereafter transfer funds from the payer's account at the payer institution to a payee account at a payee institution.

[0017] The payment request message may be sent from the payer's mobile phone in any suitable manner. In one example, a payer may send the payment request message to the payment processing network via a Web page accessed by the phone. In another example, the payer may send the payment request message to the payment processing network using an SMS message (i.e., a text message). In yet another example, the payer may send the payment request message to the payment processing network using a software application on the phone.

[0018] The payment transactions according to embodiments of the invention may take place in any suitable context. For example, suitable payment transactions

may involve purchases of goods and services from merchants or individuals in a person to business or person to person context. However, in some embodiments of the invention, a payer may make payments and the payments can be made without any return consideration (e.g., a good or service purchased). For example, a payment may be a gift to the payee or repayment of a debt to the payee where the payer does not receive immediate consideration for the payment.

[0019] I. Systems

[0020] FIG. 1 shows a system that can be used in an embodiment of the invention. Embodiments of the invention may use some or all of the components shown in FIG. 1.

[0021] The illustrated system includes a payer **302** and a first mobile phone **304** associated with the payer **302**. The payer **302** has a payer account **316** at a payer institution **314**. Similarly, the system includes a payee **306** and a second mobile phone **308** associated with the payee **306**. The payee **306** has a payee account **320** at a payee institution **315**.

[0022] In this example, the payer institution **314** and payee institution **315** are shown as separate entities. The payer **302** and payee **306** could use the same financial institution in other embodiments of the invention.

[0023] The payer institution **314** and payee institution **315** are typically banks that manage financial accounts for individuals or businesses. However, they could also be business entities such as retail stores.

[0024] The payer **302** and payee **306** may be individuals, or organizations such as businesses that are capable of entering into financial transactions (e.g., payment transactions).

[0025] The payment processing network **310** may include data processing subsystems, networks, and operations used to support and deliver authorization services, exception file services, and clearing and settlement services. An exemplary payment processing network may include VisaNet™. Payment processing networks such as VisaNet™ are able to process credit card transactions, debit card transactions, and other types of financial transactions. VisaNet™, in

particular, includes a VIP system (Visa Integrated Payments system) which processes authorization requests and a Base II system which performs clearing and settlement services.

[0026] The payment processing network **310** may include a payment server computer **312**. A "server computer" is typically a powerful computer or cluster of computers. For example, a server computer can be a large mainframe, a minicomputer cluster, or a group of servers functioning as a unit. In one example, a server computer may be a database server coupled to a Web server. The server computer **312** may form part of any suitable wired or wireless network, including the Internet.

[0027] A mobile gateway **332** may be operatively coupled to the payment processing network **310** and may allow the first and second mobile phones **304**, **306** to communicate with the payment processing network **310**. The mobile gateway **332** may be embodied by any suitable combination of hardware and/or software known to those of ordinary skill in the art.

[0028] The system may also comprise a payer client computer **330(a)** as well as a payee client computer **330(b)**. They can be in communication with an enrollment server computer **326** operating a host site **324** (e.g., a Web site), via a communication medium **328**. The communication medium **328** may comprise any suitable combination of wired and/or wireless networks including the Internet. The enrollment server computer **326** may store aliases in an enrollment and alias database **322**. The payment processing network **310** can subsequently identify the payee **302** and payer **306** using the information stored in the enrollment and alias database **322**. In other embodiments, there can be a separate enrollment database and a separate alias database.

[0029] FIG. 2 shows typical components or subsystems of a computer apparatus. Such components or any subset of such components may be present in various components shown in FIG. 1, including the payment server computer **312**, the enrollment server computer **326**, the client computers **330(a)**, **330(b)**, etc. The subsystems shown in FIG. 2 are interconnected via a system bus **775**. Additional subsystems such as a printer **774**, keyboard **778**, fixed disk **779**, monitor **776**, which is coupled to display adapter **782**, and others are shown. Peripherals and

input/output (I/O) devices, which couple to I/O controller **771**, can be connected to the computer system by any number of means known in the art, such as serial port **777**. For example, serial port **777** or external interface **781** can be used to connect the computer apparatus to a wide area network such as the Internet, a mouse input device, or a scanner. The interconnection via system bus **775** allows the central processor **773** to communicate with each subsystem and to control the execution of instructions from system memory **772** or the fixed disk **779**, as well as the exchange of information between subsystems. The system memory **772** and/or the fixed disk **779** may embody a computer readable medium.

[0030] FIG. 3 shows a block diagram of some components of the first mobile phone **304**. Some or all of the components in the first mobile phone **304** may also be present in the second mobile phone **308** (illustrated in FIG. 1).

[0031] The phone **304** may comprise a computer readable medium **304(b)** and a body **304(h)** as shown in FIG. 3. The computer readable medium **304(b)** may be present within body **304(h)**, or may be detachable from it. The body **304(h)** may be in the form a plastic substrate, housing, or other structure. The computer readable medium **304(b)** may be a memory that stores data and may be in any suitable form including a magnetic stripe, a memory chip, etc.

[0032] The computer readable medium **304(b)** may comprise code for performing any of the functions described herein. For example, it may comprise code for sending a payment request message using a mobile phone to a payment processing network, where the payment request message comprises an amount of money to be paid and an alias, where the alias is associated with a payee; code for receiving in response to the payment request message an authentication request message, where the authentication request message is received via the mobile phone; and code for sending an authentication token in response to the authentication request message.

[0033] The phone **304** may further include a contactless element **304(g)**, which is typically implemented in the form of a semiconductor chip (or other data storage element) with an associated wireless transfer (e.g., data transmission) element, such as an antenna. Contactless element **304(g)** is associated with (e.g., embedded within) portable consumer device **304** and data or control instructions

transmitted via a cellular network may be applied to contactless element **304(g)** by means of a contactless element interface (not shown). The contactless element interface functions to permit the exchange of data and/or control instructions between the mobile device circuitry (and hence the cellular network) and an optional contactless element **304(g)**.

[0034] Contactless element **304(g)** is capable of transferring and receiving data using a near field communications ("NFC") capability (or near field communications medium) typically in accordance with a standardized protocol or data transfer mechanism (e.g., ISO 14443/NFC). Near field communications capability is a short-range communications capability, such as RFID, Bluetooth™, infra-red, or other data transfer capability that can be used to exchange data between the phone **304** and a payment processing network **26** or it can be used to exchange data between the phone **304** and an access device (e.g., a POS terminal). Thus, the phone **304** is capable of communicating and transferring data and/or control instructions via both cellular network and near field communications capability.

[0035] The phone **304** may also include a processor **304(c)** (e.g., a microprocessor) for processing the functions of the phone **304** and a display **304(d)** to allow a payee to see phone numbers and other information and messages. The phone **304** may further include input elements **304(e)** to allow a payee to input information into the device, a speaker **304(f)** to allow the payee to hear voice communication, music, etc., and a microphone **304(i)** to allow the payee to transmit her voice through the phone **304**. The phone **304** may also include an antenna **304(a)** for wireless data transfer (e.g., data transmission).

[0036] II. Enrollment methods

[0037] In embodiments of the invention, payers and payees may first enroll in the system. The payee and the payer may enroll in any suitable manner. For example, referring to FIG. 1, the payee and the payer may enroll in the system via the host site **324** using the client computers **330(a)**, **330(b)**. Enrollment information such as name, account number, etc. may be stored by the server computer **326** in the enrollment and alias database **322**. This information can be used in subsequent

payment processes to identify the payer **302** or the payee **306**.

[0038] In some cases, a financial institution such as the payee institution **315** or the payer institution **314** may "push" pre-enrollment data to the enrollment and alias database **322**. The payer institution **314**, for example, may validate the payer **302** ahead of time. The payer institution **314** may do this ahead of time, because it knows the payer **302** and the payer's credit history and account balance information. After the payer **302** is enrolled in the system, the payer **302** may set up an appropriate alias to use the system. The same may be true for the payee **306**. Thus, in some embodiments, the payer **302** need not do anything to enroll and need only set up her payment alias.

[0039] In embodiments of the invention, a number of aliases may be used. Aliases may include payment processing organization aliases for the payment processing organization that operates the payment processing network, a payee alias associated with the payee and the payee's phone, and a payer alias associated with the payer and the payer's phone. Examples of payer and payee aliases include "worldtraveler" and "beachbum." An example of a service alias may be "myvisa" for a payment processing organization such as Visa.

[0040] Other aliases that can be registered include portable consumer device aliases (payment card aliases). For example, the payer **302** may have first and second credit cards and they may have the aliases CC1 and CC2. Such portable consumer device aliases may or may not be uniquely associated with their holders.

[0041] Referring to FIGS. 1 and 4, in the first step **202**, a payee **306** requests assignment of an alias. In preferred embodiments, the payee **306** may specify a particular alias. However, in other embodiments, a payment processing organization may assign an alias to the payee **306**. To register an alias, the payee **306** may use the client computer **330(b)** to contact the host site **324** on the server computer **326**. The host site **324** may comprise a wizard or other mechanism to allow the payer **302** and the payee **306** to enter information.

[0042] In the next step **204**, the server computer **326** checks the enrollment and alias database **322** to see if the requested alias is already being used by another payee or payer. If the requested alias already exists, then the payee **306** may be asked to provide another alias (step **212**). Alternatively or additionally, the alias

registration request may reject the proposed alias if it is offensive or is a third party trademark or servicemark.

[0043] If the alias has not been previously registered, then the server computer **326** may register the requested alias for the payee **208**. This information may be stored in the enrollment and alias database **322**. Once the alias has been registered for the payee **306**, the payment processing organization may begin allowing the payee to receive payments made using the alias (step **210**).

[0044] This method and other related embodiments of the invention allow for efficient cross-institution payments to be made, by uniquely identifying an individual, business, etc., via an alias. The aliases may be associated with many accounts or services operated by an individual or entity, if desired. In some embodiments, these various aliases can be registered for a fee, and consumers may be charged a registration and renewal fee for using certain aliases. Other embodiments may provide the enrollment and alias database as a free service, or charge only certain classes of entities (e.g. charge only payees, or for-profit corporations).

[0045] III. Payment Methods

[0046] FIG. 6 shows a flowchart illustrating a payment method according to an embodiment of the invention. In the first step **102** the payer **302** decides to pay the payee **306** using the first mobile phone **304**.

[0047] A payer **302** then uses the first mobile phone **304** and sends a payment request message to the payment processing network **310** and the payment processing network **310** receives the payment request message (step **104**). The payment request message comprises at least a payment amount and a payee alias. The payment request message may also comprise other information, such as an alias or number identifying a specific financial account from which payment is to be made, or a time in the future at which payment is to be initiated.

[0048] As noted above, the payment request message may take a variety of different forms. For example, the payment request message could be in the form of an SMS message. The request could also come in the form of an email, or a voice interaction with an IVR unit. The request could also be made via a software

application on the phone, which sends one or more network packets containing the request data.

[0049] In the next step **106**, using the enrollment and alias database **322**, the server computer **312** in the payment processing network **310** analyzes the payment request message and uses the payee alias in the payment request message to identify the payee **306**, and also the payer institution **314** and the payer account **316**.

[0050] To provide security to the system, an optional authentication request message is sent from the payment processing network to the first mobile phone **304** operated by the payer **108**. The authentication request message may be initiated by the payer institution **314** or by a payment processing organization affiliated with the payment processing network **310**. It may request entry of a password, or personal information such as an address or social security number to verify the identity of the payer **108**. The authentication request message may take a variety of forms, as described for the payment request message **104** above. In preferred embodiments, the authentication request message will be sent to the payer's mobile phone **304**. It could also be sent to the payer's client computer **330(a)**.

[0051] In the next step **110**, the payer **302** provides an authentication token to the payment processing network **310**. For example, the payer **302** may enter a PIN (personal identification number) into the first mobile phone **304** and may then send the authentication token back to the payment processing network **310**, and the payment processing network **310** may or may not forward it to the payer institution **314**. Other examples of authentication tokens include passwords, birthdates, and other personal information associated with the payer **302**.

[0052] The payment processing network **310** (or the payer institution **314**) then verifies the authentication token **112**. If the authentication token is invalid, the payment request in the payment request message may be rejected. Alternatively, the payment processing network **310** may re-verify the authentication token (step **120**) by sending another authentication request message to the payer **302** via the first mobile phone **304**.

[0053] If the payer **302** and/or the first mobile phone **304** are authenticated, the payment processing network **310** may send the payment request message to the payer institution **314** for approval. The payment request message may be re-formed

to remove various aliases and may include real information, if desired. The payer institution **314** may then approve of the payment request if there are sufficient funds and/or credit in the payer account **316** or disapprove it if there are insufficient funds or credit. If the payment request is approved, at some point in time (e.g., immediately or at the end of the day if clearing and settling need to take place), actual funds may be transferred from the payer account **316** to the payee account **320** via the payment processing network **310**.

[0054] Once the funds have been transferred from the payer account **316** to the payee account **320**, a payment notification message may sent to the mobile phone **308** and/or the client computer **330(b)** operated by the payee **118** after the payment request in the payment request message has been approved by the payer institution **314**.

[0055] In a specific example, a payer **302** such as Jane and a payee **306** such as John register on the host site **324** run on a remote server computer **326** using their client computers **330(a)**, **330(b)**.

[0056] As shown in FIG. 5, Jane registers personal information **502** including her name, mobile telephone number, first credit card account number, second credit card account number, and a personal alias. John may similarly register his personal information **504**. In this example, Jane creates the personal alias "worldtraveler," while John creates the personal alias "beachbum."

[0057] After registering, a payment processing organization may provide both John and Jane with a phone number for the service that will facilitate further payment processing. In other embodiments, the payment processing organization may provide John and Jane with a service alias instead of or in addition to the service phone number. For example, instead of providing John and Jane with the service phone number 555-555-5555, the payment processing organization may provide the service alias "myvisa" to John and Jane. The service alias may be referred to as a "short-code" in some cases, and may include a string of characters of variable length.

[0058] In an exemplary transaction, Jane may be a payer **302** and wants to pay $15.00 to a payee **306** named John. Payee Jane **302** initiates a payment to John by entering the payment request message "myvisa pay beachbum $15.00" into

her phone **304**, and sending the message via SMS to the server computer **312** in the payment processing network **310** via the mobile gateway **332**. The alias "beachbum" is used instead of John's phone number. The service alias "myvisa" is used instead of the phone number of the service.

[0059] Jane may also use a portable consumer device alias such as "CC2" to indicate the particular credit card that Jane wants to use to pay John. For example, payee Jane **302** may enter the payment request message "myvisa pay beachbum $15.00 CC2" into her phone **304** to indicate that her second credit card is to be used to make the intended payment. Jane may alternatively or additionally designate a default credit card account number.

[0060] After entering the payment request message "myvisa pay beachbum $15.00 CC2" into her mobile phone **304**, the payment request message is sent from her phone **304** to the payment processing network **310** (e.g., as described above), and then (in this example) to an issuer of the credit card (or other portable consumer device). In this example, the issuer of the credit card may be the payer institution **314**.

[0061] The payment processing network **310** may receive the payment request message and may then optionally respond by sending an an authentication request message to the payer **302**. In this example, an authentication request message is sent in the form of a call from an interactive voice response unit (IVR) at a telecom server or the like, which asks payer Jane **302** to enter her mobile PIN (personal identification number) **510**. After payer Jane **302** enters the correct PIN into her phone **304**, the payer institution **314** and/or the server computer **312** in the payment processing network **310** can then analyze the payment request message and can approve or decline the payment request. If the payment request is approved, appropriate funds may be transferred to the payee account **320** at the payee institution **315**. For example, payee John's portable consumer device account (e.g., credit card account) at John's bank (e.g., the payee institution **315**) can be credited with the payment amount. Payer Jane's account **316** can be subsequently debited for the payment amount.

[0062] In some embodiments, a payment notification message in the form of an SMS, e-mail, or some other type of message may be sent to the payee's mobile

phone **308**, informing the payee John **306** that a payment from the payee John **302** has been made. In preferred embodiments, the payment notification message may be sent to payee John's mobile phone **308**, but it could be sent to the client computer **330(b)** operated by the payee John **306**.

[0063] Embodiments of the invention have a number of advantages. First, the use of an alias allows for a transaction to be completed while keeping the personal information of the transacting parties confidential. This is useful because, for example, a payer may not want to disclose his or her phone number to a payee, or vice versa. Second, the alias allows for payments to be made even if a payee's telephone number or financial account changes. A payer may thus store a list of aliases for payees with whom the payer frequently does business, and may initiate repeated payments without having to verify that the payee's telephone number is the same. Third, aliases tend to be much easier to remember than either phone numbers or financial account numbers. Consequently, embodiments of the invention will be easier to use than other methods. Fourth, embodiments of the invention allow for many accounts to be accessed from a single mobile phone, eliminating the need to carry a large number of portable consumer devices.

[0064] Any of the above-described methods or steps of such methods may be embodied as software code to be executed by a processor of the server computer or any other suitable combination of devices using any suitable computer language such as, for example, Java, C++ or Perl using, for example, conventional or object-oriented techniques. The software code may be stored as a series of instructions or commands on a computer readable medium, such as a random access memory (RAM), a read only memory (ROM), a magnetic medium such as a hard-drive or a floppy disk, or an optical medium such as a CD-ROM.

[0065] It should be understood that the present invention can be implemented in the form of control logic, in a modular or integrated manner, using software, hardware or a combination of both. Based on the disclosure and teachings provided herein, a person of ordinary skill in the art will appreciate other ways and/or methods to implement the present invention.

[0066] Any of the above-described embodiments and/or any features thereof may be combined with any other embodiment(s) and/or feature(s) without departing from the scope of the invention.

[0067] The above description is illustrative and is not restrictive. Many variations of the invention will become apparent to those skilled in the art upon review of the disclosure. The scope of the invention should, therefore, be determined not with reference to the above description, but instead should be determined with reference to the pending claims along with their full scope or equivalents.

[0068] A recitation of "a", "an" or "the" is intended to mean "one or more" unless specifically indicated to the contrary.

WHAT IS CLAIMED IS:

1. A method comprising:

receiving a payment request message from a mobile phone operated by a payer, wherein the payment request message includes a request to pay a payee a predetermined amount of money, and wherein the payment request message comprises a personal alias associated with the payee and a transaction amount;

analyzing the payment request message to determine if the payer is authorized to pay the payee; and

sending a payment notification message to the payee indicating that a payment from the payer to the payee has been made.

2. The method of claim 1, further comprising:

sending an authentication request message to the payer, wherein the authentication request message includes a message asking the payer to enter a PIN; and

receiving the PIN.

3. A computer readable medium comprising code for performing the method of claim 1.

4. A server computer comprising the computer readable medium of claim 3.

5. A system comprising the server computer of claim 4 and the mobile phone.

6. A method comprising :

receiving a payment request message from a payer, the payment request message comprising an amount of money to be paid to a payee and an alias associated with the payee, where the payment request message is sent by the payer via a mobile phone operated by the payer;

sending an authentication request message to the mobile phone in response to the payment request message, where the authentication request message is sent to the mobile phone;

receiving an authentication token from the payer in response to sending the authentication request message, where the authentication token is sent by the payer using the mobile phone;

verifying that the authentication token is associated with the payer; and

if the authentication token is verified as being associated with the payer, then initiating a payment for the amount of money to the payee using the alias.

7 . The method according to claim 6, wherein the mobile phone is a first mobile phone, and wherein the method further comprises:

sending an electronic notification of the payment to a second phone mobile operated by the payee.

8. The method according to claim 6, where the payment request message is in the form of a text message.

9. The method according to claim 6, where the payment request message is in the form of an email.

10. The method according to claim 6, where the payment request message comprise a payment card alias.

11. The method according to claim 6, where the authentication request message comprises a telephone call made by an electronic interactive voice response unit.

12. The method of claim 6, where the authentication token comprises a password.

13. The method of claim 6, where the authentication token comprises a piece of personal information associated with the payee.

14. A method comprising:

receiving a registration request from a payee to create an alias uniquely associated with that payee, where the request specifies the alias requested, and wherein the payee operates a mobile phone and can receive or make payments using the alias and mobile phone;

comparing the alias with other previously registered aliases associated with other payees; and

if the requested alias has not already been associated with another payee, registering the alias with the payee.

15. A server computer configured to perform the method of claim 14.

16. A method comprising:

sending a payment request message using a mobile phone to a payment processing network, where the payment request message comprises an amount of money to be paid and an alias, where the alias is associated with a payee;

receiving in response to the payment request message an authentication request message, where the authentication request message is received via the mobile phone; and

sending an authentication token in response to the authentication request message.

17 The method according to claim 16, where the payment request message is in the form of a text message.

18. The method according to claim 16, where the payment request message is in the form of an email.

19. The method according to claim 16, where the payment request message comprises a payment card alias.

20. The method according to claim 16, where the authentication request message comprises a telephone call made by an electronic interactive voice response unit.

21. The method of claim 16, where the authentication token comprises a password.

22. The method of claim 16, where the authentication token comprises a piece of personal information associated with the consumer.

23. A computer readable medium comprising code for performing the method of claim 16.

24. A phone comprising the computer readable medium of claim 23.

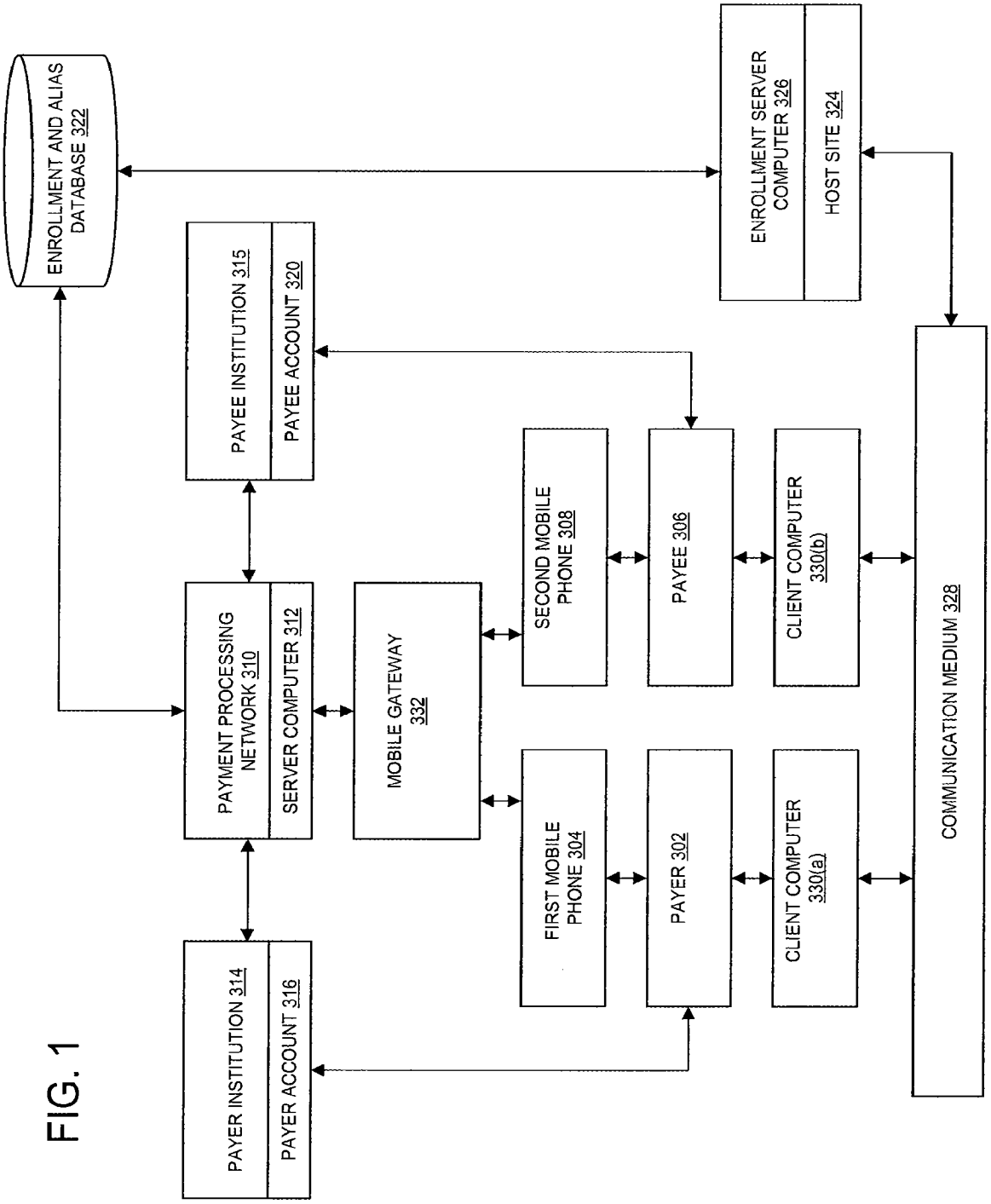

ENROLLMENT AND ALIAS DATABASE 322
ENROLLMENT SERVER COMPUTER 326
HOST SITE 324
PAYEE INSTITUTION 315
PAYEE ACCOUNT 320
PAYMENT PROCESSING NETWORK 310
SERVER COMPUTER 312
MOBILE GATEWAY 332
SECOND MOBILE PHONE 308
PAYEE 306
CLIENT COMPUTER 330(b)
COMMUNICATION MEDIUM 328
FIRST MOBILE PHONE 304
PAYER 302
CLIENT COMPUTER 330(a)
PAYER INSTITUTION 314
PAYER ACCOUNT 316

FIG. 1

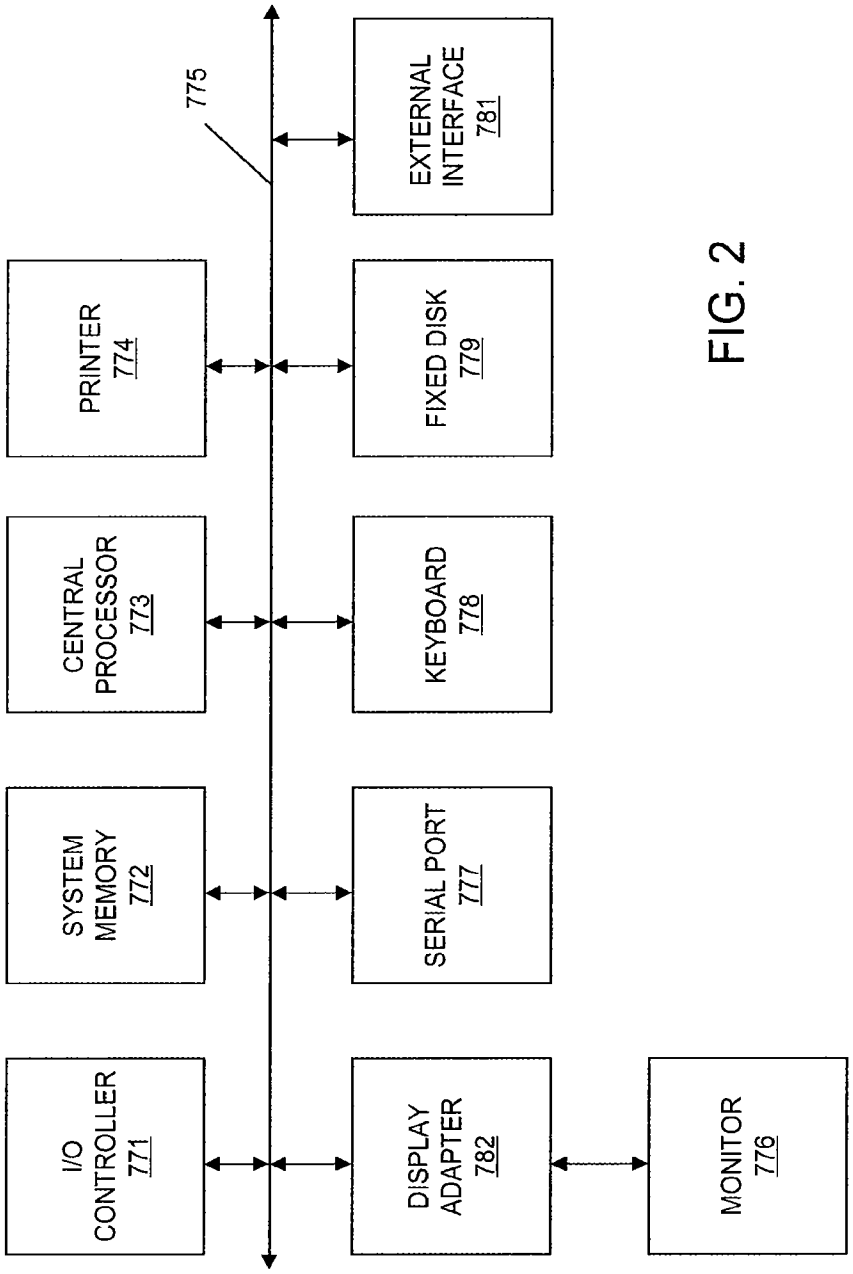

775
EXTERNAL INTERFACE 781
PRINTER 774
FIXED DISK 779
CENTRAL PROCESSOR 773
KEYBOARD 778
SYSTEM MEMORY 772
SERIAL PORT 777
I/O CONTROLLER 771
DISPLAY ADAPTER 782
MONITOR 776

FIG. 2

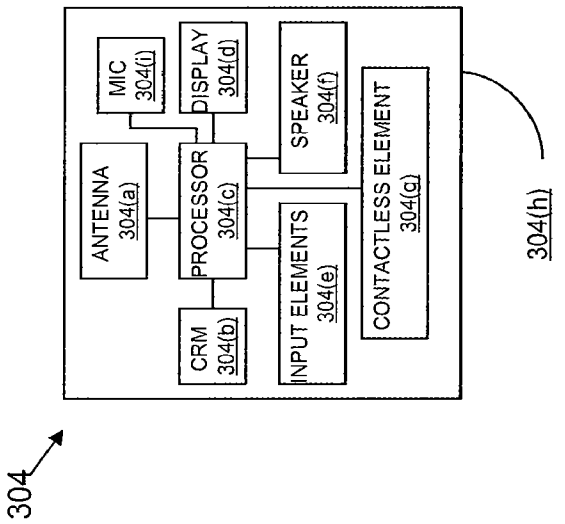
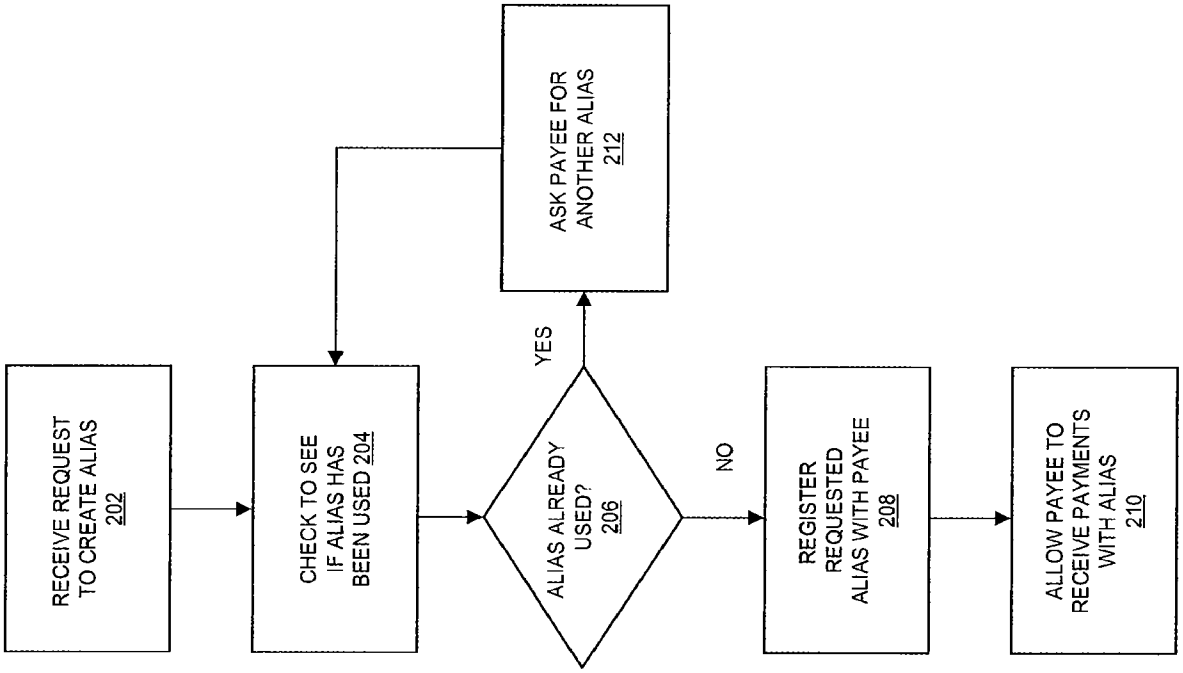

304
ANTENNA 304(a)
PROCESSOR 304(c)
CRM 304(b)
MIC 304(i)
DISPLAY 304(d)
SPEAKER 304(f)
INPUT ELEMENTS 304(e)
CONTACTLESS ELEMENT 304(g)
304(h)

FIG. 3

FIG. 4


RECEIVE REQUEST TO CREATE ALIAS 202
CHECK TO SEE IF ALIAS HAS BEEN USED 204
ALIAS ALREADY USED? 206
YES
ASK PAYEE FOR ANOTHER ALIAS 212
NO
REGISTER REQUESTED ALIAS WITH PAYEE 208
ALLOW PAYEE TO RECEIVE PAYMENTS WITH ALIAS 210

Example Account 1
•Name: **Jane Doe**
•Mobile #: (123)555-7777
•CC1: 4xxxxxxxxxx4444
•CC2: 5xxxxxxxxxx5555
•Alias: worldtraveler

502

Example Account 2
•Name: **John Doe**
•Mobile #: (123)555-8888
•CC1: 6xxxxxxxxxx6666
•CC2: 7xxxxxxxxxx7777
•Alias: beachbum

504

FIG. 5

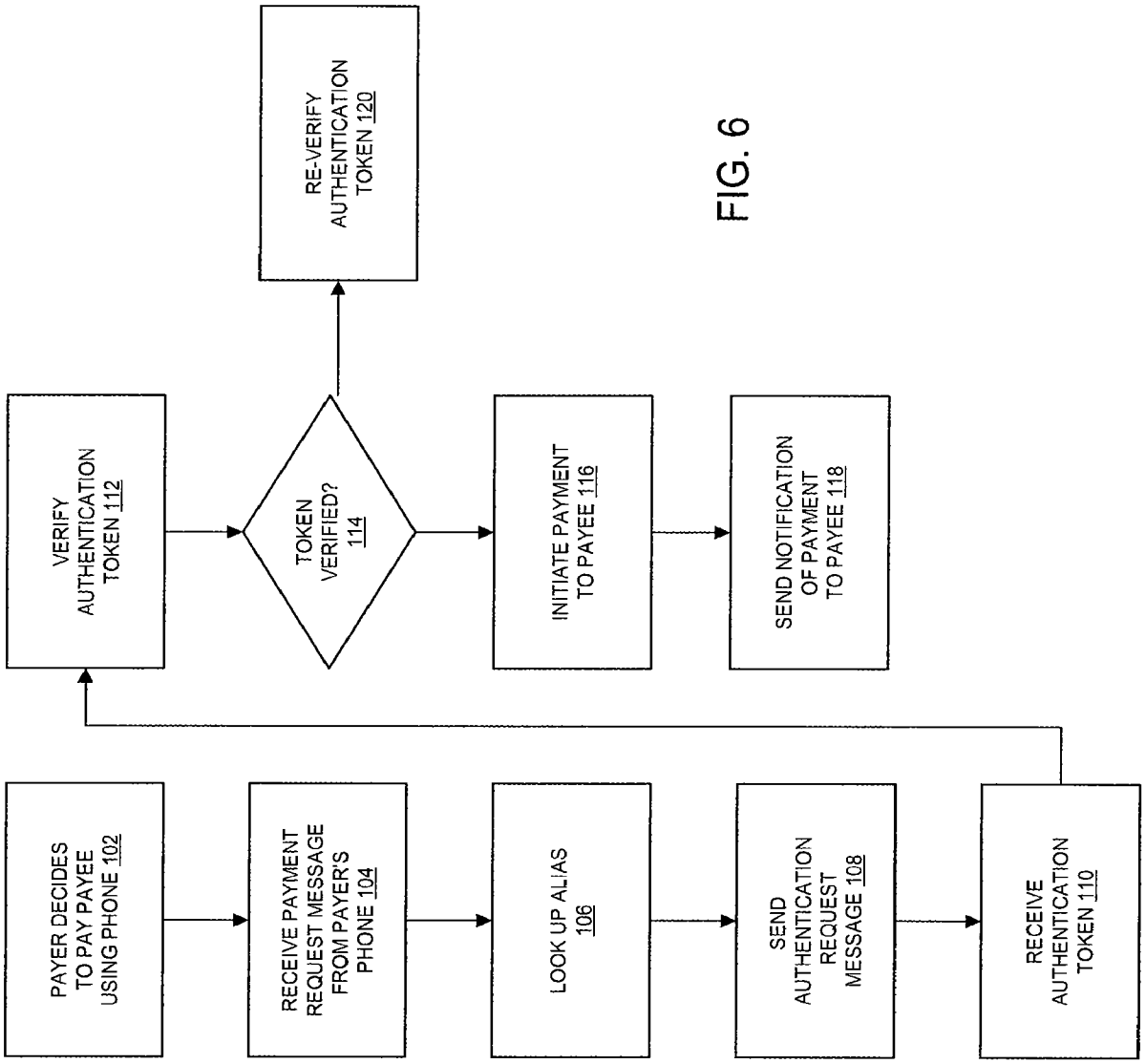

PAYER DECIDES TO PAY PAYEE USING PHONE 102
RECEIVE PAYMENT REQUEST MESSAGE FROM PAYER'S PHONE 104
LOOK UP ALIAS 106
SEND AUTHENTICATION REQUEST MESSAGE 108
RECEIVE AUTHENTICATION TOKEN 110
VERIFY AUTHENTICATION TOKEN 112
TOKEN VERIFIED? 114
INITIATE PAYMENT TO PAYEE 116
SEND NOTIFICATION OF PAYMENT TO PAYEE 118
RE-VERIFY AUTHENTICATION TOKEN 120

FIG. 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 07/88289

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06Q 40/00 (2008.4)
USPC - 705/35
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 40/00 (2008.4)
USPC: 705/35

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC: 705/64,1, 30, 35, 39

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
PubWEST (USPT, PGPB, EPAB, JPAB); Wiley Interscience; CrossRef; Google; Google Scholar
Search Terms: mobile terminal cellular phone telephone pda wireless device portable text message payment transfer alias user id identifier identification email account credit card sms pin voice

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 2005/0177510 A1 (HILT et al.) 11 August 2005 (11.08.2005) entire document, especially para [0014], [0030], [0032], [0034], [0045], [0058], [0063], [0065]-[0067], [0096]	14, 15 --- 1-13, 16-24
Y	US 2006/0202025 A1 (CALABRESE et al.) 14 September 2006 (14.09.2006) entire document, especially [0017]	1-13, 16-24
Y	WO 2004/077369 A1 (ANDERSON et al.) 10 September 2004 (10.09.2004) entire document, especially pg 23, para 2	13

☐ 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
04 April 2008 (04.04.2008)	15 MAY 2008

Name and mailing address of the ISA/US	Authorized officer:
Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (April 2007)

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 July 2008 (10.07.2008)

PCT

(10) International Publication Number
WO 2008/083025 A2

(51) International Patent Classification:
G06K 7/00 (2006.01) *H04M 1/00* (2006.01)
G06Q 20/00 (2006.01)

(21) International Application Number:
PCT/US2007/088313

(22) International Filing Date:
20 December 2007 (20.12.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/871,898 26 December 2006 (26.12.2006) US
11/749,366 16 May 2007 (16.05.2007) US

(71) Applicants *(for all designated States except US)*: **VISA U. S. A. INC.** [US/US]; P. O. Box 8999, M3-2B, San Francisco, California 94128 (US). **VISA INTERNATIONAL SERVICE ASSOCIATION** [US/US]; 900 Metro Center Boulevard, Foster City, California 94404 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **CARLSON, Mark** [US/US]; 153 Miramontes Avenue, Half Moon Bay, California 94019 (US).

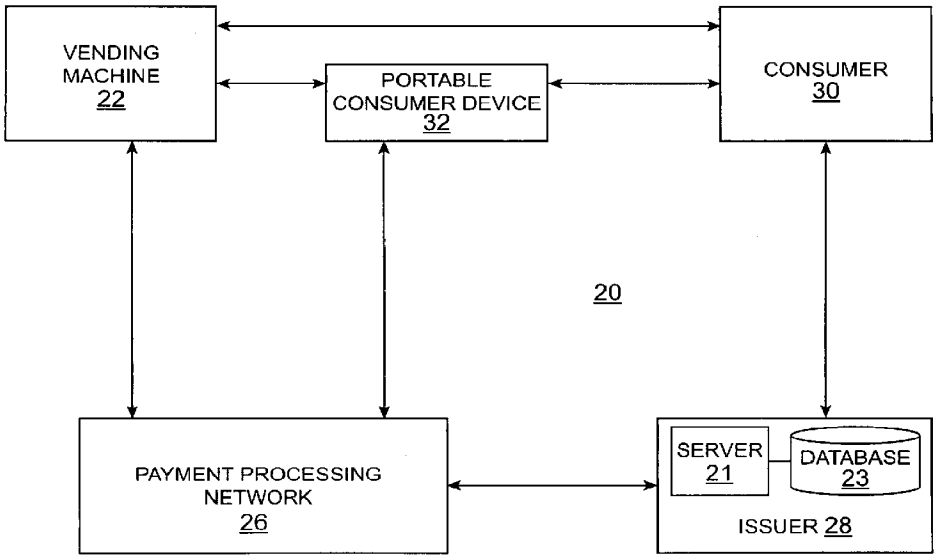
(74) Agents: **JEWIK, Patrick R.** et al.; Townsend and Townsend and Crew LLP, Two Embarcadero Center, 8th Floor, San Francisco, California 94111 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, 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, 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, MT, 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:
— *without international search report and to be republished upon receipt of that report*

(54) Title: MOBILE VENDING PURCHASING



(57) Abstract: A system and a method for using a portable consumer device such as a mobile phone for payments and the like are disclosed. One embodiment of the invention is directed to a method comprising receiving a payment request message from a portable consumer device operated by a consumer, wherein the payment request message includes a request to pay for a product from a vending machine, sending an authorization response message back to the vending machine wherein the vending machine subsequently prompts the consumer to enter a selection if the authorization response message indicates that the consumer is authorized to make a purchase, and receiving an acknowledgement message from the vending machine that the product was purchased.

WO 2008/083025 A2

MOBILE VENDING PURCHASING

CROSS-REFERENCES TO RELATED APPLICATIONS

[0001] This patent application is a non-provisional of and claims priority to U.S. provisional patent application no. 60/871,898, filed on December 26, 2006, which is herein incorporated by reference in its entirety for all purposes.

BACKGROUND

[0002] Vending machines are common place today in a variety of locations and make available a wide selection of products for purchase. In a typical purchase transaction a consumer walks up to a vending machine, inserts small change or bills into the machine, makes a selection from the machine, and then the vending machine automatically dispenses the selected merchandise to the consumer. The problem is that a consumer either may not have cash on hand or may not have small bills or change to make the purchase. Further, vending machines are offering a more diverse variety of products to purchase than just the inexpensive small snacks, drinks and newspapers that were traditionally offered for sale in vending machines. For example, a consumer can purchase CDs or DVDs, prepaid telephone cards, or electronics from a vending machine. Thus, a simple cash purchase from the vending machine is becoming a less practical option.

[0003] To solve this problem a number of solutions have evolved. For example, many vending machines now have card readers so that a consumer can make purchase via a credit card or a prepaid card. More recently, some solutions have become available to purchase items from a vending machine via a mobile phone. However, these solutions require communication directly between the phone and the vending machine which requires special hardware to interact with different types of phones and a unique way for billing to occur to the consumer depending on the phone service the consumer subscribes to. For example, a consumer may be billed via her mobile phone company or she may have to subscribe to an entirely separate service that supports this type of transaction.

[0004] A better solution is required to allow a consumer to make a purchase from a vending machine via a mobile phone or other similar device, without the complexities of setting up different billing methods and equipment for each and every vending machine to interact with different types of mobile devices and with different billing companies. Embodiments of the invention address these and other problems individually and collectively.

BRIEF SUMMARY

[0005] Embodiments of the invention are directed to systems and methods using portable consumer devices that can be used for payments and the like.

[0006] One embodiment of the invention is directed to a method comprising receiving a payment request message from a portable consumer device operated by a consumer, wherein the payment request message includes a request to pay for a product from a vending machine, sending an authorization response message back to the vending machine wherein the vending machine subsequently prompts the consumer to enter a selection if the authorization response message indicates that the consumer is authorized to make a purchase, and receiving an acknowledgement message from the vending machine that the product was purchased.

[0007] Another embodiment of the invention is directed to a method comprising reviewing contact information associated with a vending machine, sending a payment request message using the contact information and a portable consumer device wherein the vending machine subsequently receives an authorization response message indicating that payment is authorized and the vending machine thereafter prompts the consumer to make a selection, selecting a product in the vending machine, and receiving the product from the vending machine.

[0008] Another embodiment of the invention is directed to a method comprising receiving an authorization response message indicating that the consumer is authorized to make a purchase, prompting the consumer to enter a selection, and delivering an item corresponding to the selection to the consumer if the consumer makes the selection within a given amount of time.

[0009] Another embodiment of the invention is directed to a method comprising receiving a phone number associated with a vending machine and dialing the phone number, wherein after dialing, the vending machine subsequently receives authorization to dispense a product to a consumer operating the phone.

[0010] Another embodiment of the invention is directed to a method comprising automatically detecting a vending machine, prompting a consumer to enter information associated with the vending machine, and sending a payment request message wherein the vending machine subsequently receives authorization to dispense a product to the consumer.

[0011] These and other embodiments of the invention are described in further detail below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] FIG. 1 shows a block diagram of a system according to an embodiment of the invention.

[0013] FIG. 2 shows a block diagram of a vending machine according to an embodiment of the invention.

[0014] FIG. 3 shows a block diagram of a portable consumer device according to an embodiment of the invention.

[0015] FIG. 4 shows a block diagram of a payment processing network according to an embodiment of the invention.

[0016] FIG. 5 shows a flowchart illustrating steps in a method according to an embodiment of the invention.

[0017] FIG. 6 shows a flowchart illustrating steps in a method according to an embodiment of the invention.

[0018] FIG. 7 shows a flowchart illustrating steps in a method according to an embodiment of the invention.

[0019] FIG. 8(a) shows the display on an exemplary vending machine and mobile phone according to an embodiment of the invention.

[0020] FIG. 8(b) shows the display on an exemplary vending machine according to an embodiment of the invention.

[0021] FIG. 9(a) shows the display on an exemplary vending machine and mobile phone according to an embodiment of the invention.

[0022] FIG. 9(b) shows the display on an exemplary vending machine according to an embodiment of the invention.

[0023] FIG. 10(a) shows the display on an exemplary vending machine and mobile phone according to an embodiment of the invention.

[0024] FIG. 10(b) shows the display on an exemplary vending machine according to an embodiment of the invention.

DETAILED DESCRIPTION

[0025] Embodiments of the invention are directed to the use of portable consumer devices, and methods and systems that use them. Preferred portable consumer devices are mobile phones. The mobile phones can be used in payment processing systems like those shown in FIG. 1.

[0026] In some embodiments of the invention, a payment request message is sent from a portable consumer device such as a phone, directly to a payment processing network such as VisaNet. As used herein, a "payment request message" may be an implicit or explicit request to pay for a product or selection. A payment request message may take different forms. For example, a payment request message may simply be in the form of a dialed telephone number. Dialing a dedicated telephone number associated with a vending machine can be an implicit request to pay for a product, as it does not contain an explicit payment message. In other embodiments, the payment request message may be embodied by an SMS message, an e-mail, or some other type of message. Such messages may or may not include an explicit request to pay. For example, sending any text message to a dedicated address may be an implicit payment request. Alternatively, a text message may be sent which says "Pay Vending Machine 346." This is an explicit request to pay.

[0027] FIG. 1 shows a system **20** that can be used in an embodiment of the invention. For simplicity of illustration, one vending machine, one issuer, one portable consumer device, and one consumer are shown. It is understood, however, that embodiments of the invention may include multiple vending machines, issuers, portable consumer devices, and/or consumers. In addition, some embodiments of the invention may include fewer than all of the components shown in FIG. 1. Also, the components in FIG 1 may communicate via any suitable communication medium (including the Internet), using any suitable communication protocol.

[0028] The system **20** includes a vending machine **22**, a consumer **30**, a payment processing network **26**, a portable consumer device **32**, and an issuer **28** associated with the portable consumer device **32**. The portable consumer device **32** can communicate with the issuer **28** via the payment processing network **26**.

[0029] The issuer **28** may be a bank, but it could also be business entity such as a retail store. The issuer **28** may operate a server computer **21**, which may have a computer readable medium comprising code for performing the functions that the issuer **28** performs. A database **23** comprising account number information and other information may be operatively coupled to the server computer **21**. The database **23** may comprise an account associated with the consumer **30** and the portable consumer device **32**.

[0030] The consumer **30** may be an individual who may use the portable consumer device **32.**

[0031] The vending machine **22** may be owned or leased by an entity such as an organization or business that sells goods using the vending machine **22**. The vending machine **22** is typically a machine that dispenses products after a consumer **30** pays for the products. Examples of suitable products include food items (e.g., candy, gum, soft drinks, etc.), travel items, newspapers, tickets, movies, electronics, etc.

[0032] The vending machine **22** may contain components like those shown in FIG. 2. For example, the vending machine **22** may have a computer readable medium ("CRM") **22(b)** comprising code including instructions for performing the functions that the vending machine **22** performs, and a processor **22(c)** to execute

those instructions. The vending machine **22** may also have a display **22(a)** to show messages to the consumer **30** and a speaker **22(d)** to provide audio messages for the consumer **30**. The vending machine **22** may also have input elements **22(e)** (e.g., buttons, levers, or other actuators) to allow a consumer **30** to make a selection of one or more items to purchase from the vending machine **22**, as well as a network interface **22(f)** to communicate with a payment processing network **26** so that the vending machine **22** can communicate during the payment authorization process. The vending machine **22** may also have one or more selections **22(g)** of items for a consumer **30** to purchase. Selections **22(g)** may comprise products such as food items (e.g., candy, gum, soft drinks, etc.), travel items, etc.

[0033] The vending machine **22** may also have, or may receive communications from, a reader **22(h)** that can interact with the portable consumer device **32**. The reader **22(h)** may include any suitable contact or contactless mode of operation. For example, exemplary card readers can include RF (radio frequency) antennas, magnetic stripe readers, etc. to interact with the portable consumer device **32**. Contactless readers are commercially available. Suitable equipment for allowing the vending machine **22** to function in embodiments of the invention can be purchased from Bonusdata AG.

[0034] The portable consumer device **32** may be in any suitable form. For example, suitable portable consumer devices can be hand-held and compact so that they can fit into a consumer's wallet and/or pocket (e.g., pocket-sized). They may include smart cards, ordinary credit or debit cards (with a magnetic strip and without a microprocessor), keychain devices (such as the Speedpass™ commercially available from Exxon-Mobil Corp.), etc. Other examples of portable consumer devices include cellular and mobile phones, personal digital assistants (PDAs), pagers, payment cards, security cards, access cards, smart media, transponders, and the like. The portable consumer devices can also be debit devices (*e.g.*, a debit card), credit devices (*e.g.*, a credit card), or stored value devices (*e.g.*, a stored value card).

[0035] The portable consumer device **32** may comprise a computer readable medium **32(b)** and a body **32(h)** as shown in FIG. 3. The computer readable medium **32(b)** present within body **32(h)**, or may be detachable from it. The body

32(h) may in the form a plastic substrate, housing, or other structure. The computer readable medium **32(b)** may be a memory that stores data and may be in any suitable form including a magnetic stripe, a memory chip, etc.

[0036] If the computer readable medium **32(b)** is in a phone, it may comprise code for receiving a phone number and a payment request message from a consumer, wherein the payment request message includes a request to pay for a product from a vending machine. It may also comprise code for dialing the phone number; and code for sending a payment request message where the vending machine subsequently receives an authorization response message indicating that payment is authorized (or not authorized), where the vending machine thereafter prompts the consumer to make a selection.

[0037] The portable consumer device **32** may further include a contactless element **32(g)**, which is typically implemented in the form of a semiconductor chip (or other data storage element) with an associated wireless transfer (e.g., data transmission) element, such as an antenna. Contactless element **32(g)** is associated with (e.g., embedded within) portable consumer device **32** and data or control instructions transmitted via a cellular network may be applied to contactless element **32(g)** by means of a contactless element interface (not shown). The contactless element interface functions to permit the exchange of data and/or control instructions between the mobile device circuitry (and hence the cellular network) and an optional contactless element **32(g)**.

[0038] Contactless element **32(g)** is capable of transferring and receiving data using a near field communications ("NFC") capability (or near field communications medium) typically in accordance with a standardized protocol or data transfer mechanism (e.g., ISO 14443/NFC). Near field communications capability is a short-range communications capability, such as RFID, Bluetooth™, infra-red, or other data transfer capability that can be used to exchange data between the portable consumer device **32** and a payment processing network **26** or it can be used to exchange data between the portable consumer device **32** and the vending machine **22**. Thus, the portable consumer device **32** is capable of communicating and transferring data and/or control instructions via both cellular network and near field communications capability.

[0039] The portable consumer device **32** may also include a processor **32(c)** (e.g., a microprocessor) for processing the functions of the portable consumer device **32** and a display **32(d)** to allow a consumer to see phone numbers and other information and messages. The portable consumer device **32** may further include input elements **32(e)** to allow a consumer to input information into the device, a speaker **32(f)** to allow the consumer to hear voice communication, music, etc., and a microphone **32(i)** to allow the consumer to transmit her voice through the portable consumer device **32**. The portable consumer device **32** may also include an antenna **32(a)** for wireless data transfer (e.g., data transmission).

[0040] Referring to FIG. 1 again, the payment processing network **26** may include data processing subsystems, networks, and operations used to support and deliver authorization services, exception file services, and clearing and settlement services. An exemplary payment processing network may include VisaNet™. Payment processing networks such as VisaNet™ are able to process credit card transactions, debit card transactions, and other types of commercial transactions. VisaNet™, in particular, includes a VIP system (Visa Integrated Payments system) which processes authorization requests and a Base II system which performs clearing and settlement services.

[0041] Specifically, the payment processing network **26** may include a server computer **415** as shown in FIG 4. As used herein, a "server computer" is typically a powerful computer or cluster of computers. For example, a server computer can be a large mainframe, a minicomputer cluster, or a group of servers functioning as a unit. In one example, the server computer may be a database server coupled to a Web server. The payment processing network **26** may use the server computer **415**, and the server computer **415** may be present in any suitable wired or wireless network, including the Internet.

[0042] The payment processing network **26** may further include a gateway **405** whereby a dial request, text message or Short Message Service ("SMS") message, for example, from a portable consumer device **32**, can pass through to the payment processing network **26**. (SMS is typically a service available on a portable consumer device that permits the sending of short messages between portable consumer devices via an intermediate server.) The gateway **405** may be embodied

by a computer or a network that allows or controls access to another computer or network. The gateway **405** may also be a software interface between the computer or network and another computer or network.

[0043] In this example, the payment server **415** can validate and augment a payment request message received from the portable consumer device **32**. It can log the payment request message, and transmit the payment request message to the authorization process device **435** where it is formatted and transmitted to the issuer **28** for the portable consumer device **32**. The payment processing network **26** may also include an enrollment database **425** that stores portable consumer device enrollment data for verification and logging purposes.

[0044] An acquirer (which is not shown in FIG. 1) such as a bank may be in electronic communication with the payment processing network **26**, and the issuer **28**. It may also be in electronic communication with the vending machine **22**, and other vending machines, and/or an organization that owns or operates the vending machines. In embodiments of the invention, the vending machine **22** may communicate directly with the payment processing network **26** or through an acquirer.

[0045] Referring to FIGS. 1-3, in one purchase transaction embodiment, a consumer **30** may use a portable consumer device **32** to directly contact the payment processing network **26** to obtain authorization to make a purchase. In this embodiment, the portable consumer device **32** does not directly communicate with the vending machine **22** when the purchase is made. In this example, a payment request message is sent from the portable consumer device **32** to the payment processing network **26**. The payment processing network **26** then forwards the payment request message to the issuer **28** of the portable consumer device **32**.

[0046] After the issuer **28** receives the authorization request message, the issuer **28** sends an authorization response message back to the payment processing network **26** to indicate whether or not the current transaction is authorized. The issuer **28** may require additional information from the consumer **30** such as a PIN before sending the authorization response message to the vending machine **22**

and/or the portable consumer device **32**. The transaction processing network **26** then forwards the authorization response message to the vending machine **22**.

[0047] After the vending machine **22** receives the authorization response message, the authorization response message may be displayed by the vending machine **22** display **22(a)** or the vending machine **22** may voice the response message via the speaker **22(d)**. Once the vending machine **22** receives approval for the payment, the vending machine **22** may prompt the consumer **30** to make a selection. The consumer **30** may then select a product as she would with a conventional vending machine and the product may thereafter be dispensed to the consumer **30**.

[0048] At the end of the day, a normal clearing and settlement process can be conducted by the transaction processing network **26**. A clearing process is a process of exchanging financial details between the payment processing network **26**, the issuer **28**, and the vending machine **22**, or potentially an acquirer associated with the vending machine **22**. To facilitate posting to a consumer's account and reconciliation of the consumer's settlement position. As noted above, the acquirer (which is not shown in FIG. 1), may be bank that is electronically coupled to the payment processing network **26**, the issuer **28**, and the vending machine **22**.

[0049] Some of the embodiments described below may use a payment processing system like the one described above, or any suitable combination of components in the payment processing system. More specific embodiments of the invention are described below.

[0050] Other embodiments of the invention, which specifically use a mobile phone, are described in further detail below. The embodiments can use dial, interactive voice response ("IVR"), or an entered message which is sent to a payment processing network. These embodiments may further use a payment processing network such as VisaNet to authorize the transaction and tell the vending machine that payment has been accepted. By using a payment processing network such as VisaNet, there is no need to set up a separate billing situation for each mobile phone service organization or set up a separate billing service for a particular vending machine. The payment processing network, such as VisaNet, interacts with

each different billing organization so that all transactions appear the same to the vending machine.

[0051] Additional details regarding embodiments of the invention are described below.

[0052] FIG. 5 shows a flowchart including a method according to a first embodiment of the invention. The method can be described with reference to FIGS. 1-4, 8(a), and 8(b).

[0053] First, a consumer **30** enters a telephone number associated with the vending machine **22** in using input elements **32(e)** in the portable consumer device **32** to purchase one or more selections **22(g)** from the vending machine **22** (step **500**). As shown in FIG. 8(a), the number may be posted (e.g., through a static medium such as plastic or paper, or through a dynamic medium such as an LCD screen) on the vending machine **22**. Alternatively, it may be provided to the consumer **30** in some other way (e.g., a mailing, an e-mail, an SMS message, etc.).

[0054] Referring to FIG. 4, a payment request message is then sent from the portable consumer device **32** to the payment processing network **26** via a gateway **405**. The gateway **405** passes the payment request message to the payment server **415**. The payment server **415** validates the payment request message against the data in the database containing the enrollment data **425** and augments the payment request message. The payment server **415** then passes the payment request message to the authorization process device **435** where it is formatted and passed to the issuer **28** of the portable consumer device **32**.

[0055] After the issuer **28** receives the payment request message, the issuer **28** analyzes the payment request message and sends an authorization response message back to the payment server **415** to indicate whether or not the current transaction is authorized. The payment server **415** logs the response and sends the authorization response message to the vending machine **22**. If the transaction is not authorized (step **520**), the vending machine **22** notifies the consumer **30** that the transaction is denied (step **525**). If the transaction is authorized (step **520**), the vending machine **22** prompts the consumer **30** to select an item to purchase (step **530**) within an allotted time (e.g., twenty seconds or less). For example, the vending

machine **22** may display a message that says "Please choose your product," as shown in FIG. 8(b).

[0056] If the consumer **30** does not make the purchase within the allotted time (step **540**) the transaction times-out (step **545**) and the consumer **30** initiates another payment request to purchase an item. If the consumer **30** does make the purchase within the allotted time (step **540**) then the selected item is delivered to the consumer **30** and a purchase acknowledgement is sent to the payment processing network **26** (step **550**). The purchased item will appear on the consumer's next statement.

[0057] FIG. 6 shows a flowchart including a general method according to a second embodiment of the invention. The method can be described with reference to FIGS. 1-4, 9(a), and 9(b).

[0058] First, the consumer **30** sends an SMS to the number associated with the vending machine **22** to purchase an item in the vending machine **22** (step **600**). As shown in FIG. 9(a), the number may be posted on the vending machine **22**. Alternatively, it may be provided to the consumer **30** in some other way (e.g., a mailing, an e-mail, an SMS message, etc.).

[0059] Referring to FIG. 4, a payment request message is then sent from the portable consumer device **32** to the payment processing network **26** via a gateway **405**. The gateway **405** passes the payment request message to the payment server **415**. The payment server **415** validates the payment request message against the data in the database containing the enrollment data **425** and augments the payment request message. The payment server **415** then passes the payment request message to the authorization process device **435** where it is formatted and passed to the issuer **28** of the portable consumer device **32**.

[0060] The issuer **28** may require a PIN from the consumer **30** before sending an authorization response message. If this is the case, then after the issuer **28** receives and analyzes the payment request message, the issuer **28** sends a PIN request back to the payment server **415** and the payment server **415** sends the PIN request to the portable consumer device **32**. The PIN request may be in audio or textual form.

[0061] Next the consumer **30** is prompted to enter a PIN (step **610**) into the portable consumer device **32**. The PIN is then sent from the portable consumer device **32** to the payment processing network **26** via a gateway **405**. The gateway **405** passes the PIN to the payment server **415**. The payment server **415** then passes the PIN to the issuer **28** of the portable consumer device **32**.

[0062] After the issuer **28** receives the PIN, the issuer **28** verifies that the PIN matches the PIN associated with the consumer **30**. After verifying the PIN (or if the issuer **28** did not require a PIN) the issuer **28** sends an authorization response message back to the payment server **415** to indicate whether or not the current transaction is authorized. The payment server **415** logs the response and sends the authorization response message to the vending machine **22**. If the transaction is not authorized (step **620**), the vending machine **22** notifies the consumer **30** that the transaction is denied (step **625**). If the transaction is authorized (step **620**), the vending machine **22** prompts the consumer **30** to select an item to purchase within an allotted time (e.g., twenty seconds or less) (step **630**). For example, the vending machine **22** may display a message that says "Please choose your product," as shown in FIG. 9(b).

[0063] If the consumer **30** does not make the purchase within the allotted time (step **640**) the transaction times-out (step **645**) and the consumer **30** initiates another payment request to purchase an item. If the consumer **30** does make the purchase within the allotted time (step **640**) then the item selected is delivered to the consumer **30** and a purchase acknowledgement is sent to the payment processing network **26** (step **650**). The purchased item will appear on the consumer's next statement.

[0064] FIG. 7 shows a flowchart including a general method according to a third embodiment of the invention. The method can be described with reference to FIGS. 1-4, 10(a), and 10(b).

[0065] In this embodiment of the invention, a consumer **30** may use a mobile wallet to make a vending purchase (step **700**). A mobile wallet is a payment enabled mobile phone that functions as a payment mechanism similar to a debit card, credit card, or prepaid card. For example a consumer **30** may register her credit card with the issuer **28** of the portable consumer device **32** and then use the mobile phone to

make purchases or a consumer **30** may set up a prepaid account with the issuer **28** of the portable consumer device **32** or another entity that she can draw against to make purchases.

[0066] First, the consumer **30** may launch an application in the portable consumer device **32** and type in a machine alias associated with the vending machine **22** (e.g., "Pay: coke345") as shown in FIG. 10(a). Alternatively, the portable consumer device **32** may automatically detect the vending machine **22** (via RFID, etc.) and prompt the consumer **30** to enter information (e.g., a machine alias, payment information, etc.) associated with the vending machine **22**, such as a machine alias shown in FIG. 10(a). As shown in FIG. 10(a), the machine alias may be posted on the vending machine **22**. The consumer **30** may also be required to enter a PIN to authenticate the transaction.

[0067] Referring to FIG. 4, a payment request message is then sent from the portable consumer device **32** to the payment processing network **26** via a gateway **405**. The gateway **405** passes the payment request message to the payment server **415**. The payment server **415** validates the payment request message against the data in the database containing the enrollment data **425** and augments the payment request message. The payment server **415** then passes the payment request message to the authorization process device **435** where it is formatted and passed to the issuer **28** of the portable consumer device **32**.

[0068] After the issuer **28** receives the payment request message, the issuer **28** analyzes the payment request message, and sends an authorization response message back to the payment server **415** to indicate whether or not the current transaction is authorized. The payment server **415** logs the response and sends the authorization response message to the vending machine **22**. If the transaction is not authorized (step **720**), the vending machine **22** notifies the consumer **30** that the transaction is denied (step **725**). If the transaction is authorized (step **720**), the vending machine **22** prompts the consumer **30** to select an item to purchase (step **730**) within an allotted time (e.g., twenty seconds or less). For example, the vending machine **22** may display a message that says "Please choose your product," as shown in FIG. 10(b).

[0069] If the consumer **30** does not make the purchase within the allotted time (step **740**) the transaction times-out (step **745**) and the consumer **30** initiates another payment request to purchase an item. If the consumer **30** does make the purchase within the allotted time (step **740**) then the selected item is delivered to the consumer **30** and a purchase acknowledgement is sent to the payment processing network **26** (step **750**). The purchased item will appear on the consumer's next statement.

[0070] Other alternative embodiments are also possible. For example, although the examples described above request the consumer to make a selection, in other embodiments, the consumer may actually input the selection that the consumer wants into the portable consumer device (e.g., phone) before the purchase is made. For example, the consumer may dial a phone number on a vending machine, and may thereafter get an automatic callback from a payment processing network requesting that the consumer enter the number of the product desired. The consumer may then enter the number "13" into his phone, and the vending machine may automatically dispense the product associated with this number. In this embodiment, the consumer may not directly interact at all with the vending machine during the payment process. In another example, the consumer may simply enter information such as "pay vending machine 345 $2.00, and dispense product 13". This information may be sent to a payment processing and the payment processing network may thereafter automatically dispense the desired product.

[0071] Embodiments of the invention have a number of advantages. First, embodiments of the invention can contact a payment processing network directly, without requiring the consumer to initially interact with the vending machine. Thus, in some cases, it is not necessary that the vending machine have some interface (e.g., a contactless reader) that needs to interact with the consumer's portable consumer device. Since such specialized readers are not required, this makes it more likely that embodiments of the invention can be universally implemented. Also, the communication between the portable consumer device and the payment processing network is more direct in embodiments of the invention than conventional payment processing systems. This can reduce the likelihood of communication errors in the payment process. Also, by contacting the payment processing network directly

(rather than a phone company first), the payment processing network can log and process the transaction like any other credit or debit card payment transaction.

[0072] It should be understood that the present invention as described above can be implemented in the form of control logic using computer software in a modular or integrated manner. Based on the disclosure and teachings provided herein, a person of ordinary skill in the art will know and appreciate other ways and/or methods to implement the present invention using hardware and a combination of hardware and software.

[0073] Any of the software components or functions described in this application, may be implemented as software code to be executed by a processor using any suitable computer language such as, for example, Java, C++ or Perl using, for example, conventional or object-oriented techniques. The software code may be stored as a series of instructions, or commands on a computer readable medium, such as a random access memory (RAM), a read only memory (ROM), a magnetic medium such as a hard-drive or a floppy disk, or an optical medium such as a CD-ROM. Any such computer readable medium may reside on or within a single computational apparatus, and may be present on or within different computational apparatuses within a system or network.

[0074] The above description is illustrative and is not restrictive. Many variations of the invention will become apparent to those skilled in the art upon review of the disclosure. The scope of the invention should, therefore, be determined not with reference to the above description, but instead should be determined with reference to the pending claims along with their full scope or equivalents.

[0075] One or more features from any embodiment may be combined with one or more features of any other embodiment without departing from the scope of the invention.

[0076] A recitation of "a", "an" or "the" is intended to mean "one or more" unless specifically indicated to the contrary.

WHAT IS CLAIMED IS:

1. A method comprising:

receiving a payment request message from a portable consumer device operated by a consumer, wherein the payment request message includes a request to pay for a product from a vending machine;

sending an authorization response message back to the vending machine wherein the vending machine subsequently prompts the consumer to enter a selection if the authorization response message indicates that the consumer is authorized to make a purchase; and

receiving an acknowledgement message from the vending machine that the product was purchased.

2. The method of claim 1 further comprising analyzing the payment request message to determine if the consumer is authorized to pay for the product.

3. The method of claim 1 further comprising automatically calling the portable consumer device and requesting that the consumer enter a PIN into the device.

4. The method of claim 1 wherein the payment request message is received by a payment processing network, and wherein the payment request message does not pass directly from the portable consumer device to the vending machine.

5. The method of claim 1 wherein the portable consumer device is a wireless phone.

6. A computer readable medium comprising:

code for receiving a payment request message from a portable consumer device operated by a consumer, wherein the payment request message includes a request to pay for a product from a vending machine;

code for sending an authorization response message back to the vending machine wherein the vending machine subsequently prompts the consumer to enter a selection if the authorization response message indicates that the consumer is authorized to make a purchase; and

code for receiving an acknowledgement message from the vending machine that the product was purchased.

7. A server comprising the computer readable medium of claim 6.

8. A method comprising:

reviewing contact information associated with a vending machine;

sending a payment request message using the contact information and a portable consumer device wherein the vending machine subsequently receives an authorization response message indicating that payment is authorized and the vending machine thereafter prompts the consumer to make a selection;

selecting a product in the vending machine; and

receiving the product from the vending machine.

9. The method of claim 8 wherein the portable consumer device is a wireless phone.

10. A method comprising:

receiving an authorization response message indicating that the consumer is authorized to make a purchase;

prompting the consumer to enter a selection; and

delivering an item corresponding to the selection to the consumer if the consumer makes the selection within a given amount of time.

11. The method of claim 10 wherein the given amount of time is twenty seconds or less.

12. A vending machine adapted to perform the method of claim 10.

13. A method comprising:

receiving a phone number associated with a vending machine; and

dialing the phone number, wherein after dialing, the vending machine subsequently receives authorization to dispense a product to a consumer operating the phone.

14. A computer readable medium comprising:

code for receiving a phone number associated with a vending machine; and

code for dialing the phone number, wherein after dialing, the vending machine subsequently receives authorization to dispense a product to a consumer operating the phone.

15. A wireless phone comprising the computer readable medium of claim 14.

16. A method comprising:

automatically detecting a vending machine;

prompting a consumer to enter information associated with the vending machine; and

sending a payment request message wherein the vending machine subsequently receives authorization to dispense a product to the consumer.

17. The method of claim 16 further comprising prompting the consumer to enter a PIN.

18. A computer readable medium comprising:

code for automatically detecting a vending machine;

code for prompting a consumer to enter information associated with the vending machine; and

code for sending a payment request message wherein the vending machine subsequently receives authorization to dispense a product to the consumer.

19. A wireless phone comprising the computer readable medium of claim 18.

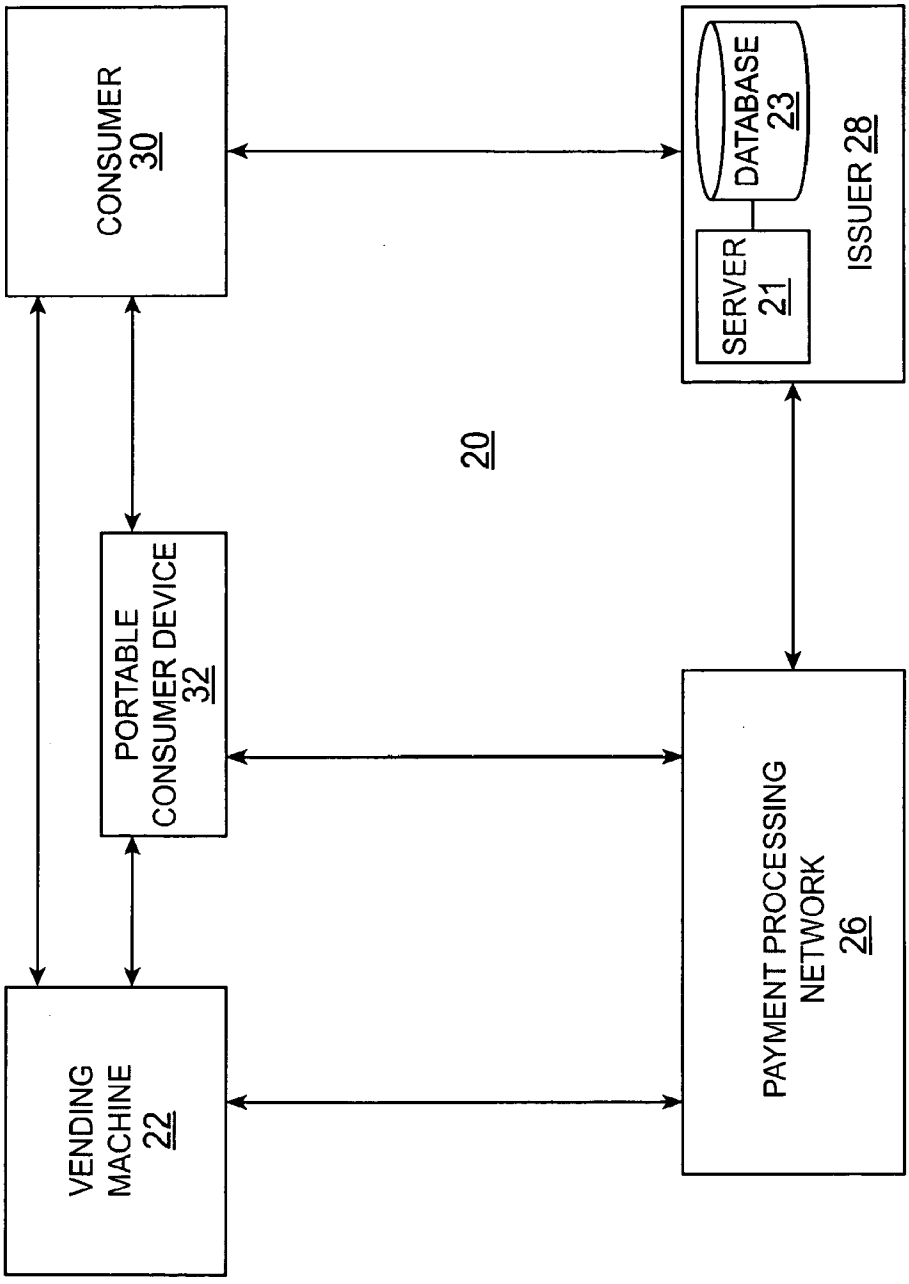

CONSUMER
30
DATABASE
23
SERVER
21
ISSUER 28
20
PORTABLE
CONSUMER DEVICE
32
PAYMENT PROCESSING
NETWORK
26
VENDING
MACHINE
22

FIG. 1

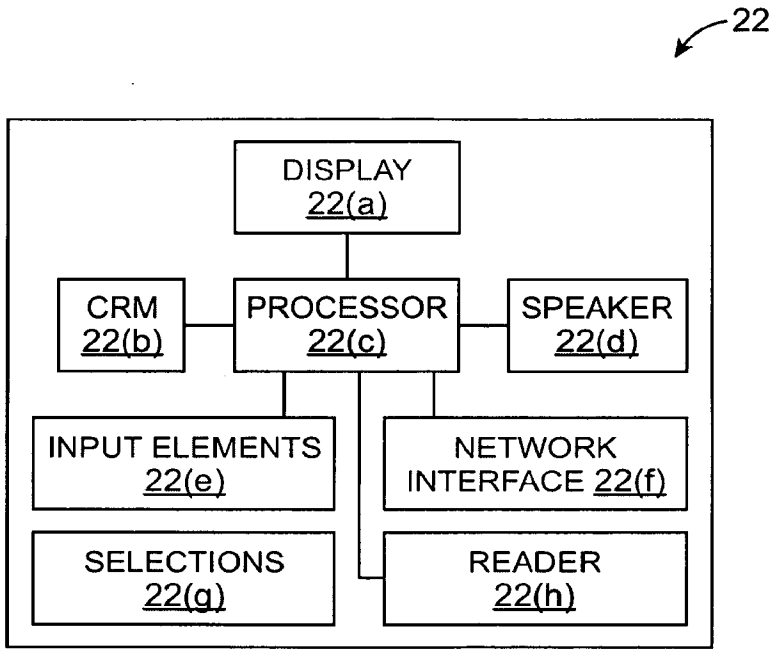

22
DISPLAY
22(a)
CRM
22(b)
PROCESSOR
22(c)
SPEAKER
22(d)
INPUT ELEMENTS
22(e)
NETWORK
INTERFACE 22(f)
SELECTIONS
22(g)
READER
22(h)

FIG. 2

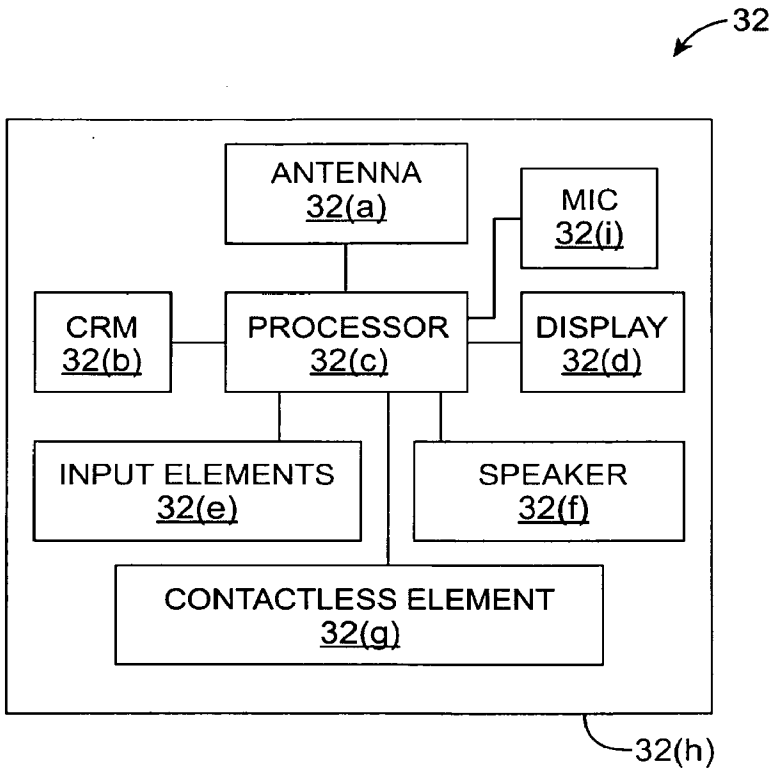

32
ANTENNA
32(a)
MIC
32(i)
CRM
32(b)
PROCESSOR
32(c)
DISPLAY
32(d)
INPUT ELEMENTS
32(e)
SPEAKER
32(f)
CONTACTLESS ELEMENT
32(g)
32(h)

FIG. 3

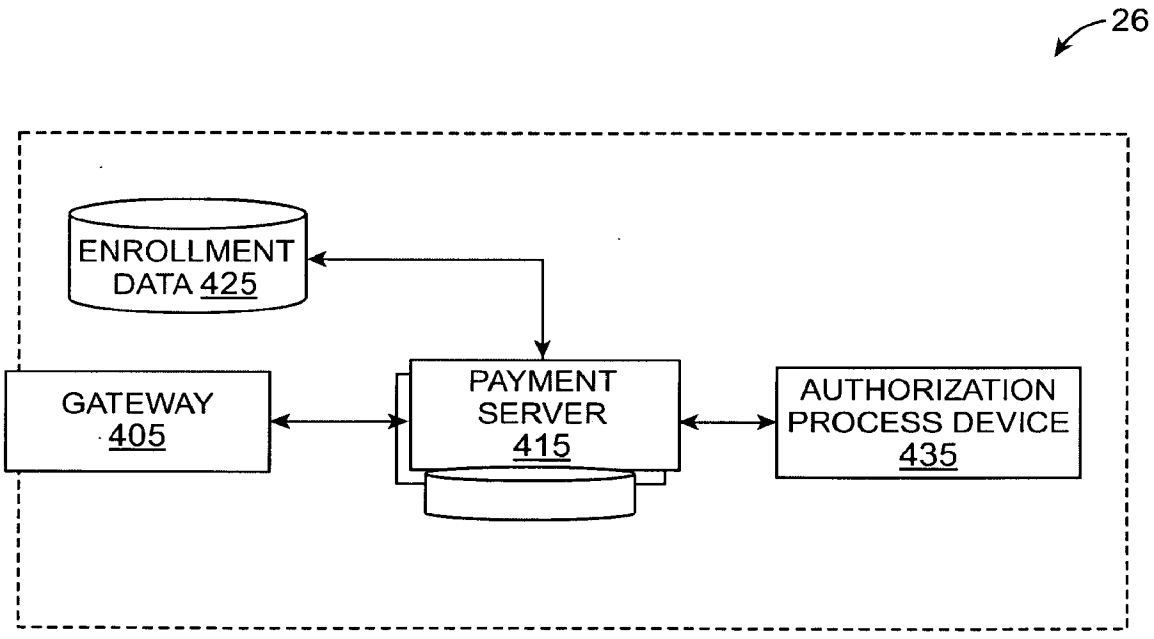

26
ENROLLMENT DATA 425
GATEWAY 405
PAYMENT SERVER 415
AUTHORIZATION PROCESS DEVICE 435

FIG. 4

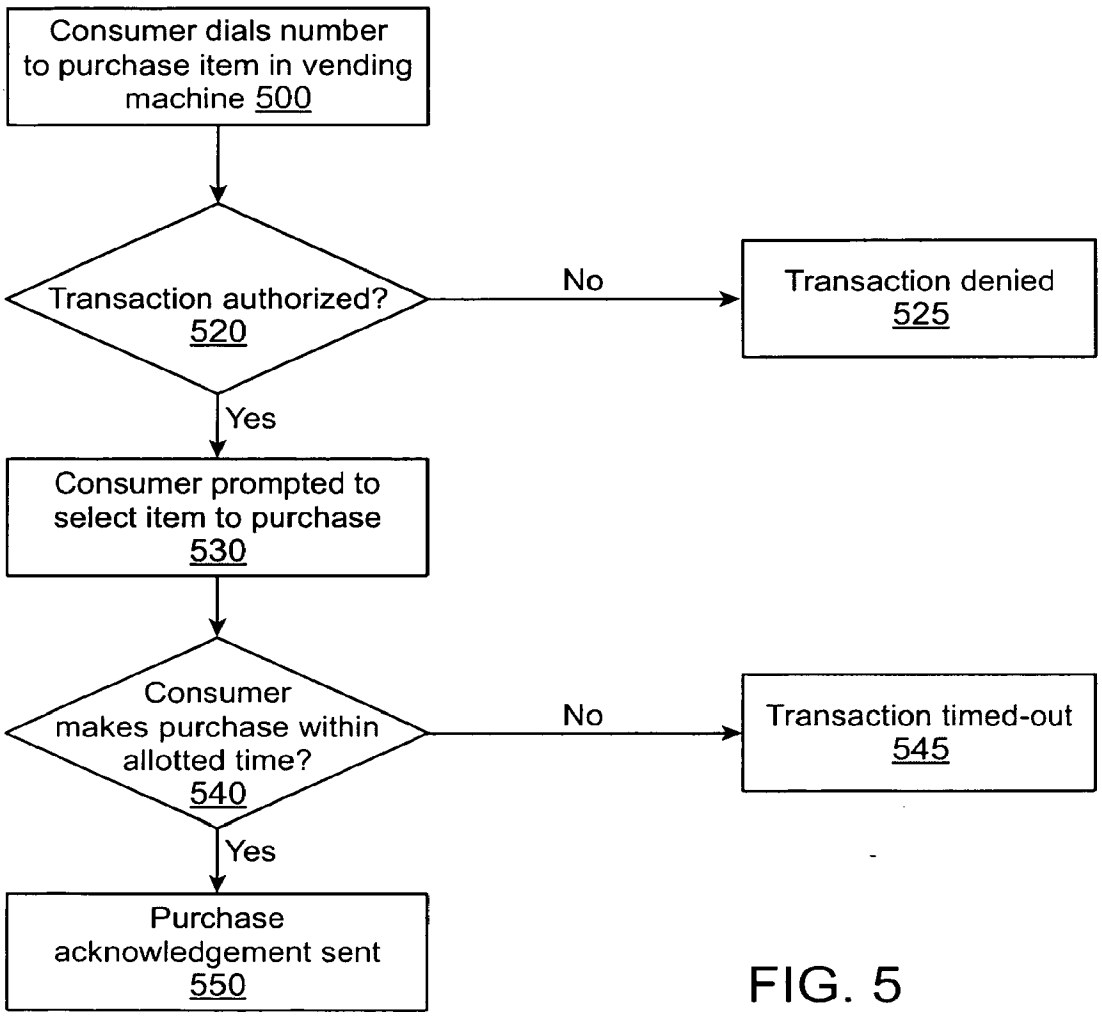

Consumer dials number to purchase item in vending machine 500
Transaction authorized? 520
No
Transaction denied 525
Yes
Consumer prompted to select item to purchase 530
Consumer makes purchase within allotted time? 540
No
Transaction timed-out 545
Yes
Purchase acknowledgement sent 550

FIG. 5

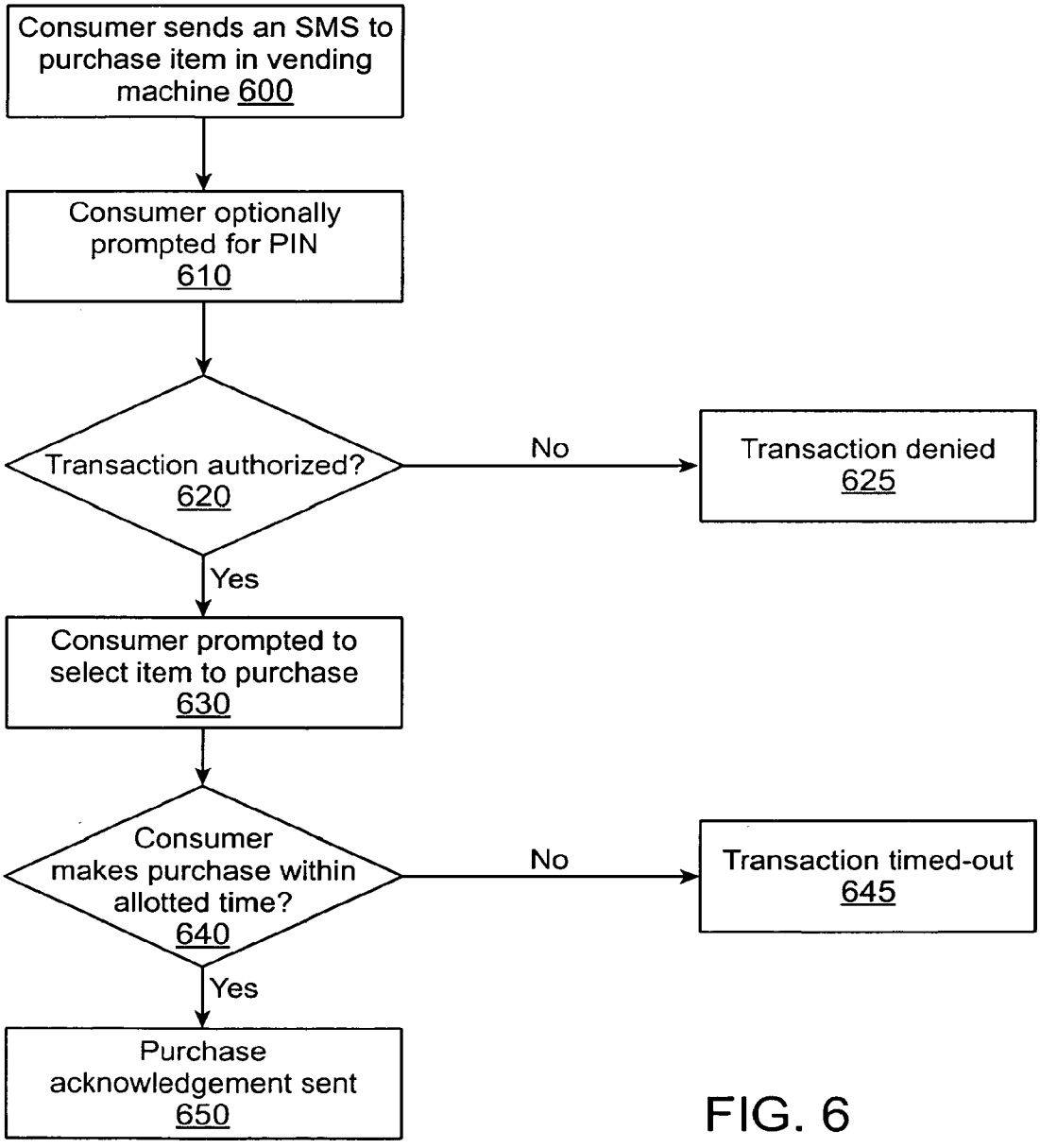

Consumer sends an SMS to purchase item in vending machine 600
Consumer optionally prompted for PIN 610
Transaction authorized? 620
No
Transaction denied 625
Yes
Consumer prompted to select item to purchase 630
Consumer makes purchase within allotted time? 640
No
Transaction timed-out 645
Yes
Purchase acknowledgement sent 650

FIG. 6

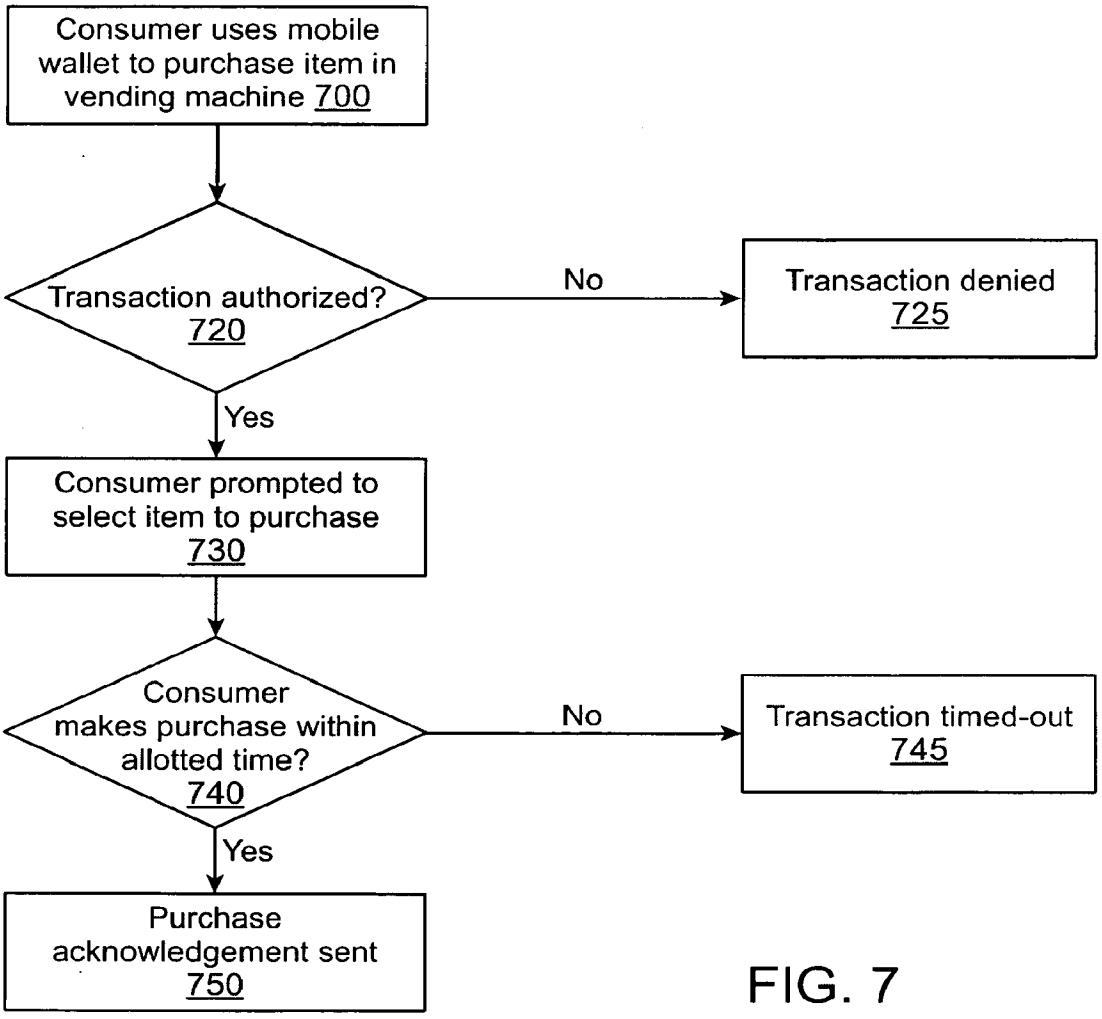

Consumer uses mobile wallet to purchase item in vending machine 700
Transaction authorized? 720
No
Transaction denied 725
Yes
Consumer prompted to select item to purchase 730
Consumer makes purchase within allotted time? 740
No
Transaction timed-out 745
Yes
Purchase acknowledgement sent 750

FIG. 7

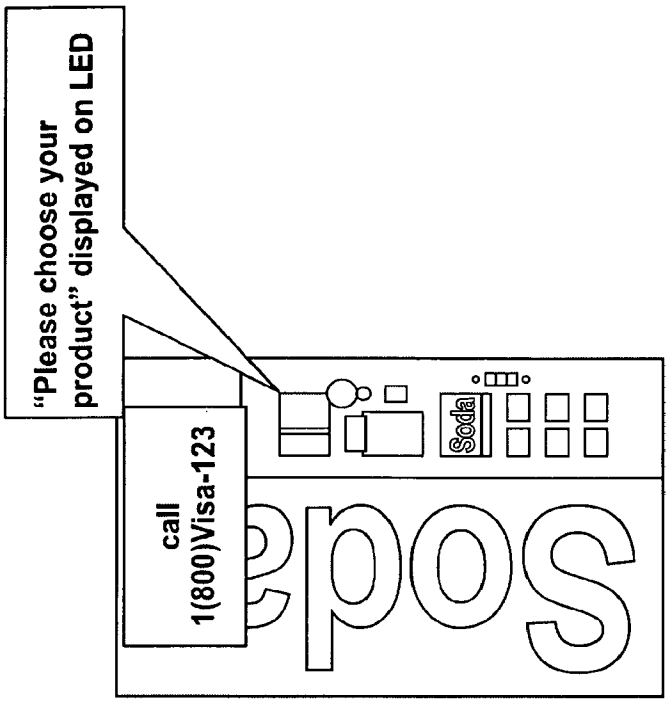

"Please choose your product" displayed on LED
call 1(800)Visa-123
Soda
epos

FIG. 8(b)

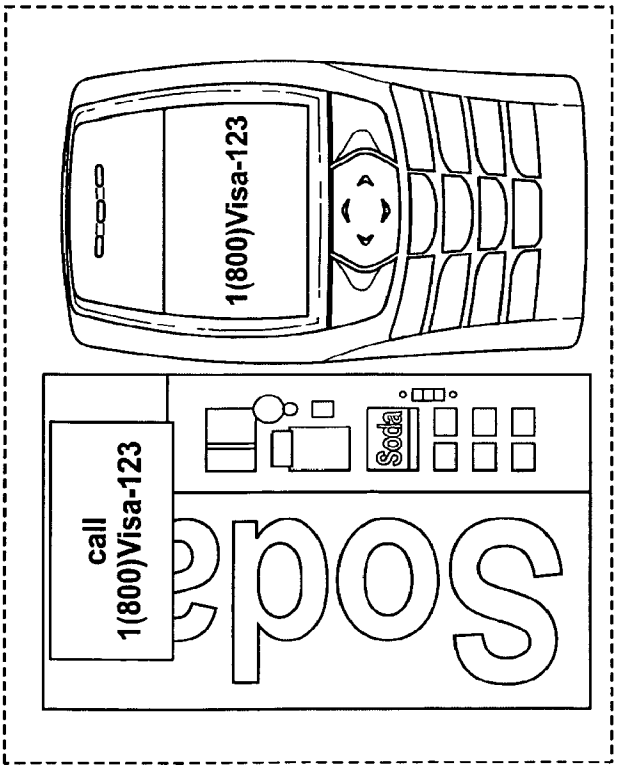

1(800)Visa-123
call 1(800)Visa-123
Soda
epos

FIG. 8(a)

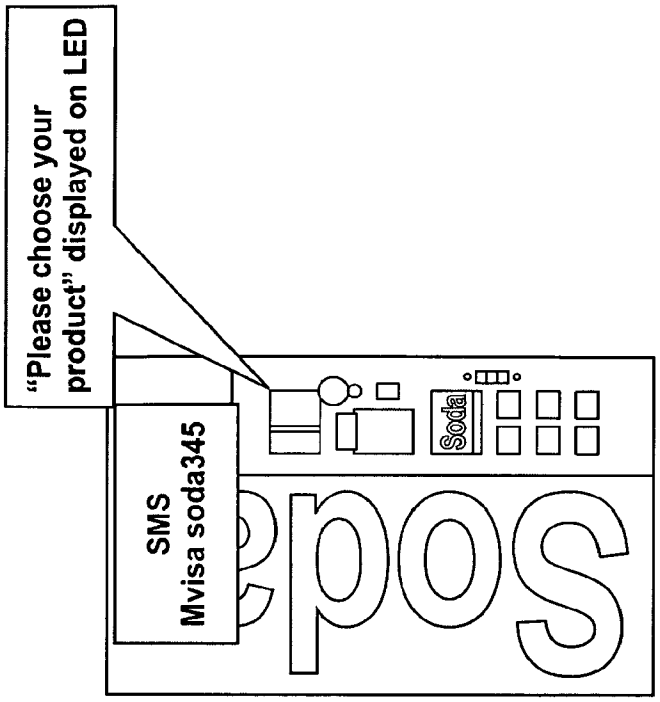

"Please choose your product" displayed on LED
SMS
Mvisa soda345
Soda
epos

FIG. 9(b)

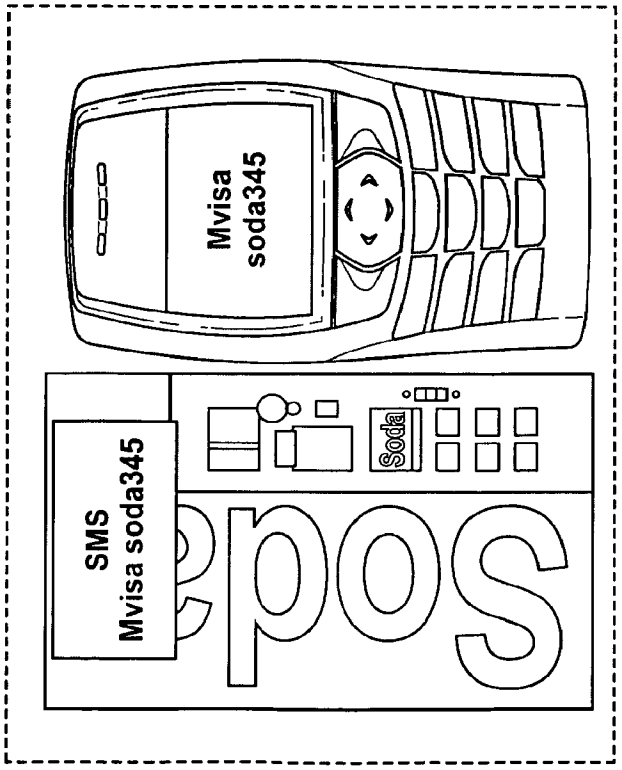

Mvisa
soda345
SMS
Mvisa soda345
Soda
epos

FIG. 9(a)

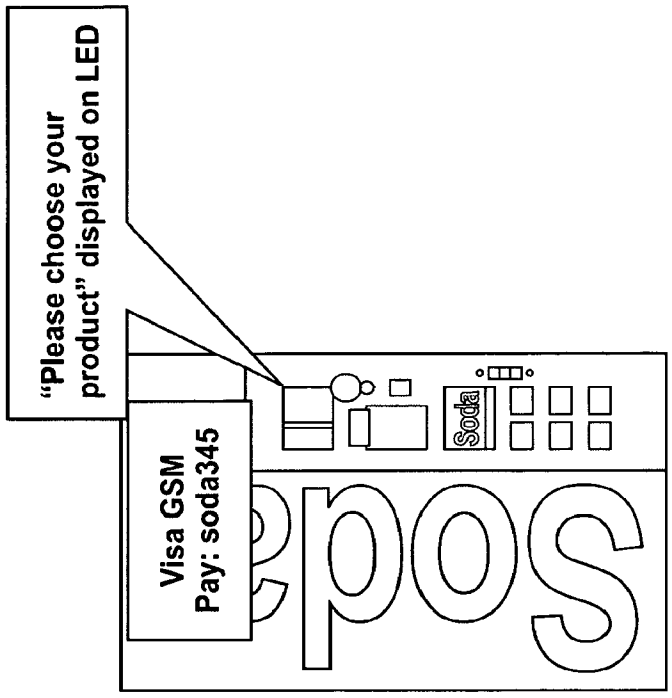


FIG. 10(b)

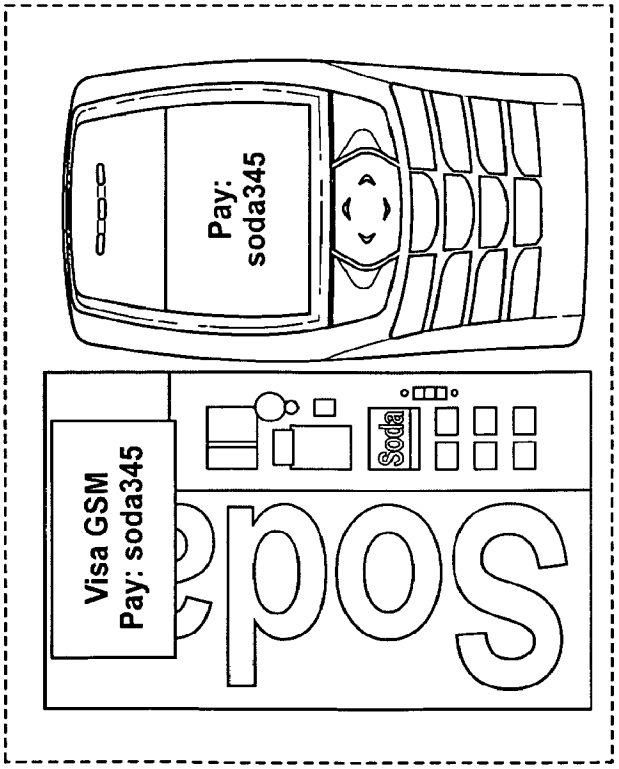


FIG. 10(a)

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 July 2008 (10.07.2008)

PCT

(10) International Publication Number
WO 2008/083078 A2

(51) International Patent Classification:
G06K 7/00 (2006.01) *H04M 1/00* (2006.01)
G06Q 20/00 (2006.01)

(21) International Application Number:
PCT/US2007/088563

(22) International Filing Date:
21 December 2007 (21.12.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/871,898 26 December 2006 (26.12.2006) US

(71) Applicants *(for all designated States except US)*: **VISA U.S.A. INC.** [US/US]; P.O. Box 8999, M3-2B, San Francisco, California 94128 (US). **VISA INTERNATIONAL SERVICE ASSOCIATION** [US/US]; 900 Metro Center Boulevard, Foster City, California 94404 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **CARLSON, Mark** [US/US]; 153 Miramonte Avenue, Half Moon Bay, California 94019 (US). **STAN, Patrick** [US/US]; California (US). **FAITH, Patrick** [US/US]; 2810 Jones Gate Court, Pleasanton, California 94566 (US).

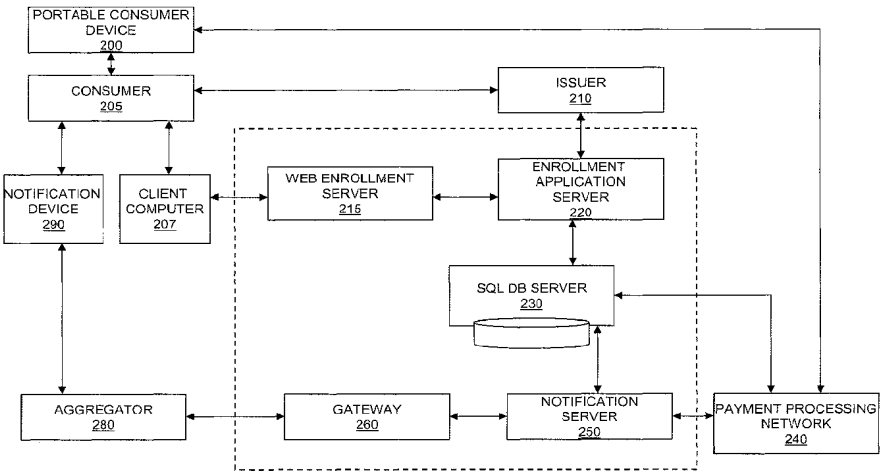
(74) Agents: **JEWIK, Patrick, R.** et al.; Townsend and Townsend and Crew LLP, Two Embarcadero Center, 8th Floor, San Francisco, California 94111-3834 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, 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, 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, MT, 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:
— *without international search report and to be republished upon receipt of that report*

(54) **Title:** CUSTOMIZED PAYMENT TRANSACTION NOTIFICATION



(57) **Abstract:** A method for customizing alerts and notifications for portable consumer device transactions is disclosed. One embodiment of the invention is directed to a method comprising receiving information that a transaction associated with a portable consumer device is occurring, and providing an alert to a consumer associated with the portable consumer device, wherein the alert indicates that the transaction is occurring, wherein the alert is sent to the consumer according to a time or communication mode previously specified by the consumer using an interface that allows the user to specify the time and communication mode for receiving the alert.

WO 2008/083078 A2

CUSTOMIZED PAYMENT TRANSACTION NOTIFICATION

CROSS-REFERENCES TO RELATED APPLICATIONS

[0001] The present application is a non-provisional application of and claims priority to U.S. Provisional Application No. 60/871,898, filed on December 26, 2006, the entire contents of which are herein incorporated by reference for all purposes.

BACKGROUND

[0002] There are many occasions where a consumer may want to be notified when his credit card or the like is used. For example, he may want to know when his credit card account number has been used to purchase a large screen television for $5000 on the Internet, when the account number is used outside the U.S. to purchase airplane tickets, or when his child uses the account number or credit card to purchase alcohol.

[0003] A consumer may be notified by the issuer that issued his credit card when the issuer determines a potentially fraudulent activity has occurred in a purchase with the consumer's credit card. The issuer may contact the consumer using the contact information it has on file for the consumer, which is typically a consumer's home phone and address. For example, the issuer may call the consumer at his home phone number or send a letter to his home address informing the consumer that potentially fraudulent or unauthorized activity is taking place. However, the consumer may not be at home or may not answer the phone and a letter may take a few days to arrive at the consumer's home. Further, the activity may occur in the early hours of the morning outside of the issuer's business hours and when the consumer does not want to receive a call. For example, if a potentially fraudulent purchase is made with the consumer's credit card at 2 a.m. in the morning, the consumer may be asleep. Thus, conventional notification methods may not be very effective for notifying the consumer of potentially fraudulent or unauthorized credit card activity.

[0004] Embodiments of the invention address these and other problems individually and collectively.

BRIEF SUMMARY

[0005] Embodiments of the invention are directed to improved consumer notification systems and methods.

[0006] One embodiment of the invention is directed to a method comprising receiving information that a transaction associated with a portable consumer device is occurring, and providing an alert to a consumer associated with the portable consumer device, wherein the alert indicates that the transaction is occurring, wherein the alert is sent to the consumer according to a time or communication mode previously specified by the consumer using an interface that allows the user to specify the time and communication mode for receiving the alert.

[0007] Another embodiment of the invention is directed to a client computer comprising a processor, and a computer readable medium, wherein the computer readable medium comprises instructions for executing a method comprising receiving information on how to be notified if a predetermined activity is occurring with respect to a portable consumer device, wherein an alert is provided in manner consistent with the information provided if the predetermined activity is occurring wherein the information provided is a result of a consumer's choice to customize an alert for each predetermined activity by using an interface that allows a user to customize the alert according to at least communication mode and time, and sending the information to a notification server.

[0008] Another embodiment of the invention is directed to a method comprising providing information on how to be notified if a predetermined activity is occurring with respect to a portable consumer device, and receiving an alert in manner consistent with the information provided if the predetermined activity is occurring wherein the information provided is a result of the consumer's choice to customize an alert for each predetermined activity by communication mode and time.

[0009] Another embodiment of the invention is directed to a phone comprising a processor, and a computer readable medium coupled to the processor, wherein the computer readable medium comprises code for receiving an alert, wherein the alert indicates that the transaction is occurring, wherein the alert is sent to the consumer according to a time or communication mode previously specified by the consumer using an interface that allows the consumer to specify the time and communication mode for receiving the alert.

[0010] Other embodiments of the invention are directed to computer readable media comprising code for performing the above-described methods as well as systems, apparatuses and devices that perform the methods and/or that use the computer readable media.

[0011] These and other embodiments of the invention are described in further detail below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] FIG. 1(a) shows a block diagram of a payment processing system according to an embodiment of the invention.

[0013] FIG. 1(b) shows a block diagram of an exemplary portable consumer device.

[0014] FIG. 2 shows a block diagram of a system according to an embodiment of the invention.

[0015] FIG. 3 shows a flowchart illustrating steps in a method according to an embodiment of the invention.

[0016] FIG. 4 shows a Web page illustrating notification parameters chosen by a consumer.

[0017] FIG. 5 shows a block diagram of a computer apparatus.

DETAILED DESCRIPTION

[0018] Customized payment transaction notification systems and methods are described in further detail below. They can be used in the context of payment transactions using payment processing systems, which are configured to process credit and debit card transactions.

[0019] **I. Payment Processing Systems**

[0020] Embodiments of the invention are directed to the use of portable consumer devices, and methods and systems that use them. The portable consumer devices can be used in payment processing systems like those shown in FIG. 1(a).

[0021] FIG. 1(a) shows a system **20** that can be used in an embodiment of the invention. For simplicity of illustration, one merchant, one issuer, one acquirer, one portable consumer device, and one consumer are shown. It is understood however, that embodiments of the invention may include multiple merchants, issuers, acquirers, portable consumer devices, and/or consumers. In addition, some embodiments of the invention may include fewer than all of the components shown in FIG.1(a). Also, the components in FIG. 1(a) may communicate via any suitable communication medium (including the Internet), using any suitable communication protocol.

[0022] The system **20** includes a merchant **22** and an acquirer **24** associated with the merchant **22**. In a typical payment transaction, a consumer **30** may purchase goods or services at the merchant **22** using a portable consumer device **32**. The acquirer **24** can communicate with an issuer **28** via a payment processing network **26**.

[0023] The acquirer **24** is typically a bank that has a merchant account. The issuer **28** may also be a bank, but could also be business entity such as a retail store. Some entities are both acquirers and issuers, and embodiments of the invention include such entities. The issuer **28** may operate a server computer **21**, which may have a computer readable medium comprising code for performing the functions that the issuer **28** performs. A database **23** comprising account number

information and other information may be operatively coupled to the server computer **21**.

[0024] The consumer **30** may be an individual, or an organization such as a business that is capable of purchasing goods or services.

[0025] The portable consumer device **32** may be in any suitable form. For example, suitable portable consumer devices can be hand-held and compact so that they can fit into a consumer's wallet and/or pocket (e.g., pocket-sized). They may include smart cards, ordinary credit or debit cards (with a magnetic strip and without a microprocessor), keychain devices (such as the Speedpass™ commercially available from Exxon-Mobil Corp.), etc. Other examples of portable consumer devices include cellular or mobile phones, personal digital assistants (PDAs), pagers, payment cards, security cards, access cards, smart media, transponders, and the like. The portable consumer devices can also be debit devices (e.g., a debit card), credit devices (e.g., a credit card), or stored value devices (e.g., a stored value card).

[0026] The portable consumer device **32** may comprise a computer readable medium (CRM) **32(a)** and a body **32(b)**. The computer readable medium **32(a)** may be on the body **32(b)**. The body **32(b)** may in the form a plastic substrate, housing, or other structure. The computer readable medium **32(a)** may be a memory that stores data and may be in any suitable form. Exemplary computer readable media **32(a)** may be in any suitable form including a magnetic stripe, a memory chip, etc. If the portable consumer device **32** is in the form of a card, it may have an embossed region **32(a)** which is embossed with a PAN (primary account number).

[0027] An exemplary wireless portable consumer device **32'** in the form of a phone may comprise a computer readable medium and a body as shown in FIG. 1(b). (FIG. 1(b) shows a number of components, and the portable consumer devices according to embodiments of the invention may comprise any suitable combination or subset of such components.) The computer readable medium **32(b)** may be present within the body **32(h)**, or may be detachable from it. The body **32(h)** may be in the form a plastic substrate, housing, or other structure. The computer readable medium **32(b)** may be a memory that stores data and may be in any suitable form including a magnetic stripe, a memory chip, etc. The memory preferably stores

information such as financial information, transit information (e.g., as in a subway or train pass), access information (e.g., as in access badges), etc. Financial information may include information such as bank account information, bank identification number (BIN), credit or debit card number information, account balance information, expiration date, consumer information such as name, date of birth, etc. Any of this information may be transmitted by the portable consumer device **32'**.

[0028] In some embodiments, and regardless of the type of wireless portable consumer device that is used, information in the memory may also be in the form of data tracks that are traditionally associated with credits cards. Such tracks include Track 1 and Track 2. Track 1 ("International Air Transport Association") stores more information than Track 2, and contains the cardholder's name as well as account number and other discretionary data. This track is sometimes used by the airlines when securing reservations with a credit card. Track 2 ("American Banking Association") is currently most commonly used. This is the track that is read by ATMs and credit card checkers. The ABA (American Banking Association) designed the specifications of this track and all world banks must abide by it. It contains the cardholder's account, encrypted PIN, plus other discretionary data.

[0029] The portable consumer device **32'** may further include a contactless element **32(g)**, which is typically implemented in the form of a semiconductor chip (or other data storage element) with an associated wireless transfer (e.g., data transmission) element, such as an antenna. Contactless element **32(g)** is associated with (e.g., embedded within) portable consumer device **32'** and data or control instructions transmitted via a cellular network may be applied to contactless element **32(g)** by means of a contactless element interface (not shown). The contactless element interface functions to permit the exchange of data and/or control instructions between the mobile device circuitry (and hence the cellular network) and an optional contactless element **32(g)**.

[0030] Contactless element **32(g)** is capable of transferring and receiving data using a near field communications ("NFC") capability (or near field communications medium) typically in accordance with a standardized protocol or data transfer mechanism (e.g., ISO 14443/NFC). Near field communications capability is a short-range communications capability, such as RFID, Bluetooth™, infra-red, or other data

transfer capability that can be used to exchange data between the portable consumer device **32'** and an interrogation device. Thus, the portable consumer device **32'** is capable of communicating and transferring data and/or control instructions via both cellular network and near field communications capability.

[0031] The portable consumer device **32'** may also include a processor **32(c)** (e.g., a microprocessor) for processing the functions of the portable consumer device **32'** and a display **32(d)** to allow a consumer to see phone numbers and other information and messages. The portable consumer device **32'** may further include input elements **32(e)** to allow a consumer to input information into the device, a speaker **32(f)** to allow the consumer to hear voice communication, music, etc., and a microphone **32(i)** to allow the consumer to transmit her voice through the portable consumer device **32'**. The portable consumer device **32'** may also include an antenna **32(a)** for wireless data transfer (e.g., data transmission).

[0032] Referring again to FIG. 1(a), the payment processing network **26** may include data processing subsystems, networks, and operations used to support and deliver authorization services, exception file services, and clearing and settlement services. An exemplary payment processing network may include VisaNet™. Payment processing networks such as VisaNet™ are able to process credit card transactions, debit card transactions, and other types of commercial transactions. VisaNet™, in particular, includes a VIP system (Visa Integrated Payments system) which processes authorization requests and a Base II system which performs clearing and settlement services.

[0033] The payment processing network **26** may include a server computer. A "server computer" or "server" is typically a powerful computer or cluster of computers. For example, the server computer can be a large mainframe, a minicomputer cluster, or a group of servers functioning as a unit. In one example, the server computer may be a database server coupled to a Web server. The payment processing network **26** may use any suitable wired or wireless network, including the Internet.

[0034] The merchant **22** may also have, or may receive communications from, an access device **34** that can interact with the portable consumer device **32**. In FIG.

1(a), the access device **34** is located at the merchant **22**. However, it could be located at any other suitable location in other embodiments of the invention.

[0035] The access devices according to embodiments of the invention can be in any suitable form. Examples of access devices include point of sale (POS) devices, cellular or mobile phones, PDAs, personal computers (PCs), tablet PCs, handheld specialized readers, set-top boxes, electronic cash registers (ECRs), automated teller machines (ATMs), virtual cash registers (VCRs), kiosks, security systems, access systems, and the like.

[0036] If the access device **34** is a point of sale terminal, any suitable point of sale terminal may include a reader **34(a)**, a processor **34(b)** and a computer readable medium **34(c)**. The reader **34(a)** may include any suitable contact or contactless mode of operation. For example, exemplary card readers can include RF (radio frequency) antennas, magnetic stripe readers, etc. to interact with the portable consumer device **32**.

[0037] In a typical purchase transaction, the consumer **30** purchases a good or service at the merchant **22** using a portable consumer device **32** such as a credit card. The consumer's portable consumer device **32** can interact with an access device **34** such as a POS (point of sale) terminal at the merchant **22**. For example, the consumer **30** may take a credit card and may swipe it through an appropriate slot in the POS terminal. Alternatively, the POS terminal may be a contactless reader, and the portable consumer device **32** may be a contactless device such as a contactless card.

[0038] An authorization request message is then forwarded to the acquirer **24**. After receiving the authorization request message, the authorization request message is then sent to the payment processing network **26**. The payment processing network **26** then forwards the authorization request message to the issuer **28** of the portable consumer device **32**.

[0039] After the issuer **28** receives the authorization request message, the issuer **28** sends an authorization response message back to the payment processing network **26** to indicate whether or not the current transaction is authorized. The payment processing network **26** then forwards the authorization response message

back to the acquirer **24**. The acquirer **24** then sends the response message back to the merchant **22**.

[0040] After the merchant **22** receives the authorization response message, the access device **34** at the merchant **22** may then provide the authorization response message for the consumer **30**. The response message may be displayed by the access device **34** or the portable consumer device **32**, or may be printed out on a receipt.

[0041] At the end of the day, a normal clearing and settlement process can be conducted by the payment processing network **26**. A clearing process is a process of exchanging financial details between and acquirer and an issuer to facilitate posting to a consumer's account and reconciliation of the consumer's settlement position.

[0042] Some of the embodiments described below may use a payment processing system like the one described above, or any suitable combination of components in the payment processing system.

[0043] II. Customized Payment Transaction Notification System and Method

[0044] Embodiments of the invention are directed to customized alerts and notifications for portable consumer device transactions. In these embodiments of the invention, a consumer may customize the alert trigger (e.g., only notify the consumer if the transaction that is occurring is greater than $5000 in value), time of the alert (e.g., from 9 a.m. to 5 p.m.), communication mode (e.g., e-mail, telephone, SMS), and/or contact (e.g., wireless e-mail address, work e-mail address, spouse's cellular phone, home phone). The consumer may use an interface such as a Web interface to indicate how and/or when the consumer is to be alerted when the consumer's portable consumer device or account number associated with the portable consumer device is used. In embodiments of the invention, the consumer can specify whether he wants alerts set separately for each account number and/or portable consumer device that he has. He can also specify that any alerts that are provided by provided at the same time and under the same conditions across all accounts or portable consumer devices associated with the consumer.

[0045] Illustratively, the consumer can visit a Web site which allows the consumer to customize the way in which he is alerted when his credit card is being used. Using a Web interface such as a Web page, the consumer may indicate that he wants to be notified by phone if his credit card or credit card account number is being used between 10 p.m. and 6 a.m. to conduct a transaction of any amount, since he will most likely be at home and sleeping during this time. Using the Web page, the consumer may also specify that the consumer wants to be notified of any account or device activity via e-mail and a mobile phone during the hour of 6:00 a.m. and 10 p.m, only if the transaction amount if greater than $500. Thus, after the consumer provides this customization information, if a $5000 credit card transaction is conducted at 2 a.m. using the consumer's credit card, a payment processing organization and/or issuer may then provide an alert to the consumer by calling the consumer on the consumer's home telephone. The consumer may thereafter contact the payment processing organization and/or the issuer to take appropriate action. For example, the consumer may prevent the transaction from taking place by not authorizing the transaction. Alternatively, if a $5000 transaction is being conducted at 10 a.m. using the consumer's credit card or credit card account number, the payment processing organization and/or the issuer of the credit card may notify the consumer by providing an alert to his e-mail device and his mobile phone.

[0046] FIG. 2 shows a block diagram of a system according to an embodiment of the invention.

[0047] FIG. 2 shows a consumer **205** who may use a portable consumer device **200** to conduct payment transactions, money transfers, access transactions, etc. The consumer **205** may also use a notification device **290** such as a mobile phone to receive alerts, and may use a client computer **207** such as a personal computer to receive alerts and/or to enroll in an alert program. As shown in FIG. 2, the client computer **207** may be in operative communication with a Web enrollment server **215**, which may in turn be in operative communication in an enrollment application server **220**, a SQL database server **230**, and a notification server **250**. An issuer **210** may be in communication with at least the enrollment application server **220**, and the payment processing network **240** may be in communication with the notification server **250**. An aggregator **280** may be in communication with a

gateway **260** and the notification device **290**, as well as the notification server **250**. Each of the components shown in FIG. 2 is described in further detail below. Methods of using the system shown in FIG. 2 are also described in detail below.

[0048] For simplicity of illustration, one portable consumer device, one consumer, one issuer, one notification device, one client computer, one aggregator, etc. is shown. It is understood however, that embodiments of the invention may include multiple portable consumer devices, consumers, issuers, notification devices, client computers, aggregators, etc. In addition, some embodiments of the invention may include fewer than all of the components shown in FIG. 2. Also, the components in FIG. 2 may communicate via any suitable communication medium (including the Internet), using any suitable communication protocol.

[0049] The system in FIG. 2 includes a portable consumer device **200** associated with a consumer **205**. Suitable portable consumer devices are described in further detail above.

[0050] The consumer **205** may operate a client computer **207**. The client computer **207** can be a desktop computer, a laptop computer, a cellular or mobile phone, a personal digital assistant (PDA), etc. It may operate using any suitable operating system including a Windows™ based operating system.

[0051] The notification device **290** can be any suitable device that can receive alerts and can provide such alerts to the consumer **205**. Examples of notification devices include computers, cellular or mobile phones (e.g., as shown in FIG. 1(b)), wired telephones, personal digital assistants (PDAs), pagers, and the like. The notification device **290** may be in any suitable form (e.g., suitable notification devices can be hand-held and compact so that they can fit into a consumer's wallet and/or pocket).

[0052] In some embodiments, the notification device **290** and the portable consumer device **200** can be embodied by the same device. For example, a wireless phone may function as both a portable consumer device that can be used to pay for goods or services, and a notification device to notify the consumer if activity associated with the wireless phone, or an account number associated with the wireless phone, is being conducted.

[0053] If the notification device is a phone, it may comprise a processor, and a computer readable medium coupled to the processor. The computer readable medium comprises code for receiving an alert, wherein the alert indicates that the transaction is occurring, where the alert is sent to the consumer according to a time or communication mode previously specified by the consumer using an interface that allows the consumer to specify the time and communication mode for receiving the alert.

[0054] As described above, the issuer **210** may be a bank or other business entity such as a retail store. The payment processing network **240** may include data processing subsystems, networks, and operations used to support and deliver authorization services, exception file services, and clearing and settlement services. An exemplary payment processing network may include VisaNet™.

[0055] A web enrollment server **215**, an enrollment application server **220**, a SQL DB server **230**, and a notification server **250** may perform different functions. For example, a web enrollment server **215** may receive enrollment or registration information from a consumer **205** via a client computer **207** and send enrollment information to an enrollment application server **220**. An enrollment application server **220** may receive enrollment information from a consumer **205** through a web enrollment server **215** or an issuer **210** and may store the new or updated enrollment information in a SQL DB server **230**. A SQL DB server **230** may receive and store new or updated enrollment information (e.g., information on what types of alerts the consumer would like to receive, etc.) as well as other consumer account information such as whether or not an alert has been received by a consumer and whether or not the consumer would like the alert to be escalated if it has not been received. A notification server **250** may receive alert trigger information, determine whether the consumer **205** would like to be notified about the trigger, and send alerts to a notification device **290** via a gateway **260** and aggregator **280** if the consumer **205** would like to receive an alert for the trigger. A notification event server **250** may also evaluate whether or not the alert should be escalated.

[0056] The system in FIG. 2 may further include a gateway **260** whereby a phone call, text message or Short Message Service ("SMS") message, for example, from the notification server **250**, can pass through to the consumer via aggregator

280. (SMS is typically a service available on a portable consumer device that permits the sending of short messages between devices via an intermediate server.) The gateway **260** may be embodied by a computer or a network that allows or controls access to another computer or network. The gateway **260** may also be a software interface between the computer or network and another computer or network.

[0057] The aggregator **280** may be an entity or organization that receives and transmits messages to a phone, e-mail account, etc. In some cases, wireless telephone companies may be considered aggregators.

[0058] Before a consumer can receive alerts, the consumer can register with the alert system. Information can be received using an interface that allows the user to specify the time and communication mode for receiving an alert when a transaction is occurring with respect to a portable consumer device associated with the consumer. The information includes the communication mode or time in which the consumer wants to be notified.

[0059] A specific registration process can now be described with reference to FIG. 2. A consumer **205** may register for alerts or update existing alerts for transactions made with the portable consumer device **200** in any number of ways. For example, the consumer **205** can register via a separate website designed for this purpose, or manually though a paper form (which may be considered a registration interface). Registration information may be received by the issuer **210**, the payment processing organization operating the payment processing network **240**, or another third party.

[0060] The issuer **210** or payment processing organization may also enroll the consumer **205** automatically for alerts and notifications. For example, if the consumer **205** is automatically enrolled by the issuer **210** or provides enrollment information to an issuer **210** associated with the portable consumer device **200**, then the issuer **210** may communicate with an enrollment application server **220** and may send the consumer's enrollment information to the enrollment application server **220**. In some cases, a consumer **205** may enroll for alerts (or update existing information) for a portable consumer device **200** (e.g., a credit card or debit card) by providing information (e.g., alert trigger, time, communication mode, and/or contact for

notification) to the issuer **210** (e.g., the bank that issued the consumer's credit card) in person, via a website, over the phone, or by mail. The alerts may be set by account (e.g., separate alerts for each account and/or portable consumer device the consumer has with the issuer) or may be set by identification so that all accounts for that consumer have the same alerts.

[0061] A consumer **205** may also register to receive alerts via a website (separate from the issuer) designed for this purpose, by entering enrollment information (or updating existing information) for a portable consumer device **200**. For example, a consumer **205** may use a client computer **207** to access the website to enter registration information. The information is then sent to a web enrollment server **215**, which sends the information to the enrollment application server **220**.

[0062] The client computer **207** may comprise a processor, and a computer readable medium. The computer readable medium comprises instructions for executing a method comprising receiving information on how to be notified if a predetermined activity is occurring with respect to a portable consumer device, wherein an alert is provided in manner consistent with the information provided if the predetermined activity is occurring wherein the information provided is a result of the consumer's choice to customize an alert for each predetermined activity by using an interface that allows a user to customize the alert according to at least communication mode and time, and sending the information to a notification server.

[0063] An exemplary Web interface is shown in FIG. 4. As shown, a consumer having a portable consumer device **200** with an account number 12345678 may indicate, for each communication mode (which may include different types of electronic devices), the particular time or times that the user wants to be alerted. FIG. 4 also shows thresholds (e.g., triggers) that will trigger the sending of an alert. As shown in FIG. 4, different triggers can be matched with different times, and different alert modes. In the illustrated example, a consumer may want to be notified when any transaction is conducted between 10:01 pm and 6:59 am, since he will probably not be conducting transactions during this time. However, during other times, the consumer may only want to be alerted if transactions are over $100.

[0064] The enrollment application server **220** may then store the new or updated enrollment information in a SQL DB server **230**. The SQL DB server may

be updated immediately after the enrollment application server **220** receives new or updated information, or periodically (e.g., every hour, at the end of the day, etc.).

[0065] The alert trigger records are then sent to the system which will be detecting the trigger for the alert so that the system knows under what conditions the consumer **205** would like an alert. These trigger records may be sent on demand (e.g., when the consumer **205** makes a change) or periodically (e.g., hourly, daily, etc.). In one embodiment, the system detecting the alert may be a payment processing network **240**. In another embodiment the system detecting the alert may be an issuer **210**.

[0066] In some embodiments, alerts may be sent after other certain conditions are met. For example, the conditions associated with a particular purchase transaction may first be evaluated by a payment processing organization or issuer to determine if an alert is to be sent. For example, a payment processing organization or issuer may determine that the particular transaction being evaluated is a mail order-telephone order type of purchase (i.e., a MOTO transaction), is a risky transaction (e.g., because the transaction is being conducted by a merchant who has had risk issues in the past), and/or is over a certain dollar limit (e.g., over $30 in value). In such embodiments, it may be that the alert is only sent if these conditions are met. Such conditions may be set by the payment processing organization or the issuer, with or without the participation or knowledge of the consumer.

[0067] FIG. 3 shows a flowchart including a general method according to an embodiment of the invention. The method can be described with reference to the block diagram in FIG. 2.

[0068] In a typical transaction a consumer **205** may use the portable consumer device **200** to make a purchase via a payment processing network **240**. For example, the consumer **205** may use a portable consumer device (step **300**), such as a credit card, to pay $5000 for a flat screen television. Once the consumer **205** uses the portable consumer device **200** (e.g., swipes his credit card at a merchant as shown in FIG. 1(a) and described earlier), an authorization request message passes to the payment processing network **240**. The payment processing network **240** checks to see if the characteristics of the transaction that has been

made with the portable consumer device **200** matches a condition (e.g., notification event trigger) under which a consumer wants to be alerted (step **310**).

[0069] There are a number of examples of notification event triggers. Examples of notification event triggers include the following: a transaction is over a certain amount of money (e.g. over $5000); any transaction conducted with a particular portable consumer device; a spending threshold (e.g., a daily or monthly spending limit) has been reached for a particular portable consumer device; a transaction is made outside a particular geographic location (e.g., outside the country that the consumer resides in); a risky transaction is being conducted ("risky" may be predefined by the consumer and/or the issuer), a transaction is made without the physical portable consumer device (e.g., Internet, mail, or telephone order); a cash transaction or withdrawal; an online account has been accessed; a person has used the portable consumer device to enter a certain location (e.g., a secure area, a business after-hours); a payment is due within a certain amount of time; a payment is overdue; a child or spouse has conducted a transaction; a balance on the portable consumer device is exceeded; a particular type of transaction is being conducted (e.g., purchases for airline tickets, lodging, auto rental, restaurants, medical, etc.), etc. Thus, embodiments of the invention are flexible enough to allow for many types of notification event triggers.

[0070] If there is no notification event trigger, then the notification process ends (step **315**). If there is a notification event trigger, the payment processing network **240** sends the trigger information to the notification server **250**. The notification server **250** checks the SQL DB Server **230** to see how (or even if) the consumer **205** would like to be notified about the credit card transaction (step **320**). If the consumer **205** does not want to be alerted about this particular type of transaction, the notification process ends (step **325**).

[0071] If the consumer **205** would like to be notified about this particular type of transaction, then an alert is then sent to the consumer **205** via the communication mode (e.g., via a specific communication channel) specified by the consumer **205** (step **330**). Examples of communication modes include voice, mobile, SMS, e-mail, instant message, IVR (interactive voice response). etc.

[0072] As noted above, consumer may specify one or more communication mode per notification event trigger. For example, a consumer may want to be notified when a purchase is made that is over $5000 by mobile phone and e-mail. In addition, a consumer may specify one or more contacts for each communication mode. For example, a consumer **205** can have multiple mobile numbers (e.g., the consumer's personal mobile phone, work mobile phone, spouse's mobile phone number), multiple phone numbers (e.g., home phone, work phone), multiple SMS addresses (e.g., mobile phone, PDA, secretary's PDA), or multiple e-mail addresses (e.g., work e-mail, personal e-mail), etc. A consumer may also customize the time that he wants to receive each or all alerts. For example, the consumer may want to be notified immediately of the transaction, only during certain hours (e.g., between 9 a.m. and 5 p.m.), may specify different communication modes for different times of the day or types of transactions, or may choose not to be notified during certain hours (e.g., between 1 a.m. and 6 a.m.).

[0073] Thus, a consumer can specify that he wants to receive a notification if his portable consumer device is used for a transaction over a certain amount of money (e.g., over $5000), via his work phone number and spouse's e-mail if it is during the day, and by SMS and home phone if the transaction occurs on the evening or weekend. The alert may be sent to a notification device **290** via a gateway **260** and aggregator **280** using the specified communication mode. The alert text or message may also be customized to the consumer, such as, "Mark, your credit card account ending in 9999 was just used for a purchase by phone for $500.00. Please contact 555-555-5555 if this is incorrect."

[0074] A consumer may also want the alert to be escalated if the alert was not received. An alert may not be received if it could not be delivered (e.g., the mobile phone network was down, the consumer's number has been de-listed), or the consumer does not acknowledge the alert message within a certain time (e.g., respond to the message, listen to the voicemail, open the SMS message or e-mail). A status message regarding whether or not a consumer has received the alert is sent to the notification server **250** via aggregator **280** and gateway **260**, and is stored in the SQL DB Server **230**. The notification server **250** evaluates whether or not the alert should be escalated (e.g., whether the alert was received and whether the consumer has specified that he wants the alert to be escalated). If the alert was not

received, then the notification server **250** can retry the same communication mode or try a different communication mode based on the consumer preference or default settings. For example, a consumer may have an alert set for a purchase made out of the country in which he resides. He may want the alert be sent to his PDA that he generally carries with him. However, if he does not receive the message on his PDA either because the PDA service is down or he does not have it with him, he can specify that the alert then be sent to a different contact or to each of his other contacts until the system knows that he has received the alert.

[0075] The system may also include timers to send status messages so that the consumer **205** knows whether or not the portable consumer device has been used for a transaction. For example, a consumer **205** may want a timer that alerts him daily at 7 a.m. that he used portable consumer device **200** twice the day before or for certain types of purchases made with the portable consumer device **200**.

[0076] Further, the consumer **205** may want to be alerted if the portable consumer device **200** is used to access a certain location. This can be characterized as an access transaction. For example, a portable consumer device **200** can be an access device to gain entrance to a building or other location. An employee may enter a particular business after-hours or enter a secure area of that business. The consumer **205** may want to receive an alert that the employee has used the portable consumer device **200** to enter the secure area. For example, if Joe Employee enters the secure server room after business hours, the consumer **205** may receive an SMS message on his mobile phone that says "Joe Employee has entered secure area A (the server room)."

[0077] Embodiments of this invention have a number of advantages. First, a consumer can completely customize how, when, and if he wants an alert for some or all transactions made with the portable consumer device, and thus has complete control over the notifications for his portable consumer device. This also allows a better chance of detecting a potentially fraudulent act because the consumer will likely receive the alert in a timely manner so that he can respond to the alert if necessary. Also, there is a better chance at stopping back to back fraudulent acts since the consumer can react quickly to the alert. Further, the consumer can track access of secure areas or general employee activity of using the portable consumer

device. The consumer can also track activity of a child or spouse using the portable consumer device. Finally, the consumer is assured of receiving the alert through the escalation process if he does not receive the alert on the first communication mode or contact it is sent to.

[0078] It should be understood that the present invention as described above can be implemented in the form of control logic using computer software in a modular or integrated manner. Based on the disclosure and teachings provided herein, a person of ordinary skill in the art will know and appreciate other ways and/or methods to implement the present invention using hardware and a combination of hardware and software.

[0079] Any of the server computers, client computers, and even some portable consumer devices described above may utilize any suitable number of subsystems. Examples of such subsystems or components are shown in FIG. 5. The subsystems shown in FIG. 5 are interconnected via a system bus **775**. Additional subsystems such as a printer **774**, keyboard **778**, fixed disk **779**, monitor **776**, which is coupled to display adapter **782**, and others are shown. Peripherals and input/output (I/O) devices, which couple to I/O controller **771**, can be connected to the computer system by any number of means known in the art, such as serial port **777**. For example, serial port **777** or external interface **781** can be used to connect the computer apparatus to a wide area network such as the Internet, a mouse input device, or a scanner. The interconnection via system bus allows the central processor **773** to communicate with each subsystem and to control the execution of instructions from system memory **772** or the fixed disk **779**, as well as the exchange of information between subsystems. The system memory **772** and/or the fixed disk **779** may embody a computer readable medium.

[0080] Any of the software components or functions described in this application, may be implemented as software code to be executed by a processor using any suitable computer language such as, for example, Java, C++ or Perl using, for example, conventional or object-oriented techniques. The software code may be stored as a series of instructions, or commands on a computer readable medium, such as a random access memory (RAM), a read only memory (ROM), a magnetic medium such as a hard-drive or a floppy disk, or an optical medium such

as a CD-ROM. Any such computer readable medium may reside on or within a single computational apparatus, and may be present on or within different computational apparatuses within a system or network.

[0081] The above description is illustrative and is not restrictive. Many variations of the invention will become apparent to those skilled in the art upon review of the disclosure. The scope of the invention should, therefore, be determined not with reference to the above description, but instead should be determined with reference to the pending claims along with their full scope or equivalents.

[0082] One or more features from any embodiment may be combined with one or more features of any other embodiment without departing from the scope of the invention.

[0083] A recitation of "a", "an" or "the" is intended to mean "one or more" unless specifically indicated to the contrary.

WHAT IS CLAIMED IS:

1. A method comprising:

receiving information that a transaction associated with a portable consumer device is occurring; and

providing an alert to a consumer associated with the portable consumer device, wherein the alert indicates that the transaction is occurring, wherein the alert is sent to the consumer according to a time or communication mode previously specified by the consumer using an interface that allows the user to specify the time and communication mode for receiving the alert.

2. The method of claim 1 wherein the alert is sent to the consumer if the transaction that is occurring is over a predetermined amount, the transaction is of a predetermined type, the transaction is made outside a geographic location specified by the consumer, the transaction is determined to be a risky transaction, the transaction being conducted without the portable consumer device being physically present at a point of sale, the transaction is a cash transaction, the transaction is a particular type of user-defined transaction, the transaction involves account access, the transaction indicates that a person is entering or exiting a location, the transaction indicates that a payment is due or overdue, or the transaction indicates that a specified person is conducting the transaction.

3. The method of claim 1 wherein the alert is sent to the consumer according to the time and communication mode previously specified by the consumer.

4. The method of claim 1 wherein a portable consumer device is in the form of a card, and wherein the alert is sent to a phone operated by the consumer.

5. The method of claim 1 wherein the alert is a first alert, and wherein a second alert is sent to the consumer through another communication mode.

6. The method of claim 1 further comprising:

receiving, via an interface, a user-specified time and communication mode for receiving the alert.

7. The method of claim 1 wherein the communication mode includes using at least one of a phone call, voicemail, SMS, instant message, and an e-mail.

8. The method of claim 1 wherein the consumer previously provided a trigger specifying a condition under which the alert would be sent.

9. A computer readable medium comprising:

code for receiving information that a transaction associated with a portable consumer device is occurring; and

code for providing an alert to a consumer associated with the portable consumer device, wherein the alert indicates that the transaction is occurring, wherein the alert is sent to the consumer according to a time or communication mode previously specified by the consumer using an interface that allows the user to specify the time and communication mode for receiving the alert.

10. The computer readable medium of claim 9 wherein the alert is a first alert, and wherein the computer readable medium further comprises code for sending the second alert to the consumer through another communication mode.

11. The computer readable medium of claim 9 wherein the information is received via a payment processing network, and wherein the payment processing network is configured to process credit and debit card transactions.

12. The computer readable medium of claim 9 wherein the alert is in the form of a phone call.

13. A server computer comprising the computer readable medium of claim 9.

14. The server computer of claim 13 wherein the server computer is in communication with a payment processing network.

15. The server computer of claim 13 wherein the alert is a first alert, and wherein the computer readable medium further comprises code for sending the second alert to the consumer through another communication mode.

16. A client computer comprising a processor, and a computer readable medium, wherein the computer readable medium comprises instructions for executing a method comprising:

receiving information on how to be notified if a predetermined activity is occurring with respect to a portable consumer device, wherein an alert is provided in manner consistent with the information provided if the predetermined activity is occurring wherein the information provided is a result of a consumer's choice to customize an alert for each predetermined activity by using an interface that allows a user to customize the alert according to at least communication mode and time; and

sending the information to a notification server.

17. The client computer of claim 16 further comprising a display coupled to the processor, wherein the display displays an interface showing the consumer customized times, communication modes, and triggers for alerts.

18. The client computer of claim 16 wherein the interface is a Web interface.

19. The client computer of claim 16 wherein the alert is in the form of a phone call.

20. A method comprising:

providing information on how to be notified if a predetermined activity is occurring with respect to a portable consumer device; and

receiving an alert in manner consistent with the information provided if the predetermined activity is occurring wherein the information provided is a result of

the consumer's choice to customize an alert for each predetermined activity by communication mode and time.

21. The method of claim 20 wherein the information provided includes a time when a consumer wants to be notified.

22. The method of claim 20 wherein the information provided includes a date when a consumer wants to be notified.

23. The method of claim 20 wherein the information provided includes a communication mode by which a consumer wants to be notified.

24. The method of claim 20 wherein the communication mode includes a phone call, voicemail, SMS, instant message, and e-mail.

25. The method of claim 20 wherein the alert is initiated after conditions set by an issuer or payment processing organization are met.

26. A phone comprising a processor, and a computer readable medium coupled to the processor, wherein the computer readable medium comprises code for receiving an alert, wherein the alert indicates that the transaction is occurring, wherein the alert is sent to the consumer according to a time or communication mode previously specified by the consumer using an interface that allows the consumer to specify the time and communication mode for receiving the alert.

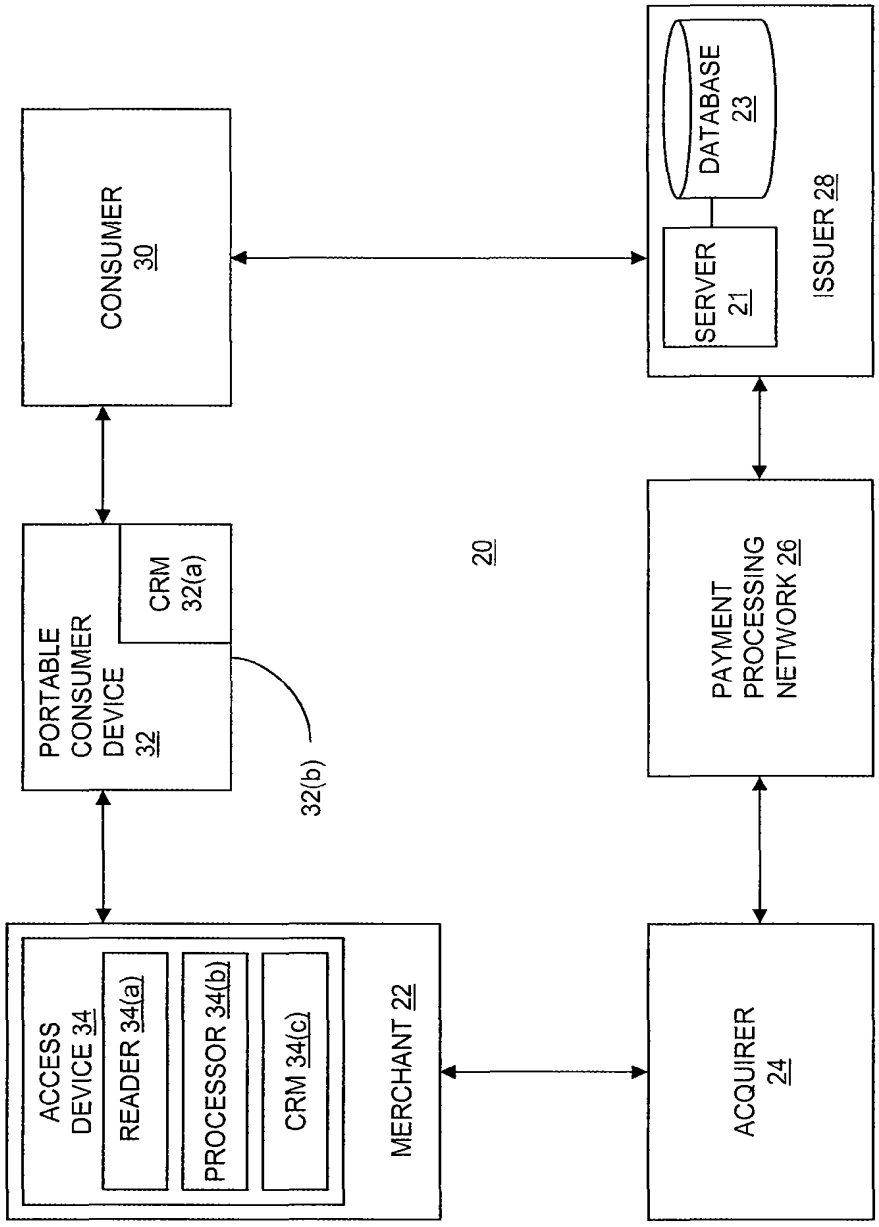

CONSUMER 30
PORTABLE CONSUMER DEVICE 32
CRM 32(a)
32(b)
ACCESS DEVICE 34
READER 34(a)
PROCESSOR 34(b)
CRM 34(c)
MERCHANT 22
ACQUIRER 24
PAYMENT PROCESSING NETWORK 26
SERVER 21
DATABASE 23
ISSUER 28
20

FIG. 1(a)

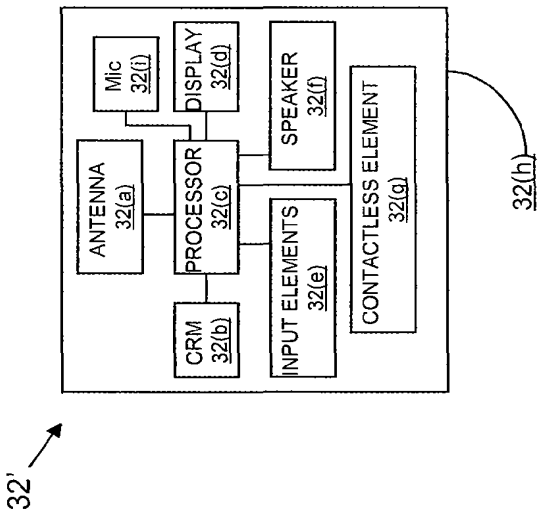

32'
ANTENNA 32(a)
PROCESSOR 32(c)
CRM 32(b)
Mic 32(i)
DISPLAY 32(d)
SPEAKER 32(f)
INPUT ELEMENTS 32(e)
CONTACTLESS ELEMENT 32(g)
32(h)

FIG. 1(b)

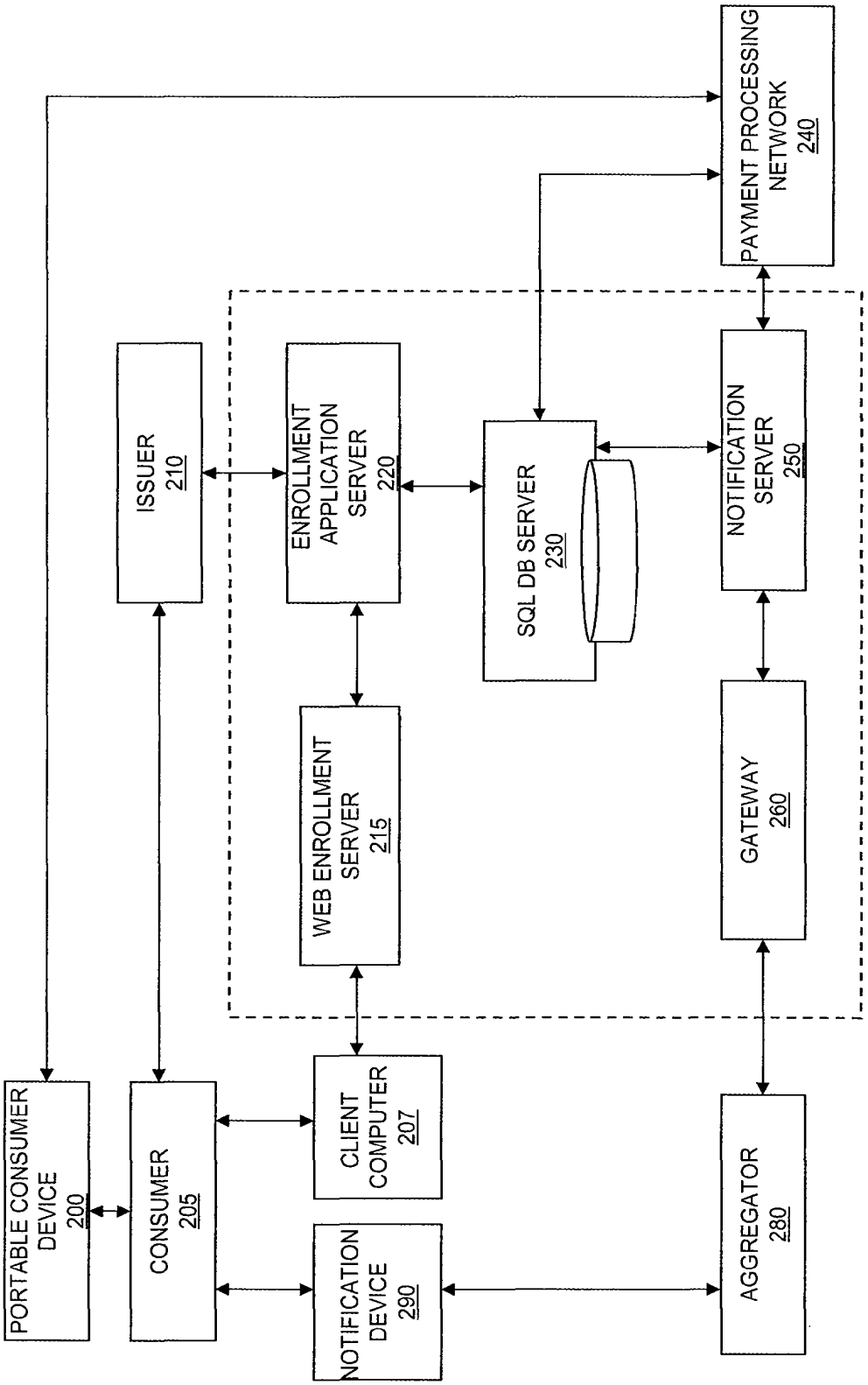

PAYMENT PROCESSING NETWORK 240
ISSUER 210
ENROLLMENT APPLICATION SERVER 220
SQL DB SERVER 230
NOTIFICATION SERVER 250
WEB ENROLLMENT SERVER 215
GATEWAY 260
PORTABLE CONSUMER DEVICE 200
CONSUMER 205
CLIENT COMPUTER 207
NOTIFICATION DEVICE 290
AGGREGATOR 280

FIG. 2

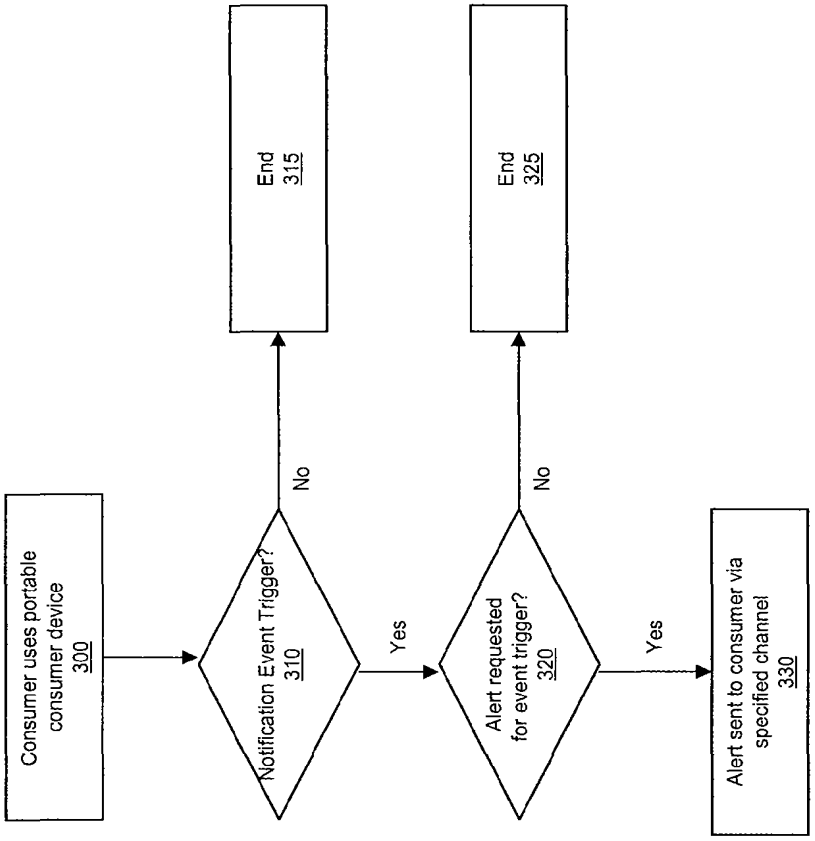

Consumer uses portable consumer device 300
Notification Event Trigger? 310
No
End 315
Yes
Alert requested for event trigger? 320
No
End 325
Yes
Alert sent to consumer via specified channel 330

FIG. 3

Customized Notification Page

Account Number: 12345678

Alert Mode	Alert times	Alert trigger
Cell Phone 415-555-5555	7 am to 10 pm	Over $100
Home Phone 415-555-5555	10:01 pm to 6:59 am	Any amount
Mobile e-mail device	All day	Over $100

FIG. 4

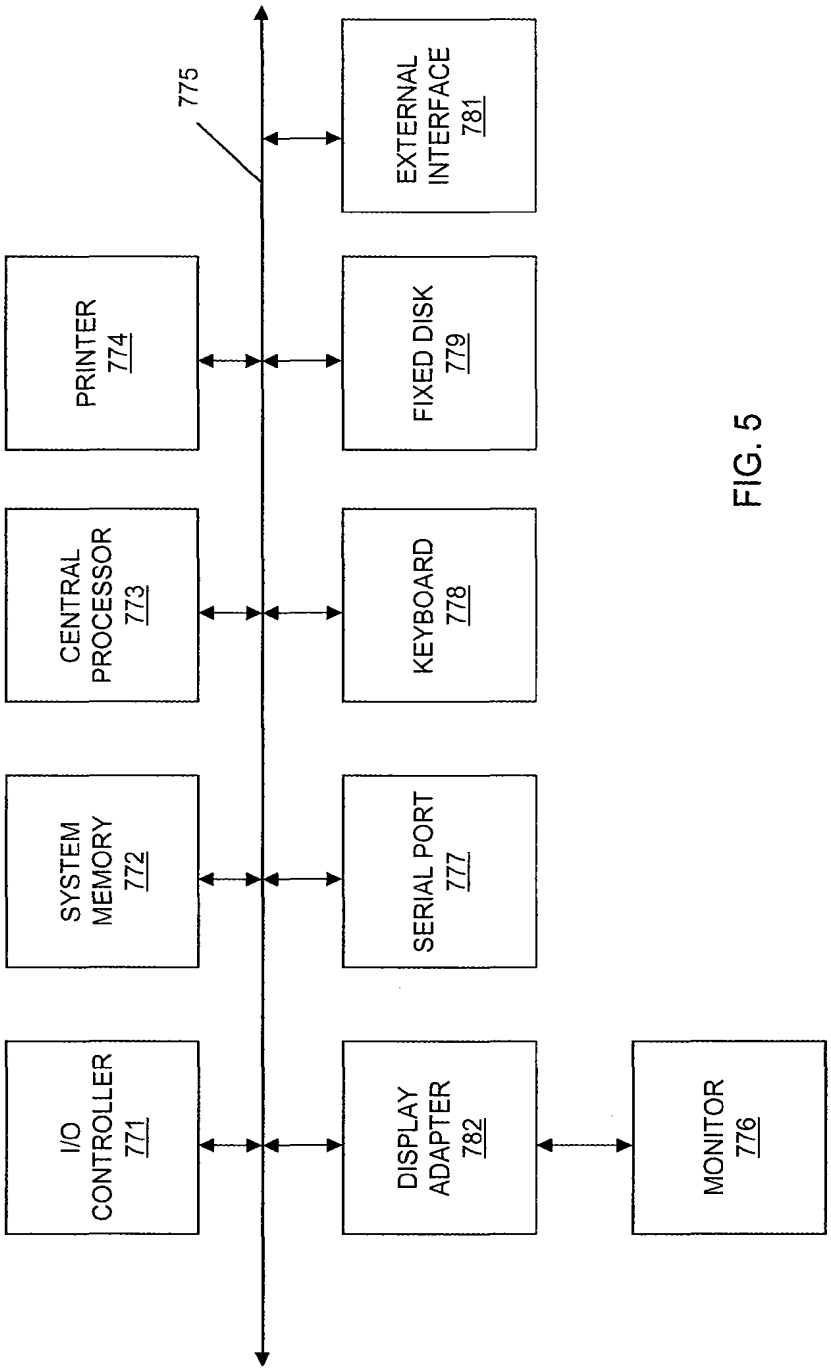

775
EXTERNAL INTERFACE 781
PRINTER 774
FIXED DISK 779
CENTRAL PROCESSOR 773
KEYBOARD 778
SYSTEM MEMORY 772
SERIAL PORT 777
I/O CONTROLLER 771
DISPLAY ADAPTER 782
MONITOR 776

FIG. 5

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 July 2008 (10.07.2008)

PCT

(10) International Publication Number
WO 2008/083089 A1

(51) International Patent Classification:
G06Q 40/00 (2006.01)

(21) International Application Number:
PCT/US2007/088615

(22) International Filing Date:
21 December 2007 (21.12.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/871,898 26 December 2006 (26.12.2006) US

(71) Applicants *(for all designated States except US)*: **VISA U.S.A. INC.** [US/US]; P.O. Box 8999, MS M3-2B, San Francisco, California 94128 (US). **VISA INTERNATIONAL SERVICE CORPORATION** [US/US]; 900 Metro Center Boulevard, Foster City, California 94404 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **CARLSON, Mark** [US/US]; 153 Miramontes Avenue, Half Moon Bay, California 94019 (US).

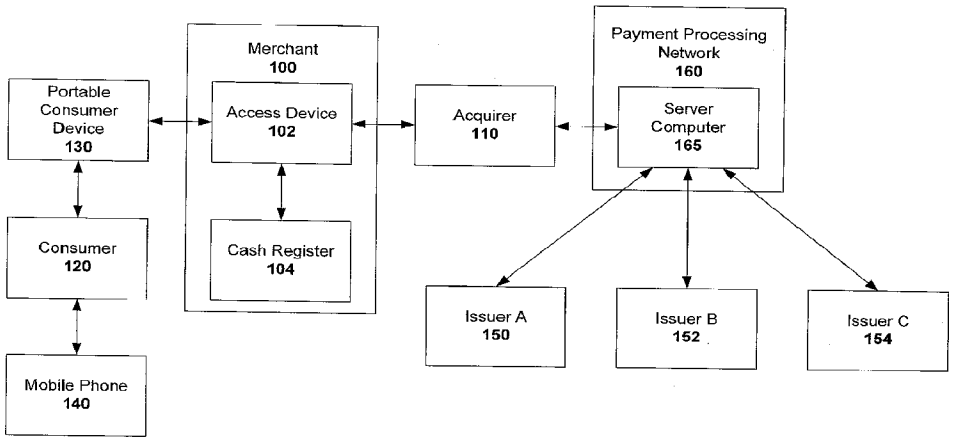
(74) Agents: **FARRELL, John J.** et al.; TOWNSEND AND TOWNSEND AND CREW LLP, Two Embarcadero Center, 8th Floor, San Francisco, California 94111 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, 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, 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, MT, 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*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(54) **Title:** COUPON OFFERS FROM MULTIPLE ENTITIES



(57) **Abstract:** Offers from multiple entities provide an incentive for consumers to behave in a manner that is beneficial to the offer provider. Each offer is associated with rules that establish conditions that must be met for the offer to be valid. For example, a rule may be established to promote the use a specific form of payment, such as a particular credit card. Thus, the offer would only be valid if the consumer paid for the merchandise using the particular credit card. A merchant may generate its own offers or receive offers from a variety of sources (e.g., a payment processing organization, an issuer, or other external sources).

WO 2008/083089 A1

COUPON OFFERS FROM MULTIPLE ENTITIES

CROSS-REFERENCES TO RELATED APPLICATIONS

[0001] The present application claims priority from U.S. Provisional Patent Application No. 60/871,898, filed December 26, 2006, which is incorporated by reference herein in its entirety.

BACKGROUND

[0002] A coupon is a ticket or a document that can be exchanged for a financial discount or rebate when purchasing a product. Coupons provide a popular method to promote the sale of goods and services. Customarily, coupons are issued by manufacturers of consumer packaged goods or by retailers to be used in retail stores as a part of sales promotions. Coupons are often widely distributed through mail, magazines, newspapers, the Internet, and mobile devices such as cell phones.

[0003] To redeem a coupon, a consumer presents merchandise to be purchased to a cashier at a retail outlet. After the merchandise is scanned for purchase, the consumer provides the coupon to the cashier. The cashier then scans or keys in the coupon at a cash register. Conventional coupons only relay a limited amount of information to the cash register. Examples of data relayed to the cash register include a coupon number, an expiration date, a number of redeemed coupons, and the product for which the coupon is applicable. The cash register uses this information to access a local database and accept or reject the offer provided by the coupon. The coupons corresponding to the accepted offers are applied to the corresponding goods.

[0004] Coupons are generally issued by merchants and manufacturers to promote particular goods. However, other entities may also wish to influence consumer behavior. What is needed is a method to provide different entities such as a merchant, a payment processing organization, and an issuer with a means to provide offers to a consumer.

BRIEF SUMMARY

[0005] Embodiments of the invention are directed to providing coupon offers from multiple entities to consumers. The offers provide an incentive for consumers to behave in a manner that is beneficial to the offer provider. Each offer is associated with rules that establish conditions that must be satisfied for the offer to be valid. For example, a rule may be established to promote the use of a specific form of payment, such as a particular credit card. Thus, the offer would only be valid if the consumer paid for the merchandise using the particular credit card. A merchant may generate its own offers or receive offers from a variety of sources (e.g., a payment processing organization, an issuer, or other external sources). Such offers may be generated in real time or during the transaction in embodiments of the invention.

[0006] Illustratively, a consumer shops for goods in a store. A merchant computer (e.g., a cash register) retrieves a SKU or barcode value associated with the goods to be purchased, or data associated with the goods to be purchased is manually entered into the merchant computer. The consumer provides at least one coupon that may be scanned or manually entered into the merchant computer. A server computer communicates with the merchant computer and a computer associated with the entity which provides the coupon to determine if rules associated with the coupon are satisfied. If the rules are satisfied, the savings provided by the coupon is subtracted from a total of the cost of the goods to be purchased. The new total is then presented to the consumer.

[0007] In an illustrative example, the consumer may have a coupon that provides an incentive to purchase the goods using a particular form of payment. For example, the goods to be purchased may be associated with one total that applies to a cash payment, a lower total if payment is made using a payment processing organization-sponsored card (e.g., a Visa card), and another lower total if payment is completed with a particular issuer's credit card. After the goods are scanned at the cash register, the consumer presents the coupon that provides a discount offer if a particular credit card is used. The consumer may then swipe the particular credit card at a point of sale terminal associated with the cash register. The merchant computer accesses a computer associated with the offer provider to determine

whether the rules associated with the offer are satisfied. For example, the merchant computer access a rules engine in a computer associated with the particular credit card issuer to determine that the credit card swiped by the consumer at the point of sale corresponds to the particular credit card. After the rules engine determines that the rules associated with the offer are satisfied, the discounted total is presented to the consumer at the point of sale terminal. The point of sale terminal may also prompt the consumer to submit payment. The consumer then selects to pay for the goods such that the discounted total is charged to the particular credit card.

[0008] One embodiment of the invention is directed to a method including receiving a consumer identifier and an offer during a transaction. A validated offer is received from an entity which provides the offer, such as a payment processing organization or an issuer, when rules associated with the offer are satisfied. The offer is validated based on the consumer identifier. A selection of the valid offer is received to complete the transaction.

[0009] Another embodiment of the invention is directed to a method including receiving an offer and a consumer identifier for a consumer during a transaction and receiving a validated offer. The offer is validated by an entity which provides the offer when rules associated with the offer are satisfied. The offer is validated based on the consumer identifier. A selection of the validated offer is received to complete the transaction.

[0010] Another embodiment of the invention is directed to a system including an access device and a server computer in communication with the access device. The access device or the server computer is configured to: receive a consumer identifier and an offer during a transaction conducted with the access device and the server computer; receive a validated offer from an entity which provides the offer, wherein the offer is validated when rules associated with the offer are satisfied, the offer being validated based on the consumer identifier, wherein the entity is a payment processing organization or an issuer; and receive a selection of the valid offer to complete the transaction..

[0011] These and other embodiments of the invention are described in further detail below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] FIG. 1 shows an exemplary block diagram of a system for providing offers from multiple entities to a consumer according to embodiments of the invention.

[0013] FIG. 2 shows an exemplary block diagram of some elements that may be present in a mobile phone according to an embodiment of the invention.

[0014] FIG. 3 shows an exemplary block diagram of some elements that may be present in a server computer according to an embodiment of the invention.

[0015] FIG. 4 shows an exemplary block diagram of some elements that may be present in an access device according to an embodiment of the invention.

[0016] FIG. 5 shows a flow diagram of a method for providing offers to a consumer according to embodiments of the invention.

[0017] FIG. 6 shows a screen shot of an access device displaying different totals based on a particular payment method according to an embodiment of the invention.

DETAILED DESCRIPTION

[0018] Different entities may attempt to influence consumer behavior for different reasons. For example, a first party may include an issuing bank who may only care if a credit card being used is issued from the issuing bank. A second party may include a payment processing organization (e.g., Visa, a third party processor, etc.) who may only care if the payment processing organization's card is used. A third party may be a merchant who may only care if purchases are made at that merchant.

[0019] Embodiments of the invention can be used to introduce different types of coupon offers or other types of offers during a transaction. Such offers may include issuer coupons, payment processing organization coupons (e.g., acquirer coupons), merchant coupons, manufacturer coupons, etc.

[0020] In accordance with embodiments of the present invention, a point of sale terminal is configured to provide and/or redeem coupons only if appropriate rules are satisfied. For example, a payment processing organization offer may be redeemable by a consumer or provided to a consumer only if a payment processing organization branded credit card is used. In another example, an issuer (e.g., Citibank) may provide or redeem an offer if the consumer uses an issuer-specific credit card. In response to receiving various offers from the merchant, payment processing organization, or issuer, the consumer could then select a particular form a payment based upon the best offer that is provided to the consumer, and/or provide offers to encourage the consumer to buy specific products.

[0021] Some specific examples of coupon offers from different entities are provided below. In some embodiments of the invention, these different types of offers can be processed by a single access device (e.g., point of sale terminal), or could be processed by a server computer (e.g., residing at a payment processing organization or another location). The access device or the server computer could communicate with each of these entities during a payment transaction to determine which offers are valid.

- Partner merchant issued offers: Here, a merchant sets the goals of an offer. Although the merchant may care about the type of payment form that is used (e.g., cash vs. credit card), the merchant is generally not concerned with the brand of payment that is being used by a consumer as long as the consumer accepts that brand of payment. The merchant's goal is to persuade consumers to buy the merchant's products or services, and to potentially purchase specific products or services (e.g., items that are overstocked).
- Payment processing organization (e.g., acquirer) issued offers: The payment processing organization's goal may be to increase brand usage. The payment processing organization may only provide and redeem an offer if the consumer pays with a portable consumer device branded with the payment processing organization's service mark.
- Offers issued by an issuer: The issuer is generally not concerned with the particular payment processing organization that a portable consumer device is affiliated with. For example, an issuer such as Bank of America may issue credit cards using the Visa and Mastercard brands. Typically, the issuer may

be less concerned with whether the consumer uses a Visa or Mastercard branded credit card, as long as the consumer uses a card that is issued by Bank of America.

[0022] As used herein, a "transaction" may include, but is not limited to, the time when the consumer has selected goods or services to purchase and is ready to pay for them. For example, an exemplary transaction may include a time when a consumer selects products to purchase in a grocery store, and the selected products are scanned at a point of sale terminal such as a cash register. The consumer also provides at least one coupon at the point of sale terminal. The consumer is identified at the point of sale terminal by, for example, scanning a portable consumer device such as a credit or debit card. This scanned information (e.g., a SKU or stock keeping unit, an NLU or coupon identification number, an account number that identifies the consumer, etc.) may then be transmitted to a server computer. The server computer may then communicate with the entity associated with the offer (e.g., the merchant, payment processing organizations, and various issuers) to determine if rules associated with the offer are satisfied. If the rules are satisfied, the offer is applied to the goods to be purchased (e.g., the consumer is presented with a reduced total).

[0023] Illustratively, embodiments of the present invention are directed to offers from a variety of different entities that provide incentives to influence consumer behavior. Each offer is associated with certain rules that establish conditions to be satisfied in order for the offer to be valid. The merchant receives offers from a variety of sources (e.g., an acquirer, an issuer, or other external sources). The merchant may also generate its own offers to provide to consumers.

[0024] After a consumer selects goods in a store, the consumer approaches a point of sale terminal (e.g., a cash register or self-service check out terminal) to scan or otherwise enter the goods into a merchant computer. The consumer also provides a consumer identifier (e.g., a credit card number, alias, e-mail address, etc.) so that the identity of the consumer may be determined. The merchant computer retrieves a SKU or barcode value associated with the scanned goods, and any information associated with the consumer identifier. The consumer also provides at least one offer that may apply to the transaction. A server computer communicates

with an entity associated with the offer (e.g. the merchant computer, an acquirer computer, and/or various issuer computers) to determine if the rules associated with the offer are satisfied. If the rules associated with the offer are satisfied, the offer is validated and a discounted total is presented to the consumer at the point of sale terminal. The point of sale terminal may also prompt the consumer to submit payment. The consumer then selects to pay for the goods.

[0025] FIG. 1 shows an exemplary block diagram of a system for providing offers from multiple entities to a consumer in accordance with embodiments of the invention. The system includes a merchant **100** and an acquirer **110** associated with the merchant **100**. In a typical payment transaction, a consumer **120** may purchase goods or services at the merchant **100** using a portable consumer device **130** or a mobile phone **140**. FIG. 2 shows an exemplary block diagram of some elements that may be present in the mobile phone **140** according to an embodiment of the invention. The acquirer **130** can communicate with issuers (A, B, and C) **150**, **152**, **154** via a payment processing network **160** having a server computer **165**.

[0026] The acquirer **130** is typically a bank that has a merchant account. The issuers **150**, **152**, **154** may each also be a bank, but could be any business entity such as a retail store. Some entities are both acquirers and issuers, and embodiments of the invention include such entities. Each issuer **150**, **152**, **154** may operate its own server computer (not shown), which may have a computer readable medium comprising code for performing the functions that the issuer **150**, **152**, **154** performs. An issuer database (not shown) comprising account number information and other information may be operatively coupled to the server computer **165**.

[0027] The consumer **120** may be an individual or an organization such as a business that is capable of purchasing goods or services.

[0028] The portable consumer device **130** may be in any suitable form. For example, suitable portable consumer devices can be hand-held and compact so that they can fit into a consumer's wallet and/or pocket. Example portable consumer devices may include smart cards, ordinary credit or debit cards (with a magnetic strip and without a microprocessor), keychain devices (such as the Speedpass™ commercially available from Exxon-Mobil Corp.), etc. Other examples of portable consumer devices include cellular phones, personal digital assistants (PDAs),

pagers, contactless cards (e.g., an RFID card), payment cards, security cards, access cards, smart media, transponders, and the like. The portable consumer devices can also be debit devices (e.g., a debit card), credit devices (e.g., a credit card), or stored value devices (e.g., a stored value card).

[0029] The payment processing network **160** may include data processing subsystems, networks, and operations used to support and deliver authorization services, exception file services, and clearing and settlement services. An exemplary payment processing network may include VisaNet™. Payment processing networks such as VisaNet™ are able to process credit card transactions, debit card transactions, and other types of commercial transactions. VisaNet™, in particular, includes a VIP system (Visa Integrated Payments system) which processes authorization requests and a Base II system which performs clearing and settlement services.

[0030] The server computer **165** of the payment processing network **160** is typically a powerful computer or cluster of computers. For example, the server computer **165** can be a large mainframe, a minicomputer cluster, or a group of servers functioning as a unit. In one example, the server computer **165** may be a database server coupled to a Web server. FIG. 3 shows an exemplary block diagram of some elements that may be present in the server computer **165** according to an embodiment of the invention. The payment processing network **160** may use any suitable wired or wireless network, including the Internet.

[0031] The merchant **100** includes an access device **102** that can interact with the portable consumer device **130** and the mobile phone **140**. FIG. 4 shows an exemplary block diagram of some elements that may be present in the access device **102** according to an embodiment of the invention. The merchant also includes a cash register **104** coupled to the access device **102**.

[0032] In a typical purchase transaction, the consumer **120** purchases goods or services at the merchant **100** using the portable consumer device **130**. The consumer's portable consumer device **130** interacts with the access device **102**. For example, the consumer **120** may swipe a credit card through a reader of the access device **102**. Alternatively, the reader may include a contactless reader, and the

portable consumer device **130** may be a contactless device such as the mobile phone **140**.

[0033] An authorization request message is then forwarded to the acquirer **110**. After receiving the authorization request message, the acquirer **110** sends the authorization request message to the payment processing network **160**. The server computer **165** forwards the authorization request message to the issuer **150**, **152** or **154** of the portable consumer device **130**.

[0034] After the issuer **150**, **152** or **154** receives the authorization request message, the issuer **150**, **152** or **154** sends an authorization response message back to the payment processing network **160** to indicate whether or not the current transaction is authorized. The server computer **165** forwards the authorization response message back to the acquirer **110**. The acquirer **110** sends the response message back to the merchant **100**.

[0035] After the merchant **100** receives the authorization response message, the access device **102** may provide the authorization response message to the consumer **120**. The authorization response message may be displayed on a touch screen, or may be printed out on a receipt.

[0036] At the end of the business day, a clearing and settlement process may be conducted by the payment processing network **160**. The clearing process exchanges financial details between the acquirer **110** and the issuer **150**, **152**, **154** to facilitate posting to a consumer's account and reconciliation of the consumer's settlement position.

[0037] Some of the embodiments described below may use a payment processing system like the one described above, or any suitable combination of components in the payment processing system.

[0038] In accordance with embodiments of the present invention, the system for providing coupon offers from multiple entities to a consumer is described below with reference to FIG. 1. The offers may be provided by the merchant **100**, the acquirer **110**, the issuer **150**, **152**, **154**, or any other entity seeking to influence consumer behavior such as the manufacturer of goods offered for sale by the merchant **100**.

[0039] Each issuer **150**, **152**, **154** may provide offers. The acquirer **110** may also generate offers. The merchant **100** may receive offers from other external sources such as from a manufacturer of goods offered for sale at the merchant **100**. The merchant **100** may also generate its own offers to provide to the consumer **120**. In one embodiment, the merchant **100** decides which offers to accept and which offers to decline. For example, an acquirer offer may conflict with an issuer offer. Thus, the merchant **100** may decide to provide only the acquirer offer to consumers.

[0040] Each offer is associated with one or more rules. The rules establish conditions to be satisfied for the offer to be valid. For example, an offer may be provided to a consumer that is valid only when the consumer uses a particular credit card. By using the credit card that corresponds to the offer, the consumer may receive a reduced price for the purchased goods or other incentives such as frequent flyer points. In another example, the rules may establish that an offer is only valid for a particular time period. Specifically, to provide an incentive for consumers to shop during off-peak hours, an offer may correspond to a particular time of day (e.g., the first two hours of retail operation). In another embodiment, the offer may correspond to the identity of the consumer combined with a particular day of the week or month (e.g., senior citizen discount on the third Tuesday of the month). Similarly, an offer may be provided for seasonal items after the season has ended. For example, summer merchandise discount offers may be valid during the months of September and October in an attempt to unload overstocked items.

[0041] The consumer **120** initiates a transaction by scanning merchandise that may be purchased at the merchant **100**. For example, after selecting goods to purchase at a retail outlet, the consumer **120** may approach a cashier or self-service check-out terminal to pay for the items. The transaction may be initiated when the consumer **120** or a cashier scans or keys in the items to be purchased using the cash register **104**. Any coupons or other offers may also be submitted using the cash register **104** or the access device **102**. For example, paper coupons may be scanned at the cash register **104** and electronic offers stored on the mobile phone **140** may be provided to the access device **102**.

[0042] A consumer identifier is provided during the transaction to identify the consumer. In one embodiment, the consumer **120** is identified at the access device

102 by the mobile phone **140**. In another embodiment, the consumer **120** is identified by scanning the portable consumer device **130** (e.g., a credit card, a savings card associated with the merchant, a contactless card, etc.) at the access device **102**. The consumer identifier may correspond to the account number associated with the scanned payment card. In another embodiment, the consumer **120** identifies himself by entering a personal identification code at the access device **102** using a touch screen or some other input/output device.

[0043] After the consumer identifier and the item information are entered into the access device **102**, the offers are validated. The access device **102** identifies the entity associated with an applicable offer, and may then route the appropriate message to the entity associated with the applicable offer. The logic to do this may reside in hardware and/or software in the access device **102** or at a computer (e.g., a backend merchant computer) accessible to the access device **102**. In one embodiment, more than one offer may apply to the same item. If the offer is associated with the merchant **100**, the offer is validated at the merchant **100** to determine whether the rules that apply to the offer are satisfied. If the offer is associated with the acquirer **110**, the offer and the consumer identifier are forwarded to the acquirer **110** and a determination is made whether the offer is valid. Similarly, if the offer is provided by an issuer **150**, **152**, **154**, the offer and the consumer identifier are forwarded to the corresponding issuer **150**, **152**, **154** via the server computer **165** to determine the validity of the offer. In one embodiment, an offer is validated when the terms of the offer are satisfied. This may be done by matching conditions associated with the offer to a rules engine (not shown). The rules engine may be located at the merchant **100**, the acquirer **110**, the server computer **165**, and/or the issuers **150**, **152**, **154**.

[0044] For example, an offer provided by an issuer may only be valid if the consumer **120** purchases a quantity of three or more of a particular item. After the consumer **120** provides an offer indicator (e.g., an electronic coupon code) to the access device **102**, it retrieves the three or more item rule from the rules engine from the issuer which provides the offer via the server computer **165**, and then accesses the cash register **104** to identify whether three or more items have been purchased. The offer will not be validated if less than three of that item have been purchased.

[0045] In one embodiment, more than one rule may apply to an offer. For example, an offer may only be valid for a specific form of payment when an account balance associated with the specific form of payment is more than a predetermined amount. Thus, if the consumer **120** uses a different form of payment or if an account balance associated with the valid form of payment is less than the predetermined amount, the offer will not be validated.

[0046] Any number of rules may be associated with any offer. Example rules include: the type of payment, the time of day, the day of the week, the day of the month, the month of the year, the total quantity of items to be purchased, the quantity of a particular item to be purchased, consumer characteristics (e.g., age, gender, resident address, income level), etc. As one having ordinary skill in the art would appreciate, the list of example rules is not exhaustive and additional rules could be associated with an offer without departing from the spirit and scope of embodiments of the invention.

[0047] In accordance with one type of offer, the offer may be associated with the type of portable consumer device **130** that the consumer **120** used to identify himself (e.g., a credit card). The offer is validated by determining that the credit card that the consumer swiped at the access device **102** corresponds to the credit card that is associated with the offer. In one embodiment, the access device **102** may display a discounted amount to provide an incentive to pay using the credit card associated with the offer. Thus, the user is prompted to submit payment using the previously swiped credit card. Alternatively, the consumer **120** may be informed that the discount will be applied to the consumer's monthly credit card statement.

[0048] In one embodiment, the access device **102** may display different amounts based on the form of payment used by the consumer 120. Specifically, the access device **102** may display one amount if a particular credit card is used, another amount if a different credit card is used, and still another amount if payment is made by cash, check or a debit card. The consumer **120** then selects a payment method at the access device **102**. If the consumer **120** presents a new form of payment at the access device **102** (e.g., a credit card that had not been previously used at the merchant **100**), information associated with the new form of payment is stored at the merchant **100**. Thus, if the same form of payment is used at a later

date, the access device **102** will recognize the consumer **120** and may provide offers associated with that form of payment.

[0049] In another example, the offer may provide incentives such as free or discounted items, or reward points based on a particular item that the consumer **120** has selected for purchase. Specifically, the consumer **120** may purchase ground coffee and the access device **102** provides this product information to an issuer that seeks to provide offers to consumers who purchase coffee. The issuer may then provide an offer to the consumer **120** at the access device **102** to receive a free cup of coffee at a nearby coffee retailer. The consumer **120** may accept the offer at the access device **102**. In one embodiment, the number of accepted offers is limited. For example, an offer for a free cup of coffee may be limited to thirty accepted offers on any given day.

[0050] The access device **102** sends the payment information provided by the consumer **120** to the cash register **104** to complete the purchase transaction. The access device **102** may begin reconciling the remittance for the offer. For example, if the offer was provided by an issuer **150**, **152** or **154**, the merchant **100** may request and retrieve the amount corresponding to the offer (e.g., the discounted amount) from that issuer. In one embodiment, offer remittance occurs at the end of the day during the clearing and settlement process.

[0051] FIG. 2 shows a block diagram of some components of the mobile phone **140**. The phone **140** may comprise a computer readable medium **200** and a body **210**. The computer readable medium **200** may be present within the body **210**, or may be detachable from it. The body **210** may be in the form of a plastic substrate, housing, or other structure. The computer readable medium **200** may be a memory that stores data and may be in any suitable form including a magnetic stripe, a memory chip, etc.

[0052] The computer readable medium **200** may comprise code for performing any of the functions described herein. For example, the computer readable medium **200** may comprise code for identifying a consumer at an access device. The computer readable medium **200** may also comprise code for communicating with an access device to identify offers corresponding to items scanned by the phone **140**.

[0053] The phone **140** may further include a contactless element **220**, which is typically implemented in the form of a semiconductor chip (or other data storage element) with an associated wireless transfer (e.g., data transmission) element, such as an antenna. Data or control instructions transmitted via a cellular network may be applied to the contactless element **220** by a contactless element interface (not shown). The contactless element interface functions to permit the exchange of data and/or control instructions between the mobile device circuitry (and hence the cellular network) and the contactless element **220**.

[0054] The contactless element **220** is capable of transferring and receiving data using a near field communications ("NFC") capability (or near field communications medium) typically in accordance with a standardized protocol or data transfer mechanism (e.g., ISO 14443/NFC). Near field communications capability is a short-range communications capability, such as RFID, Bluetooth™, infra-red, or other data transfer capability that can be used to exchange data between the phone **140** and the payment processing network **160** or it can be used to exchange data between the phone **140** and the access device **102**. Thus, the phone **140** is capable of communicating and transferring data and/or control instructions via both cellular network and near field communications capability.

[0055] The phone **140** may also include a processor **230** (e.g., a microprocessor) for processing the functions of the phone **140** and a display **240** to allow the consumer to view offers associated with items that may be purchased and other information and messages. The phone **140** may further include input elements **250** to allow a user to input information into the phone **140**, a speaker **260** to allow the user to hear voice communication, music, etc., and a microphone **270** to allow the user to transmit her voice through the phone **140**. The phone **140** may also include an antenna **280** for wireless data transfer (e.g., data transmission).

[0056] FIG. 3 shows an exemplary block diagram of some elements that may be present in the computer server **165** according to an embodiment of the invention. The subsystems shown in FIG. 3 are interconnected via a system bus **300**. Additional subsystems such as a printer **310**, a keyboard **320**, a fixed disk **330**, a monitor **340**, which is coupled to a display adapter **350**, and others are shown. Peripherals and input/output (I/O) devices, which couple to an I/O controller **360**, can

be connected to the computer system by any number of means known in the art, such as a serial port **370**. For example, the serial port **370** or an external interface **380** can be used to connect the computer apparatus to a wide area network such as the Internet, a mouse input device, or a scanner. The interconnection via the system bus **300** allows a central processor **390** to communicate with each subsystem and to control the execution of instructions from a system memory **395** or the fixed disk **330**, as well as the exchange of information between subsystems. The system memory **395** and/or the fixed disk **330** may embody a computer readable medium.

[0057] FIG. 4 shows an exemplary block diagram of some elements that may be present in the access device **102** according to an embodiment of the invention. The access device **102** may comprise a processor **400**, a computer readable medium **410**, a network interface **420**, an output device **430**, a reader **440**, and a keypad **450** operatively coupled to the processor **400**.

[0058] The processor **400** may be embodied by one or more microprocessors, and the computer readable medium **410** may use any suitable electrical, magnetic or optical means of data storage. The computer readable medium **410** may store computer code for performing the functions of the access device **102**. For example, the computer readable medium **410** may store instructions or code for communicating with the issuer of the consumer's portable consumer device, the payment processing organization associated with the consumer's portable consumer device, the merchant selling the item to be purchased, and the manufacturer of the item, during the transaction, or even before the transaction, after it receives a consumer identifier such as a payment card account number.

[0059] The network interface **420** may be any suitable interface that will allow the access device **102** to communicate with external apparatuses. The network interface **420** allows the access device **102** to communicate with the acquirer **110** and the payment processing network **160**.

[0060] The reader **440** may include any suitable contact or contactless mode of operation. For example, exemplary card readers can include RF (radio frequency) antennas, magnetic stripe readers, etc. to interact with the portable consumer device **130** such as a credit card or a debit card. The reader **440** may be used to enter bill information into the access device **102**.

[0061] The keypad **450** may be an ordinary keypad that is associated with a point of sale terminal. The keypad **450** may be embodied by a number of depressible buttons, or could be embodied on a touch screen on a display. The keypad **450** may be used to enter bill information into the access device **102**.

[0062] FIG. 5 shows a flow diagram of a method for providing offers to a consumer in accordance with embodiments of the invention. The offers may be provided by any entity that seeks to provide an incentive to consumers to purchase a product or service, to shop at a particular time, to use a particular form of payment, or to otherwise influence consumer behavior. Each offer is associated with one or more different rules that establish conditions to be satisfied for the offer to be valid.

[0063] Offers may be associated with an issuer. The acquirer may also generate offers. The merchant may generate offers to provide to the consumer. Offers may also be provided to the merchant from other external sources such as a product manufacturer or a service provider such as a payment processing organization. The provider of the offer determines which rules apply to the offer. In one embodiment, the merchant determines which offers to provide to consumers and which offers to decline. For example, if an external source and the merchant provide an offer for the same item, the merchant may decline to validate the external source offer in order to promote its own offer for that item.

[0064] The consumer shops for goods at a retail outlet. The goods are scanned by the consumer or a cashier at a point of sale terminal (e.g., cash register or self-service checkout terminal) (step **500**). Information corresponding to items to be purchased are entered via a bar code reader or by keying in the item information directly into a cash register.

[0065] The consumer is identified at the point of sale terminal using an access device or a mobile phone (step **510**). For example, the consumer may identify himself using a consumer identifier (e.g., a mobile phone unique identifier or an account number associated with a payment card). The consumer identifier may also be directly entered at the point of sale terminal as, for example, a personal identification number.

[0066] The consumer may provide offers to the access device (step **520**). The offers may be paper coupons, electronic coupons stored on the mobile device, or any other type of offer that may be provided at the merchant.

[0067] The offers are then validated based on rules associated with the offers (step **530**). The offers are validated by accessing a rules engine associated with the entity which provides the offer to ensure that the conditions established by the rules are satisfied. In accordance with one type of offer, a determination may be made whether the credit card provided to identify the consumer corresponds to the credit card applicable to the offer. If the credit cards do not correspond, the offer is not validated. Thus, the consumer cannot take advantage of the incentive associated with the offer. In another example, a rule may be established to provide an offer for a particular consumer. After the rule is retrieved from the rules engine of the entity which provides the offer, a determination is made whether the consumer corresponds to the target consumer of the offer. Illustratively, an offer may only be valid for a consumer living within a particular geographic location. Thus, the offer cannot be validated until the consumer's current resident address is verified.

[0068] In one embodiment, the consumer identifier such as a payment card account number is used to validate offers associated with the consumer. For example, the access device may receive a consumer identifier such as a payment card account number, and may communicate with the issuer associated with the payment card account number. Information regarding the consumer's identity may then be sent from the issuer to the access device. The access device may identify the consumer as being over the age of sixty-five. Thus, any offers associated with senior citizens would be validated.

[0069] After the offers are validated (or invalidated), the valid offers are presented to the consumer (step **540**). The applicable offers may be provided to the consumer by, for example, the access device or the mobile phone. In accordance with one type of offer, the access device or the mobile phone may display the offers that are applicable to the consumer and the goods selected for purchase. In accordance with another type of offer, as shown in FIG. 6, the output device **430** of the access device **102** displays one amount if a payment card associated with a particular payment processing organization (e.g., Payment Processing Organization

Z) is used, another amount if a payment card by a particular issuer is used (e.g., Issuer A), another amount if a particular payment card by a particular issuer and by a particular payment processing organization is used, and still another amount if payment is made by cash or check. The consumer may then select a particular form of payment to accept the offer (e.g., pay using a card that is branded with Issuer A and Payment Processing Organization Z) or may select to decline the offer (e.g., pay by cash).

[0070] The consumer selects the valid offers to accept and pays for the goods (step **550**). For example, using a touch screen on the access device, the consumer may select an offer corresponding to the payment card used to identify the consumer to accept the discounted amount that would apply when payment is made using that payment card. In another example, the consumer may select a coupon for a discount on goods or services associated with a purchased item.

[0071] The valid offers are remitted by requesting payment associated with the incentive from the entity which provided the offer (step **560**). For example, if the offer was provided by an issuer, the merchant may request and retrieve the amount corresponding to the offer (e.g., the discounted amount) from that issuer. In one embodiment, offer remittance occurs at the end of the day during the clearing and settlement process.

[0072] As can be seen from the above description, embodiments of the invention have a number of advantages. For example, multiple entities may provide coupon offers to a consumer. The coupon offers provide incentives to influence consumer behavior in such a way that benefits the offer provider. The offers may be established to provide non-traditional incentives. Such offers may be issuer coupons, acquirer coupons, merchant coupons, or coupons from other external sources (e.g., a manufacturer of goods that the merchant offers for sale, other retailers located in the vicinity of the merchant). The provider of the offer associates the offer with certain rules that establish conditions to be fulfilled for the offer to be valid. An access device is configured to provide or redeem the offer coupons only if the rules are satisfied.

[0073] It should be understood that the present invention as described above can be implemented in the form of control logic using computer software in a

modular or integrated manner. Based on the disclosure and teachings provided herein, a person of ordinary skill in the art will know and appreciate other ways and/or methods to implement the present invention using hardware and a combination of hardware and software.

[0074] Any of the software components or functions described in this application, may be implemented as software code to be executed by a processor using any suitable computer language such as, for example, Java, C++ or Perl using, for example, conventional or object-oriented techniques. The software code may be stored as a series of instructions, or commands on a computer readable medium, such as a random access memory (RAM), a read only memory (ROM), a magnetic medium such as a hard-drive or a floppy disk, or an optical medium such as a CD-ROM. Any such computer readable medium may reside on or within a single computational apparatus, and may be present on or within different computational apparatuses within a system or network.

[0075] The above description is illustrative and is not restrictive. Many variations of the invention will become apparent to those skilled in the art upon review of the disclosure. The scope of the invention should, therefore, be determined not with reference to the above description, but instead should be determined with reference to the pending claims along with their full scope or equivalents.

[0076] One or more features from any embodiment may be combined with one or more features of any other embodiment without departing from the scope of the invention.

[0077] A recitation of "a", "an" or "the" is intended to mean "one or more" unless specifically indicated to the contrary.

WHAT IS CLAIMED IS:

1. A method comprising:

receiving a consumer identifier and an offer during a transaction

receiving a validated offer from an entity which provides the offer, wherein the offer is validated when rules associated with the offer are satisfied, the offer being validated based on the consumer identifier, wherein the entity is a payment processing organization or an issuer; and

receiving a selection of the valid offer to complete the transaction.

2. The method of claim 1, wherein receiving the consumer identifier and receiving the selection of the valid offer are performed by a point of sale terminal, and wherein the transaction is a payment transaction.

3. The method of claim 1, wherein receiving the validated offer is performed by a point of sale terminal or a computer in communication with the point of sale terminal, and wherein the point of sale terminal or computer is configured to communicate with at least two of a merchant, the issuer, and the payment processing organization to determine if offers provided by the merchant, the issuer, and the payment processing organization are valid.

4. The method of claim 1, further comprising receiving a product identifier, wherein the product identifier is associated with a product that a consumer has purchased using a portable consumer device, and wherein the offer relates to the product.

5. The method of claim 1, wherein the offer is associated with a consumer.

6. The method of claim 1, wherein the consumer identifier is an identifier associated with a portable consumer device.

7. The method of claim 6, wherein the portable consumer device is a payment card.

8. The method of claim 1, wherein the consumer identifier is an account number associated with a portable consumer device associated with a consumer.

9. The method of claim 1, wherein the portable consumer device is a wireless phone.

10. A computer readable medium comprising:

code for receiving a consumer identifier and an offer during a transaction;

code for receiving a validated offer from an entity which provides the offer, wherein the offer is validated when rules associated with the offer are satisfied, the offer being validated based on the consumer identifier, wherein the entiry is a payment processing organization or an issuer; and

code for receiving a selection of the valid offer to complete the transaction.

11. The computer readable medium of claim 10, further comprising code for receiving a product identifier, wherein the product identifier is associated with a product that a consumer has purchased using the portable consumer device, wherein the offer relates to the product.

12. An access device comprising the computer readable medium of claim 10.

13. A server computer comprising the computer readable medium of claim 10.

14. A method comprising:

receiving an offer and a consumer identifier for a consumer during a transaction;

receiving a validated offer, wherein the offer is validated by an entity which provides the offer when rules associated with the offer are satisfied, the offer being validated based on the consumer identifier; and

receiving a selection of the validated offer to complete the transaction.

15. The method of claim 14, wherein receiving the offer, receiving the validated offer, and receiving the selection are performed by a point of sale terminal, wherein the point of sale terminal or a computer in communication with the point of sale terminal is configured to communicate with at least two of a merchant, an issuer, and a payment processing organization to determine if offers provided by the merchant, the issuer, and the payment processing organization are valid.

16. The method of claim 15 wherein the offer relates to a product identifier of a product to be purchased by the consumer.

17. A computer readable medium comprising:

code for receiving an offer and a consumer identifier for a consumer during a transaction;

code for receiving a validated offer, wherein the offer is validated by an entity which provides the offer when rules associated with the offer are satisfied, the offer being validated based on the consumer identifier; and

code for receiving a selection of the validated offer to complete the transaction.

18. An access device comprising the computer readable medium of claim 17.

19. A system comprising:

an access device;

a server computer in communication with the access device,

wherein the access device or the server computer is configured to:

receive a consumer identifier and an offer during a transaction conducted with the access device and the server computer;

receive a validated offer from an entity which provides the offer, wherein the offer is validated when rules associated with the offer are satisfied, the offer being validated based on the consumer identifier, wherein the entity is a payment processing organization or an issuer; and

receive a selection of the valid offer to complete the transaction.

20. The system of claim 19 wherein the transaction is a payment transaction.

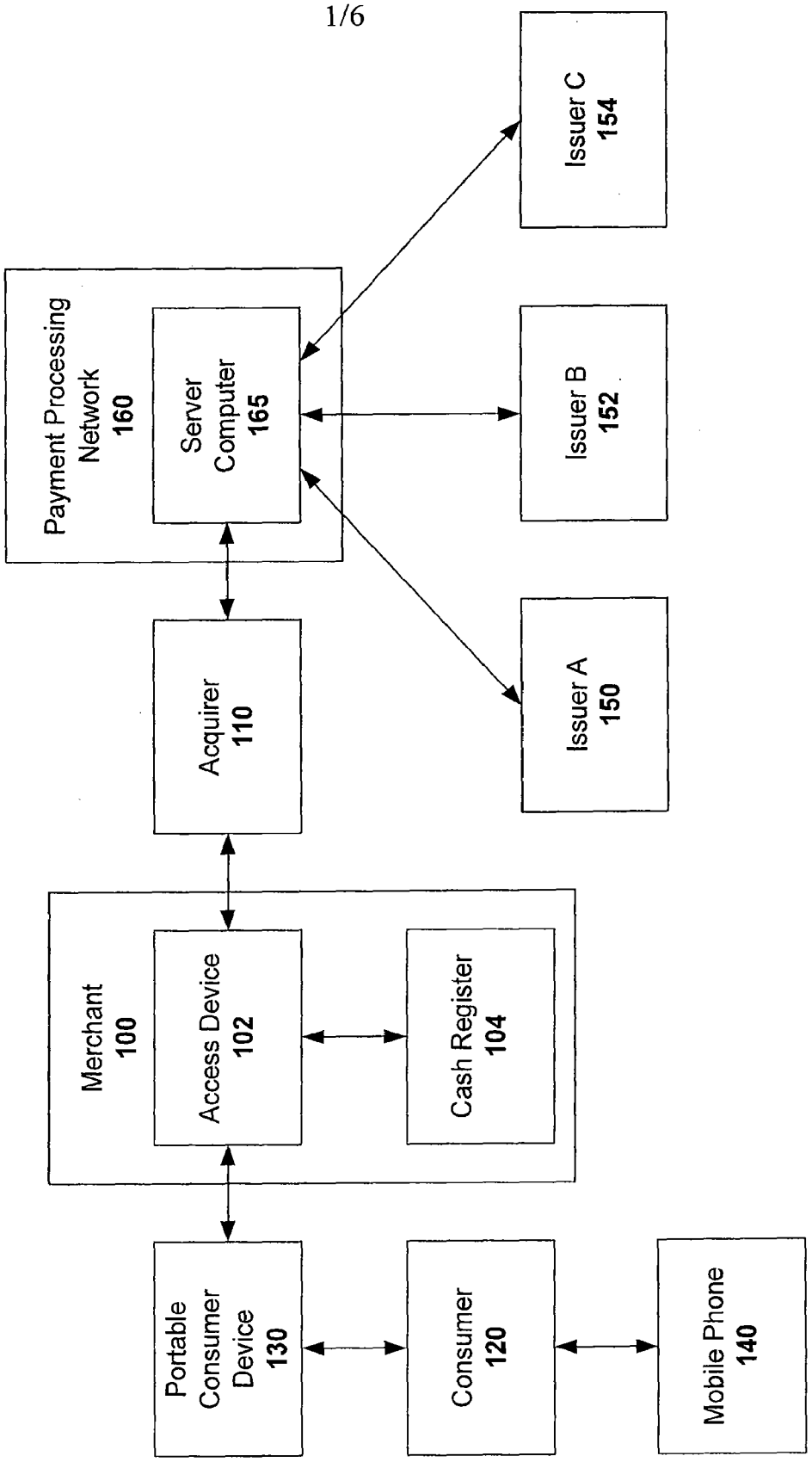

Payment Processing Network 160
Server Computer 165
Issuer C 154
Issuer B 152
Issuer A 150
Acquirer 110
Merchant 100
Access Device 102
Cash Register 104
Portable Consumer Device 130
Consumer 120
Mobile Phone 140

FIG. 1

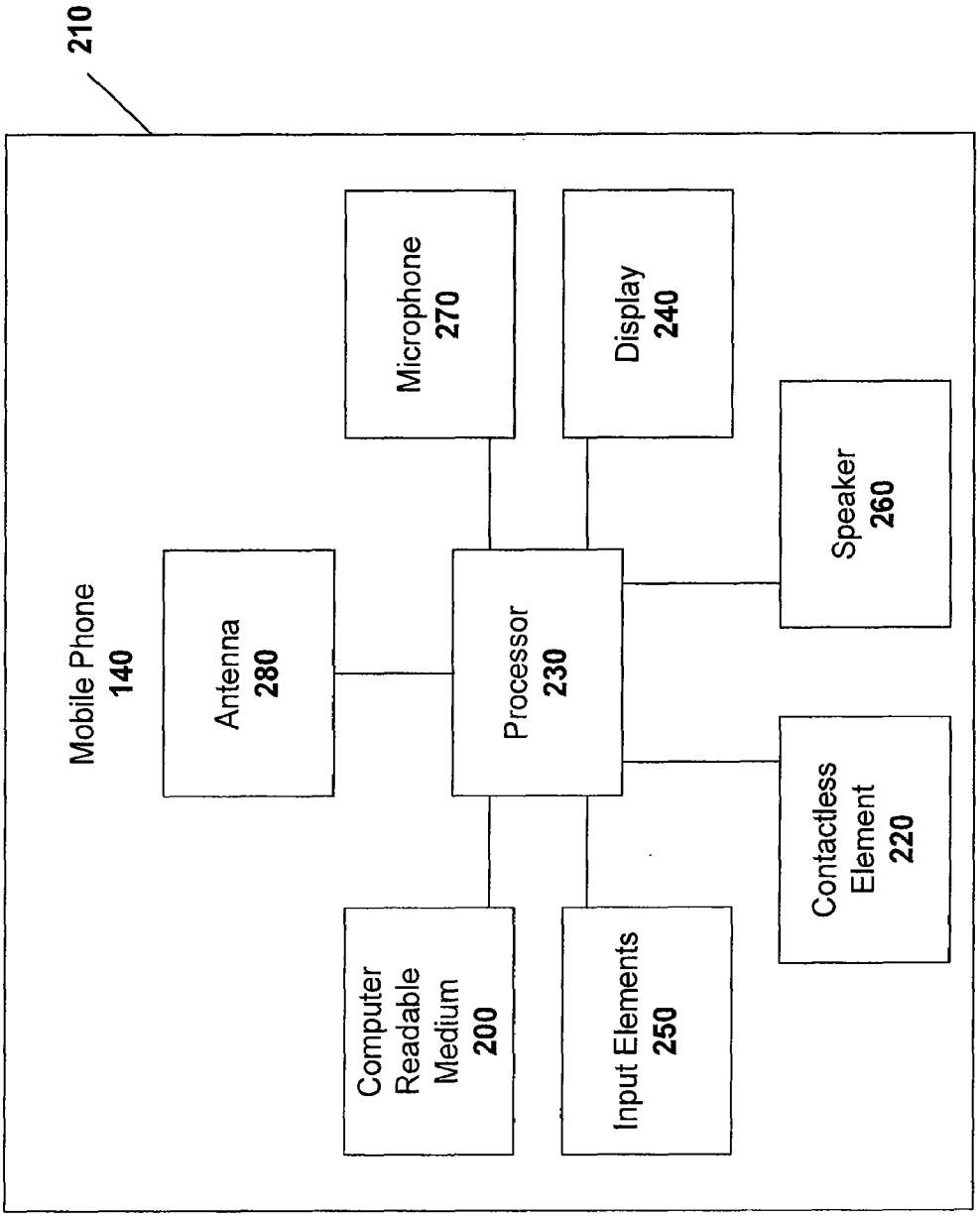

210
Mobile Phone
140
Antenna
280
Processor
230
Microphone
270
Display
240
Speaker
260
Contactless
Element
220
Computer
Readable
Medium
200
Input Elements
250

FIG. 2

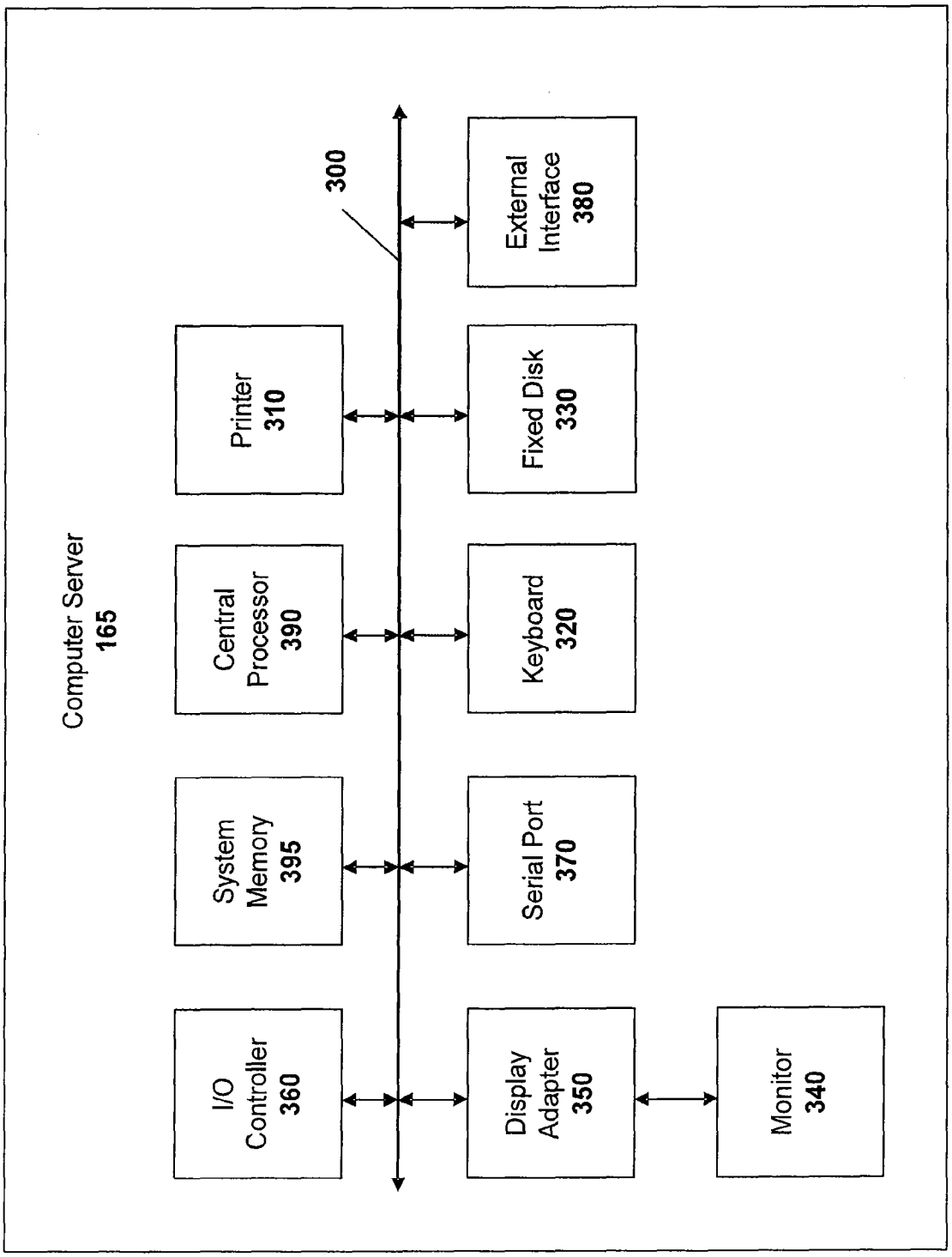

Computer Server
165
300
I/O Controller
360
System Memory
395
Central Processor
390
Printer
310
Display Adapter
350
Serial Port
370
Keyboard
320
Fixed Disk
330
Monitor
340
External Interface
380

FIG. 3

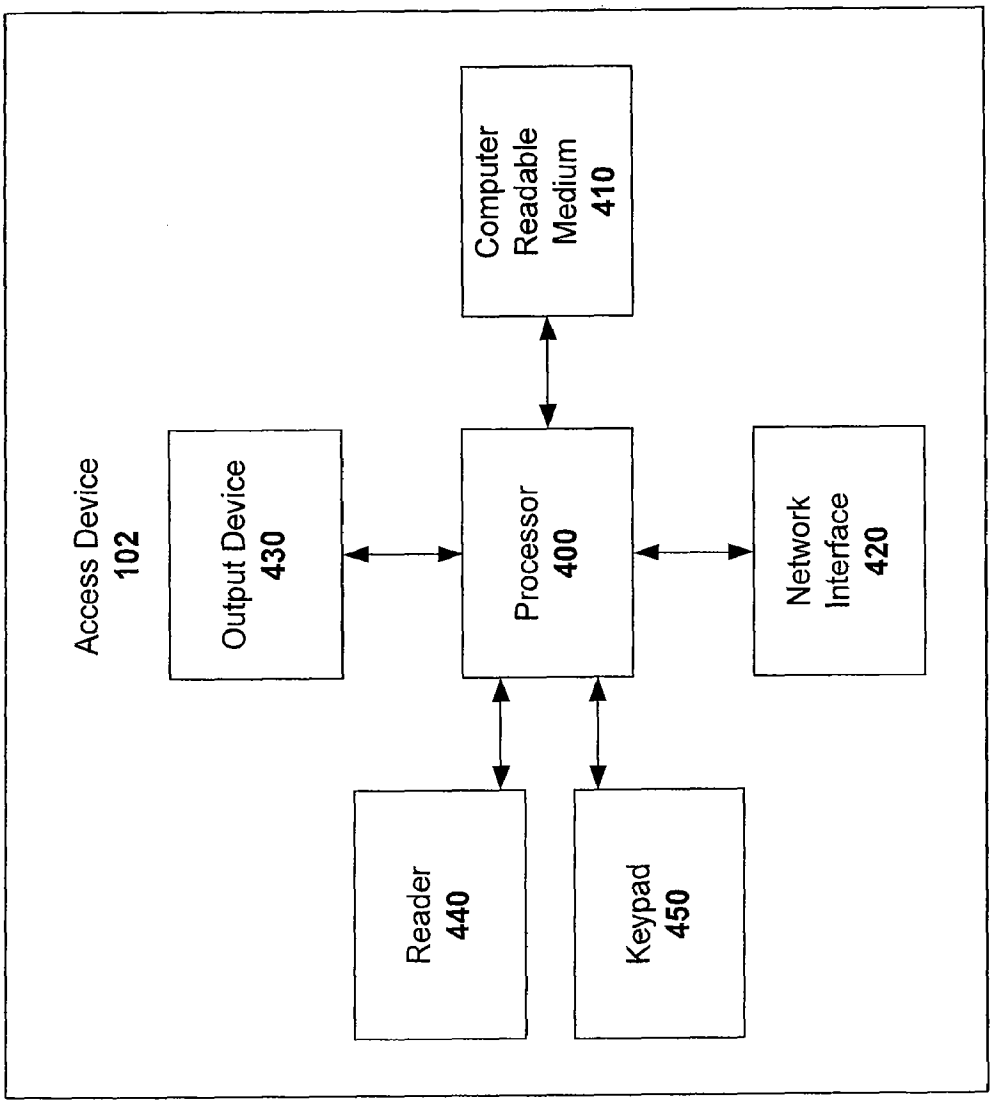

Access Device
102
Output Device
430
Computer
Readable
Medium
410
Processor
400
Network
Interface
420
Reader
440
Keypad
450

FIG. 4

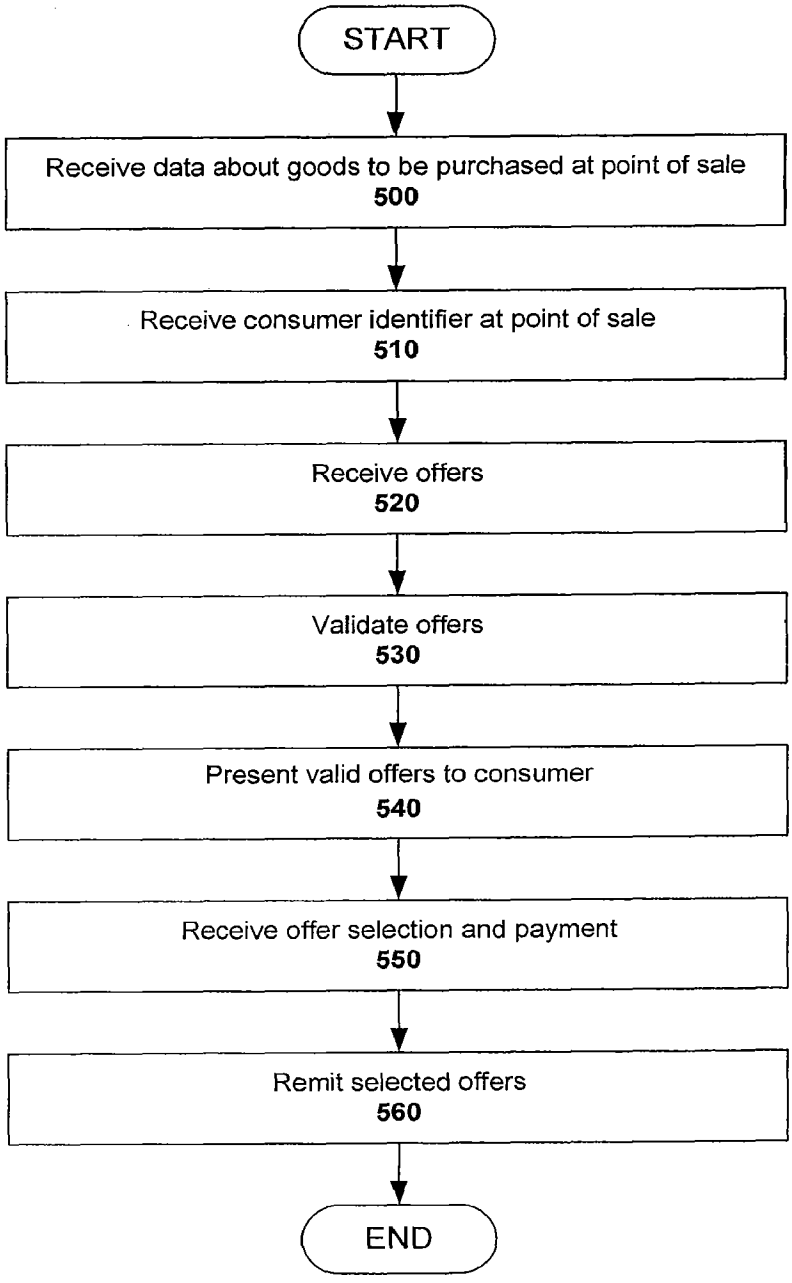

START
Receive data about goods to be purchased at point of sale
500
Receive consumer identifier at point of sale
510
Receive offers
520
Validate offers
530
Present valid offers to consumer
540
Receive offer selection and payment
550
Remit selected offers
560
END

FIG. 5

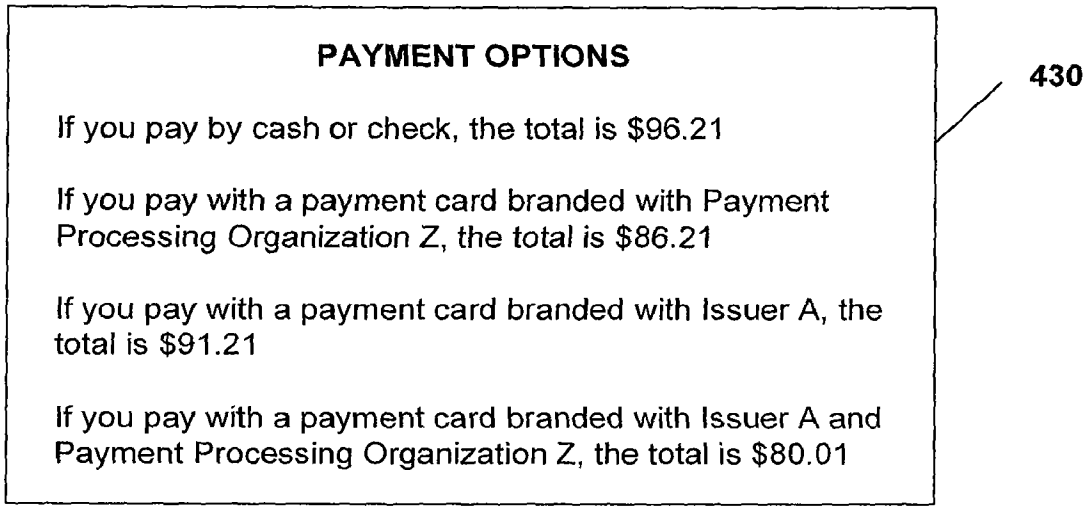

PAYMENT OPTIONS
If you pay by cash or check, the total is $96.21
If you pay with a payment card branded with Payment Processing Organization Z, the total is $86.21
If you pay with a payment card branded with Issuer A, the total is $91.21
If you pay with a payment card branded with Issuer A and Payment Processing Organization Z, the total is $80.01
430

FIG. 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2007/088615

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06Q 40/00(2006.01)
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) - G06F 17/60 (2008.04)
USPC - 705/41

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2002/0169719 A1 (DIVELY et al) 14 November 2002 (14.11.2002) entire document	1-20
A	US 2003/208406 A1 (OKAMOTO et al) 06 November 2003 (06.11.2003) entire document	1-20
A	US 6,594,376 B2 (HOFFMAN et al) 15 July 2003 (15.07.2003) entire document	1-20

☐ 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
27 May 2008	10 JUN 2008
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) (April 2005)

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 July 2008 (10.07.2008)

PCT

(10) International Publication Number
WO 2008/083105 A2

(51) International Patent Classification:
G06Q 30/00 (2006.01) *G01S 5/00* (2006.01)

(21) International Application Number:
PCT/US2007/088659

(22) International Filing Date:
21 December 2007 (21.12.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/871,898 26 December 2006 (26.12.2006) US
11/960,162 19 December 2007 (19.12.2007) US

(71) Applicants *(for all designated States except US)*: **VISA U.S.A. INC.** [US/US]; P.O. Box 8999, M3-2B, San Francisco, California 94128 (US). **VISA INTERNATIONAL SERVICE ASSOCIATION** [US/US]; 900 Metro Center Boulevard, Foster City, California 94404 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **CARLSON, Mark** [US/US]; 153 Miramontes Avenue, Half Moon Bay, California 94109 (US). **CIUREA, Peter** [US/US]; 6352 Greenridge Court, Martinez, California 94553 (US).

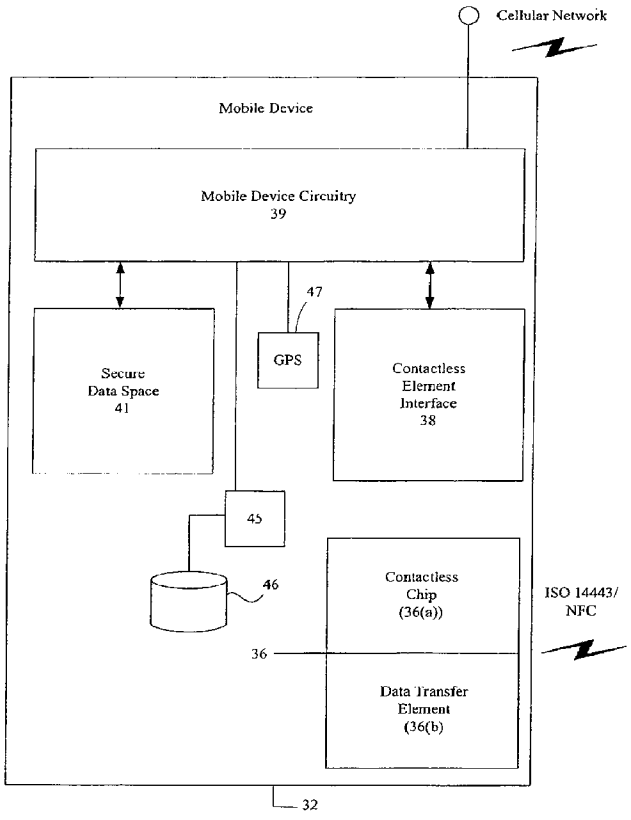
(74) Agents: **TOBIN, Kent J.** et al.; Townsend and Townsend and Crew LLP, Two Embarcadero Center, Eighth Floor, San Francisco, California 94111-3834 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, 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, 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),

[Continued on next page]

(54) Title: MOBILE COUPON METHOD AND PORTABLE CONSUMER DEVICE FOR UTILIZING SAME



(57) Abstract: Embodiments of the present invention relate to systems and methods involving mobile coupons. In one embodiment, an indication of a prior purchase transaction over a payment processing network, serves as a trigger to generate and disseminate a mobile coupon for a subsequent transaction. By generating and promulgating the coupon within a limited time of the first transaction, the recipient is disposed to be receptive based upon his or her current shopping status and also possibly geographic location. According to another embodiment, information from a mobile coupon may be presented from the consumer to a merchant in a contactless manner, utilizing an antenna of a portable device operated by a consumer. Coupon information may be communicated to the merchant with the payment information, or prior to or subsequent to transmission of the payment information to the merchant.

WO 2008/083105 A2

European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, 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:

— *without international search report and to be republished upon receipt of that report*

MOBILE COUPON METHOD AND PORTABLE CONSUMER DEVICE FOR UTILIZING SAME

CROSS-REFERENCE TO RELATED APPLICATION

[0001] The instant nonprovisional patent application claims priority to U.S. Provisional Patent Application No. 60/871,898, filed December 26, 2006 and incorporated by reference in its entirety herein for all purposes.

BACKGROUND

[0002] Coupons are a useful marketing tool to enhance brand loyalty and introduce new products. By allowing customization of the effective duration and value of an offer, a coupon provides a flexible incentive for a consumer to purchase a particular product or line of products.

[0003] Conventionally, coupons have been available in printed form from sources such as newspapers. Increased adoption of electronic sources of information such as the world-wide-web, however, has led to the increase in popularity of electronic coupons.

[0004] In addition, most consumers now own and operate a cell phone or other portable electronic device. This renders such consumers accessible to the distribution of electronic coupons as they do their shopping, and moreover allows such distributed electronic coupons to be redeemed directly at the store location.

[0005] Accordingly, there is a need in the art for methods and systems allowing for the distribution and use of electronic coupons by mobile electronic devices.

BRIEF SUMMARY

[0006] Embodiments of the present invention relate to systems and methods involving mobile coupons. In one embodiment, indication of a prior purchase transaction over a payment processing network, may serve as a trigger to generate and disseminate a mobile coupon for a subsequent transaction. By generating and promulgating the coupon within a limited time of the first transaction, the recipient is disposed to be receptive based upon his or her current shopping status and also possibly geographic location. According to another embodiment, information from a

mobile coupon may be presented to a merchant in a contactless manner, utilizing an antenna of a portable device operated by a consumer. Such mobile coupon information may be communicated to the merchant in a contactless manner with payment information, or may be communicated prior to or subsequent to transmission of payment information to the merchant.

[0007] These and other embodiments of the invention are described in further detail below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] FIG. 1 shows a simplified block diagram of a payment processing system.

[0009] FIG. 1A shows a block diagram of a portable consumer device for use with the payment processing system of FIG. 1.

[0010] FIG. 2 shows a simplified block diagram of an embodiment of a system for implementing a mobile coupon program in accordance with an embodiment of the present invention.

[0011] FIG. 3 shows a simplified flow diagram of a process for enrolling in a mobile coupon program according to an embodiment of the present invention.

[0012] FIG. 4 shows a screen from a POS terminal.

[0013] FIGS. 5(a)-5(c) show different screenshots on a phone. The screenshots include coupons.

[0014] Figure 6 is a schematic illustration of a computer system for use in accordance with embodiments of the present invention.

[0015] Figure 6A is an illustration of basic subsystems the computer system of Figure 6.

[0016] Figure 7 shows a simplified flow of a process of utilizing an embodiment of an electronic coupon according to the present invention.

DETAILED DESCRIPTION

[0017] I. Payment Processing Systems

[0018] Embodiments of the invention are directed to the use of portable consumer devices, and methods and systems employing them. Preferred portable consumer

devices are mobile phones. The mobile phones can be used in payment processing systems like those shown in FIG. 1.

[0019] FIG. 1 shows a system 20 that can be used in an embodiment of the invention. The system 20 includes a merchant 22 and an acquirer 24 associated with the merchant 22. In a typical payment transaction, a consumer 30 may purchase goods or services at the merchant 22 using a portable consumer device 32. The acquirer 24 can communicate with an issuer 28 via a payment processing system 26.

[0020] The acquirer 24 is typically a bank that has a merchant account. The issuer 28 may also be a bank, but could also be business entity such as a retail store. Some entities are both acquirers and issuers, and embodiments of the invention include such entities. The issuer 28 may operate a server computer 21, which may have a computer readable medium comprising code for performing the functions that the issuer 28 performs. A database 23 comprising account number information and other information may be operatively coupled to the server computer 21.

[0021] The consumer 30 may be an individual, or an organization such as a business that is capable of purchasing goods or services.

[0022] The portable consumer device 32 may be in any suitable form. For example, suitable portable consumer devices can be hand-held and compact so that they can fit into a consumer's wallet and/or pocket (e.g., pocket-sized). They may include smart cards, ordinary credit or debit cards (with a magnetic strip and without a microprocessor), keychain devices (such as the Speedpass™ commercially available from Exxon-Mobil Corp.), etc. Other examples of portable consumer devices include cellular phones, personal digital assistants (PDAs), pagers, payment cards, security cards, access cards, smart media, transponders, and the like. The portable consumer devices can also be debit devices (*e.g.*, a debit card), credit devices (*e.g.*, a credit card), or stored value devices (*e.g.*, a stored value card).

[0023] The portable consumer device 32 may comprise a computer readable medium 32(a) and a body 32(b). The computer readable medium 32(a) may be on the body 32(b). The body 32(b) may in the form a plastic substrate, housing, or other structure. The computer readable medium 32(a) may be a memory that stores data and may be in any suitable form. Exemplary computer readable media 32(a)

may be in any suitable form including a magnetic stripe, a memory chip, etc. If the portable consumer device 32 is in the form of a card, it may have an embossed region 32(a) which is embossed with a PAN (primary account number).

[0024] Figure 1A shows an enlarged view of the portable (mobile) device. Device 32 further includes a contactless element 36, typically implemented in the form of a semiconductor chip 36(a) (or other data storage element) with an associated wireless data transfer (e.g., data transmission) element 36(b), such as an antenna. Contactless element 36 is associated with (e.g., embedded within) mobile device 32 and data such as a coupon or control instructions transmitted via cellular network may be applied to contactless element 36 by means of contactless element interface 38. Contactless element interface 38 functions to permit the exchange of data and/or control instructions between the mobile device circuitry 39 (and hence the cellular network) and contactless element 36.

[0025] Mobile device 32 may also include a secure data space 41, which may be used by the device to store operating parameters and/or other data utilized in operation of the device. The secure data space 41 may be in the form of a chip that is separate and apart from the chip in the contactless element 36, or alternatively, could be a section of memory in the chip that forms part of the contactless element 36. Note that the chip in the contactless element 36 may include data storage capability in the form of a memory that may be accessed via interface 38 to permit the implementation of read, write, and erase functions, for example.

[0026] In accordance with still other embodiments, the mobile device may further include a processor 45 and computer readable storage medium 46 for storing code and configured to direct the processor to perform various tasks. For example, the computer readable storage medium may comprise a magnetic disk drive or a flash memory chip.

[0027] As discussed below, the computer readable storage medium may contain code that is configured to cause a processor of the portable consumer device to receive and recognize a message including a coupon and code that is delivered to the mobile device. The computer readable storage medium may also include code that is configured to decrypt an encrypted message including the code that is received by the mobile device.

[0028] Contactless element 36 is capable of transferring and receiving data using a near field communications capability (or near field communications medium) typically in accordance with a standardized protocol or data transfer mechanism (identified as ISO 14443/NFC in the figure). Near field communications capability is a short-range communications capability, such as RFID, Bluetooth™, infra-red, or other data transfer capability that can be used to exchange data between the mobile device 32 and a local apparatus, for example located a point-of-sale of a merchant or another location at which coupons are expected to be redeemed. Thus, mobile device 32 is capable of communicating and transferring data and/or control instructions via both cellular network and near field communications capability.

[0029] In accordance with certain embodiments, the mobile device further includes a Global Positioning System (GPS) element 47. GPS element 47 is configured to allow determination of the location of the user at any time. In particular, GPS element 47 relies upon signals from a plurality of orbiting satellites in order to allow the user's location to be determined. Location information obtained from the GPS element 47 may in turn be communicated through the antenna to allow monitoring of the user's position.

[0030] Returning to Figure 1, the payment processing network 26 may include data processing subsystems, networks, and operations used to support and deliver authorization services, exception file services, and clearing and settlement services. An exemplary payment processing network may include VisaNet™. Payment processing networks such as VisaNet™ are able to process credit card transactions, debit card transactions, and other types of commercial transactions. VisaNet™, in particular, includes a VIP system (Visa Integrated Payments system) which processes authorization requests and a Base II system which performs clearing and settlement services.

[0031] The payment processing network 26 may include a server computer. A server computer is typically a powerful computer or cluster of computers. For example, the server computer can be a large mainframe, a minicomputer cluster, or a group of servers functioning as a unit. In one example, the server computer may be a database server coupled to a Web server. The payment processing network 26 may use any suitable wired or wireless network, including the Internet.

[0032] The merchant 22 may also have, or may receive communications from, an access device 34 that can interact with the portable consumer device 32. In embodiment of a system of FIG. 1, the access device 34 is located at the merchant 22. However, it could be located at any other suitable location in other embodiments of the invention.

[0033] The access devices according to embodiments of the invention can be in any suitable form. Examples of access devices include point of sale (POS) devices, cellular phones, PDAs, personal computers (PCs), tablet PCs, handheld specialized readers, set-top boxes, electronic cash registers (ECRs), automated teller machines (ATMs), virtual cash registers (VCRs), kiosks, security systems, access systems, and the like.

[0034] If the access device 34 is a point of sale terminal, any suitable point of sale terminal may include a reader 34(a), a processor 34(b) and a computer readable medium 34(c). The reader 34(b) may include any suitable contact or contactless mode of operation. For example, exemplary card readers can include RF (radio frequency) antennas, magnetic stripe readers, etc. to interact with the portable consumer device 32.

[0035] In a typical purchase transaction, the consumer 30 purchases a good or service at the merchant 22 using a portable consumer device 32 such as a credit card. The consumer's portable consumer device 32 can interact with an access device 34 such as a POS (point of sale) terminal at the merchant 22. For example, the consumer 30 may take a credit card and may swipe it through an appropriate slot in the POS terminal.

[0036] Alternatively, the POS terminal may be a contactless reader, and the portable consumer device 32 may be a contactless device such as a contactless card. In certain embodiments, the portable consumer device may be a mobile device such as shown in FIG. 1A above. As described in detail below, the antenna of the mobile device may be utilized to communicate not only payment information to the POS, but also may also communicate information (such as a code) from a mobile coupon to a POS device.

[0037] An authorization request message is then forwarded to the acquirer 24. After receiving the authorization request message, the authorization request

message is then sent to the payment processing network 26. The payment processing network 26 then forwards the authorization request message to the issuer 28 of the portable consumer device 32.

[0038] After the issuer 28 receives the authorization request message, the issuer 28 sends an authorization response message back to the payment processing network 26 to indicate whether or not the current transaction is authorized (or not authorized). The transaction processing network 26 then forwards the authorization response message back to the acquirer 24. The acquirer 24 then sends the response message back to the merchant 22.

[0039] After the merchant 22 receives the authorization response message, the access device 34 at the merchant 22 may then provide the authorization response message for the consumer 30. The response message may be displayed by the access device 34, or may be printed out on a receipt.

[0040] At the end of the day, a normal clearing and settlement process can be conducted by the transaction processing network 26. A clearing process is a process of exchanging financial details between and acquirer and an issuer to facilitate posting to a consumer's account and reconciliation of the consumer's settlement position.

[0041] Some of the embodiments described below may use a payment processing system like the one described above, or any suitable combination of components in the payment processing system.

[0042] II. Mobile Coupon Method and System

[0043] Particular embodiments in accordance with the present invention relate to methods and apparatuses which allow distribution and/or redemption of electronic coupons at a mobile personal device. Various embodiments of such a system are described in the following figures.

[0044] Figure 2 shows an overall view of an embodiment of a system in accordance with the present invention for administering a mobile coupon program. A first entity 200 (i.e. Visa) is responsible for operating a payment processing network. Under the control of entity 200 are a number of different operational elements.

[0045] For example, mobile campaign server 202 functions as the interface between entity 200 and the outside world, here represented by the internet "cloud" 204. Mobile campaign server 202 can include at least three components.

[0046] Specifically, mobile enrollment server 206 provides a browser interface for potential users to enroll in the mobile coupon program using an enrollment webpage 208. Mobile enrollment server 206 is configured to receive from potential users certain pieces of information allowing their participation in the program. For example, in an enrollment form supplied electronically to server 206, the prospective participant can provide information such as the telephone number of their portable device, a security password, and preferences regarding the types of mobile coupons that they wish to receive.

[0047] Figure 3 provides a simplified flow chart of the steps for enrolling in a mobile coupon program. In step 302 of enrollment flow 300, a consumer navigates to the website of the enrollment server utilizing his or her browser.

[0048] In the next step 304, the consumer creates a mobile coupon account by inputting identification and validation information. Examples of such identification information include the user's name, the telephone number of the user's mobile electronic device, financial account numbers, and optional aliases. At this stage, the consumer also verifies that they have read appropriate disclaimers and affirmatively indicate that they seek to opt-into the mobile coupon program.

[0049] In step 306 of enrollment flow 300, information entered by the consumer is verified. Examples of such verification include confirming that the consumer identified is actually in possession of the portable device, that the portable device belongs to the consumer, and that any identified account belongs to the consumer.

[0050] Returning to FIG. 2, mobile enrollment server 206 is in turn in electronic communication with user database 210. Database 210 includes data relating to the user of the mobile coupon system, including the specific information provided during enrollment. Access to the contents of database 210 is shared with gateway server 212.

[0051] Gateway server 212 serves as the interface with outside entities responsible for implementing the mobile coupon program. For example, telecommunications

companies ("telecoms") 214 provide the infrastructure necessary to communicate the coupon to the user's mobile device wherever they happen to be. The telecom entities must provide sufficient capacity to handle a sufficiently high volume of coupon messages outgoing to recipients.

[0052] Where such volume of messages is expected to be small (for example at the inception of the mobile coupon program), another type of company called an aggregator will secure sufficient bandwidth for all of the expected messages from the telecom, and then aggregate the messages from different sources.

[0053] In an exemplary embodiment, a coupon is sent to a user's phone or other portable device. The coupon may be sent in any one of a number of different forms, including but not limited to an short messaging service (SMS) message, a SMS link, a multimedia messaging service (MMS) message, or e-mail message.

[0054] The coupon may be communicated utilizing any one of several types of communications systems. For example, the coupon may be communicated to the cell phone utilizing SMS. Such an embodiment offers a number of possible advantages, including broad access as SMS is available on almost every cell phone. Possible disadvantages to mobile coupon distribution utilizing SMS is a weak mechanism for confirming receipt of the coupon by the designated recipient, and also a high transaction cost as charges are typically incurred for each SMS message transmitted.

[0055] In accordance with alternative embodiments, the mobile coupon could be distributed by a Global System for Mobile Communications (GSM) system. Such GSM communication are cheap and secure, and would support confirmation of receipt of the coupon by a designated user.

[0056] Further alternatively, the coupons could be distributed utilizing a Near Field Communications (NFC) system. Such an embodiment would require the portable consumer device to be equipped with an NFC chip and programmed with a software application. The source of the near field signal providing the electronic coupon could be local kiosks, for example as present in a shopping mall. An alternative source of electronic coupons available utilizing such near field communication is the point of sale itself. Other sources are possible.

[0057] The coupon may be communicated to the portable consumer device in encrypted form. Such encryption would prevent interception and unauthorized use of a coupon by other than the intended recipient. A processor present in the portable consumer device could in turn decrypt the message upon its receipt.

[0058] FIG. 4 shows a screen 400 from a POS terminal. The screen 400 shows buttons 402 that a cashier might select in order to initiate a pre-arranged discount utilizing an electronic coupon. For example, button 402a allows the cashier to implement a 30% discount for employees etc. Button 402b allows the cashier to manually enter a number for numeric look-up (NLU) from an electronic coupon displayed on a user's portable electronic device.

[0059] FIGS. 5A-5C are examples of three screenshots showing graphical coupons in different forms. These screenshots are configured to be able to be displayed on the small screen of a mobile phone, personal digital assistant (PDA), or other mobile device.

[0060] FIG. 5A shows a screenshot 500 which includes both a bar code 502 (which is an example of a machine readable code) and a seven digit number 504. The bar code 502 can be scanned with a scanner. One type of scanner which may be used to read a bar code on the screen of a cell phone is a charge coupled device (CCD) scanner. However, a laser-type scanner may not be able to read the bar code displayed due to reflection from the screen.

[0061] In order to process the electronic coupon shown in FIG. 5A, the user accesses and displays the coupon on the screen of his or her portable device. The cashier then accesses the discount screen shown in FIG. 4, and either scans the bar code in directly or enters the seven-digit number utilizing a numeric key pad.

[0062] FIG. 5B illustrates a screenshot 520 showing a different embodiment of a mobile electronic coupon in accordance with the present invention, which includes a visual display 522 and a personalized message 523. This visual display may be related to the nature of the coupon, representing for example the purchase of flowers. Alternatively, the display may simply illustrate the nature of the coupon, for example the display of flowers generically representing a gift.

[0063] Instead of a barcode, a six digit number "024248" is shown by the electronic coupon 520. In processing of coupon 520 by a cashier, this six digit number can be entered into a POS terminal to give the consumer a discount on a purchase. In accordance with one embodiment, the number can be entered by having the cashier type in the individual digits of the code on a numeric keypad. In accordance with an alternative embodiment, the number can be entered by having the cashier activate a predetermined key, or combination thereof, which allows recognition of the coupon and the discount.

[0064] The embodiment of Figure 5B may offer certain advantages over a coupon employing a bar code as shown in Figure 5A. One advantage is ease of operation, as there is no requirement for optical recognition/reading of a code from the screen of the phone. Another possible advantage is reduced cost of implementation, as a bar code scanner device is not required to be purchased or rented by the merchant. In addition, software and hardware upgrades relating to electronic scanning would not be required by this alternative embodiment.

[0065] Lastly, FIG. 5C shows a screenshot 550 showing a "30% off" coupon. This electronic coupon includes a visual display 552 but lacks either a bar code or an identifying number.

[0066] To use this coupon, the user shows the display to the cashier and the cashier selects a button on a POS terminal display (see FIG. 4) to provide the discount to the consumer. According to still further embodiments of the present invention, coupon information such as a code may be communicated to a portable device in a proprietary format.

[0067] Figure 7 shows a simplified flow of a process of utilizing a mobile coupon according to an embodiment of the present invention. In a first step 702 of process flow 700, a purchaser presents items to a cashier. In step 704, the cashier hits the purchase key and enters the items. In step 706, the coupon asks the purchaser whether or not she intends to use coupons. In step 708, the purchaser responds that she intends to use a coupon.

[0068] In step 710 of process flow 700, the cashier hits the coupons key to alert the register to the use of coupons. In step 712, the cashier hits the accept coupon button on the back of the VISA terminal.

[0069] In step 714, the VISA terminal displays a message requesting the purchaser to wave the phone to enter a coupon. In step 716, the purchaser waves the phone and the terminal receives the scanned code. In step 718 the processor in communication with the terminal looks up the scanned code. In step 720, the processor returns to the terminal, customer and branding information. In step 722, the terminal displays a branding message customized to the particular purchaser. Finally, in step 724, the terminal sends to the register a numeric look up representing the bar code.

[0070] A variation according to embodiments of the present invention may utilize near field communication of the coupon or a code therein, to the cashier. In this variation, a multi-digit numerical code (i.e. six digits) can be transmitted to the POS terminal via a reader using a contactless device such as the mobile device of FIG. 1A including an antenna. The coupon may be communicated in such a contactless manner using a short range communication method, such as a near field communications (NFC) capability. Examples of such NFC technologies include ISO standard 14443, RFID, Bluetooth™ and Infra-red communications methods. In accordance with such embodiments, the six digit code may or may not be shown on the display of the phone. Embodiments in accordance with the present invention are not limited to communicating coupon code information. In accordance with alternative embodiments, coupon information communicated from a mobile device to a POS terminal may include other information, for example a product code limiting applicability of the mobile coupon to a particular product, or an expiration date/time of the mobile coupon.

[0071] In certain embodiments, payment information (such as a credit card number, debit card number, home zip code of the card holder, or a three digit card verification value code) may be communicated from a mobile device in a contactless manner to the POS terminal. In such embodiments, the coupon information from the mobile device may also be communicated to the POS terminal in a contactless manner. In some embodiments, such communication of mobile coupon information may take place as part of the same message communicating payment information to the POS terminal. Alternatively, the coupon information may be communicated prior to, or following, contactless communication of the payment information to the POS terminal.

[0072] The consumer may receive a text message, a phone call, or e-mail indicating that the consumer has received a coupon. The consumer may then use his or her phone to transmit a code corresponding to the coupon, to a contactless reader coupled to a POS terminal. The near field communication can utilize, for example, infrared or an RF communication mode such as Bluetooth. The system shown in FIG. 1 can be used in conjunction with such an embodiment.

[0073] Returning to Figure 2, apart from the mobile campaign server, a number of other elements are also under the control of entity 200. Notification module 250 is responsible for notifying participants in the program of particular events, for example limited time promotions or even the possibility of fraudulent transactions.

[0074] Mobile targeting module 260 is responsible for generating coupons targeted to a user. According to certain embodiments, the coupons can be targeted based upon a location based services (LBS) approach, utilizing prior purchasing activity by a consumer as detected over a payment processing network.

[0075] Specifically, where a payment transaction is conducted over a payment processing network, certain information is communicated that can be used for targeting of a mobile coupon. One piece of information that is potentially useful for targeting is the timing of the prior payment transaction.

[0076] In particular, the very existence of the prior purchase transaction reveals the consumer to be actively engaged in shopping rather than other activities (i.e. sleeping or working). Based upon this timing information, the consumer is known to likely be receptive to a mobile coupon for a subsequent transaction. Accordingly, embodiments of the present invention may thus generate and disseminate a mobile coupon to the consumer within a predetermined, limited time period from receiving an indication from the payment processing network that a prior payment transaction has occurred. Examples of time periods for dissemination of mobile coupons include, but are not limited to, one minute or less, five minutes, ten minutes, fifteen minutes, one-half hour, forty-five minutes, one hour, one and one half hours, two hours, three hours, four hours, and five hours or longer from the time that a prior purchasing activity is detected from the payment processing network. Such an approach allows for dissemination of a timely, non-intrusive mobile coupons to the consumer.

[0077] In certain embodiments, the duration of effectiveness of such a mobile coupon can also be limited by time. Such an embodiment would provide an incentive for the recipient to monitor his or her portable device for receipt of a mobile coupon, and use that coupon within the limited period that it is effective. Moreover, in certain embodiments, upon expiration the mobile coupon could be configured to automatically disappear from the consumer's portable device. This would reduce intrusiveness of the mobile coupon, as the consumer is not obligated to delete a backlog of expired coupons from his or her portable device.

[0078] Embodiments of the present invention are not limited to generating and promulgating mobile coupons based upon temporal information gleaned from a prior purchase transaction over a payment processing network. In accordance with alternative embodiments, the mobile coupons can be targeted based upon a geographic location of the user as determined from the payment processing network.

[0079] According to one embodiment, the location of the consumer can be determined from purchasing activity of the user based upon a Location Based Services (LBS) approach. For example, when the user swipes a card at a POS, an authorization message is returned from the payment network which includes a Merchant Identification Number (MID). The user's location at that time of sale can be determined from the MID number.

[0080] According to other embodiments, information regarding the nature of the prior purchase conducted over the payment processing network can be referenced to generate the coupon. Thus, a prior purchase of one product (for example a vacuum cleaner), could lead to generation of a second product (bags for the vacuum cleaner). This coupon generation could be irrespective of the time or physical location of a prior purchasing transaction. Still further alternatively, an LBS approach could be based upon the seller of the second product having an affinity agreement with the seller of the previous product purchased.

[0081] Moreover, a mobile coupon may be generated based upon more than one piece of information gleaned from a prior purchasing transaction conducted over a payment processing network. Specifically, the time, geographic location, and/or nature of the prior purchase transaction could be combined to generate the targeted coupon.

[0082] According to still other embodiments, information from a prior purchase transaction available from a payment processing network, may be combined with other information to generate a targeted coupon. For example, information regarding the location of the consumer can be determined from sources other than the payment processing network.

[0083] According to one approach, the location of a consumer can be determined by analyzing the location of the current base station through which the portable user device is transmitting and receiving information. Such current base station information is available from the telecommunications provider with which the consumer is affiliated, and in other applications is utilized to allow the user to contact the closest medical services provider in the case of a medical emergency. Thus, in certain embodiments, geographic information from this source could be combined with information (time, nature of prior purchases) available from the payment processing network, to generate a targeted coupon.

[0084] According to another approach, the location of a consumer can be determined by the use of Global Positioning System (GPS) technology. In this approach, the location of the portable device of the consumer is monitored utilizing a plurality of orbiting satellites. Thus, in other embodiments, geographic information from this source could be combined with information (time, nature of prior purchase) available from the payment processing network, to generate a targeted coupon.

[0085] Utilizing any of these approaches, or others, alone or in combination, the mobile targeting module 260 may send out a targeted mobile coupon to a consumer. For example, the mobile electronic coupon can be targeted in whole or in part based upon the recipient belonging to a particular group, such as an employee of a business or a member of a club.

[0086] Reward module 270 (such as "Visa Extras") is responsible for coordinating and administering an incentive or reward program that is tied to use of the payment network Thus a targeted mobile coupon may be generated and then electronically distributed to a portable consumer device as part of an incentive program. For example, the accrual of a certain volume of purchases utilizing a Visa card, may render the program participant eligible for a particularly valuable type of electronic coupon not typically available to other participants in the mobile coupon program.

This targeted electronic coupon is then communicated to the consumer's mobile device for redemption.

[0087] Other elements indicated under the control of entity 200 in FIG. 2, may relate to the function of the payment network to execute purchase and payment transactions. Partners and banks 280 are outside of the control of entity 200 but interact therewith as part of the processing of payment transactions.

[0088] It should be understood that the present invention as described above can be implemented in the form of control logic using computer software in a modular or integrated manner. Based on the disclosure and teachings provided herein, a person of ordinary skill in the art will know and appreciate other ways and/or methods to implement the present invention using hardware and a combination of hardware and software.

[0089] The various components of the mobile coupon system described above may be implemented with a computer system having various features. FIG. 6 shows an example of a generic computer system 610 including display device 620, display screen 630, cabinet 640, keyboard 650, and mouse 670. Mouse 670 and keyboard 650 are representative "user input devices." Mouse 670 includes buttons 680 for selection of buttons on a graphical user interface device. Other examples of user input devices are a touch screen, light pen, track ball, data glove, microphone, and so forth. FIG. 6 is representative of but one type of system for embodying the present invention. It will be readily apparent to one of ordinary skill in the art that many system types and configurations are suitable for use in conjunction with the present invention. In a preferred embodiment, computer system 610 includes a Pentium class based computer, running Windows NT operating system by Microsoft Corporation. However, the apparatus is easily adapted to other operating systems and architectures by those of ordinary skill in the art without departing from the scope of the present invention.

[0090] As noted, mouse 670 can have one or more buttons such as buttons 680. Cabinet 640 houses familiar computer components such as disk drives, a processor, storage device, etc. Storage devices include, but are not limited to, disk drives, magnetic tape, solid state memory, bubble memory, etc. Cabinet 640 can include additional hardware such as input/output (I/O) interface cards for connecting

computer system 610 to external devices external storage, other computers or additional peripherals, further described below.

[0091] FIG. 6A is an illustration of basic subsystems in computer system 610 of FIG. 6. This diagram is merely an illustration and should not limit the scope of the claims herein. One of ordinary skill in the art will recognize other variations, modifications, and alternatives. In certain embodiments, the subsystems are interconnected via a system bus 675. Additional subsystems such as a printer 674, keyboard 678, fixed disk 679, monitor 676, which is coupled to display adapter 682, and others are shown. Peripherals and input/output (I/O) devices, which couple to I/O controller 671, can be connected to the computer system by any number of means known in the art, such as serial port 677. For example, serial port 677 can be used to connect the computer system to a modem 681, which in turn connects to a wide area network such as the Internet, a mouse input device, or a scanner. The interconnection via system bus allows central processor 673 to communicate with each subsystem and to control the execution of instructions from system memory 672 or the fixed disk 679, as well as the exchange of information between subsystems. Other arrangements of subsystems and interconnections are readily achievable by those of ordinary skill in the art. System memory, and the fixed disk are examples of tangible media for storage of computer programs, other types of tangible media include floppy disks, removable hard disks, optical storage media such as CD-ROMS and bar codes, and semiconductor memories such as flash memory, read-only-memories (ROM), and battery backed memory.

[0092] Any of the software components or functions described in this application, may be implemented as software code to be executed by a processor using any suitable computer language such as, for example, Java, C++ or Perl using, for example, conventional or object-oriented techniques. The software code may be stored as a series of instructions, or commands on a computer readable medium, such as a random access memory (RAM), a read only memory (ROM), a magnetic medium such as a hard-drive or a floppy disk, or an optical medium such as a CD-ROM. Any such computer readable medium may reside on or within a single computational apparatus, and may be present on or within different computational apparatuses within a system or network.

[0093] The above description is illustrative and is not restrictive. Many variations of the invention will become apparent to those skilled in the art upon review of the disclosure. The scope of the invention should, therefore, be determined not with reference to the above description, but instead should be determined with reference to the pending claims along with their full scope or equivalents.

[0094] One or more features from any embodiment may be combined with one or more features of any other embodiment without departing from the scope of the invention.

[0095] A recitation of "a", "an" or "the" is intended to mean "one or more" unless specifically indicated to the contrary.

WHAT IS CLAIMED IS:

1. A method comprising:

receiving through a payment processing network, an indication of a purchase transaction by a consumer;

generating a mobile coupon based upon information from the purchase transaction; and

disseminating the mobile coupon to the consumer.

2. The method of claim 1 wherein the mobile coupon is generated based upon a time of the purchase transaction, and the mobile coupon is disseminated to the consumer within a predetermined amount of time from the time of the purchase transaction.

3. The method of claim 2 wherein the mobile coupon is effective for a limited time from the first time.

4. The method of claim 1 wherein the coupon is generated based upon a geographic location of the consumer.

5. The method of claim 4 wherein the geographic location of the consumer is determined from the purchase transaction.

6. The method of claim 4 wherein the geographic location of the consumer is determined from a location of the portable device.

7. The method of claim 6 wherein the geographic location of the consumer is determined from a global positioning system (GPS) element of the portable device.

8. The method of claim 1 wherein the information comprises at least one of a time of the purchase transaction, a geographic location of the purchase transaction, or a product purchased in the purchase transaction.

9. A method comprising:

receiving a coupon comprising a code at a portable consumer device comprising an antenna operated by a consumer;

using the antenna to provide payment information for a purchase transaction to a merchant; and

using the antenna to also provide the code to the merchant.

10. The method of claim 9 wherein the antenna is an RF antenna and the portable consumer device is a mobile phone.

11. The method of claim 9 wherein the payment information comprises a credit card number, a debit card number, a home zip code of the consumer, or a three digit card verification value code.

12. The method of claim 9 wherein the code is provided to the merchant utilizing a near field communication (NFC) channel.

13. The method of claim 9 wherein the portable consumer device includes a global positioning system (GPS), the method further comprising the portable consumer device sending to a remote location a signal indicating its geographic location.

14. A portable consumer device comprising:

a contactless element;

a wireless data transfer element associated with the contactless element;

a processor; and

a computer readable storage medium configured to store a coupon including a code, the contactless element configured to transmit the code to a merchant upon receipt of a command from a user.

15. The portable consumer device of claim 14 wherein the computer readable storage medium is configured to store instructions for the processor to decrypt an encrypted coupon message received by the wireless data transfer element.

16. The portable consumer device of claim 14 wherein the computer readable storage medium is configured to store instructions for the processor to receive and recognize an incoming message including the coupon and the code.

17. The portable consumer device of claim 16 wherein the coupon is received as a short messaging service (SMS) message, a near field communication (NFC) message, or as a global system for mobile communications (GSM) message.

18. The portable consumer device of claim 14 further comprising a global positioning system (GPS) element.

19. The portable consumer device of claim 18 wherein the computer readable storage medium is configured to store instructions for the processor to communicate a geographic location generated by the GPS element to an entity generating the coupon.

20. The portable consumer device of claim 14 further comprising a screen, wherein the computer readable storage medium is configured to store instructions for the processor to display at least a portion of the coupon on the screen.

21. The portable consumer device of claim 14 wherein the wireless data transfer element comprises an infra-red (IR) transmitter or a radio frequency (RF) transmitter.

22. A method comprising:

receiving a coupon comprising a code at a mobile phone operated by a consumer;

displaying the code on a screen of the mobile phone; and

showing the screen including the code to a merchant, thereby allowing the merchant to thereafter provide a discount to the consumer.

23. The method of claim 22 wherein displaying the code comprises displaying a numeric code.

24. The method of claim 22 further comprising providing a visual display with the code on the screen.

25. The method of claim 22 wherein receiving the coupon comprises receiving a short messaging service (SMS) message, a near field communication (NFC) message, or a global system for mobile communications (GSM) message.

26. The method of claim 22 further comprising decrypting the incoming message including the coupon.

27. The method of claim 22 wherein the coupon is generated based upon a of the consumer based upon location-based service (LBS) approach or a global positioning system (GPS) approach.

28. A method comprising:

receiving a coupon comprising a code at a portable consumer device comprising an antenna operated by a consumer; and

providing the code to a merchant using an antenna.

29. The method of claim 28 wherein the antenna is an RF antenna and the portable consumer device is a mobile phone.

30. The method of claim 28 wherein the portable consumer device receives the coupon with the antenna.

31. The method of claim 28 wherein the code is provided to the merchant utilizing a near field communication (NFC) channel.

32. The method of claim 28 wherein the portable consumer device includes a global positioning system (GPS), the method further comprising the portable consumer device sending to a remote location a signal indicating its geographic location.

33. The method of claim 28 wherein the coupon is applicable to a merchant proximate to the geographic location of the portable consumer device.

34. The method of claim 33 wherein the coupon is generated based upon a location of the consumer based upon location-based service (LBS) approach or a global positioning system (GPS) approach.

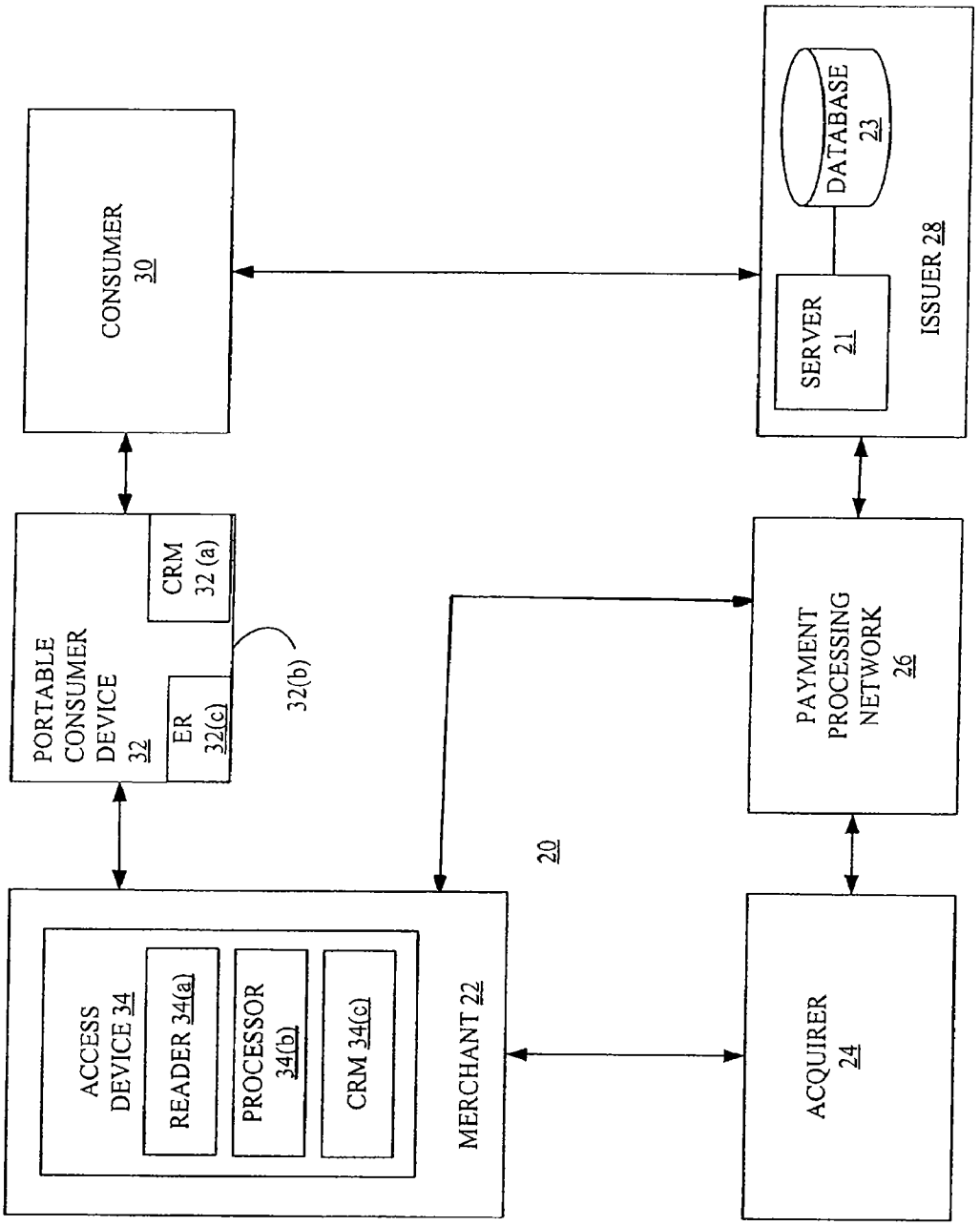

CONSUMER
30
DATABASE
23
SERVER
21
ISSUER 28
PORTABLE
CONSUMER
DEVICE
32
CRM
32 (a)
ER
32(c)
32(b)
PAYMENT
PROCESSING
NETWORK
26
20
ACCESS
DEVICE 34
READER 34(a)
PROCESSOR
34(b)
CRM 34(c)
MERCHANT 22
ACQUIRER
24

FIG. 1

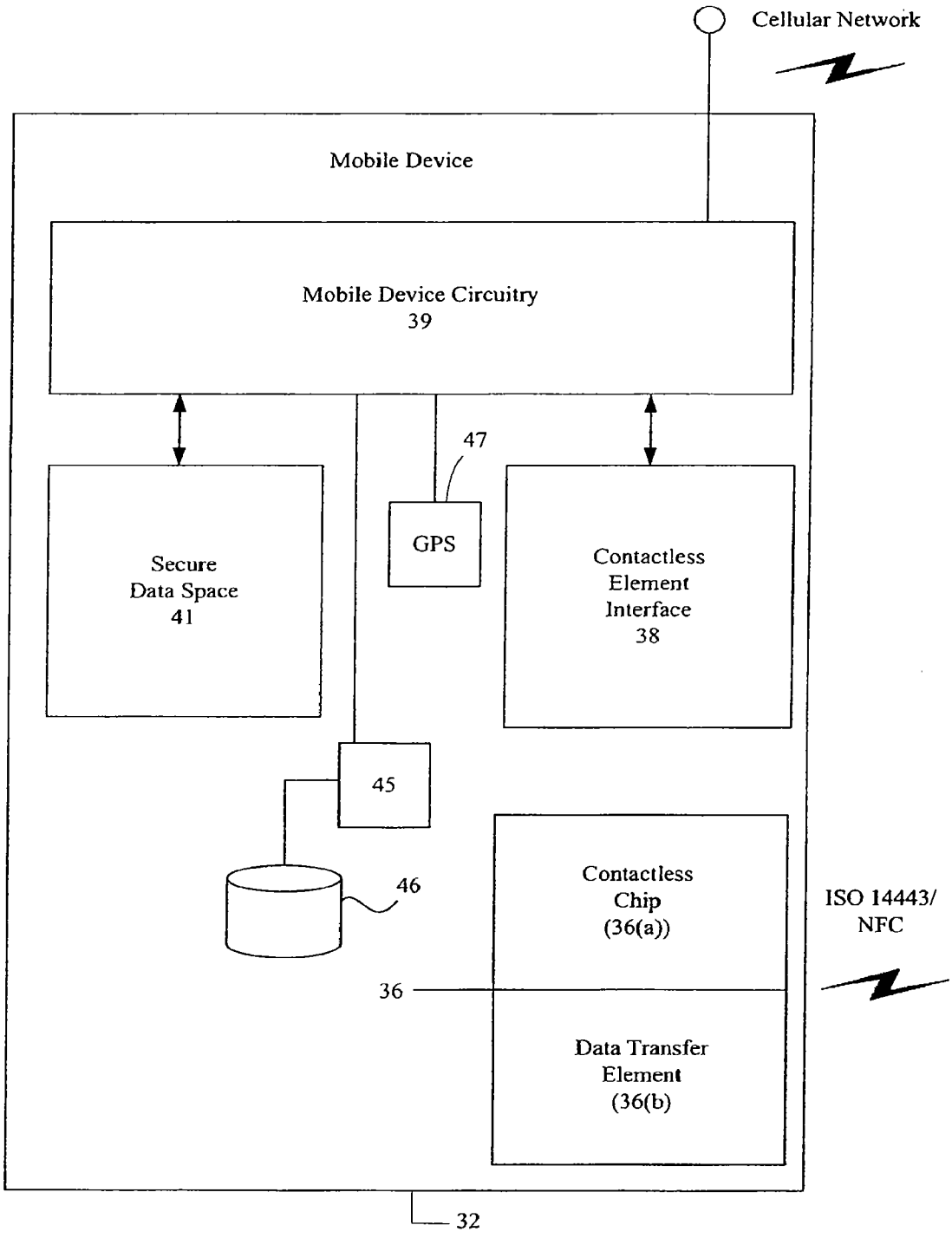

Cellular Network
Mobile Device
Mobile Device Circuitry
39
47
GPS
Secure
Data Space
41
Contactless
Element
Interface
38
45
46
Contactless
Chip
(36(a))
ISO 14443/
NFC
36
Data Transfer
Element
(36(b)
32

FIG. 1A

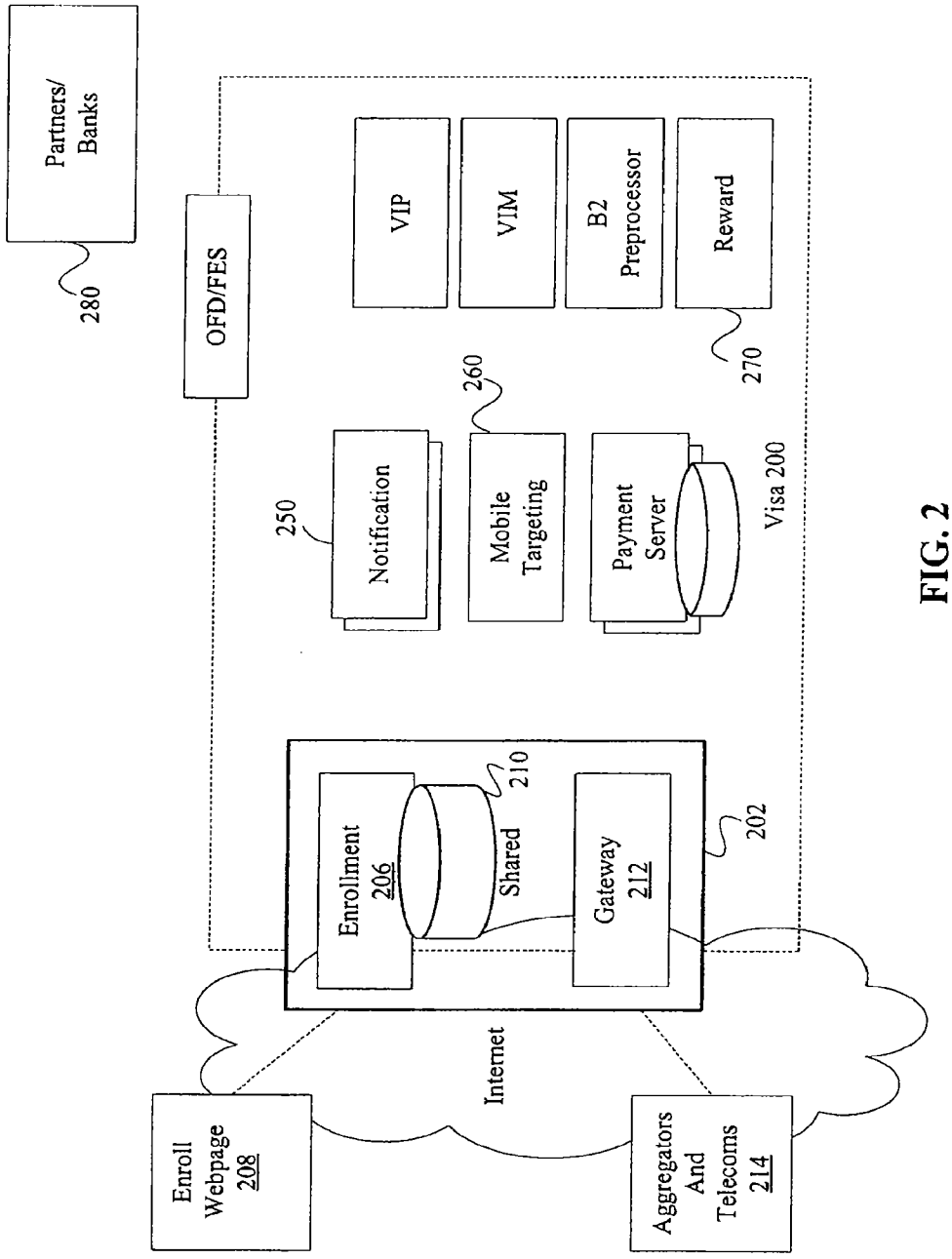

Partners/ Banks
280
OFD/FES
VIP
VIM
B2 Preprocessor
Reward
270
260
250
Notification
Mobile Targeting
Payment Server
Visa 200
Enrollment 206
Shared
210
Gateway 212
202
Internet
Enroll Webpage 208
Aggregators And Telecoms 214

FIG. 2

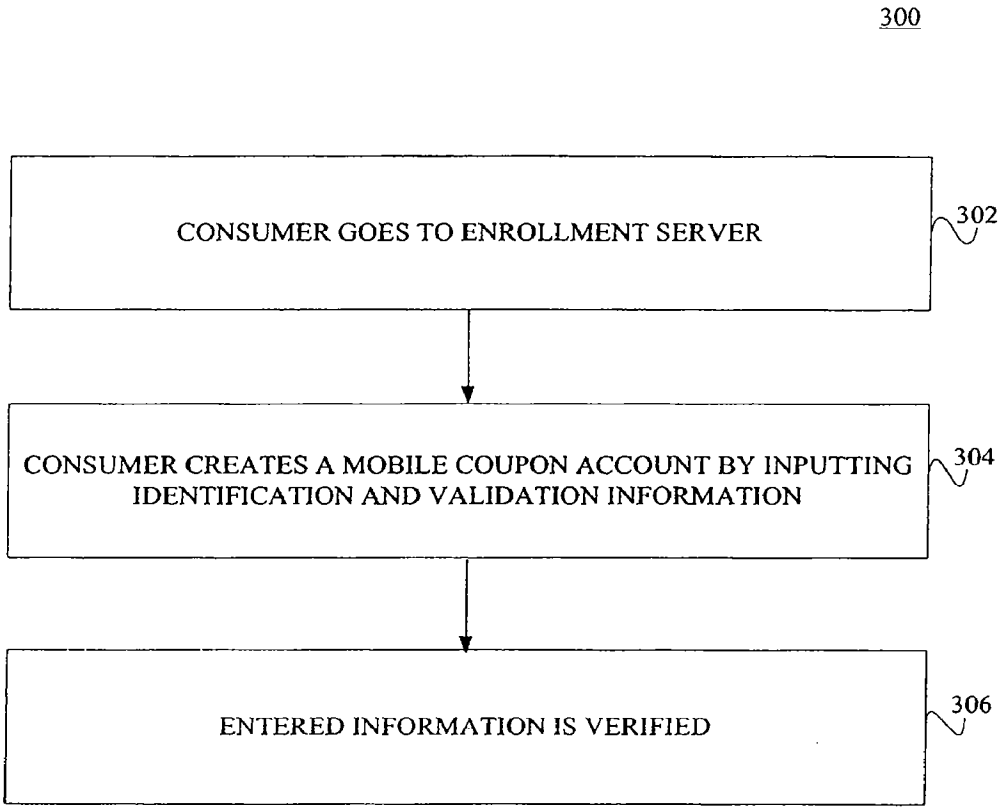

300
CONSUMER GOES TO ENROLLMENT SERVER
302
CONSUMER CREATES A MOBILE COUPON ACCOUNT BY INPUTTING IDENTIFICATION AND VALIDATION INFORMATION
304
ENTERED INFORMATION IS VERIFIED
306

FIG. 3

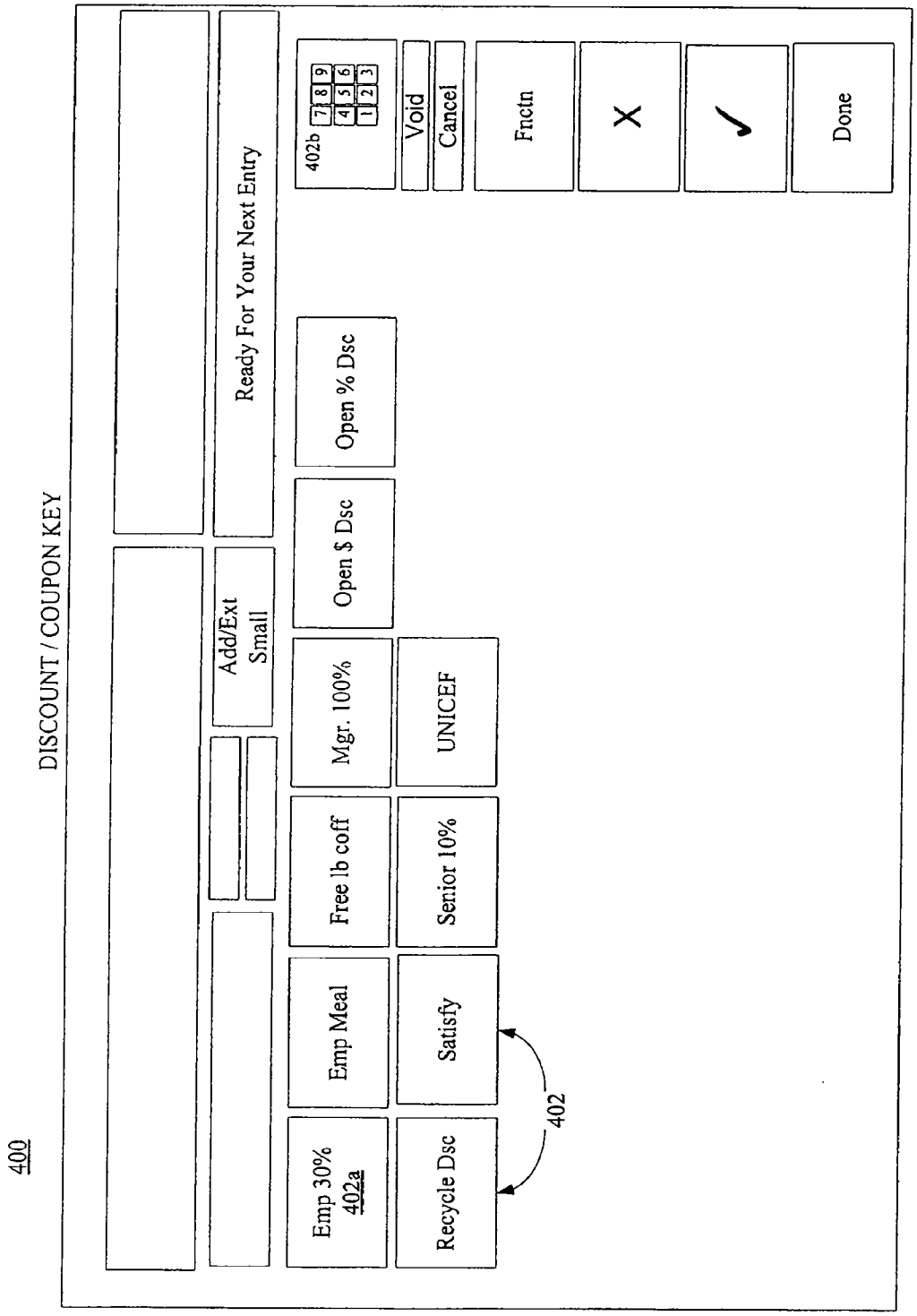

400
DISCOUNT / COUPON KEY
Ready For Your Next Entry
Add/Ext Small
Open % Dsc
Open $ Dsc
Mgr. 100%
UNICEF
Free lb coff
Senior 10%
Emp Meal
Satisfy
Emp 30% 402a
Recycle Dsc
402
402b
7 8 9
4 5 6
1 2 3
Void
Cancel
Fnctn
X
✓
Done

FIG. 4

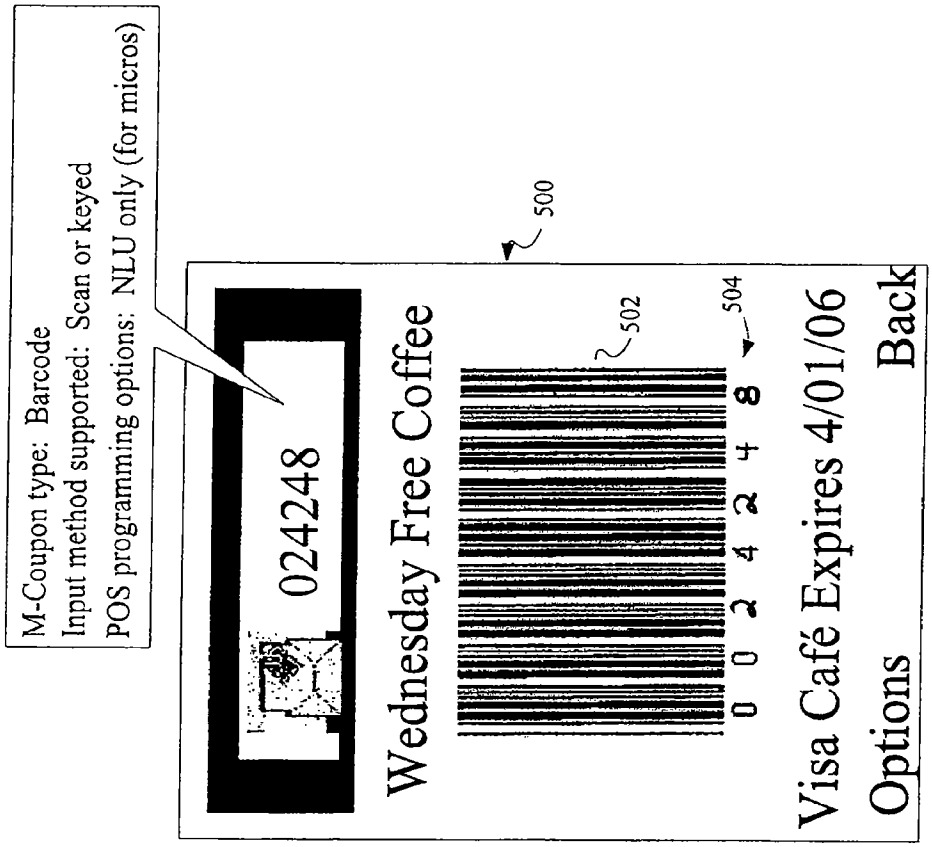

M-Coupon type: Barcode
Input method supported: Scan or keyed
POS programming options: NLU only (for micros)
024248
Wednesday Free Coffee
500
502
504
0 0 2 4 2 4 8
Visa Café Expires 4/01/06
Options
Back

FIG. 5A

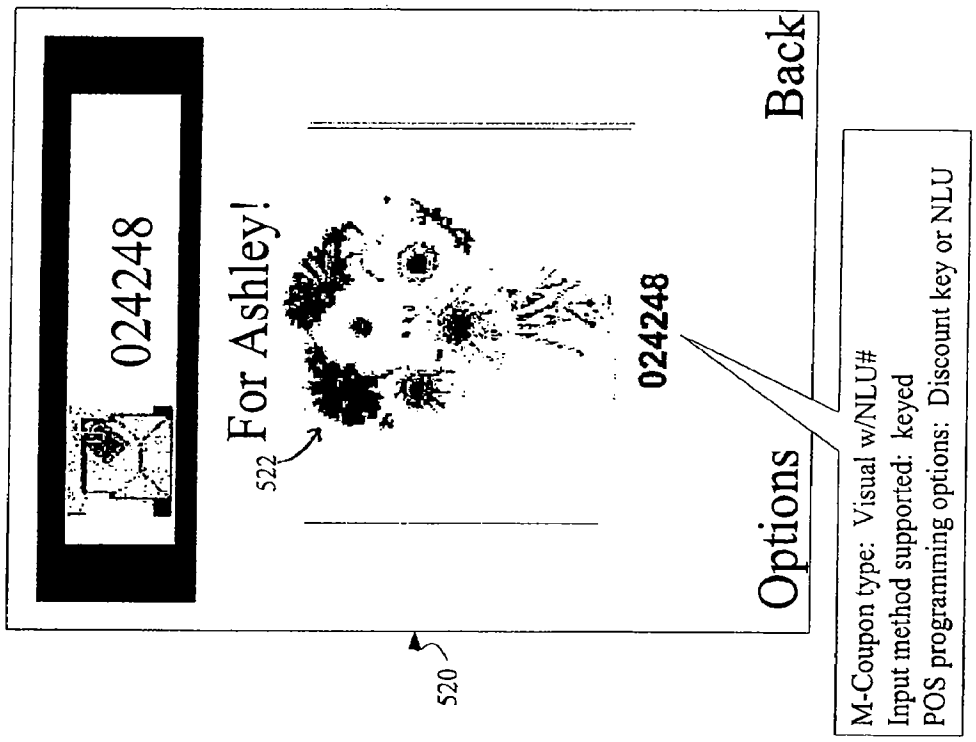

024248
For Ashley!
522
024248
Options
Back
520
M-Coupon type: Visual w/NLU#
Input method supported: keyed
POS programming options: Discount key or NLU

FIG. 5B

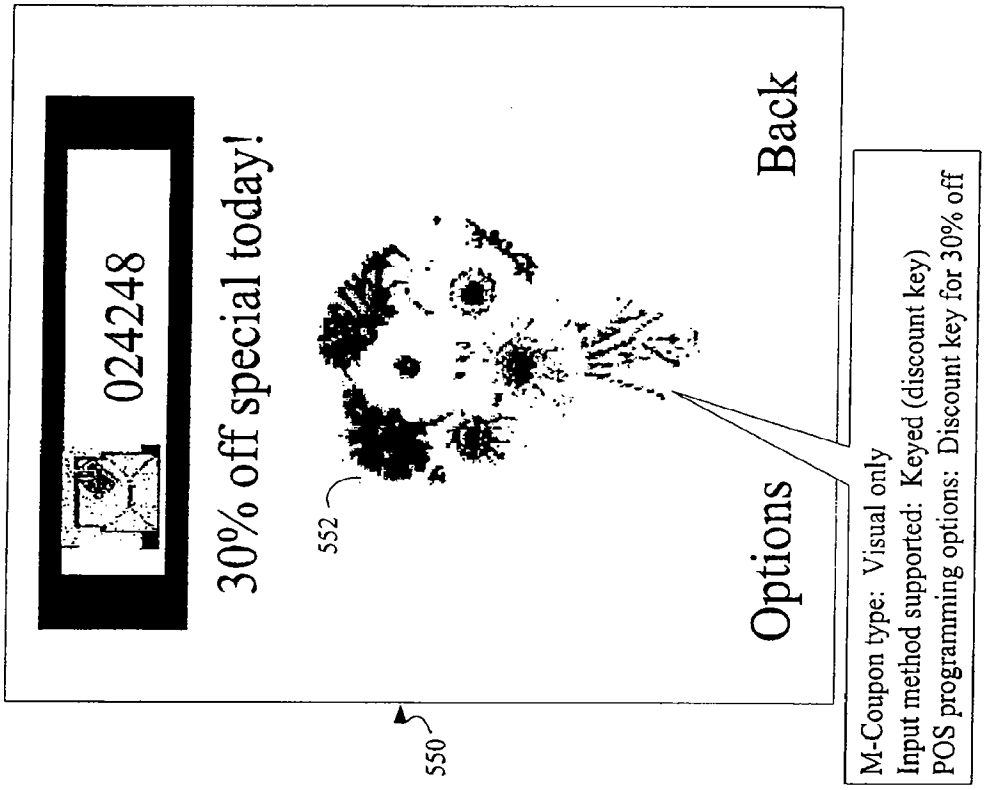

024248
30% off special today!
552
Options
Back
550
M-Coupon type: Visual only
Input method supported: Keyed (discount key)
POS programming options: Discount key for 30% off

FIG. 5C

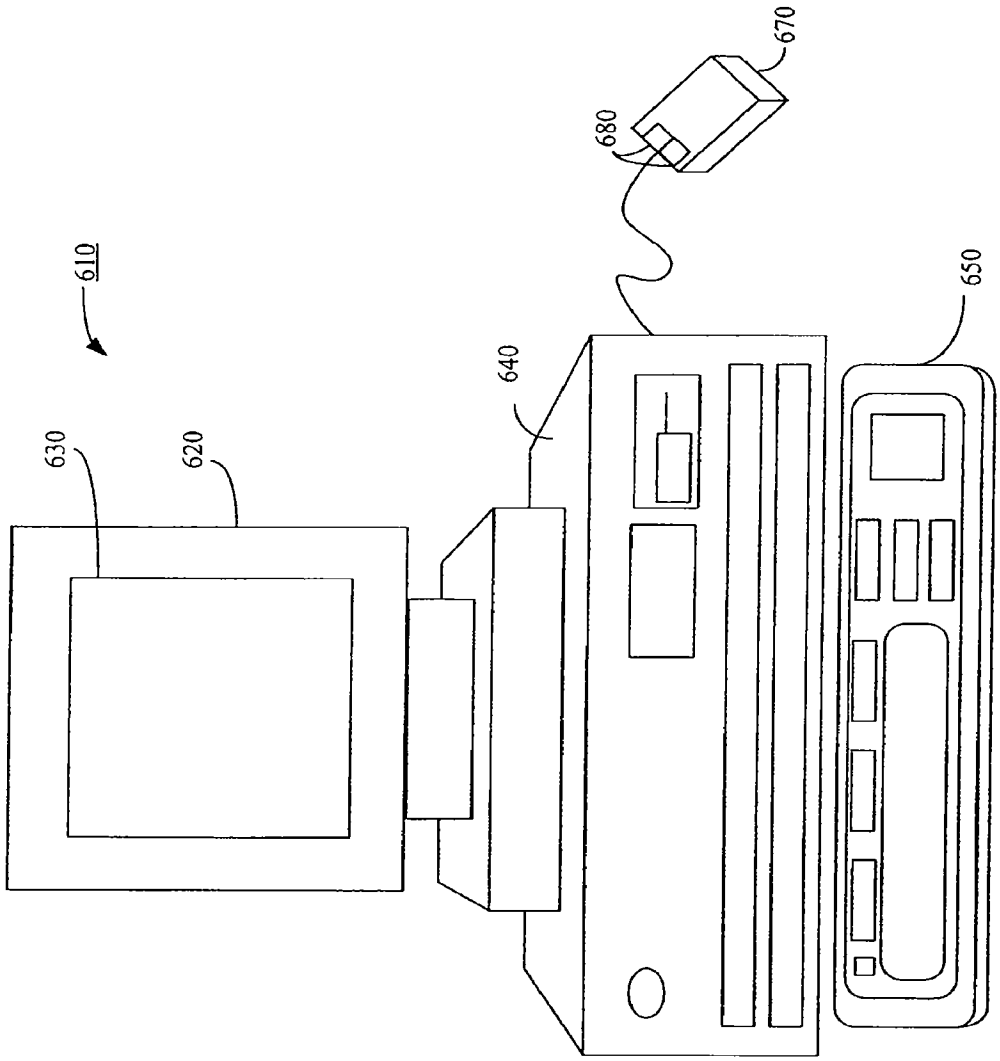


FIG. 6

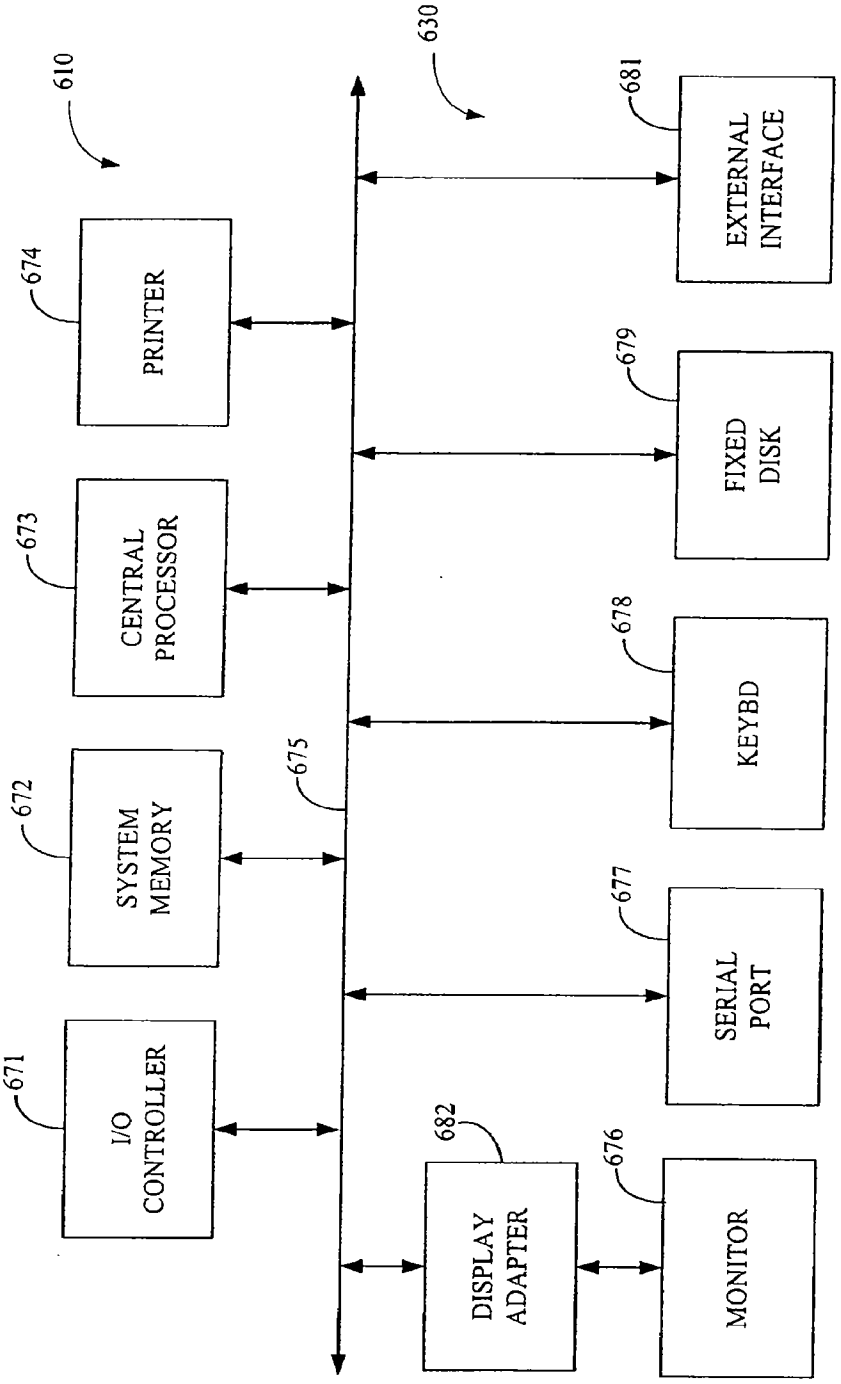

610
630
674
PRINTER
681
EXTERNAL INTERFACE
673
CENTRAL PROCESSOR
679
FIXED DISK
672
SYSTEM MEMORY
675
678
KEYBD
671
I/O CONTROLLER
677
SERIAL PORT
682
DISPLAY ADAPTER
676
MONITOR

FIG. 6A

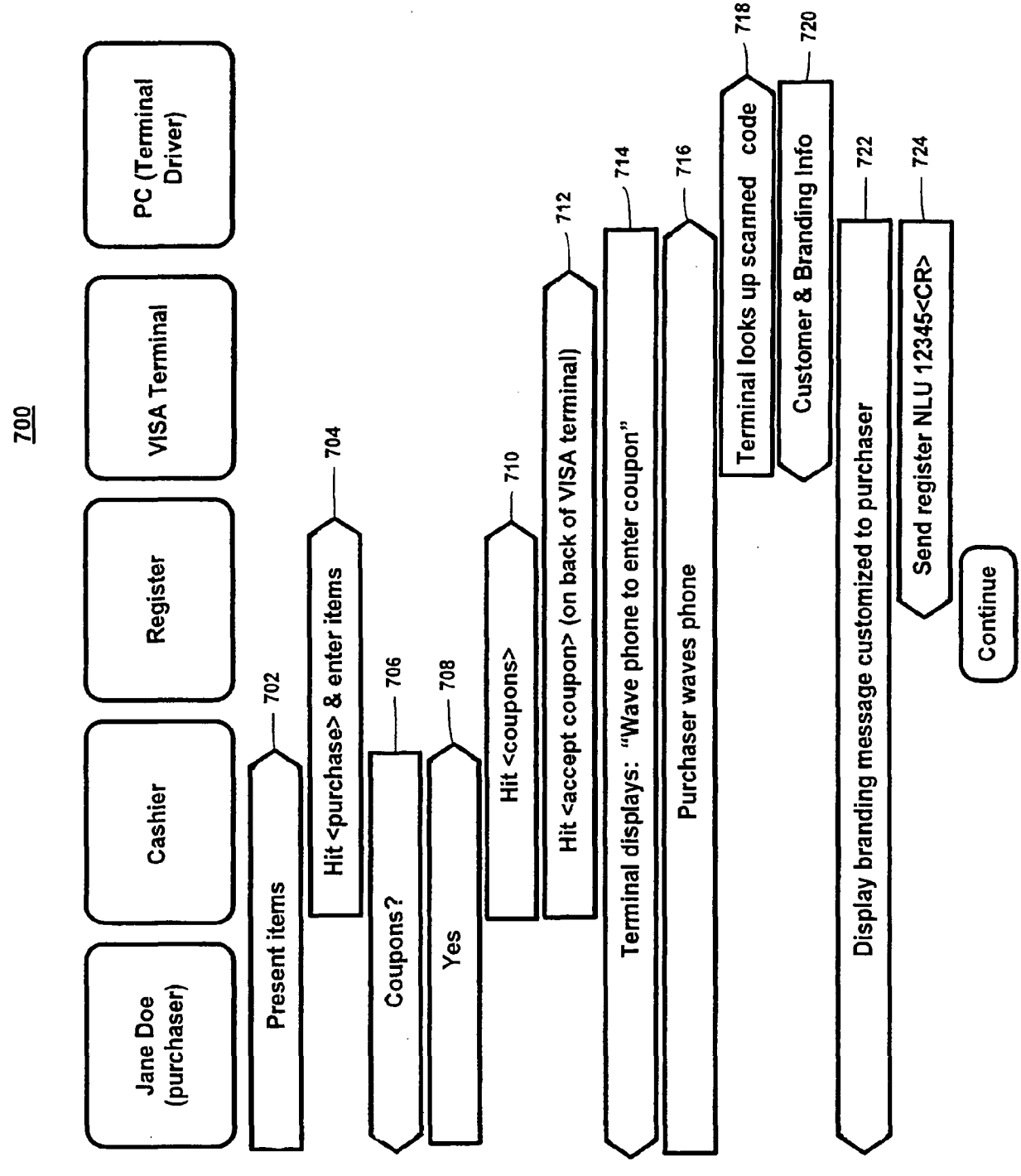

700
Jane Doe (purchaser)
Cashier
Register
VISA Terminal
PC (Terminal Driver)
Present items
702
Hit <purchase> & enter items
704
Coupons?
706
Yes
708
Hit <coupons>
710
Hit <accept coupon> (on back of VISA terminal)
712
Terminal displays: "Wave phone to enter coupon"
714
Purchaser waves phone
716
Terminal looks up scanned code
718
Customer & Branding Info
720
Display branding message customized to purchaser
722
Send register NLU 12345<CR>
724
Continue

FIG. 7

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 July 2008 (10.07.2008)

PCT

(10) International Publication Number
WO 2008/083115 A1

(51) International Patent Classification:
G06Q 30/00 (2006.01)

(21) International Application Number:
PCT/US2007/088687

(22) International Filing Date:
21 December 2007 (21.12.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/871,898 26 December 2006 (26.12.2006) US
11/960,173 19 December 2007 (19.12.2007) US

(71) Applicants *(for all designated States except US)*: **VISA USA INC.** [US/US]; P.O. Box 8999, M3-2B, San Francisco, California 94128 (US). **VISA INTERNATIONAL SERVICE CORPORATION** [US/US]; 900 Metro Center Boulevard, Foster City, California 94404 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **CARLSON, Mark, Steven** [US/US]; 153 Miramontes Avenue, Half Moon Bay, California 94019 (US). **CIUREA, Peter** [US/US]; 6352 Greenridge Court, Martinez, California 94553 (US).

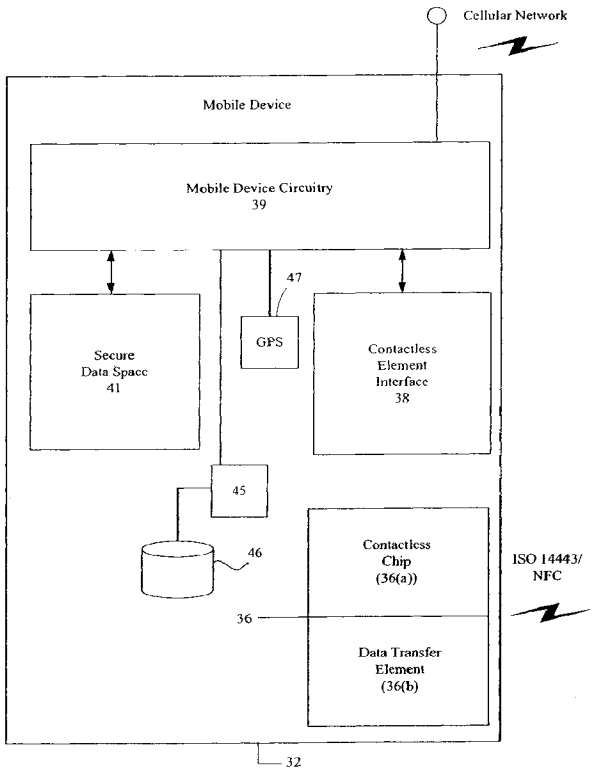
(74) Agents: **TOBIN, Kent, J.** et al.; Townsend And Townsend And Crew Llp, Two Embarcadero Center, 8th Floor, San Francisco, California 94111-3834 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, 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, 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,

[Continued on next page]

(54) Title: MOBILE COUPON METHOD AND SYSTEM



(57) Abstract: A system and a method for using a portable consumer device such as a mobile phone are disclosed. In one embodiment, a method according to the present invention comprises referencing data regarding an individual consumer stored as part of a payment processing network to generate an electronic coupon targeted to the individual consumer. The electronic coupon is transmitted to a mobile device of the individual consumer over a communications network, and purchase transaction utilizing the electronic coupon is processed over the payment processing network. In certain embodiments, the electronic coupon may be generated based upon temporal and/or geographic information of a prior purchase transaction conducted using the payment processing network.

WO 2008/083115 A1

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, MT, 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*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

MOBILE COUPON METHOD AND SYSTEM

CROSS-REFERENCE TO RELATED APPLICATION

[0001] The instant nonprovisional patent application claims priority to U.S. Provisional Patent Application No. 60/871,898, filed December 26, 2006 and incorporated by reference in its entirety herein for all purposes.

BACKGROUND

[0002] Coupons are a useful marketing tool to enhance brand loyalty and introduce new products. By allowing customization of the effective duration and value of an offer, a coupon provides a flexible incentive for a consumer to purchase a particular product or line of products.

[0003] Conventionally, coupons have been available in printed form from sources such as newspapers. Increased adoption of electronic sources of information such as the world-wide-web, however, has led to the increase in popularity of electronic coupons.

[0004] In addition, most consumers now own and operate a cell phone or other portable electronic device. This renders such consumers accessible to the distribution of electronic coupons as they do their shopping, and moreover allows such distributed electronic coupons to be redeemed directly at the store location.

[0005] Accordingly, there is a need in the art for methods and systems allowing for the distribution and use of electronic coupons by mobile electronic devices.

BRIEF SUMMARY

[0006] A system and a method for using a portable consumer device such as a mobile phone are disclosed. In one embodiment, a method according to the present invention comprises referencing data regarding an individual consumer stored as part of a payment processing network to generate an electronic coupon targeted to the individual consumer. The electronic coupon is transmitted to a mobile device of the individual consumer over a communications network, and purchase transaction utilizing the electronic coupon is processed over the payment processing network. In

certain embodiments, the electronic coupon may be generated based upon temporal and/or geographic information of a prior purchase transaction conducted using the payment processing network.

[0007] These and other embodiments of the invention are described in further detail below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] FIG. 1 shows a simplified block diagram of a payment processing system.

[0009] FIG. 1A shows a block diagram of a portable consumer device for use with the payment processing system of FIG. 1.

[0010] FIG. 2 shows a simplified block diagram of an embodiment of a system for implementing a mobile coupon program in accordance with an embodiment of the present invention.

[0011] FIG. 3 shows a simplified flow diagram of a process for enrolling in a mobile coupon program according to an embodiment of the present invention.

[0012] FIG. 4 shows a screen from a POS terminal.

[0013] FIGS. 5(a)-5(c) show different screenshots on a phone. The screenshots include coupons.

[0014] Figure 6 is a schematic illustration of a computer system for use in accordance with embodiments of the present invention.

[0015] Figure 6A is an illustration of basic subsystems the computer system of Figure 6.

[0016] Figure 7 shows a simplified flow of a process of utilizing an embodiment of an electronic coupon according to the present invention.

DETAILED DESCRIPTION

[0017] I. Payment Processing Systems

[0018] Embodiments of the invention are directed to the use of portable consumer devices, and methods and systems employing them. Preferred portable consumer devices are mobile phones. The mobile phones can be used in payment processing systems like those shown in FIG. 1.

[0019] FIG. 1 shows a system 20 that can be used in an embodiment of the invention. The system 20 includes a merchant 22 and an acquirer 24 associated with the merchant 22. In a typical payment transaction, a consumer 30 may purchase goods or services at the merchant 22 using a portable consumer device 32. The acquirer 24 can communicate with an issuer 28 via a payment processing system 26.

[0020] The acquirer 24 is typically a bank that has a merchant account. The issuer 28 may also be a bank, but could also be business entity such as a retail store. Some entities are both acquirers and issuers, and embodiments of the invention include such entities. The issuer 28 may operate a server computer 21, which may have a computer readable medium comprising code for performing the functions that the issuer 28 performs. A database 23 comprising account number information and other information may be operatively coupled to the server computer 21.

[0021] The consumer 30 may be an individual, or an organization such as a business that is capable of purchasing goods or services.

[0022] The portable consumer device 32 may be in any suitable form. For example, suitable portable consumer devices can be hand-held and compact so that they can fit into a consumer's wallet and/or pocket (e.g., pocket-sized). They may include smart cards, ordinary credit or debit cards (with a magnetic strip and without a microprocessor), keychain devices (such as the Speedpass™ commercially available from Exxon-Mobil Corp.), etc. Other examples of portable consumer devices include cellular phones, personal digital assistants (PDAs), pagers, payment cards, security cards, access cards, smart media, transponders, and the like. The portable consumer devices can also be debit devices (*e.g.*, a debit card), credit devices (*e.g.*, a credit card), or stored value devices (*e.g.*, a stored value card).

[0023] The portable consumer device 32 may comprise a computer readable medium 32(a) and a body 32(b). The computer readable medium 32(a) may be on the body 32(b). The body 32(b) may in the form a plastic substrate, housing, or other structure. The computer readable medium 32(a) may be a memory that stores data and may be in any suitable form. Exemplary computer readable media 32(a) may be in any suitable form including a magnetic stripe, a memory chip, etc. If the

portable consumer device 32 is in the form of a card, it may have an embossed region 32(a) which is embossed with a PAN (primary account number).

[0024] Figure 1A shows an enlarged view of the portable (mobile) device. Device 32 further includes a contactless element 36, typically implemented in the form of a semiconductor chip 36(a) (or other data storage element) with an associated wireless data transfer (e.g., data transmission) element 36(b), such as an antenna. Contactless element 36 is associated with (e.g., embedded within) mobile device 32 and data such as a coupon or control instructions transmitted via cellular network may be applied to contactless element 36 by means of contactless element interface 38. Contactless element interface 38 functions to permit the exchange of data and/or control instructions between the mobile device circuitry 39 (and hence the cellular network) and contactless element 36.

[0025] Mobile device 32 may also include a secure data space 41, which may be used by the device to store operating parameters and/or other data utilized in operation of the device. The secure data space 41 may be in the form of a chip that is separate and apart from the chip in the contactless element 36, or alternatively, could be a section of memory in the chip that forms part of the contactless element 36. Note that the chip in the contactless element 36 may include data storage capability in the form of a memory that may be accessed via interface 38 to permit the implementation of read, write, and erase functions, for example.

[0026] In accordance with still other embodiments, the mobile device may further include a processor 45 and computer readable storage medium 46 for storing code and configured to direct the processor to perform various tasks. For example, the computer readable storage medium may comprise a magnetic disk drive or a flash memory chip.

[0027] As discussed below, the computer readable storage medium may contain code that is configured to cause a processor of the portable consumer device to receive and recognize a message including a coupon and code that is delivered to the mobile device. The computer readable storage medium may also include code that is configured to decrypt an encrypted message including the code that is received by the mobile device.

[0028] Contactless element 36 is capable of transferring and receiving data using a near field communications capability (or near field communications medium) typically in accordance with a standardized protocol or data transfer mechanism (identified as ISO 14443/NFC in the figure). Near field communications capability is a short-range communications capability, such as RFID, Bluetooth™, infra-red, or other data transfer capability that can be used to exchange data between the mobile device 32 and a local apparatus, for example located a point-of-sale of a merchant or another location at which coupons are expected to be redeemed. Thus, mobile device 32 is capable of communicating and transferring data and/or control instructions via both cellular network and near field communications capability.

[0029] In accordance with certain embodiments, the mobile device further includes a Global Positioning System (GPS) element 47. GPS element 47 is configured to allow determination of the location of the user at any time. In particular, GPS element 47 relies upon signals from a plurality of orbiting satellites in order to allow the user's location to be determined. Location information obtained from the GPS element 47 may in turn be communicated through the antenna to allow monitoring of the user's position.

[0030] Returning to Figure 1, the payment processing network 26 may include data processing subsystems, networks, and operations used to support and deliver authorization services, exception file services, and clearing and settlement services. An exemplary payment processing network may include VisaNet™. Payment processing networks such as VisaNet™ are able to process credit card transactions, debit card transactions, and other types of commercial transactions. VisaNet™, in particular, includes a VIP system (Visa Integrated Payments system) which processes authorization requests and a Base II system which performs clearing and settlement services.

[0031] The payment processing network 26 may include a server computer. A server computer is typically a powerful computer or cluster of computers. For example, the server computer can be a large mainframe, a minicomputer cluster, or a group of servers functioning as a unit. In one example, the server computer may be a database server coupled to a Web server. The payment processing network 26 may use any suitable wired or wireless network, including the Internet.

[0032] The merchant 22 may also have, or may receive communications from, an access device 34 that can interact with the portable consumer device 32. In embodiment of a system of FIG. 1, the access device 34 is located at the merchant 22. However, it could be located at any other suitable location in other embodiments of the invention.

[0033] The access devices according to embodiments of the invention can be in any suitable form. Examples of access devices include point of sale (POS) devices, cellular phones, PDAs, personal computers (PCs), tablet PCs, handheld specialized readers, set-top boxes, electronic cash registers (ECRs), automated teller machines (ATMs), virtual cash registers (VCRs), kiosks, security systems, access systems, and the like.

[0034] If the access device 34 is a point of sale terminal, any suitable point of sale terminal may include a reader 34(a), a processor 34(b) and a computer readable medium 34(c). The reader 34(b) may include any suitable contact or contactless mode of operation. For example, exemplary card readers can include RF (radio frequency) antennas, magnetic stripe readers, etc. to interact with the portable consumer device 32.

[0035] In a typical purchase transaction, the consumer 30 purchases a good or service at the merchant 22 using a portable consumer device 32 such as a credit card. The consumer's portable consumer device 32 can interact with an access device 34 such as a POS (point of sale) terminal at the merchant 22. For example, the consumer 30 may take a credit card and may swipe it through an appropriate slot in the POS terminal.

[0036] Alternatively, the POS terminal may be a contactless reader, and the portable consumer device 32 may be a contactless device such as a contactless card. In certain embodiments, the portable consumer device may be a mobile device such as shown in FIG. 1A above. As described in detail below, the antenna of the mobile device may be utilized to communicate not only payment information to the POS, but also may also communicate information (such as a code) from a mobile coupon to a POS device.

[0037] An authorization request message is then forwarded to the acquirer 24. After receiving the authorization request message, the authorization request

message is then sent to the payment processing network 26. The payment processing network 26 then forwards the authorization request message to the issuer 28 of the portable consumer device 32.

[0038] After the issuer 28 receives the authorization request message, the issuer 28 sends an authorization response message back to the payment processing network 26 to indicate whether or not the current transaction is authorized (or not authorized). The transaction processing network 26 then forwards the authorization response message back to the acquirer 24. The acquirer 24 then sends the response message back to the merchant 22.

[0039] After the merchant 22 receives the authorization response message, the access device 34 at the merchant 22 may then provide the authorization response message for the consumer 30. The response message may be displayed by the access device 34, or may be printed out on a receipt.

[0040] At the end of the day, a normal clearing and settlement process can be conducted by the transaction processing network 26. A clearing process is a process of exchanging financial details between and acquirer and an issuer to facilitate posting to a consumer's account and reconciliation of the consumer's settlement position.

[0041] Some of the embodiments described below may use a payment processing system like the one described above, or any suitable combination of components in the payment processing system.

[0042] II. Mobile Coupon Method and System

[0043] Particular embodiments in accordance with the present invention relate to methods and apparatuses which allow distribution and/or redemption of electronic coupons at a mobile personal device. Various embodiments of such a system are described in the following figures.

[0044] Figure 2 shows an overall view of an embodiment of a system in accordance with the present invention for administering a mobile coupon program. A first entity 200 (i.e. Visa) is responsible for operating a payment processing network. Under the control of entity 200 are a number of different operational elements.

[0045] For example, mobile campaign server 202 functions as the interface between entity 200 and the outside world, here represented by the internet "cloud" 204. Mobile campaign server 202 can include at least three components.

[0046] Specifically, mobile enrollment server 206 provides a browser interface for potential users to enroll in the mobile coupon program using an enrollment webpage 208. Mobile enrollment server 206 is configured to receive from potential users certain pieces of information allowing their participation in the program. For example, in an enrollment form supplied electronically to server 206, the prospective participant can provide information such as the telephone number of their portable device, a security password, and preferences regarding the types of mobile coupons that they wish to receive.

[0047] Figure 3 provides a simplified flow chart of the steps for enrolling in a mobile coupon program. In step 302 of enrollment flow 300, a consumer navigates to the website of the enrollment server utilizing his or her browser.

[0048] In the next step 304, the consumer creates a mobile coupon account by inputting identification and validation information. Examples of such identification information include the user's name, the telephone number of the user's mobile electronic device, financial account numbers, and optional aliases. At this stage, the consumer also verifies that they have read appropriate disclaimers and affirmatively indicate that they seek to opt-into the mobile coupon program.

[0049] In step 306 of enrollment flow 300, information entered by the consumer is verified. Examples of such verification include confirming that the consumer identified is actually in possession of the portable device, that the portable device belongs to the consumer, and that any identified account belongs to the consumer.

[0050] Returning to FIG. 2, mobile enrollment server 206 is in turn in electronic communication with user database 210. Database 210 includes data relating to the user of the mobile coupon system, including the specific information provided during enrollment. Access to the contents of database 210 is shared with gateway server 212.

[0051] Gateway server 212 serves as the interface with outside entities responsible for implementing the mobile coupon program. For example, telecommunications

companies ("telecoms") 214 provide the infrastructure necessary to communicate the coupon to the user's mobile device wherever they happen to be. The telecom entities must provide sufficient capacity to handle a sufficiently high volume of coupon messages outgoing to recipients.

[0052] Where such volume of messages is expected to be small (for example at the inception of the mobile coupon program), another type of company called an aggregator will secure sufficient bandwidth for all of the expected messages from the telecom, and then aggregate the messages from different sources.

[0053] In an exemplary embodiment, a coupon is sent to a user's phone or other portable device. The coupon may be sent in any one of a number of different forms, including but not limited to an short messaging service (SMS) message, a SMS link, a multimedia messaging service (MMS) message, or e-mail message.

[0054] The coupon may be communicated utilizing any one of several types of communications systems. For example, the coupon may be communicated to the cell phone utilizing SMS. Such an embodiment offers a number of possible advantages, including broad access as SMS is available on almost every cell phone. Possible disadvantages to mobile coupon distribution utilizing SMS is a weak mechanism for confirming receipt of the coupon by the designated recipient, and also a high transaction cost as charges are typically incurred for each SMS message transmitted.

[0055] In accordance with alternative embodiments, the mobile coupon could be distributed by a Global System for Mobile Communications (GSM) system. Such GSM communication are cheap and secure, and would support confirmation of receipt of the coupon by a designated user.

[0056] Further alternatively, the coupons could be distributed utilizing a Near Field Communications (NFC) system. Such an embodiment would require the portable consumer device to be equipped with an NFC chip and programmed with a software application. The source of the near field signal providing the electronic coupon could be local kiosks, for example as present in a shopping mall. An alternative source of electronic coupons available utilizing such near field communication is the point of sale itself. Other sources are possible.

[0057] The coupon may be communicated to the portable consumer device in encrypted form. Such encryption would prevent interception and unauthorized use of a coupon by other than the intended recipient. A processor present in the portable consumer device could in turn decrypt the message upon its receipt.

[0058] FIG. 4 shows a screen 400 from a POS terminal. The screen 400 shows buttons 402 that a cashier might select in order to initiate a pre-arranged discount utilizing an electronic coupon. For example, button 402a allows the cashier to implement a 30% discount for employees etc. Button 402b allows the cashier to manually enter a number for numeric look-up (NLU) from an electronic coupon displayed on a user's portable electronic device.

[0059] FIGS. 5A-5C are examples of three screenshots showing graphical coupons in different forms. These screenshots are configured to be able to be displayed on the small screen of a mobile phone, personal digital assistant (PDA), or other mobile device.

[0060] FIG. 5A shows a screenshot 500 which includes both a bar code 502 (which is an example of a machine readable code) and a seven digit number 504. The bar code 502 can be scanned with a scanner. One type of scanner which may be used to read a bar code on the screen of a cell phone is a charge coupled device (CCD) scanner. However, a laser-type scanner may not be able to read the bar code displayed due to reflection from the screen.

[0061] In order to process the electronic coupon shown in FIG. 5A, the user accesses and displays the coupon on the screen of his or her portable device. The cashier then accesses the discount screen shown in FIG. 4, and either scans the bar code in directly or enters the seven-digit number utilizing a numeric key pad.

[0062] FIG. 5B illustrates a screenshot 520 showing a different embodiment of a mobile electronic coupon in accordance with the present invention, which includes a visual display 522 and a personalized message 523. This visual display may be related to the nature of the coupon, representing for example the purchase of flowers. Alternatively, the display may simply illustrate the nature of the coupon, for example the display of flowers generically representing a gift.

[0063] Instead of a barcode, a six digit number "024248" is shown by the electronic coupon 520. In processing of coupon 520 by a cashier, this six digit number can be entered into a POS terminal to give the consumer a discount on a purchase. In accordance with one embodiment, the number can be entered by having the cashier type in the individual digits of the code on a numeric keypad. In accordance with an alternative embodiment, the number can be entered by having the cashier activate a predetermined key, or combination thereof, which allows recognition of the coupon and the discount.

[0064] The embodiment of Figure 5B may offer certain advantages over a coupon employing a bar code as shown in Figure 5A. One advantage is ease of operation, as there is no requirement for optical recognition/reading of a code from the screen of the phone. Another possible advantage is reduced cost of implementation, as a bar code scanner device is not required to be purchased or rented by the merchant. In addition, software and hardware upgrades relating to electronic scanning would not be required by this alternative embodiment.

[0065] Lastly, FIG. 5C shows a screenshot 550 showing a "30% off" coupon. This electronic coupon includes a visual display 552 but lacks either a bar code or an identifying number.

[0066] To use this coupon, the user shows the display to the cashier and the cashier selects a button on a POS terminal display (see FIG. 4) to provide the discount to the consumer. According to still further embodiments of the present invention, coupon information such as a code may be communicated to a portable device in a proprietary format.

[0067] Figure 7 shows a simplified flow of a process of utilizing a mobile coupon according to an embodiment of the present invention. In a first step 702 of process flow 700, a purchaser presents items to a cashier. In step 704, the cashier hits the purchase key and enters the items. In step 706, the coupon asks the purchaser whether or not she intends to use coupons. In step 708, the purchaser responds that she intends to use a coupon.

[0068] In step 710 of process flow 700, the cashier hits the coupons key to alert the register to the use of coupons. In step 712, the cashier hits the accept coupon button on the back of the VISA terminal.

[0069] In step 714, the VISA terminal displays a message requesting the purchaser to wave the phone to enter a coupon. In step 716, the purchaser waves the phone and the terminal receives the scanned code. In step 718 the processor in communication with the terminal looks up the scanned code. In step 720, the processor returns to the terminal, customer and branding information. In step 722, the terminal displays a branding message customized to the particular purchaser. Finally, in step 724, the terminal sends to the register a numeric look up representing the bar code.

[0070] A variation according to embodiments of the present invention may utilize near field communication of the coupon or a code therein, to the cashier. In this variation, a multi-digit numerical code (i.e. six digits) can be transmitted to the POS terminal via a reader using a contactless device such as the mobile device of FIG. 1A including an antenna. The coupon may be communicated in such a contactless manner using a short range communication method, such as a near field communications (NFC) capability. Examples of such NFC technologies include ISO standard 14443, RFID, Bluetooth™ and Infra-red communications methods. In accordance with such embodiments, the six digit code may or may not be shown on the display of the phone. Embodiments in accordance with the present invention are not limited to communicating coupon code information. In accordance with alternative embodiments, coupon information communicated from a mobile device to a POS terminal may include other information, for example a product code limiting applicability of the mobile coupon to a particular product, or an expiration date/time of the mobile coupon.

[0071] In certain embodiments, payment information (such as a credit card number, debit card number, home zip code of the card holder, or a three digit card verification value code) may be communicated from a mobile device in a contactless manner to the POS terminal. In such embodiments, the coupon information from the mobile device may also be communicated to the POS terminal in a contactless manner. In some embodiments, such communication of mobile coupon information may take place as part of the same message communicating payment information to the POS terminal. Alternatively, the coupon information may be communicated prior to, or following, contactless communication of the payment information to the POS terminal.

[0072] The consumer may receive a text message, a phone call, or e-mail indicating that the consumer has received a coupon. The consumer may then use his or her phone to transmit a code corresponding to the coupon, to a contactless reader coupled to a POS terminal. The near field communication can utilize, for example, infrared or an RF communication mode such as Bluetooth. The system shown in FIG. 1 can be used in conjunction with such an embodiment.

[0073] Returning to Figure 2, apart from the mobile campaign server, a number of other elements are also under the control of entity 200. Notification module 250 is responsible for notifying participants in the program of particular events, for example limited time promotions or even the possibility of fraudulent transactions.

[0074] Mobile targeting module 260 is responsible for generating coupons targeted to a user. According to certain embodiments, the coupons can be targeted based upon a location based services (LBS) approach, utilizing prior purchasing activity by a consumer as detected over a payment processing network.

[0075] Specifically, where a payment transaction is conducted over a payment processing network, certain information is communicated that can be used for targeting of a mobile coupon. One piece of information that is potentially useful for targeting is the timing of the prior payment transaction.

[0076] In particular, the very existence of the prior purchase transaction reveals the consumer to be actively engaged in shopping rather than other activities (i.e. sleeping or working). Based upon this timing information, the consumer is known to likely be receptive to a mobile coupon for a subsequent transaction. Accordingly, embodiments of the present invention may thus generate and disseminate a mobile coupon to the consumer within a predetermined, limited time period from receiving an indication from the payment processing network that a prior payment transaction has occurred. Examples of time periods for dissemination of mobile coupons include, but are not limited to, one minute or less, five minutes, ten minutes, fifteen minutes, one-half hour, forty-five minutes, one hour, one and one half hours, two hours, three hours, four hours, and five hours or longer from the time that a prior purchasing activity is detected from the payment processing network. Such an approach allows for dissemination of a timely, non-intrusive mobile coupons to the consumer.

[0077] In certain embodiments, the duration of effectiveness of such a mobile coupon can also be limited by time. Such an embodiment would provide an incentive for the recipient to monitor his or her portable device for receipt of a mobile coupon, and use that coupon within the limited period that it is effective. Moreover, in certain embodiments, upon expiration the mobile coupon could be configured to automatically disappear from the consumer's portable device. This would reduce intrusiveness of the mobile coupon, as the consumer is not obligated to delete a backlog of expired coupons from his or her portable device.

[0078] Embodiments of the present invention are not limited to generating and promulgating mobile coupons based upon temporal information gleaned from a prior purchase transaction over a payment processing network. In accordance with alternative embodiments, the mobile coupons can be targeted based upon a geographic location of the user as determined from the payment processing network.

[0079] According to one embodiment, the location of the consumer can be determined from purchasing activity of the user based upon a Location Based Services (LBS) approach. For example, when the user swipes a card at a POS, an authorization message is returned from the payment network which includes a Merchant Identification Number (MID). The user's location at that time of sale can be determined from the MID number.

[0080] According to other embodiments, information regarding the nature of the prior purchase conducted over the payment processing network can be referenced to generate the coupon. Thus, a prior purchase of one product (for example a vacuum cleaner), could lead to generation of a second product (bags for the vacuum cleaner). This coupon generation could be irrespective of the time or physical location of a prior purchasing transaction. Still further alternatively, an LBS approach could be based upon the seller of the second product having an affinity agreement with the seller of the previous product purchased.

[0081] Moreover, a mobile coupon may be generated based upon more than one piece of information gleaned from a prior purchasing transaction conducted over a payment processing network. Specifically, the time, geographic location, and/or nature of the prior purchase transaction could be combined to generate the targeted coupon.

[0082] According to still other embodiments, information from a prior purchase transaction available from a payment processing network, may be combined with other information to generate a targeted coupon. For example, information regarding the location of the consumer can be determined from sources other than the payment processing network.

[0083] According to one approach, the location of a consumer can be determined by analyzing the location of the current base station through which the portable user device is transmitting and receiving information. Such current base station information is available from the telecommunications provider with which the consumer is affiliated, and in other applications is utilized to allow the user to contact the closest medical services provider in the case of a medical emergency. Thus, in certain embodiments, geographic information from this source could be combined with information (time, nature of prior purchases) available from the payment processing network, to generate a targeted coupon.

[0084] According to another approach, the location of a consumer can be determined by the use of Global Positioning System (GPS) technology. In this approach, the location of the portable device of the consumer is monitored utilizing a plurality of orbiting satellites. Thus, in other embodiments, geographic information from this source could be combined with information (time, nature of prior purchase) available from the payment processing network, to generate a targeted coupon.

[0085] Utilizing any of these approaches, or others, alone or in combination, the mobile targeting module 260 may send out a targeted mobile coupon to a consumer. For example, the mobile electronic coupon can be targeted in whole or in part based upon the recipient belonging to a particular group, such as an employee of a business or a member of a club.

[0086] Reward module 270 (such as "Visa Extras") is responsible for coordinating and administering an incentive or reward program that is tied to use of the payment network Thus a targeted mobile coupon may be generated and then electronically distributed to a portable consumer device as part of an incentive program. For example, the accrual of a certain volume of purchases utilizing a Visa card, may render the program participant eligible for a particularly valuable type of electronic coupon not typically available to other participants in the mobile coupon program.

This targeted electronic coupon is then communicated to the consumer's mobile device for redemption.

[0087] Other elements indicated under the control of entity 200 in FIG. 2, may relate to the function of the payment network to execute purchase and payment transactions. Partners and banks 280 are outside of the control of entity 200 but interact therewith as part of the processing of payment transactions.

[0088] It should be understood that the present invention as described above can be implemented in the form of control logic using computer software in a modular or integrated manner. Based on the disclosure and teachings provided herein, a person of ordinary skill in the art will know and appreciate other ways and/or methods to implement the present invention using hardware and a combination of hardware and software.

[0089] The various components of the mobile coupon system described above may be implemented with a computer system having various features. FIG. 6 shows an example of a generic computer system 610 including display device 620, display screen 630, cabinet 640, keyboard 650, and mouse 670. Mouse 670 and keyboard 650 are representative "user input devices." Mouse 670 includes buttons 680 for selection of buttons on a graphical user interface device. Other examples of user input devices are a touch screen, light pen, track ball, data glove, microphone, and so forth. FIG. 6 is representative of but one type of system for embodying the present invention. It will be readily apparent to one of ordinary skill in the art that many system types and configurations are suitable for use in conjunction with the present invention. In a preferred embodiment, computer system 610 includes a Pentium class based computer, running Windows NT operating system by Microsoft Corporation. However, the apparatus is easily adapted to other operating systems and architectures by those of ordinary skill in the art without departing from the scope of the present invention.

[0090] As noted, mouse 670 can have one or more buttons such as buttons 680. Cabinet 640 houses familiar computer components such as disk drives, a processor, storage device, etc. Storage devices include, but are not limited to, disk drives, magnetic tape, solid state memory, bubble memory, etc. Cabinet 640 can include additional hardware such as input/output (I/O) interface cards for connecting

computer system 610 to external devices external storage, other computers or additional peripherals, further described below.

[0091] FIG. 6A is an illustration of basic subsystems in computer system 610 of FIG. 6. This diagram is merely an illustration and should not limit the scope of the claims herein. One of ordinary skill in the art will recognize other variations, modifications, and alternatives. In certain embodiments, the subsystems are interconnected via a system bus 675. Additional subsystems such as a printer 674, keyboard 678, fixed disk 679, monitor 676, which is coupled to display adapter 682, and others are shown. Peripherals and input/output (I/O) devices, which couple to I/O controller 671, can be connected to the computer system by any number of means known in the art, such as serial port 677. For example, serial port 677 can be used to connect the computer system to a modem 681, which in turn connects to a wide area network such as the Internet, a mouse input device, or a scanner. The interconnection via system bus allows central processor 673 to communicate with each subsystem and to control the execution of instructions from system memory 672 or the fixed disk 679, as well as the exchange of information between subsystems. Other arrangements of subsystems and interconnections are readily achievable by those of ordinary skill in the art. System memory, and the fixed disk are examples of tangible media for storage of computer programs, other types of tangible media include floppy disks, removable hard disks, optical storage media such as CD-ROMS and bar codes, and semiconductor memories such as flash memory, read-only-memories (ROM), and battery backed memory.

[0092] Any of the software components or functions described in this application, may be implemented as software code to be executed by a processor using any suitable computer language such as, for example, Java, C++ or Perl using, for example, conventional or object-oriented techniques. The software code may be stored as a series of instructions, or commands on a computer readable medium, such as a random access memory (RAM), a read only memory (ROM), a magnetic medium such as a hard-drive or a floppy disk, or an optical medium such as a CD-ROM. Any such computer readable medium may reside on or within a single computational apparatus, and may be present on or within different computational apparatuses within a system or network.

[0093] The above description is illustrative and is not restrictive. Many variations of the invention will become apparent to those skilled in the art upon review of the disclosure. The scope of the invention should, therefore, be determined not with reference to the above description, but instead should be determined with reference to the pending claims along with their full scope or equivalents.

[0094] One or more features from any embodiment may be combined with one or more features of any other embodiment without departing from the scope of the invention.

[0095] A recitation of "a", "an" or "the" is intended to mean "one or more" unless specifically indicated to the contrary.

WHAT IS CLAIMED IS:

1. A method comprising:

referencing data regarding an individual consumer stored as part of a payment processing network to generate an electronic coupon targeted to the individual consumer;

transmitting the electronic coupon to a mobile device of the individual consumer over a communications network; and

processing a purchase transaction utilizing the electronic coupon over the payment processing network.

2. The method of claim 1 wherein the electronic coupon is generated based upon a prior transaction conducted over the payment processing network.

3. The method of claim 2 wherein the electronic coupon is generated within a predetermined time from a time of the prior transaction.

4. The method of claim 1 wherein the electronic coupon is targeted based upon a geographic location of the individual consumer.

5. The method of claim 4 wherein the geographic location of the consumer is determined from a location based services (LBS) approach based upon a prior transaction conducted over the payment processing network.

6. The method of claim 5 wherein the geographic location is determined from a merchant identification number in the prior transaction.

7. The method of claim 4 wherein the geographic location of the consumer is determined from a global positioning system (GPS) element in the mobile device.

8. The method of claim 4 wherein the geographic location of the consumer is determined from the mobile device communicating through the communications network.

9. The method of claim 1 wherein the electronic coupon is communicated in encrypted form.

10. The method of claim 1 wherein the electronic coupon is communicated including a code able to be electronically transmitted from the mobile device to a point of sale.

11. The method of claim 1 wherein the data regarding the individual consumer is obtained based upon an enrollment form submitted by the individual consumer.

12. The method of claim 1 wherein the data regarding the individual consumer is obtained based upon the individual consumer's use of the payment processing network.

13. A server for a mobile coupon program, the server comprising:

a processor; and

a computer readable storage medium in electronic communication with the processor, the computer readable storage medium having stored thereon, code instructing the processor to,

reference data regarding an individual consumer stored as part of a payment processing network to generate an electronic coupon targeted to the individual consumer, and

transmit the electronic coupon to a mobile device of the individual consumer over a communications network.

14. The server of claim 13 wherein the code instructs generation of the electronic coupon based upon a prior transaction conducted over the payment processing network.

15. The server of claim 14 wherein the code instructs generation of the electronic coupon within a predetermined time of a time of the prior transaction.

16. The server of claim 13 wherein code instructs generation of the electronic coupon based upon a geographic location of the individual consumer.

17. The server of claim 16 wherein the geographic location of the consumer is determined from a location based services (LBS) approach based upon a prior transaction conducted over the payment processing network.

18. The server of claim 16 wherein the geographic location of the consumer is determined from a merchant identification number in the prior transaction.

19. The server of claim 16 wherein the geographic location of the consumer is determined from a global positioning system (GPS) element in the mobile device.

20. The server of claim 16 wherein the geographic location of the consumer is determined from the mobile device communicating through the communications network.

21. A method comprising:

a consumer conducting a first purchasing transaction over a payment processing network;

generating an electronic coupon targeted to the consumer based upon the first purchasing transaction;

transmitting the electronic coupon to a mobile device of the consumer; and

processing a second purchasing transaction over the payment processing network, the second purchasing transaction involving use of the electronic coupon to obtain a discount.

22. The method of claim 21 wherein the coupon is generated within a predetermined time of a time of the first purchasing transaction.

23. The method of claim 21 wherein the coupon is generated based upon a geographic location of the first purchasing transaction.

24. The method of claim 21 wherein the first purchasing transaction or the second purchasing transaction allow the consumer to receive an award.

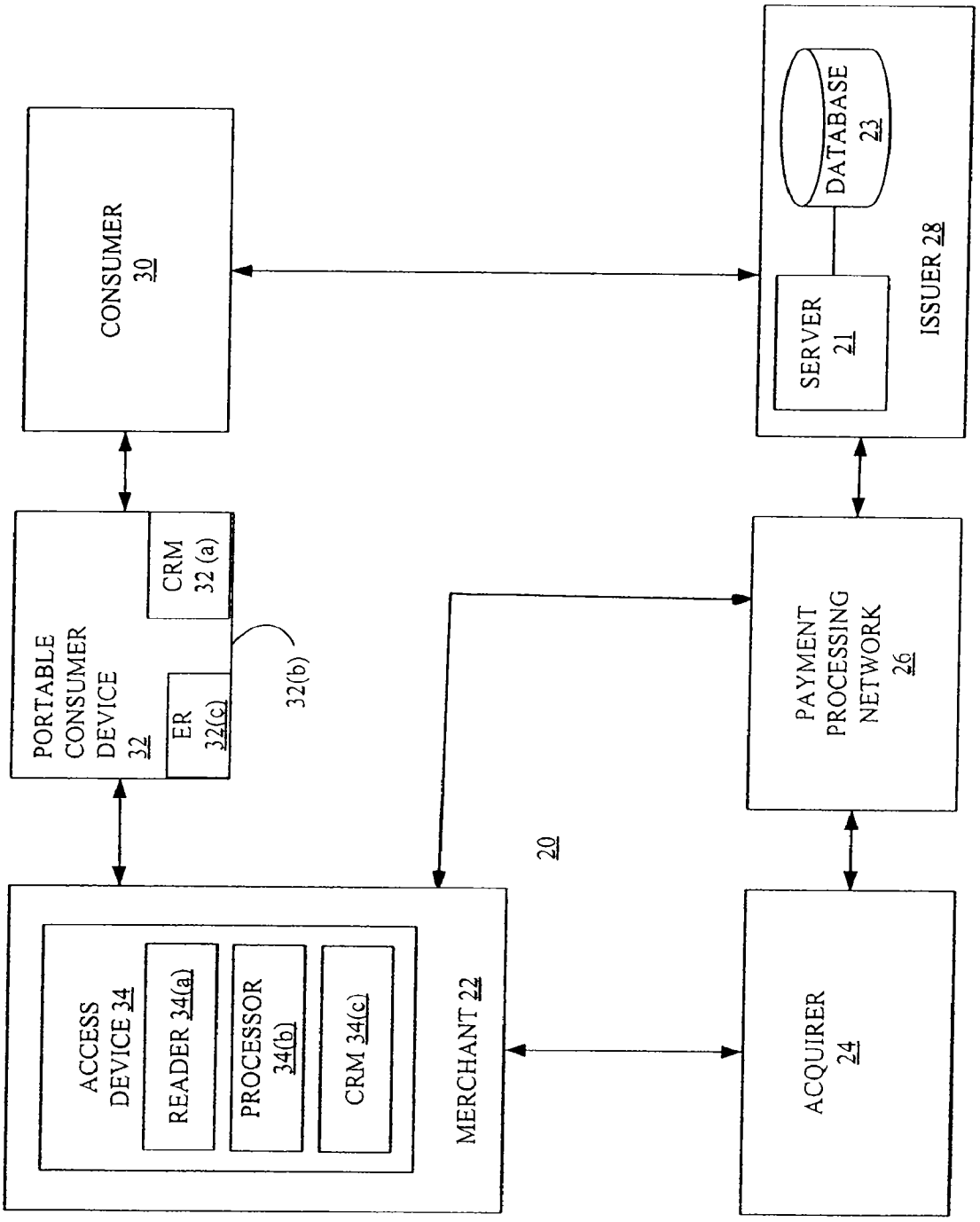

CONSUMER
30
DATABASE
23
SERVER
21
ISSUER 28
PORTABLE
CONSUMER
DEVICE
32
CRM
32 (a)
ER
32(c)
32(b)
PAYMENT
PROCESSING
NETWORK
26
20
ACCESS
DEVICE 34
READER 34(a)
PROCESSOR
34(b)
CRM 34(c)
MERCHANT 22
ACQUIRER
24

FIG. 1

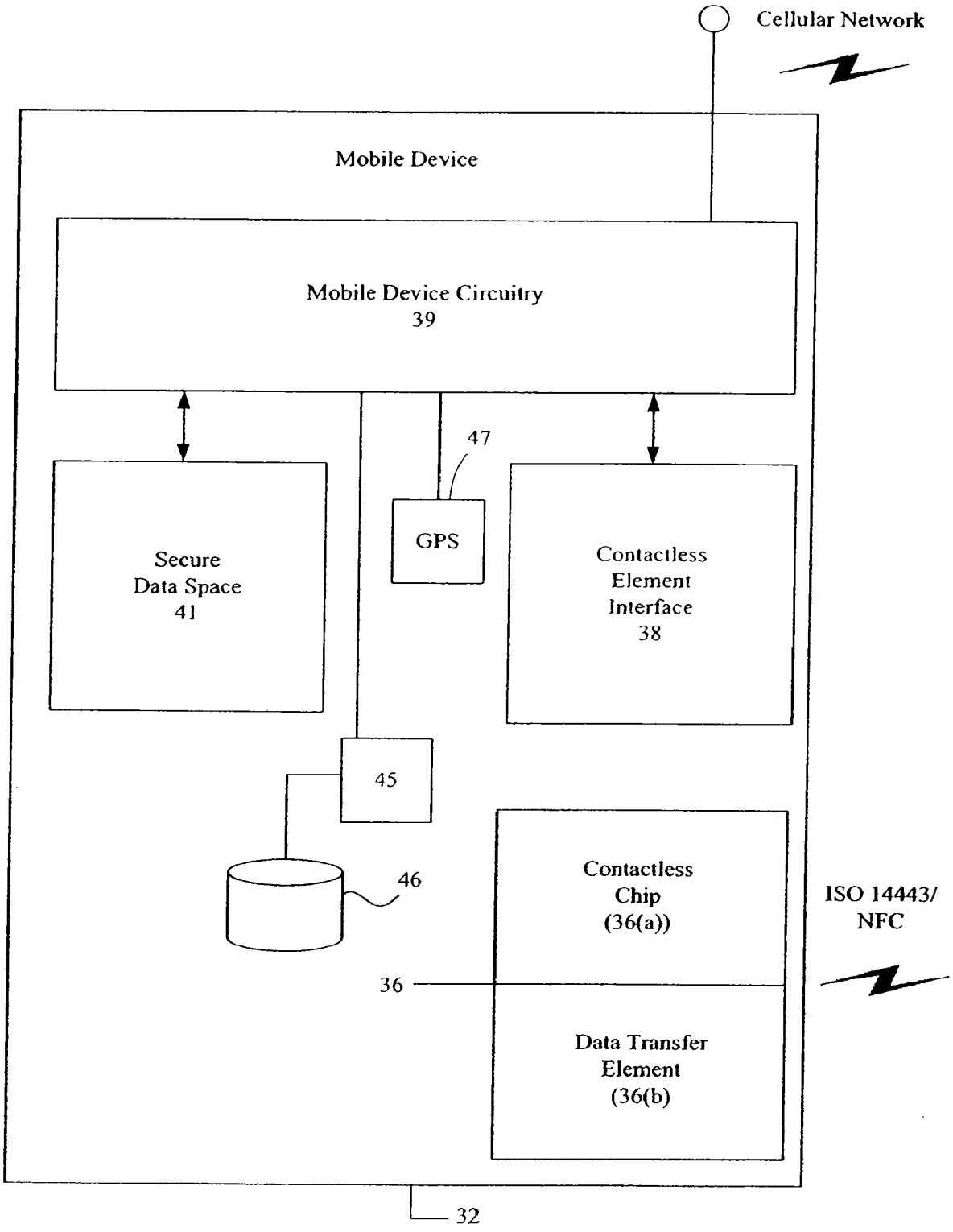

Cellular Network
Mobile Device
Mobile Device Circuitry
39
47
GPS
Secure
Data Space
41
Contactless
Element
Interface
38
45
46
Contactless
Chip
(36(a))
ISO 14443/
NFC
36
Data Transfer
Element
(36(b)
32

FIG. 1A

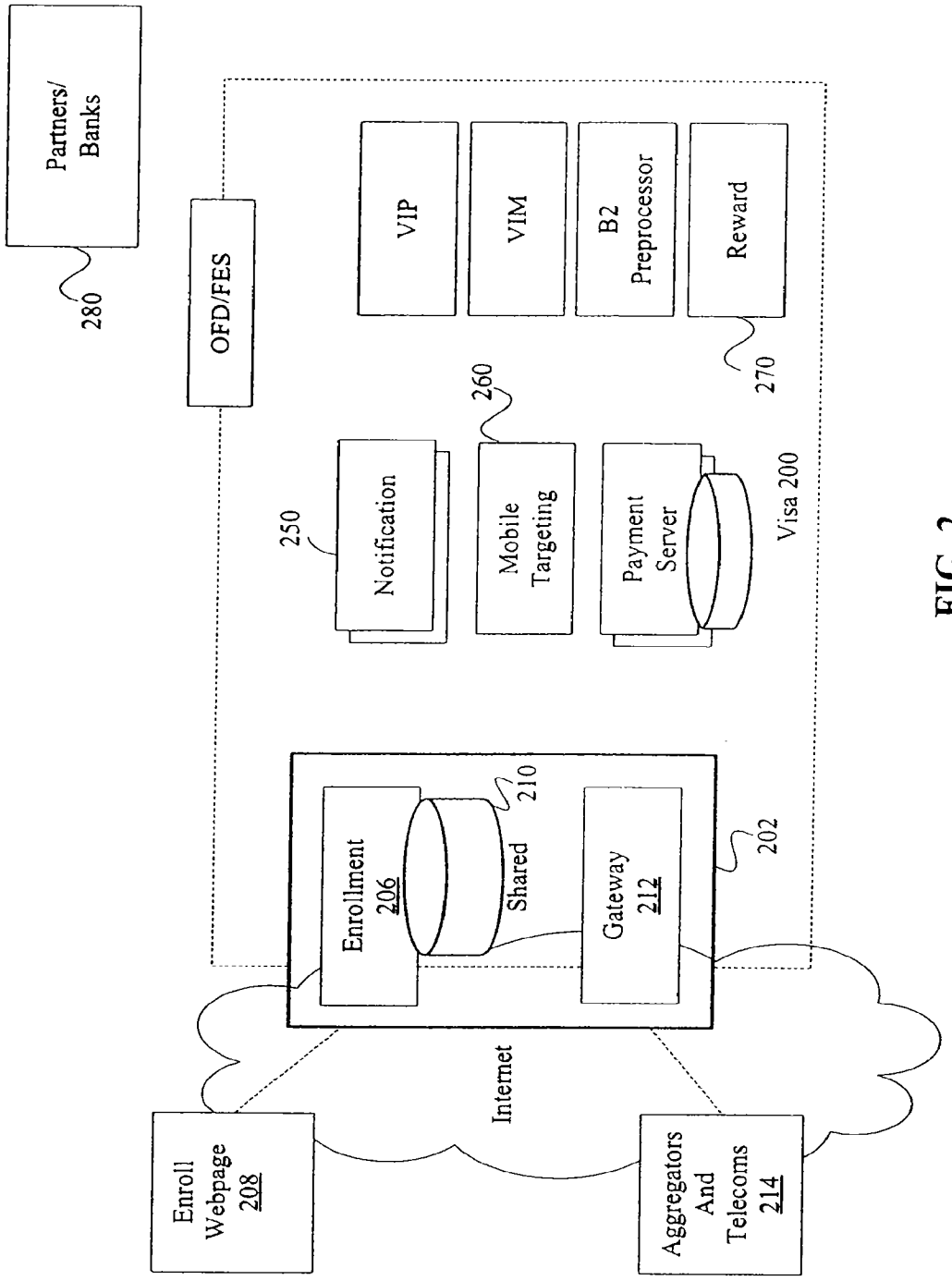

Partners/
Banks
280
OFD/FES
VIP
VIM
B2
Preprocessor
Reward
270
260
250
Notification
Mobile
Targeting
Payment
Server
Visa 200
Enrollment
206
Shared
210
Gateway
212
202
Internet
Enroll
Webpage
208
Aggregators
And
Telecoms
214

FIG. 2

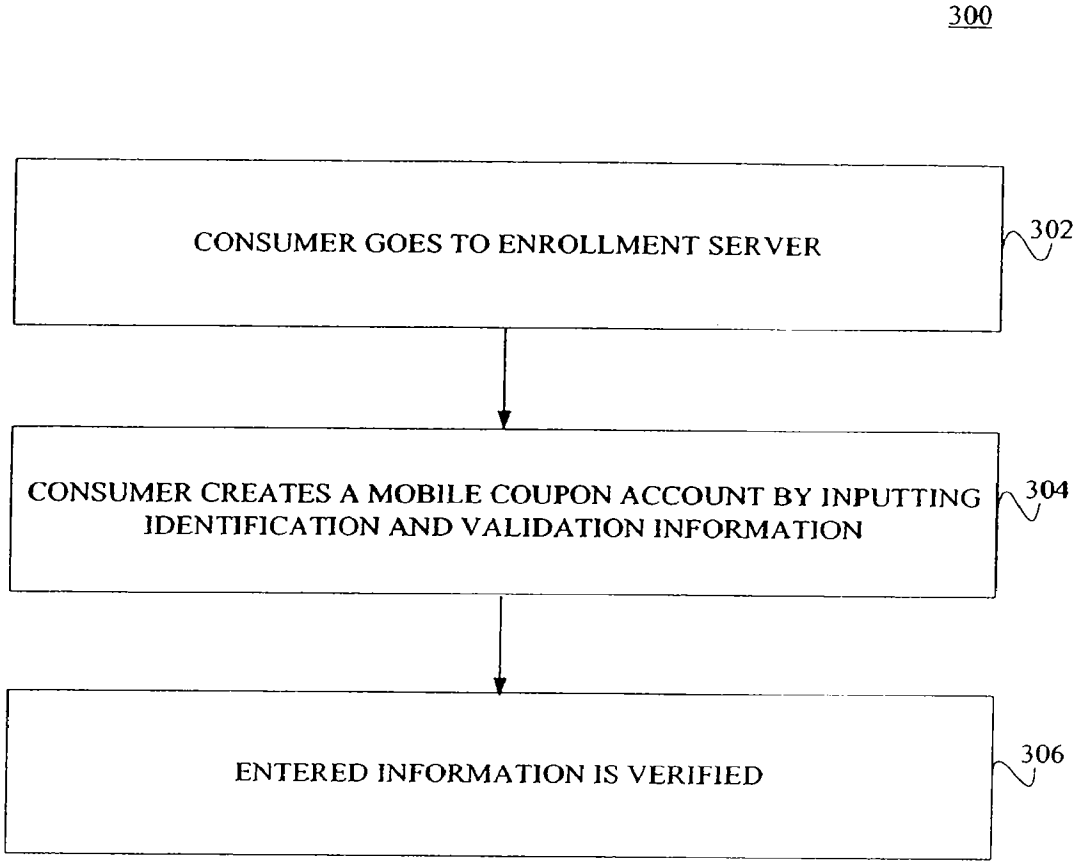

300
CONSUMER GOES TO ENROLLMENT SERVER
302
CONSUMER CREATES A MOBILE COUPON ACCOUNT BY INPUTTING IDENTIFICATION AND VALIDATION INFORMATION
304
ENTERED INFORMATION IS VERIFIED
306

FIG. 3

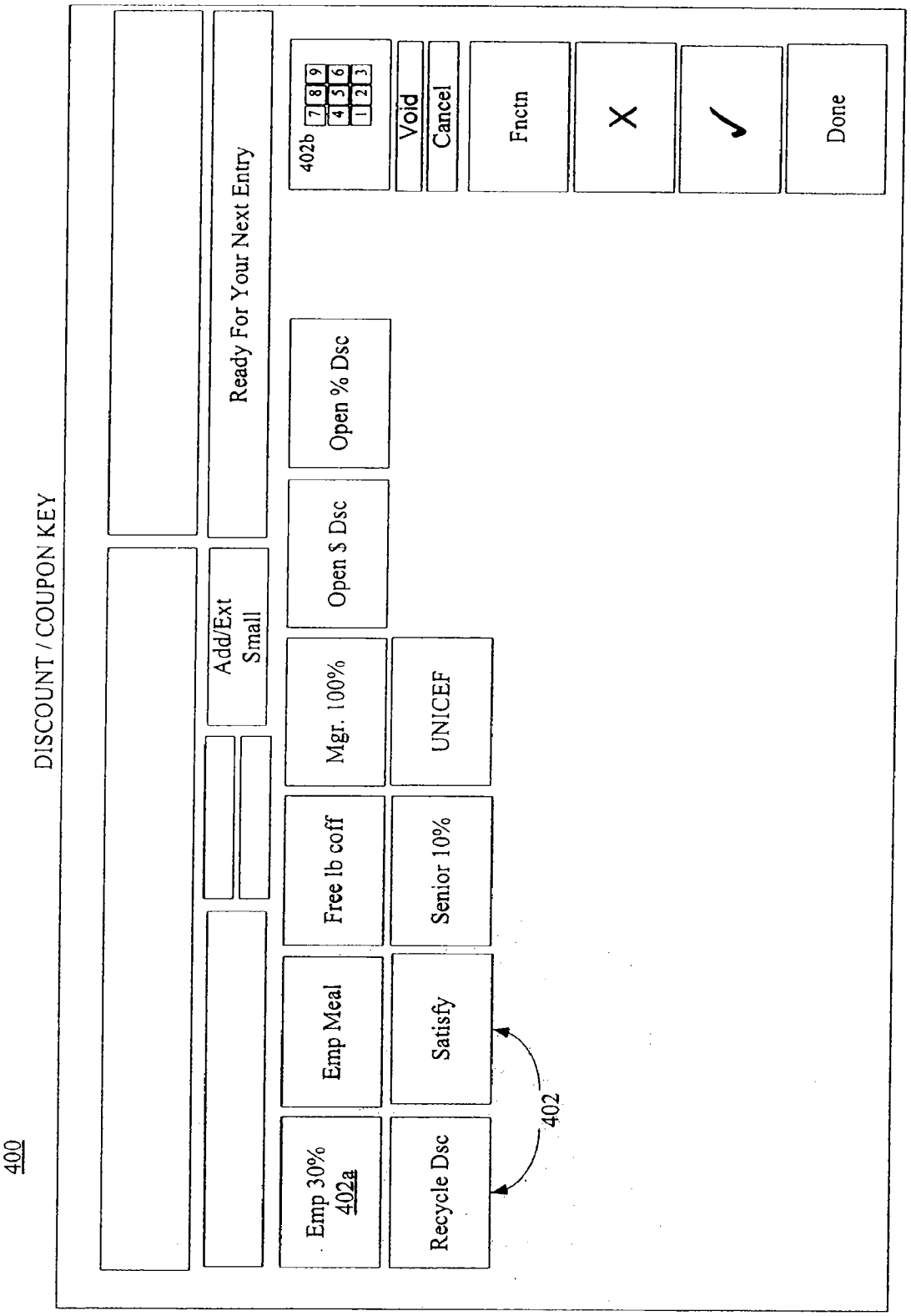

400
DISCOUNT / COUPON KEY
Ready For Your Next Entry
Add/Ext Small
Emp 30% 402a
Recycle Dsc
Emp Meal
Satisfy
Free lb coff
Senior 10%
Mgr. 100%
UNICEF
Open $ Dsc
Open % Dsc
402
402b
7 8 9
4 5 6
1 2 3
Void
Cancel
Fnctn
X
✓
Done

FIG. 4

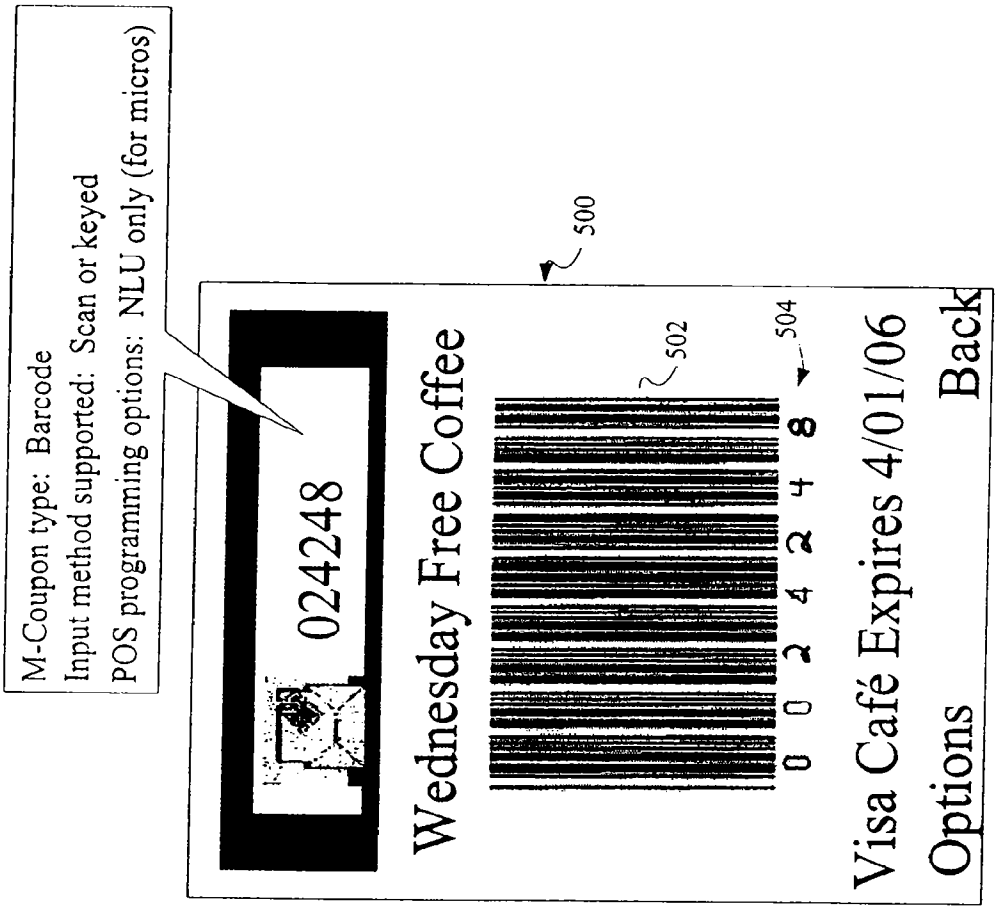

M-Coupon type: Barcode
Input method supported: Scan or keyed
POS programming options: NLU only (for micros)
024248
Wednesday Free Coffee
500
502
504
0 0 2 4 2 4 8
Visa Café Expires 4/01/06
Options
Back

FIG. 5A

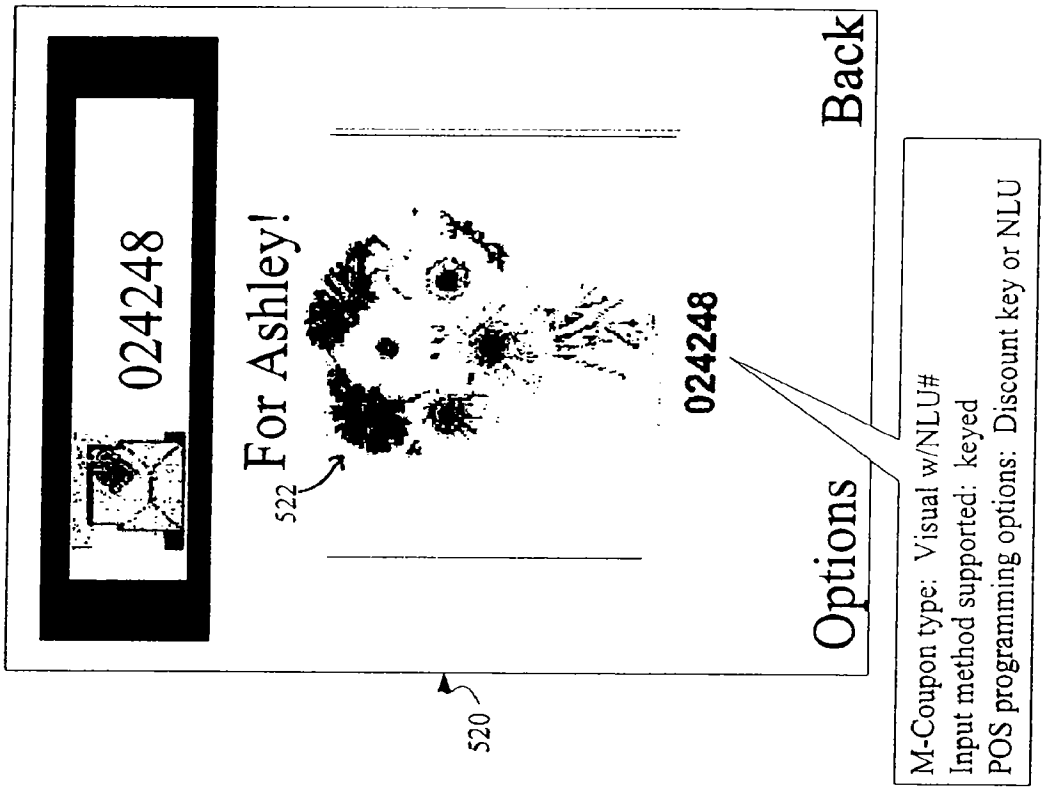

024248
For Ashley!
522
024248
Back
Options
520
M-Coupon type: Visual w/NLU#
Input method supported: keyed
POS programming options: Discount key or NLU

FIG. 5B

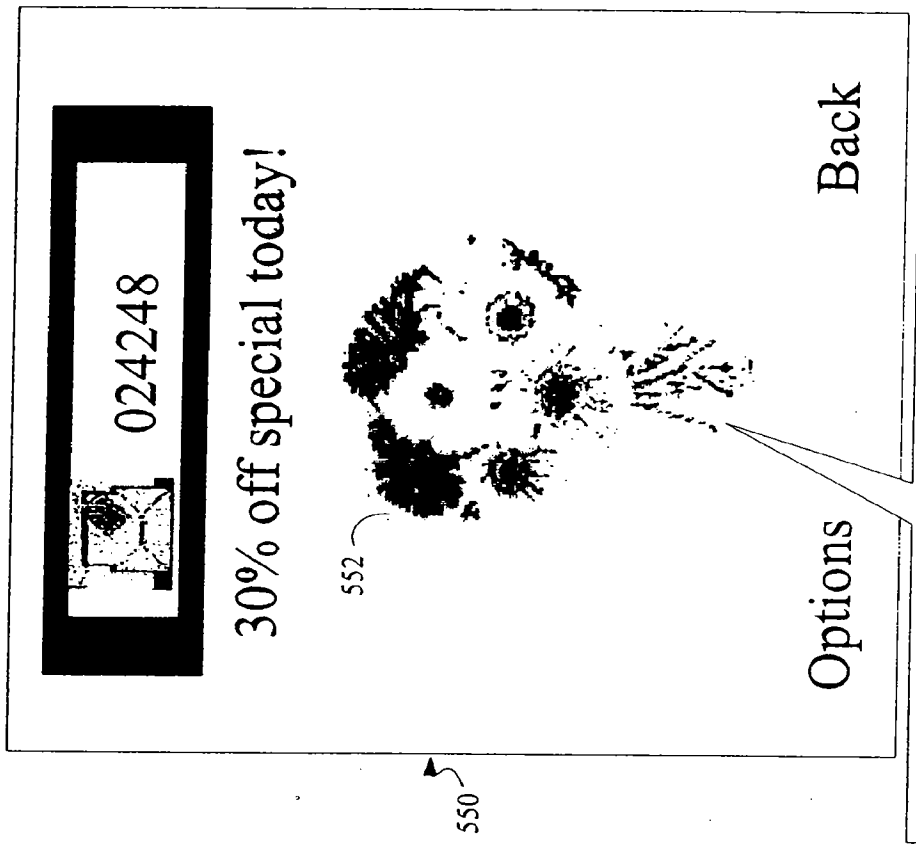

024248
30% off special today!
552
Options
Back
550
M-Coupon type: Visual only
Input method supported: Keyed (discount key)
POS programming options: Discount key for 30% off

FIG. 5C

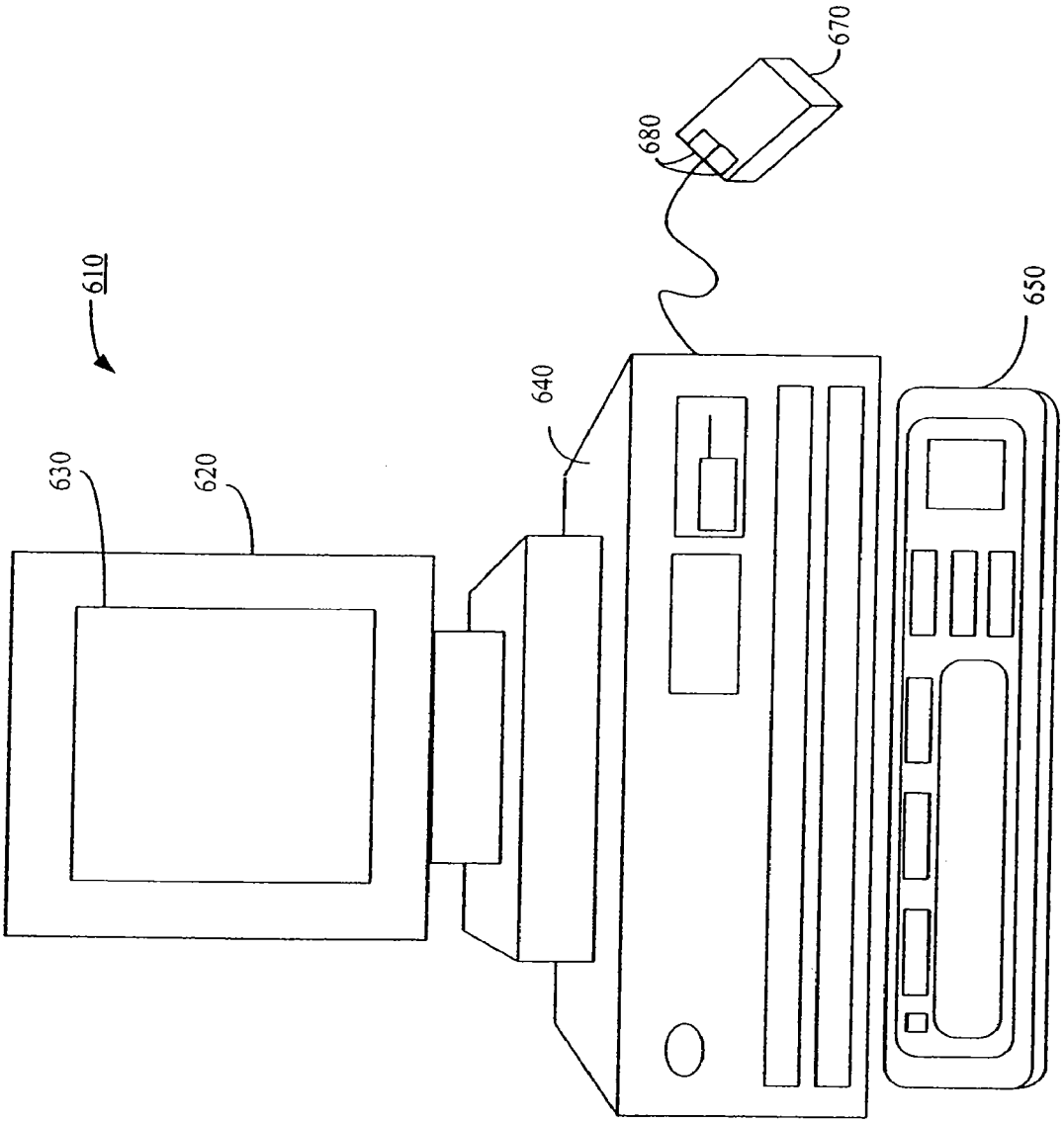


FIG. 6

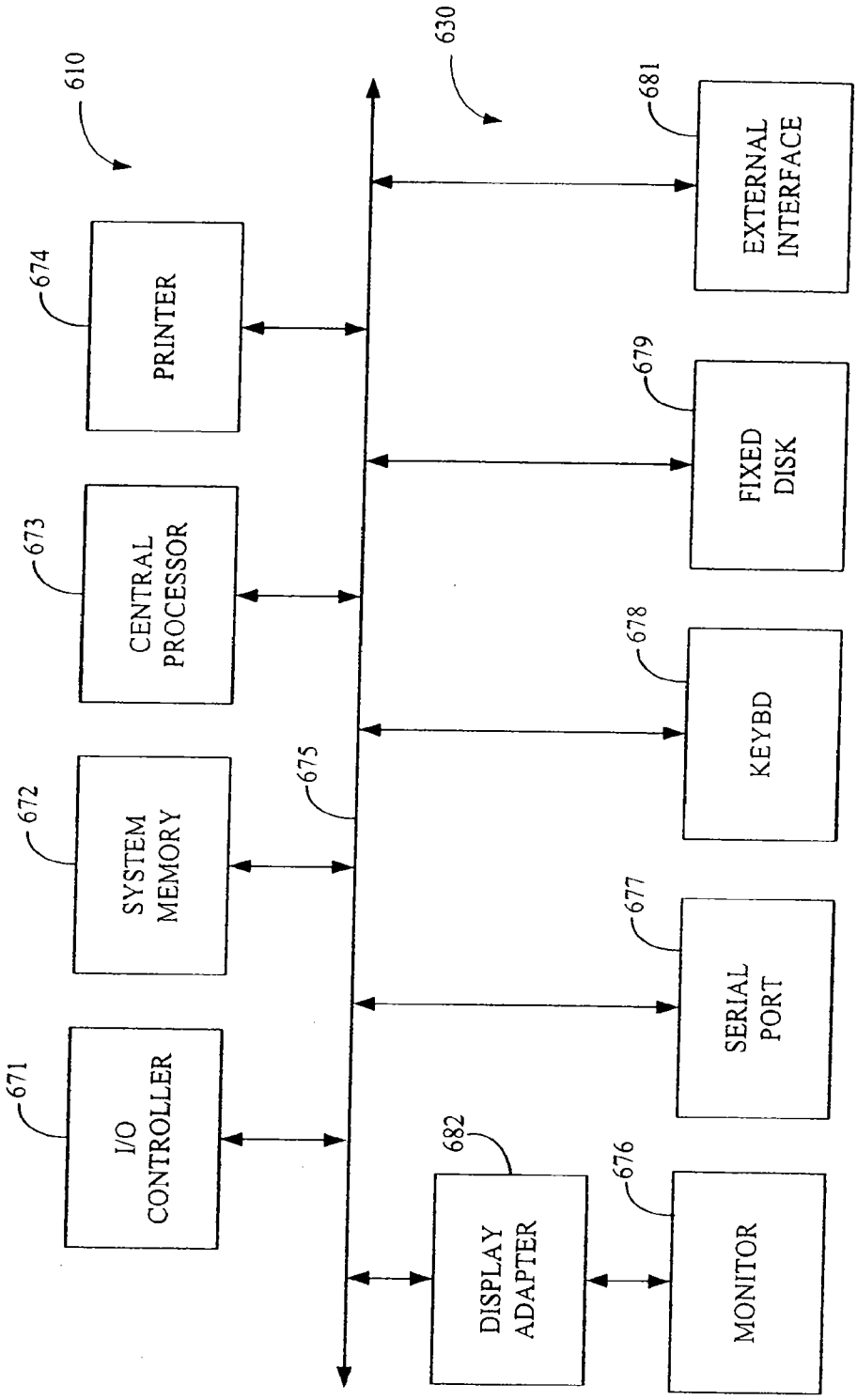

610
630
674
PRINTER
681
EXTERNAL INTERFACE
673
CENTRAL PROCESSOR
679
FIXED DISK
672
SYSTEM MEMORY
675
678
KEYBD
671
I/O CONTROLLER
677
SERIAL PORT
682
DISPLAY ADAPTER
676
MONITOR

FIG. 6A

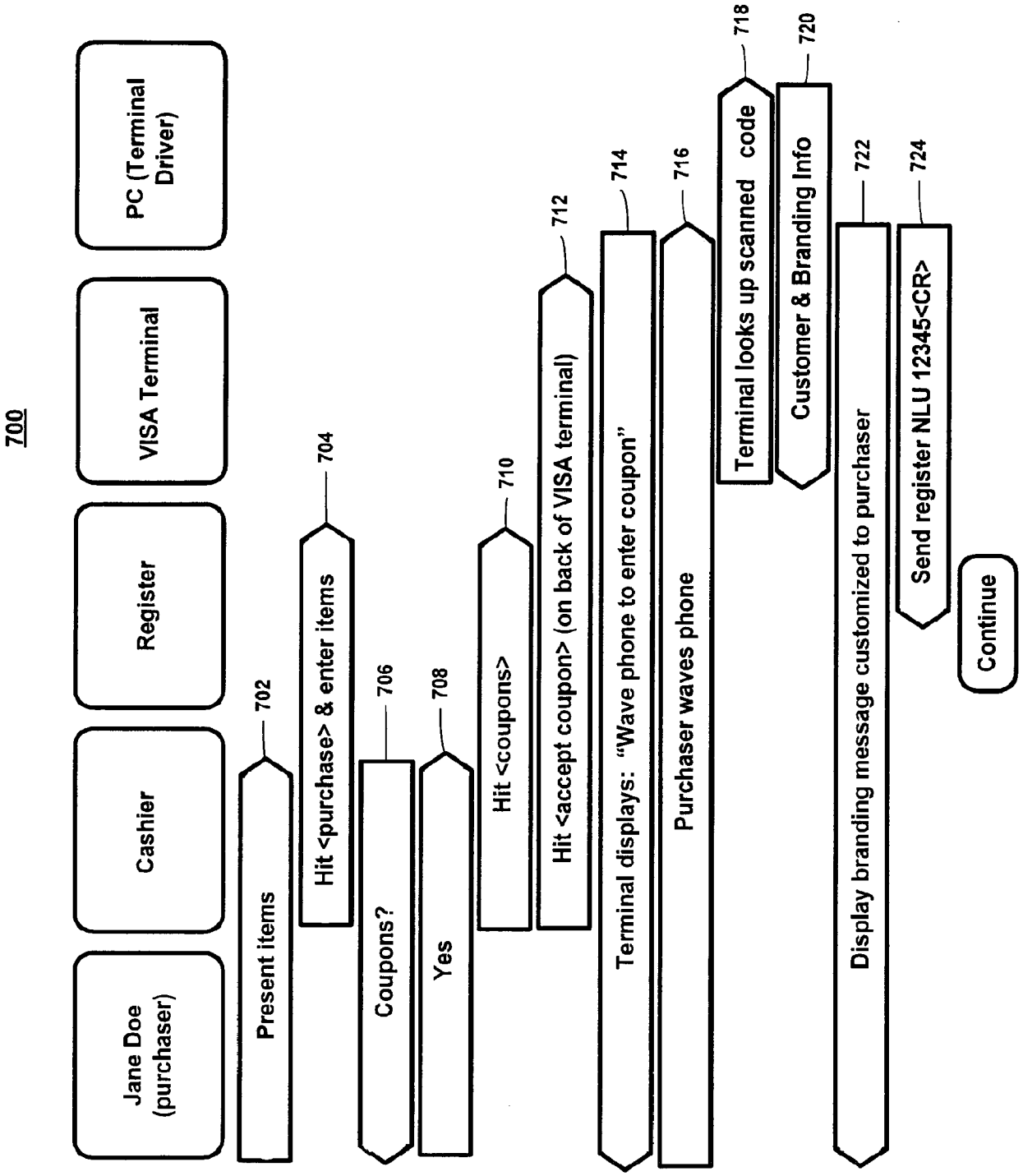

700
Jane Doe (purchaser)
Cashier
Register
VISA Terminal
PC (Terminal Driver)
Present items
702
Hit <purchase> & enter items
704
Coupons?
706
Yes
708
Hit <coupons>
710
Hit <accept coupon> (on back of VISA terminal)
712
Terminal displays: "Wave phone to enter coupon"
714
Purchaser waves phone
716
Terminal looks up scanned code
718
Customer & Branding Info
720
Display branding message customized to purchaser
722
Send register NLU 12345<CR>
724
Continue

FIG. 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 07/88687

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06Q 30/00 (2008.04)
USPC - 705/14
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)
USPC - 705/14

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC - 705/1; 705/37; 705/50; 707/104.1; 709/217

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
WEST(USPAT, USPUB, EPO, JPO, DERWENT) DialogPRO(Engineering); Google Scholar - payment and processing and network and generate and electronic and coupon and targeted and individual and consumer

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2004/0030607 A1 (Gibson) 12 February 2004 (12.02.2004), para [0011],[0018],[0006].	1-24
Y	US 2003/0004808 A1 (Elhaoussine et al.) 02 January 2003 (02.01.2003), para [0021],[0022],[0035],[0099].	1-24
A	US 2006/0282382 A1 (Balasubramanian et al.) 14 December 2006 (14.12.2006), entire document.	1-24
A	US 2006/0253390 A1 (McCarthy et al.) 09 November 2006 (09.11.2006), entie document.	1-24
A	US 2006/0224449 A1 (Byerley et al.) 05 October 2006 (05.10.2006), entire document.	1-24
A	US 2006/0149529 A1 (Nguyen et al.) 06 July 2006 (06.07.2006), entire document.	1-24

☐ 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
29 March 2008 (29.03.2008)	12 MAY 2008

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:
Lee W. Young
PCT Helpdesk: 571-272-4300
PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (April 2007)

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 July 2008 (10.07.2008)

PCT

(10) International Publication Number
WO 2008/083119 A1

(51) International Patent Classification:
G06Q 40/00 (2006.01)

(21) International Application Number:
PCT/US2007/088704

(22) International Filing Date:
21 December 2007 (21.12.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/871,898 26 December 2006 (26.12.2006) US

(71) Applicants *(for all designated States except US)*: **VISA INTERNATIONAL SERVICE ASSOCIATION** [US/US]; 900 Metro Center Boulevard, Foster City, California 94404 (US). **VISA U.S.A. INC.** [US/US]; P.O. Box 8999, M3-2B, San Francisco, California 94128 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **CARLSON, Mark** [US/US]; 153 Miramonte Avenue, Half Moon Bay, California 94019 (US). **HAMMAD, Ayman** [US/US]; 6048 Corte Montanas, Pleasanton, California 94566 (US). **FAITH, Patrick** [US/US]; 2810 Jones Gate Court, Pleasanton, California 94566 (US).

(74) Agents: **MARTINEZ-LEMKE, Sheila P.** et al.; Townsend and Townsend and Crew LLP, Two Embarcadero Center, 8th Floor, San Francisco, California 94111 (US).

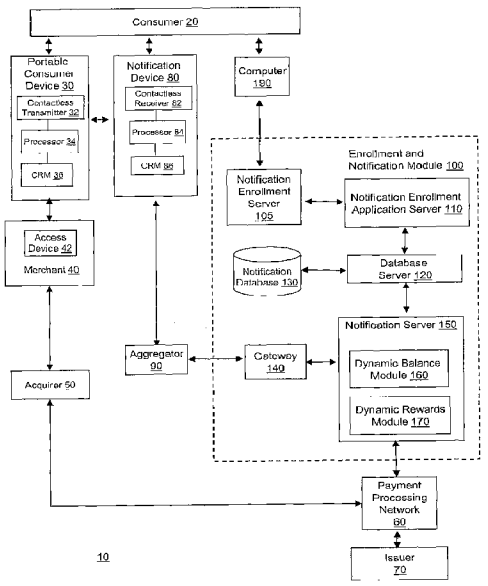
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN,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



(57) Abstract: A method and a system that receive retrieve dynamic data when a notification with dynamic data is triggered. The dynamic data is associated with an account that is associated with a portable consumer device associated with a consumer. The method and system automatically send the notification with the dynamic data to a notification device, wherein the notification with the dynamic data is provided to the consumer.

WO 2008/083119 A1

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

REAL-TIME BALANCE UPDATES

CROSS-REFERENCES TO RELATED APPLICATIONS

[0001] This is a non-provisional patent application of and claims the benefit of the filing date of U.S. Provisional Patent Application No. 60/871,898 filed on December 26, 2006. This application is herein incorporated by reference in its entirety for all purposes.

BACKGROUND

[0002] Some prior systems send consumers notices regarding current transactions. For example, an issuer may notify a consumer when their credit card is being used to make a large purchase. These prior systems often rely on contact information in the account information to notify the consumer. If, for example, only the consumer's home address is on file, the notice may not get to the consumer until well after the transaction has been completed.

[0003] Consumers with prepaid cards may want to know the balance left on their prepaid cards before a transaction or as soon as a transaction is completed. For example, a consumer may want to know whether they can afford to purchase a product with the prepaid card before they check out or even before they go to the store. Typically, a consumer contacts the issuer of their prepaid card such as a bank to determine their current balance on the prepaid card. In some cases, however, a prepaid card e.g. gift card may not be associated with an account with an issuer such as those cards purchased at retail stores. The consumer may not easily be able to get their current balance.

[0004] Embodiments of the present disclosure address these and other problems, individually and collectively.

SUMMARY OF THE INVENTION

[0005] Embodiments of the invention relate to automatic notifications, methods of providing and requesting automatic notifications, and systems that provide automatic notifications.

[0006] Embodiments of the invention address the above-noted problems by providing methods and systems of providing notifications with dynamic data to the

consumer. Dynamic data refers to information that reflects all transactions on a portable consumer device made through the time a notification is triggered. An example of dynamic data is a real-time updated account balance. Examples of dynamic data include real-time updated account balance and a real-time updated rewards information associated with an account on a portable consumer device. When triggered, a notification with dynamic data is sent to the notification device e.g. cellular phone. The notification can be triggered on a periodic basis or when the consumer uses their portable consumer device to make a transaction. The notification can also be triggered when the consumer requests the dynamic data. For example, consumer could request dynamic data by placing their portable consumer device next to their notification device so that a transmitter in the portable consumer device sends a request to a receiver in the notification device. The consumer could also request the dynamic data by selecting a programmed key on their notification device. Dynamic data is then delivered to the notification device and provided to the consumer if the consumer is enrolled to receive the notification.

[0007] An embodiment of the invention is directed to a method that retrieves when a notification with dynamic data is triggered. The dynamic data is associated with an account associated with a portable consumer device associated with a consumer. The method also automatically sends the notification to the notification device, wherein the notification with dynamic data is provided to the consumer.

[0008] Another embodiment of the invention is directed to a method that triggers a notification with dynamic data using a notification device. The dynamic data is associated with an account on a portable consumer device associated with a consumer. The method also receives the notification on the notification device.

[0009] Another embodiment of the invention is directed to a system that includes a payment processing network for generating and storing dynamic data and a notification server coupled to the payment processing network. The notification server is configured to retrieve the dynamic data from the payment processing network when a notification with dynamic data is triggered. The dynamic data is associated with an account associated with a portable consumer device associated with a consumer. The notification server is also configured to automatically send the

notification with the dynamic data to the notification device, wherein the notification with dynamic data is provided to consumer.

[0010] Another embodiment of the invention is directed to a phone having a processor, a receiver coupled to the processor, an output device coupled to the processor, and a computer readable medium coupled to the processor. The computer readable medium includes code for displaying a notification including dynamic data to the output device after a portable consumer device is used by a consumer.

[0011] These and other embodiments of the invention are described in further detail below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] FIG. 1 is a block diagram illustrating a dynamic data notification system, in accordance with an embodiment of the invention.

[0013] FIG. 2 is a flow chart illustrating a method of providing dynamic data notifications, in accordance with an embodiment of the invention.

[0014] FIG. 3 is a schematic drawing of a cellular phone displaying a real-time balance update, in accordance with an embodiment of the invention.

DETAILED DESCRIPTION

[0015] Embodiments of the invention are directed to a method of providing notifications with dynamic data, a method of requesting notifications with dynamic data, and a dynamic data notification system. More specifically, a notification with dynamic data is triggered when the consumer requests the notification or when the consumer uses the portable consumer device. The consumer can also have notifications automatically sent to the notification device on a periodic basis. Once the notification is triggered, dynamic data is retrieved and delivered to the notification device if the consumer is enrolled to receive the notification.

[0016] Certain embodiments of the invention may provide one or more technical advantages to issuers and consumers. One technical advantage to a consumer may be knowing their current balance or rewards available on their card without having to

contact the issuer which could save time and could save the consumer money. Another technical advantage to a consumer may be that the consumer can request the current balance left on their card so that they can determine whether they have sufficient funds or credit to make a purchase or complete a transaction. A technical advantage to an issuer may be that automatic notifications are sent to consumers and issuer does not have to provide notifications by other means.

[0017] Certain embodiments of the invention may include none, some, or all of the above technical advantages. One or more other technical advantages may be readily apparent to one skilled in the art from the figures, descriptions, and claims included herein.

[0018] **FIG. 1** is a block diagram illustrating a dynamic data notification system **10**, in accordance with an embodiment of the invention. Dynamic data notification system **10** includes a consumer **20**, a portable consumer device **30**, a merchant **40**, an acquirer **50**, a payment processing network **60**, an issuer **70**, a notification device **80**, an aggregator **90**, an enrollment and notification module **100**, and a computer **190**. Although one consumer **20**, one portable device **30**, one merchant **40**, one acquirer **50**, one issuer **70**, one notification device **80**, and one computer **190** are shown, there may be any suitable number of any of these entities in dynamic data notification system **10**.

[0019] Dynamic data notification system **10** includes a consumer **20** in operative communication with portable consumer device **30**. Dynamic data notification system **10** also includes a merchant **40** having an access device **42** for interacting with portable consumer device **30** and an acquirer **50** associated with merchant **40**. Acquirer **50** is in communication with issuer **70** through payment processing network **60**.

[0020] Dynamic data notification system **10** also includes a notification device **80** in operative communication with consumer **20** for displaying notifications to consumer **20** and for receiving request or instructions for notifications from consumer **20**. Notification device **80** is also in communication with portable consumer device **30** for receiving a request for a notification from consumer **20**.

[0021] Dynamic data notification system **10** also includes an enrollment and notification module **100** for processing notifications and an aggregator **90** for

collecting and forwarding notifications from enrollment and notification module **100** to notification device **80**. Dynamic data notification system **10** also includes a computer **190** in communication with enrollment notification module **100** and consumer **20**. Consumer can use computer **190** to receive notifications and to enroll in notifications. Dynamic data notification system **10** also includes a payment processing network **60** that is in communication with enrollment and notification module **100**, with acquirer **50**, and with issuer **70**.

[0022] Consumer **20** refers to an individual or organization such as a business that is capable of purchasing goods or services or making any suitable transaction with merchant **40**.

[0023] Portable consumer device **30** refers to any suitable device that allows the transaction to be conducted with merchant **40**. Portable consumer device **30** may be in any suitable form. For example, suitable portable consumer devices **30** can be hand-held and compact so that they can fit into a consumer's wallet and/or pocket (e.g., pocket-sized). They may include smart cards, magnetic stripe cards, keychain devices (such as the Speedpass™ commercially available from Exxon-Mobil Corp.), etc. Other examples of portable consumer devices **30** include cellular phones, personal digital assistants (PDAs), pagers, payment cards, security cards, access cards, smart media, transponders, and the like. In some cases, portable consumer device **30** may be associated with an account of consumer **20** such as a bank account.

[0024] In the illustrated example, portable consumer device **30** includes a contactless transmitter **32** for sending wireless signals, a processor **34**, and a computer readable medium (CRM) **36**. These elements of portable consumer device **30** are in communication with each other. Processor **34** (e.g., a microprocessor) processes the functions of portable consumer device **30**.

[0025] Contactless transmitter **32** refers to any suitable device for sending wireless signals with information stored in memory (e.g. CRM **36**) on portable consumer device **30** to notification device **80**. Contactless transmitter **32** transmits signals using a near field communications (NFC) capability to send information from portable consumer device **30** to the contactless receiver **82** on notification device **82**. Typically, NFC capability is in accordance with a standardized protocol or data

transfer mechanism (e.g., ISO 14443/NFC). Some examples of NFC capability are radio-frequency identification (RFID), Bluetooth™, infra-red, and other suitable communications capability. In other embodiments, contactless transmitter **32** transmits information via a cellular network by means of an interface (not shown). The interface functions to permit exchange of data between the cellular network (not shown) and contactless transmitter **32**.

[0026] CRM **36** may be on the body of portable consumer device **30**. The body may in the form of a plastic substrate, a housing, or other structure. CRM **36** may be a memory that stores data and may be in any suitable form. Exemplary CRM **36** may be in any suitable form including a magnetic stripe, a memory chip, etc. If portable consumer device **30** is in the form of a card, it may have an embossed region (ER) which is embossed with a PAN (primary account number). CRM **36** may electronically store the PAN as well as other data such as PIN data.

[0027] Merchant **40** refers to any suitable entity or entities that makes a transaction with consumer **20**. Merchant **40** may use any suitable method to make the transaction. For example, merchant **40** may use an e-commerce business to allow the transaction to be conducted by merchant **40** through the Internet. Other examples of merchant **40** include a department store, a gas station, a drug store, a grocery store, or other suitable business.

[0028] Access device **42** may be any suitable device for communicating with merchant **40** and for interacting with portable consumer device **30**. Access device **42** can be in any suitable location such as at the same location as merchant **40**. Access device **42** may be in any suitable form. Some examples of access devices **42** include POS devices, cellular phones, PDAs, personal computers (PCs), tablet PCs, handheld specialized readers, set-top boxes, electronic cash registers (ECRs), automated teller machines (ATMs), virtual cash registers (VCRs), kiosks, security systems, access systems, websites, and the like. Access device **42** may use any suitable contact or contactless mode of operation to send or receive data from portable consumer devices **30**.

[0029] If access device **42** is a POS terminal, any suitable POS terminal may be used and may include a reader, a processor, and a computer readable medium. Reader may include any suitable contact or contactless mode of operation. For

example, exemplary card readers can include radio frequency (RF) antennas, optical scanners, bar code reader, magnetic stripe readers, etc. to interact with portable consumer device **30**.

[0030] Acquirer **50** refers to any suitable entity that has an account with merchant **40**. In some embodiments, issuer **70** may also be acquirer **50**.

[0031] Issuer **70** refers to any suitable entity that may open and maintain an account associated with portable consumer device **30** for consumer **20**. Some examples of issuers may be a bank, a business entity such as a retail store, or a governmental entity. In many cases, issuer **70** may also issue portable consumer device **30** associated with the account to consumer **20**.

[0032] Payment processing network **60** refers to a network of suitable entities that have information related an account associated with portable consumer device **30**. This information includes data associated with the account on portable consumer device **30** such as profile information, dynamic data, and other suitable information. Dynamic data refers to any suitable information that is updated to reflect the transactions made using portable consumer device **30**.

[0033] Although not shown in the illustrated embodiment, payment processing network **60** may have or operate a server computer and may include a database. The database may include any hardware, software, firmware, or combination of the preceding for storing and facilitating retrieval of information. Also, the database may use any of a variety of data structures, arrangements, and compilations to store and facilitate retrieval of information. The server computer may be coupled to the database and may include any hardware, software, other logic, or combination of the preceding for servicing the requests from one or more client computers. Server computer may use any of a variety of computing structures, arrangements, and compilations for servicing the requests from one or more client computers. In one embodiment, the server computer may be a powerful computer or cluster of computers. For example, the server computer can be a large mainframe, a minicomputer cluster, or a group of servers functioning as a unit. In one example, the server computer may be a database server coupled to a Web server. Server computer services the requests of one or more client computers.

[0034] Payment processing network **60** may include data processing subsystems, networks, and operations used to support and deliver authorization services, exception file services, and clearing and settlement services. An exemplary payment processing network **60** may include VisaNet™. Networks that include VisaNet™ are able to process credit card transactions, debit card transactions, and other types of commercial transactions. VisaNet™, in particular, includes a VIP system (Visa Integrated Payments system) which processes authorization requests and a Base II system which performs clearing and settlement services. Payment processing network **60** may use any suitable wired or wireless network, including the Internet.

[0035] Notification device **80** refers to any suitable device for receiving notifications and for providing the notifications to consumer **20**. Notifications refer to communications of dynamic data to consumer **20** on notification device **80**. Notifications may be in any suitable form and may be delivered by any suitable method. Some examples of notifications includes a phone call, a voice message, a voicemail message, a short message service (SMS) message e.g. a text message, an instant messaging (IM) message, or an email message, or a periodically updated display on a device. An exemplary embodiment of a notification is a real-time balance update. The real-time balance update is a communication to notify consumer **20** of the funds available (balance) on portable consumer device **30** after the last transaction is accounted for. Another embodiment of a notification is real-time rewards information update that is a communication to notify consumer **20** of rewards available for redemption after the last transaction.

[0036] Dynamic data refers to any suitable information that reflects all transactions on a portable consumer device **30** made through the time a notification of the dynamic data is triggered. Dynamic data relates to an account associated with a portable consumer device **30** associated with consumer **20**. For example, dynamic data can be account balances such as credit card account balances, stored value account balances, rewards balances, checking account balances, savings account balances, investment account balances, brokerage account balances, and other suitable account balances.

[0037] Notification device **80** may be in any suitable form. For example, suitable notification devices **80** can be hand-held and compact so that they can fit into a consumer's wallet and/or pocket (e.g., pocket-sized). Some examples of notification device **80** include desktop or laptop computers, cellular phones (e.g., as shown in FIG. 3), personal digital assistants (PDAs), pagers, payment cards, security cards, access cards, smart media, transponders, and the like. In some embodiments, notification device **80** and portable consumer device **30** are embodied in the same device.

[0038] Notification device **80** includes a contactless receiver **82** for receiving wireless signals, a processor **84** coupled to the receiver **82**, and a computer readable medium (CRM) **36** coupled to processor **84**. Although not shown, notification device **80** may also include one or more input devices (e.g., keypads) or output devices (e.g., displays, speakers) coupled to processor **84**. Contactless receiver **82** refers to any suitable device for receiving wireless signals. The signals are received by contactless receiver **82** by any suitable method (e.g., using NFC capability). In one example, contactless receiver **82** receives a wireless signal with a request for a notification from contactless transmitter **32** of portable consumer device **30**. In another example, contactless receiver **82** receives a wireless signal with a notification(s) from aggregator **90** via a cellular network. Processor **84** (e.g., a microprocessor) processes the functions of notification device **80**. CRM **86** comprises code for processing requests for notifications, for receiving notifications, and for providing notifications to consumer **20**. An example of code for providing notifications to consumer **20** includes code for displaying notifications including dynamic data to an output device.

[0039] Consumer **20** uses computer **190** to receive notifications and/or enroll in a program to receive notifications. Computer **190** can be a desktop computer, a laptop computer, a cellular or mobile phone, a personal digital assistant (PDA), or other suitable device.

[0040] Enrollment and notification module **100** comprises a notification enrollment server **105**, a notification enrollment application server **110**, a database server **120**, a notification database **130**, a notification server **150** having a dynamic balance module **160** and a dynamic rewards module **170**, and a gateway **140**. Notification

enrollment server **105** in communication with a notification enrollment application server **110** which is in communication with database server **120** for storing and retrieving information to and from notification database **130**. Database server **120** is also in communication with notification server **150**. Notification server **150** is also in communication with gateway **140**, dynamic balance module **160**, and dynamic rewards module **170**. Although enrollment and notification module **100** is shown as being separate from issuer **70**, enrollment and notification module **100** can be at issuer **70** in some embodiments. In these embodiments, issuer **70** processes the notifications sent to notification device **80**.

[0041] Notification enrollment server **105** refers to a device that receives enrollment information from consumer **20** via computer **190** and sends the enrollment information to notification enrollment application server **110**. Notification enrollment application server **110** receives the enrollment information from consumer **20** through notification enrollment server **105** or from issuer **70** and may store the enrollment information in notification database **130**. Notification database **130** may receive and store new or updated enrollment information and other account information.

[0042] Enrollment information includes trigger information that describes the occurrences that must take place to trigger notifications and the types of dynamic data that consumer **20** wants to receive in the notifications. Consumer **20** may define the trigger information when enrolling in a program to receive notifications.

[0043] In some cases, notifications are triggered by actions taken by consumer **20** or another suitable entity. For example, a notification may be triggered by using of portable consumer device **30** at access device **42** by consumer **20** or by merchant **40**. In another example, a notification may be triggered by the sending of a request by consumer **20** for a notification using portable consumer device **30**, notification device **80**, computer **190**, or other suitable device. In yet another example, a notification may be triggered by placing portable consumer device **30** near notification device **80** so that a signal with a request for a notification is transmitted from contactless transmitter **32** on portable consumer device **30** to contactless receiver **82** on notification device **80**. In another example, a notification may be triggered by the completion of a transaction on an account associated with portable

consumer device **30**. In other cases, periodic notifications may be triggered by the termination a time period defined by consumer **20**. Examples of a time period include a week, a day, and an hour. For example, if consumer **20** selects the time period of a day, daily notifications will be sent to notification device **80**. Typically, daily notifications would be sent at approximately the same time every day.

[0044] Notification server **150** includes dynamic balance module **160** for processing notifications with dynamic balances and dynamic rewards module **170** for processing notifications with dynamic rewards information.

[0045] Notification server **150** processes notifications with dynamic data and sends the notifications through gateway **140** to aggregator **90**. If the dynamic data is a dynamic balance, dynamic balance module **160** processes the notification. If the dynamic data is dynamic rewards, dynamic rewards module **170** processes the notification. Gateway **140** is a any suitable device that converts information from the protocol or format used in enrollment and notification module **100** to those used in aggregator **90**. Aggregator **90** refers to any suitable entity or device that receives notifications, collects the notifications, and transmits the notifications to notification device **80** for consumer **20**. In some cases, aggregator **90** may be a wireless telephone company.

[0046] Notification server **150** is triggered to send a notification with dynamic data and processes the notification. Notification server **150** retrieves enrollment information with trigger information from notification database **130** using database server **120**. Notification server **150** confirms that consumer **20** is enrolled to receive the notification triggered based on the trigger information. Notification server **150** retrieves the dynamic data from issuer **70** or other suitable entity and sends the notification with the dynamic data through gateway **140** to aggregator **90**. Aggregator **90** collects notifications according to enrollment information and forwards the notifications to notification device **80**. If the notification triggered is associated with dynamic balance data, dynamic balance module **160** processes the notification. If the notification triggered is associated with dynamic rewards data, dynamic rewards module **170** processes the notification.

[0047] In one example embodiment, consumer **20** enrolls in a program using computer **190** to receive notifications on their notification device **80** (e.g. a cellular

phone) in the form of text or voice messages. Consumer **20** enrolls to receive notifications with the dynamic balance on the account associated with their portable consumer device **30** (e.g. a prepaid or gift card). Consumer **20** specifies that the notification will be sent every time portable consumer device **30** interacts with access device **42**.

[0048] In a typical payment transaction, consumer **20** uses portable consumer device **30** at access device **42** to purchase goods or services from merchant **40**. For example, a consumer may use a gift card with $50 to buy a $25 game cartridge at a toy store using a POS (point of sale) terminal at the toy store. The consumer may swipe the gift card through a slot in the POS terminal and the POS terminal may read data including an account number from the gift card.

[0049] An authorization request message is then forwarded to acquirer **50** and acquirer **50** forwards the message through payment processing network **60** to issuer **70**. Using portable consumer device **30** at access device **42** triggers notification server **150** to send a notification.

[0050] Issuer **70** determines whether or not to authorize the transaction. The transaction may be authorized if there are sufficient funds, and may be declined if there are insufficient funds. An authorization response message is then sent back through payment processing network **60** to acquirer **50** who forwards it to merchant **40**. At the end of the day, a normal clearing and settlement process can be conducted by payment processing network **60**. A clearing process is a process of exchanging financial details between and acquirer and an issuer to facilitate posting to a consumer's account and reconciliation of the consumer's settlement position.

[0051] In this example, the notification triggered is associated with a dynamic balance and dynamic balance module **160** processes the notification. Dynamic balance module **160** is triggered to send a notification when consumer used portable consumer device **30**. For example, dynamic balance module **160** may receive information that the previously described and registered gift card has been used to purchase a $25 game cartridge.

[0052] Dynamic balance module **160** retrieves enrollment information with trigger information from notification database **130** using database server **120**. Dynamic balance module **160** uses the trigger information to confirm that consumer **20** wants

to receive the notification that has been triggered. Dynamic balance module **160** also determines from the trigger information that consumer **20** wants to receive the triggered notification in the form of a text message. Dynamic balance module **160** retrieves the dynamic balance on the account associated with portable consumer device **30**. For example, the module **160** may determine that there is the balance on the gift card is $25. The dynamic balance will reflect the last transaction authorized including the transaction associated with the action of using portable consumer device **30** that triggered the notification. Dynamic balance module **160** sends a text message with the dynamic balance to notification device **80**. For example, the text message may indicate that the gift card now has a balance of $25 after buying the $25 game cartridge. Notification device **80** provides the text message to consumer **10**. For example, the consumer's phone may display the balance of $25 plus the account number associated with the gift card. Consumer **20** may thereafter store this information in the notification device **80** for future use in determining how much money is left on the portable consumer device **30**.

[0053] Modifications, additions, or omissions may be made to dynamic data notification system **10** without departing from the scope of the disclosure. The components of dynamic data notification system **10** may be integrated or separated according to particular needs. Moreover, the operations of dynamic data notification system **10** may be performed by more, fewer, or other system modules. Additionally, operations of dynamic data notification system **10** may be performed using any suitable logic comprising software, hardware, other logic, or any suitable combination of the preceding.

[0054] **FIG. 2** is a flow chart illustrating a method of providing dynamic data notifications, in accordance with an embodiment of the invention.

[0055] Consumer **20** enrolls in a program using computer **190** to receive notifications on their portable consumer device **30** (step **200**). Computer **190** sends enrollment information from consumer **20** to notification enrollment server **105**. Notification enrollment server **105** sends the enrollment information to notification enrollment application server **110**. Notification enrollment application server **110** sends the enrollment information to database server **120** to store it in notification database **130**.

[0056] A notification is triggered (step **210**). Notification server **150** detects that the notification has been triggered. Consumer **20** or other suitable entity triggers the notification.

[0057] In one embodiment, consumer **20** or other suitable entity triggers a notification by using portable consumer device **30** at access device **42**. In some cases, a notification is only triggered if the transaction is authorized and completed. When portable consumer device **30** is used, information indicating that a notification has been triggered is sent from access device **42** to acquirer **50** which forwards it to notification server **150** through payment processing network **60**.

[0058] In another embodiment, consumer **20** triggers a notification by requesting it on notification device **80** or computer **190** which forwards the request for a notification to notification server **150**. For example, consumer **20** may request a notification by selecting a programmed button on their cellular phone. The cellular phone sends the request to notification server **150**.

[0059] In another embodiment, consumer **20** triggers a notification by placing portable consumer device **30** next to notification device **80**. A signal with a request for a notification is emitted from contactless transmitter **32** in portable consumer device **30** and received by contactless receiver **82** on notification device **80**. Notification device **80** forwards the request to notification server **150**.

[0060] In yet another embodiment, a notification is triggered automatically on a periodic basis by notification server **150**. Typically, the notification is triggered at the end of the time period although any time during that time period can be used. Consumer **20** selects the time period such as daily, hourly, or weekly. For example, consumer **20** can select daily notifications sent at 12:00 a.m.

[0061] In one example embodiment, consumer **20** enrolls in a program using computer **190** to receive notifications on their notification device **80** e.g. cellular phone in the form of email messages. Consumer **20** enrolls to receive notifications with the dynamic balance on the account on their portable consumer device **30** e.g. a prepaid card. Consumer **20** specifies that the notification will be sent every time portable consumer device **30** interacts with access device **42**.

[0062] Notification server **150** retrieves enrollment information (step **220**) retrieved from notification database **130** using database server **120**. The enrollment information is associated with an account on portable consumer device **30**. In embodiments where consumer **20** requested the notification, notification server **150** may skip retrieving the enrollment information and checking enrollment for the notification (steps **220** and **230**) and go to retrieving dynamic data (step **240**).

[0063] Notification server **150** analyzes trigger information in the enrollment information to determine whether consumer **20** is enrolled to receive the notification that has been triggered (step **230**). If consumer **20** is not enrolled for the notification, the method ends (step **270**) and a notification is not sent to consumer **20**.

[0064] If consumer **20** is enrolled to receive the notification, notification server **150** retrieves the dynamic data (step **240**). Notification server **150** generates a notification with the dynamic data and sends it to aggregator **90** through gateway **140**. Aggregator **90** forwards the notification to notification device **160** for delivery to consumer **20** (step **250**). Notification device **80** provides the notification to consumer **20** (step **260**).

[0065] In one embodiment, the notification may be shown to consumer **20** on a screen on notification device **80**. The display of the notification may be a text message displayed on a screen or other suitable display until consumer **20** turns off the display. In other cases, the notification may be displayed for a predetermined period of time.

[0066] In another embodiment, the notification may be sent to consumer in the form of a voice message or voicemail message to consumer **20**. For example, the notification may be an automated voice announcement that is sent to the notification device **20**.

[0067] After providing the notification, the method ends (step **270**). Modifications, additions, or omissions may be made to the method without departing from the scope of the disclosure. The method may include more, fewer, or other steps. Additionally, steps may be performed in any suitable order without departing from the scope of the disclosure.

[0068] FIG. 3 is a schematic drawing of a cellular phone displaying a real-time balance update, in accordance with an embodiment of the invention. Notification device **80** includes a display **320** for displaying information such as notifications with dynamic data, buttons **330** for inputting information such as requests for notifications, a speaker (not shown) to send aural signals to consumer **20**, and a microphone (not shown) to receive aural signals from consumer **20**.

[0069] Display **320** includes a dynamic data display **322** for displaying the notification of the updated dynamic data consumer **20**. In the illustrated example, dynamic data display **322** is showing the real-time balance update on the account associated with portable consumer device **30**. Dynamic data can be updated at any suitable time. Some examples of when the dynamic data is updated include when consumer requests the dynamic data, when consumer **20** uses portable consumer device **30**, or periodically.

[0070] Buttons **330** include a balance request button **334** for requesting a real-time balance update and a rewards request button **336** for requesting a real-time rewards information update. Display **320** also includes a balance request button indicator **324** indicating that selecting balance request button **334** will request a real-time balance update. Display **320** also includes a rewards request button indicator **326** indicating that selecting rewards request button **336** will request a real-time rewards information update.

[0071] In operation, consumer **20** selects balance request button **334** to display real-time balance update on dynamic data display **322**. The request is forwarded to notification server **150**. Notification server **150** retrieves the real-time balance from issuer **70** or other suitable entity over payment processing network **60**. Notification server **150** sends the real-time balance update to notification device **80** and notification device **80** displays the update to consumer **20**.

[0072] Modifications, additions, or omissions may be made to notification device **80** without departing from the scope of the disclosure. For example, notification device **80** and portable consumer device **30** may be integrated into the same device. Also, the components of notification device **80** may be integrated or separated according to particular needs. Moreover, the operations of notification device **80** may be performed by more, fewer, or other modules. Additionally, operations of notification

device **80** may be performed using any suitable logic comprising software, hardware, other logic, or any suitable combination of the preceding.

[0073] It should be understood that the present disclosure as described above can be implemented in the form of control logic using computer software in a modular or integrated manner. Based on the disclosure and teachings provided herein, a person of ordinary skill in the art will know and appreciate other ways and/or methods to implement the present disclosure using hardware and a combination of hardware and software.

[0074] Any of the software components or functions described in this application, may be implemented as software code to be executed by a processor using any suitable computer language such as, for example, Java, C++ or Perl using, for example, conventional or object-oriented techniques. The software code may be stored as a series of instructions, or commands on a computer readable medium, such as a random access memory (RAM), a read only memory (ROM), a magnetic medium such as a hard-drive or a floppy disk, or an optical medium such as a CD-ROM. Any such computer readable medium may reside on or within a single computational apparatus, and may be present on or within different computational apparatuses within a system or network.

[0075] A recitation of "a", "an" or "the" is intended to mean "one or more" unless specifically indicated to the contrary.

[0076] The above description is illustrative and is not restrictive. Many variations of the disclosure will become apparent to those skilled in the art upon review of the disclosure. The scope of the disclosure should, therefore, be determined not with reference to the above description, but instead should be determined with reference to the pending claims along with their full scope or equivalents.

[0077] One or more features from any embodiment may be combined with one or more features of any other embodiment without departing from the scope of the disclosure.

WHAT IS CLAIMED IS:

1. A method comprising:

when a notification with dynamic data is triggered, retrieving the dynamic data associated with an account associated with a portable consumer device associated with a consumer; and

automatically sending the notification with the dynamic data to a notification device, wherein the notification with the dynamic data is provided to the consumer.

2. A method of Claim 1, wherein the dynamic data is a real-time balance update.

3. A method of Claim 1, wherein the dynamic data is a real-time rewards information update.

4. A method of Claim 1, further comprising:

retrieving enrollment information; and

confirming that consumer is enrolled to receive the notification based on the enrollment information.

5. A method of Claim 1,

wherein the notification is triggered by a transaction being conducted using a portable consumer device associated with the consumer, and

wherein the dynamic data is based on an amount of the transaction being conducted.

6. A method of Claim 1,

wherein the notification is triggered based on a time period predefined by the consumer,

wherein automatically sending the notification to the notification device includes periodically sending the notification to the notification device based on the predefined time period.

7. A method of Claim 1, wherein the notification is triggered by a request for the notification with dynamic data sent from the notification device.

8. A method of Claim 1, wherein the notification is triggered by a signal sent from a contactless transmitter on portable consumer device to a contactless receiver on the notification device.

9. A method of Claim 1, wherein the notification with dynamic data is provided to consumer on a display.

10. A method of Claim 1,

wherein the notification device is a phone, and

wherein the notification sent to the notification device includes at least one of a phone call, voicemail, SMS, IM, or email.

11. A method comprising:

triggering a notification with dynamic data using a notification device, the dynamic data associated with an account associated with a portable consumer device associated with a consumer; and

receiving the notification on the notification device.

12. A system comprising:

a payment processing network for generating and storing dynamic data; and

a notification server coupled to the payment processing network, the notification server configured to:

when a notification with dynamic data is triggered, retrieve the dynamic data from the payment processing network, the dynamic data associated with an account associated with a portable consumer device associated with a consumer;

automatically send the notification with the dynamic data to the notification device, wherein the notification with dynamic data is provided to consumer.

13. The system of Claim 12, wherein the notification server is further configured to:

retrieve enrollment information; and

confirm that consumer is enrolled to receive the notification based on the enrollment information.

14. The system of Claim 12,

wherein the notification is triggered by a transaction being conducted using a portable consumer device associated with the consumer, and

wherein the dynamic data is based on an amount of the transaction being conducted.

15. The system of Claim 12,

wherein the notification is triggered based on a time period predefined by the consumer, and

wherein automatically sending the notification to the notification device includes periodically sending the notification to the notification device based on the predefined time period.

16. The system of Claim 12, wherein the notification is triggered by a request for the notification with dynamic data sent from the notification device.

17. The system of Claim 12, wherein the notification is triggered by a signal sent from a contactless transmitter on portable consumer device to a contactless receiver on the notification device.

18. A phone, comprising:

a processor;

a receiver coupled to the processor;

an output device coupled to the processor; and

a computer readable medium coupled to the processor, the computer readable medium includes code for displaying a notification including dynamic data to the output device after a portable consumer device is used by a consumer.

19. The phone of Claim 18, wherein the dynamic data is a balance associated with the portable consumer device.

20. The phone of Claim 18, wherein the portable consumer device is a prepaid card.

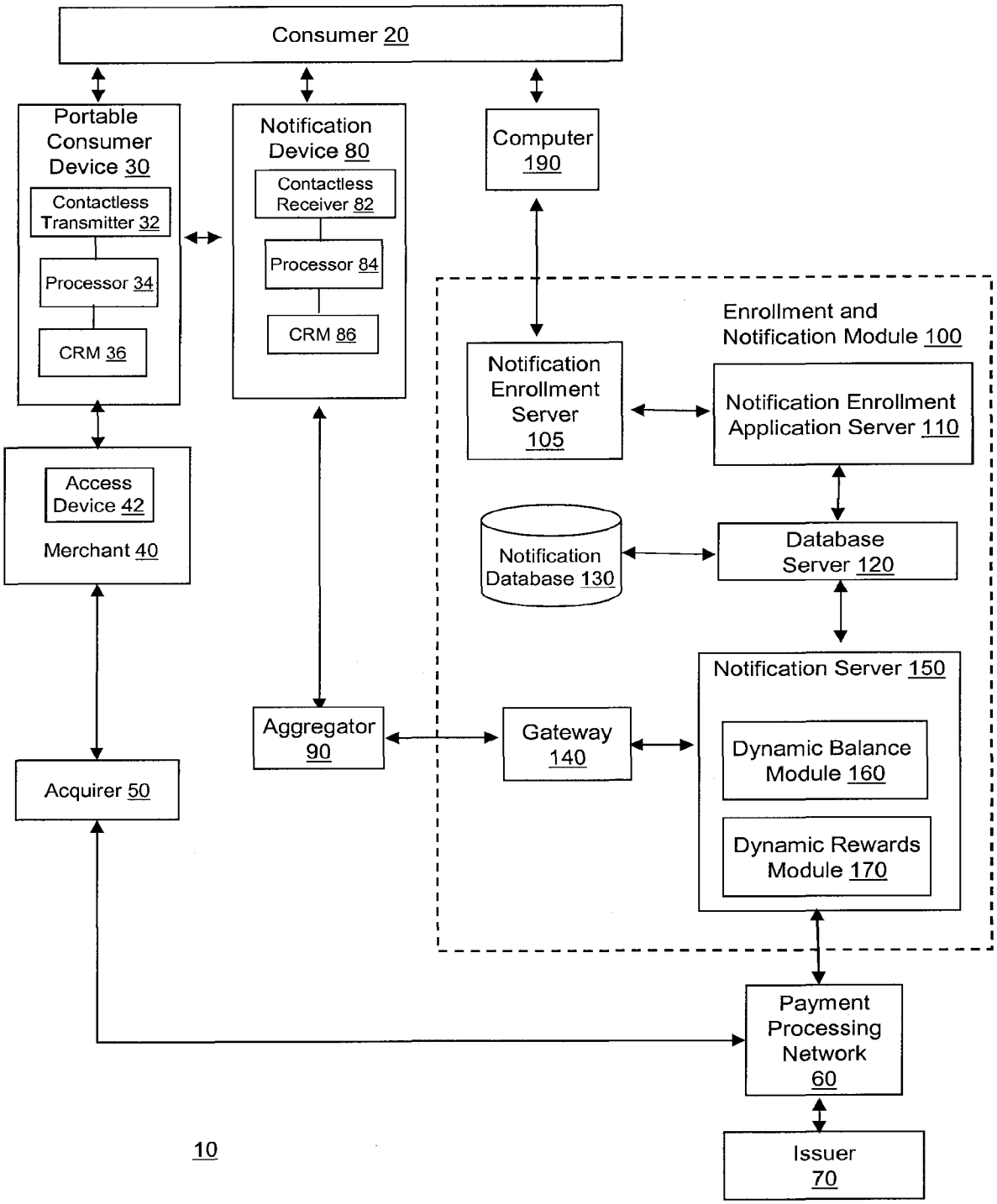

Consumer 20
Portable Consumer Device 30
Contactless Transmitter 32
Processor 34
CRM 36
Notification Device 80
Contactless Receiver 82
Processor 84
CRM 86
Computer 190
Enrollment and Notification Module 100
Notification Enrollment Server 105
Notification Enrollment Application Server 110
Access Device 42
Merchant 40
Notification Database 130
Database Server 120
Notification Server 150
Aggregator 90
Gateway 140
Dynamic Balance Module 160
Dynamic Rewards Module 170
Acquirer 50
Payment Processing Network 60
10
Issuer 70

FIG. 1

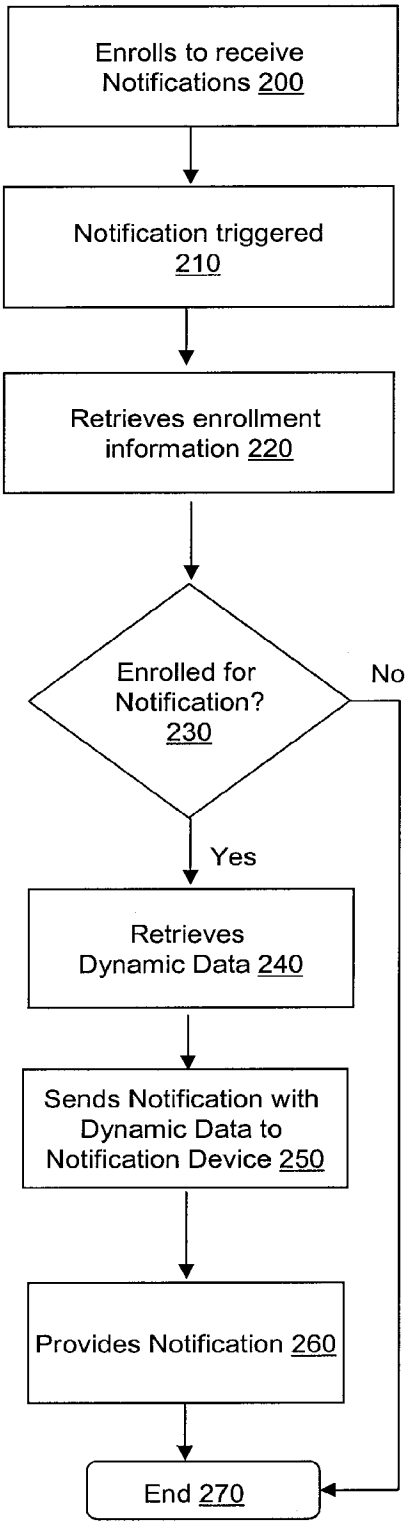

Enrolls to receive Notifications 200
Notification triggered 210
Retrieves enrollment information 220
Enrolled for Notification? 230
No
Yes
Retrieves Dynamic Data 240
Sends Notification with Dynamic Data to Notification Device 250
Provides Notification 260
End 270

FIG. 2

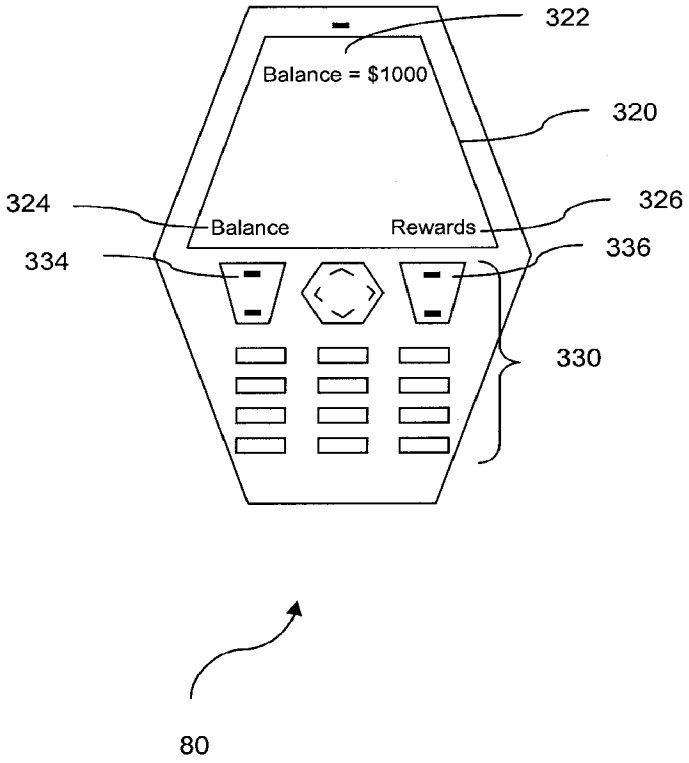


FIG. 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 07/88704

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06Q 40/00 (2008.04)
USPC - 705/39
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)
USPC: 705/39

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC: 705/35, 40 (see also text search below)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Electronic Databases Searched: pubWEST, USPTO, Google, Answers.com, Google Patents
Search Terms Used: dynamic, data, rewards, information, portable, device, transaction, pay, notification, voicemail, email, SMS, cell phone, telephone, balance, computer, prepaid, card, realtime, transmit, contactless, dynamic, automatic

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 2006/0053056 A1 (ALSPACH-GOSS et al.) 09 March 2006 (09.03.2006) para [0006]-[0007], [0022], [0024]-[0025], [0027]-[0029], [0033], [0036]-[0037], [0050]-[0051], [0056]-[0058], [0069], [0071], [0077], [0091], [0103], [0109]-[0112], [0114], [0123], [0136], [0144], [0148], [0160], [0167], [0170], [0175], [0177] and [0179]	1-3, 5-12 and 14-20 --- 4 and 13
Y	US 2005/0035847 A1 (BONALLE et al.) 17 February 2005 (17.02.2005) para [0057], [0063], [0083], [0085]), [0104] and [0124	4 and 13
A	US 2006/0248007 A1 (HOFER et al.) 02 November 2006 (02.11.2006)	1-20

☐ 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
25 May 2008 (25.05.2008)	11 JUN 2008
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: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (April 2007)

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 November 2013 (28.11.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/177416 A2

(51) International Patent Classification:
G06Q 20/32 (2012.01)

(21) International Application Number:
PCT/US2013/042455

(22) International Filing Date:
23 May 2013 (23.05.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

61/651,276	24 May 2012 (24.05.2012)	US
61/772,260	4 March 2013 (04.03.2013)	US
61/794,545	15 March 2013 (15.03.2013)	US

(71) Applicant: **JVL VENTURES, LLC** [US/US]; 230 Park Avenue, Suite 2829, New York, NY 10169-0005 (US).

(72) Inventors: **BUSH, Larry, L.**; 13637 N. 12th Way, Phoenix, AZ 85022 (US). **TOMCZAK, Christopher, J.**; 1319 Lochness Drive, Allen, TX 75013 (US).

(74) Agents: **BERSCHADSKY, Jonathan** et al.; Fitzpatrick, Cella, Harper & Scinto, 1290 Avenue Of The Americas, New York, NY 10104-3800 (US).

(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, BN, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

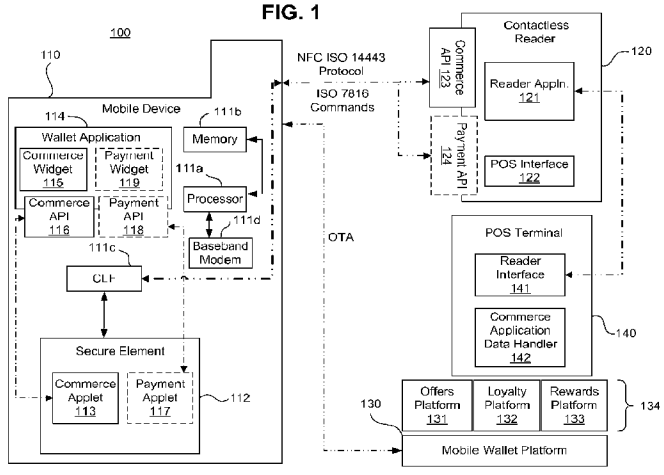
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

(54) **Title**: SYSTEMS, METHODS, AND COMPUTER PROGRAM PRODUCTS FOR PROVIDING A CONTACTLESS PROTOCOL

FIG. 1



(57) **Abstract**: Systems, methods and computer program products are provided for managing contactless transactions. A first tap is performed when a system is placed within a predetermined proximity to a payment terminal. A first select command including an AID corresponding to a first application is received from the payment terminal. A first response based on the first select command is transmitted to the payment terminal. A data request including information indicating supported data types is received from the payment terminal. A second response based on the data request and including transaction data is transmitted to the payment terminal. The transaction data includes at least a portion of commerce data stored in the at least one memory.

WO 2013/177416 A2

SYSTEMS, METHODS, AND COMPUTER PROGRAM PRODUCTS FOR PROVIDING A CONTACTLESS PROTOCOL

BACKGROUND

Field

[0001] Example aspects described herein relate generally to contactless protocols and more particularly to systems, methods, and computer program products for providing a contactless protocol allowing interoperation between mobile devices, near field communication (NFC) readers, and point of sale (POS) systems.

Related Art

[0002] NFC technology is a standards-based wireless communication technology that allows data to be exchanged between devices that are positioned within a certain proximity, generally less than ten centimeters apart. One use of such NFC technology is for making contactless transactions, including those for payment,

access and ticketing. For example, an NFC-enabled mobile device can be provisioned with a payment application and payment account information (*i.e.*, credentials associated with a financial instrument such as credit or debit card) issued by a consumer's financial institution. Each payment application can store and manage multiple sets of commerce data associated with multiple merchants, manufacturers or brands on a secure element. The application and payment account information are typically encrypted and stored in a secure area in the mobile device. The mobile device can, in turn, use the NFC technology to communicate with NFC-enabled point of sale (POS) systems at attended locations such as stores and unattended locations such as vending machines. To pay, the consumer simply brings the mobile device to within approximately ten centimeters of a contactless payment-capable POS system and the transaction occurs. The process is typically the same as that used by the contactless credit and debit cards.

[0003] Placing the mobile device or contactless credit or debit card near an NFC-enabled reader so that they can be communicatively coupled is sometimes referred to as a "wave" or "tap". An application for a mobile device that allows consumers to "tap to pay" at a NFC-enabled POS systems is generally referred to as a "wallet application" or "mobile wallet client application." An application related to payments is generally referred to as a "payment" application. Common contactless payment applications are facilitated using any of the following technologies: American Express® "ExpressPay," Discover® "ZIP," Mastercard® "PayPass" or Visa® "PayWave".

[0004] NFC can also be used to read information about products or receive special offers, loyalty or rewards information from, for example, NFC tags, smart posters or smart billboards. An application related to offers, loyalty and rewards is generally referred to herein as a "commerce" application.

[0005] One technical challenge associated with utilizing payment and commerce technologies cooperatively involves the ability to allow the same tap event that sends payment information to include additional information associated with merchant loyalty cards, offers, rewards, and the like. To this end, messaging technologies in existing NFC readers or NFC-enabled payment POS terminals

stand to be upgraded to effectively support a messaging technology that retrieves and/or receives both payment credentials (using the aforementioned payment protocols) and additional commerce data (loyalty, offers, rewards, etc.) from mobile devices used to perform the transactions. Yet another technical challenge involves publishing commerce elements (*e.g.*, offers, loyalty card credentials, rewards, and the like) into a mobile device such that those commerce elements may, in turn, be presented as part of a typical POS transaction (*e.g.*, a purchase).

BRIEF DESCRIPTION

[0006] The example embodiments presented herein meet the above-identified needs by providing systems, methods and computer program products for providing a contactless protocol.

[0007] In one embodiment, a system for managing contactless transactions includes at least one memory operable to store commerce data and financial instrument data, and at least one processor coupled to the at least one memory. A first tap is performed, the first tap occurring when the system is placed within a predetermined proximity to a payment terminal. A first select command including an AID corresponding to a first application is received from the payment terminal. A first response based on the first select command is transmitted to the payment terminal. A data request including information indicating supported data types is received from the payment terminal. A second response based on the data request and including transaction data is transmitted to the payment terminal. The transaction data includes at least a portion of the commerce data stored in the at least one memory.

[0008] In another embodiment, a method for managing contactless transactions includes: performing a first tap, the first tap occurring when a mobile device is placed within a predetermined proximity to a payment terminal; receiving from the payment terminal a first select command including an AID corresponding to a first application; transmitting to the payment terminal a first response based on the first select command; receiving from the payment terminal a data request including information indicating supported data types; and transmitting to the payment terminal a second response based on the data request, the second

response including transaction data. The transaction data includes at least a portion of commerce data stored in at least one memory.

[0009] In another embodiment, a non-transitory computer-readable medium has sequences of instructions stored thereon for causing one or more processors to: perform a first tap, the first tap occurring when a mobile device is placed within a predetermined proximity to a payment terminal; receive from the payment terminal a first select command including an AID corresponding to a first application; transmit to the payment terminal a first response based on the first select command; receive from the payment terminal a data request including information indicating supported data types; and transmit to the payment terminal a second response based on the data request, the second response including transaction data. The transaction data includes at least a portion of commerce data stored in at least one memory.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] The features and advantages of the example embodiments of the invention presented herein will become more apparent from the detailed description set forth below when taken in conjunction with the following drawings.

[0011] FIG. 1 is a graphical representation of a platform architecture in accordance with an exemplary embodiment.

[0012] FIG. 2 illustrates a single tap timing diagram according to an exemplary embodiment.

[0013] FIG. 3 shows a timing diagram illustrating a commerce process flow including a double tap and post transaction data transmission according to an exemplary embodiment.

[0014] FIG. 4 shows a timing diagram illustrating a commerce process flow including a double tap, and post transaction data and payment transmissions according to an exemplary embodiment.

[0015] FIG. 5 illustrates an exemplary multi-block data flow according to an example embodiment.

[0016] FIG. 6 illustrates windows or screen shots generated by the graphical user interface for a wallet application in accordance with an example embodiment of the present invention.

[0017] FIG. 7 illustrates a flow diagram illustrating an exemplary instant offer implementation according to an embodiment of the present invention.

[0018] FIG. 8 is a collaboration diagram of functional modules deployed on a computer system in accordance with an example embodiment of the present invention.

DETAILED DESCRIPTION

[0019] The example embodiments presented herein are directed to systems, methods and computer program products for providing a contactless protocol, which are now described herein in terms of an example merchant transaction. This description is not intended to limit the application of the example embodiments presented herein. In fact, after reading the following description, it will be apparent to one skilled in the relevant art(s) how to implement the following example embodiments in alternative embodiments (*e.g.*, involving mass transit transactions requiring a wireless communications connection between a mass transit terminal and a mobile device).

[0020] The terms "application," "applet," "widget," and/or the plural form of these terms are used interchangeably herein to refer to an application (functioning independently or in conjunction with other applications) or set or subset of instructions or code, which when executed by one or more processors (*e.g.*, in a mobile device, card reader, terminal, point of sale (POS) system, or server) causes the processor(s) to perform specific tasks. For example, a wallet application can be used to conduct transaction- or interface-related functions such as storing, processing, accessing or transmitting financial, loyalty, offer, membership, or account data. A wallet application may also incorporate or interact with one or more payment applications, such as ExpressPay from American Express®, Discover® Network Zip^{SM}, MasterCard® PayPass™ and Visa payWave™ payment applets.

[0021] Generally, commerce-related services are made available through a suite of applications available on several different platforms. The first application (or suite of applications) exists onboard a server within a mobile commerce (MoCom) platform. The MoCom platform is responsible for the management of consumer data, including loyalty accounts and offers. In addition, the MoCom platform serves as a campaign manager for offers, providing a remote data store for offers made available to the consumer via the available merchant portals within a wallet application.

[0022] A second application exist onboard a mobile device in the form of a wallet application. The wallet application provides the consumer's primary user interface (UI) and additional commerce application services through which the wallet application may access additional resources onboard a secure element (SE) of a mobile device.

[0023] A third application exists onboard a secure element of a mobile device in the form of JavaCard applet. This applet stores commerce-related data such as loyalty and offer data and provides an interface through which the data may be managed. The applet is accessible through the use of Application Protocol Data Unit (APDU) commands as defined in International Standards Organization (ISO) 7816-4.

[0024] The fourth application exists onboard an NFC-enabled reader (referred to herein simply as a "reader"). The reader can be either a stand-alone device or attached to (and managed by) a point of sale (POS) terminal. This application facilitates or provides access to the interface with a secure element on a mobile device, performing specific tasks that optimize the APDU command/data exchange tasks. For example, it includes the reading of loyalty or offer information following the placement of a mobile device in proximity of a reader (*i.e.*, a "tap").

[0025] A fifth application (or suite of applications) exists onboard a merchant POS system, including a POS terminal and any additional merchant-specific hardware/software. These applications manage the data related to payment/loyalty/offers/rewards received from a secure element on a mobile

device via a reader. In most cases, this data will then be forwarded to a corresponding MoCom or merchant specific platform(s).

[0026] FIG. 1 is a graphical representation of a platform architecture in accordance with an exemplary embodiment. As shown in FIG. 1, system 100 includes a mobile device 110 communicatively coupled to a contactless (*e.g.*, proximity or NFC) reader 120 and a mobile wallet platform 130. Reader 120 also is communicatively coupled to a POS terminal 140. POS terminal 140 may be within the same housing as reader 120. Alternatively, POS terminal 140 and reader 120 are communicatively coupled with each other but each of these components is housed separately.

[0027] Mobile device 110 may be, for example, a cellular phone or the like, and includes a processor 111a, memory 111b, a contactless frontend (CLF) 111c, a baseband modem 111d, and a user interface such as a display (not shown). Baseband modem 111d is a digital modem that is used for mobile network communications. CLF 111c is circuitry which handles the analog aspect of contactless or NFC communications and the communication protocol layers of a contactless transmission link. CLF 111c also is used to exchange data between reader 120 and a secure element (or SE) 112 contained in mobile device 110, for example, to execute contactless transactions.

[0028] Secure element 112 may be implemented as a Universal Integrated Circuit Card (UICC), embedded SE card, secure micro secure digital (microSD) card, and the like. Secure element 112 is generally considered secure because it is a self-contained system, including dedicated memory, and is protected by hardware and software hardening techniques that are verified by independent testing.

[0029] Secure element 112 includes (*e.g.*, stored thereon) one or more commerce applets 113. Each commerce applet 113 is associated with a commerce service and an account issued by a commerce service provider (SP). A service provider is a company, organization, entity, or the like, that provides services to customers or consumers. Examples of service providers include account-issuing entities such as banks, merchants, card associations, marketing companies, and transit authorities. A service may be an activity, capability, functionality, work, or use

that is permitted or provided by a service provider, such as a payment service, credit, debit, checking, gift, offer or loyalty service, transit pass service, and the like.

[0030] A commerce service provider can provision (or have provisioned) onto secure element 112 one or more separate commerce applets 113. In addition, other independent service providers can provision (or have provisioned) onto secure element 112 their own commerce applet(s) 113. Generally, a commerce applet 113 stores both loyalty and offers related data, providing an APDU interface through which this data can be managed. Commerce applet 113 operates as a generic storage container, allowing multiple loyalty/offers services to share mechanisms (*e.g.*, secure element, mobile device) for loyalty/offer data management. If memory restrictions and performance requirements limit the amount of loyalty/offers data that can be stored on secure element 112, additional data can be stored in mobile device memory 111b and managed by the consumer via commerce widget 115. For example, any graphic images related to an offer can be stored in memory 111b in order to optimize secure element memory allocation. Loyalty/offers data management can be handled by the corresponding offer platform 131, loyalty platform 132, or rewards platform 133.

[0031] Commerce applet 113 includes a cached merchant data table enabling the storage/management of all data related to a given merchant. This allows the commerce data for a given merchant to be pre-loaded in secure element 112 or mobile device 110 by a wallet application. Exemplary commerce elements (and their corresponding tag values used during Tag Length Value (TLV) encoding) that are included in the cached merchant data table are defined below. This data is stored in a record oriented data buffer. In an exemplary embodiment, a merchant identifier (Merchant Identifier) is used as the key field for search/retrieval tasks. Optionally, an index (or hash table) may be created to improve performance.

[0032] One or more commerce applets 113 can be loaded onto the secure element 112, for example, during manufacture and/or configuration of the secure element 112 and may be personalized to enable its use to conduct commerce transactions. A commerce applet 113 interfaces with reader 120 via a commerce

application programming interface (API) 123. In an exemplary embodiment, a commerce applet 113 is in the form of a JavaCard applet and is accessible through the use of APDU commands as defined in ISO 7816-4. Particularly, commerce applet 113 communicates commerce elements to reader 120 via secure element 112 using ISO 7816 commands over the NFC ISO 14443 protocol.

[0033] Secure element 112 can also include one or more payment applets 117 where each payment applet 117 is associated with a payment service and an account issued by a payment service provider. One or more payment applets 117 also can be loaded onto the secure element 112, for example, during manufacture and/or configuration of the secure element 112 and may be personalized to enable its use to conduct payment transactions. A payment applet 117 interfaces with reader 120 via API 124. In an exemplary embodiment, payment applet 117 is in the form of a JavaCard applet and is accessible through the use of APDU commands as defined in ISO 7816-4. Payment applet 113 also communicates payment elements to reader 120 via secure element 112 using ISO 7816 commands over the NFC ISO 14443 protocol.

[0034] It should be understood that other communications between the aforementioned devices may include communications with or through other intervening systems, hardware, and/or software, and such communications may include receiving, transferring, and/or managing data.

[0035] A wallet application 114 stored on mobile device 110 includes instructions which, when executed by the processor of the mobile device 110, cause the mobile device 110 to act as an instrument, for example, for processing transactions such as contactless commerce and/or payment transactions. Wallet application 114 communicates, through the use of APDU commands as defined in ISO 7816-4, with the commerce applet 113 via commerce API 116 and to payment applet 117 via payment API 118.

[0036] Commerce widget 115 is a component of the wallet application 114 that provides an interface for consumers to manage commerce elements (*e.g.*, loyalty card credentials, offers and rewards), for example, through interactions with the display or user interface of a mobile device. Commerce widget 115 maintains, for example, a master list of commerce elements present on the handset in a

memory of the mobile device (*e.g.*, 111b). A subset of offers that have been identified as ready to be used are, in turn, moved to secure element 112 to be communicated to contactless reader 120 and POS terminal 140. Sensitive information, such as loyalty account identifiers can be stored on secure element 112.

[0037] Payment widget 119 is a component of the wallet application 114 that provides an interface for consumers to manage payment elements (*e.g.*, credit or debit card credentials), for example, through interactions with the display or user interface of a mobile device.

[0038] Reader 120 includes a reader commerce application 121 (referred to herein simply as a "reader application") and a POS interface 122. Reader 120 manages two interfaces: one interface is with the secure element 112 in the mobile device 110 and the other interface is with POS terminal 140 which includes a reader interface 141 and a commerce application data handler 142. The functionality of reader 120 is the same whether reader 120 is standalone and connected to a payments terminal or merchant POS, or is integrated therein. Contactless payment functionality is also contained in reader 120 but is not shown.

[0039] Mobile device 110 is further communicatively coupled to a mobile wallet platform 130, which in turn is communicatively coupled to offers platform 131, loyalty platform 132 and rewards platform 133. Collectively, offers platform 131, loyalty platform 132 and rewards platform 133 can be referred to as a mobile commerce (MoCom) platform 134 and are implemented on one or more servers, referred to herein individually and collectively as a MoCom server (now shown).

[0040] In one embodiment, a customer may use mobile device 110 to conduct a contactless transaction at a POS equipped with reader 120. The customer places the mobile device 110 within a predetermined required proximity of the contactless reader 120 (*i.e.*, taps) causing CLF 111c of the mobile device 110 to communicate with reader 120 using, for example, NFC ISO 14443 protocols. Reader 120 also communicates with wallet application 114, commerce applet

113, and/or payment applications on the mobile device 110 to execute contactless transactions.

[0041] A secure element employs a Proximity Payment System Environment (PPSE) that serves as a directory of available credentials currently stored in secure element 112. Each credential is assigned a corresponding application identifier (AID) associated with a payment application and stored in the PPSE. When an NFC enabled-mobile device containing secure element 112 is placed in the vicinity of an NFC-enabled contactless reader, the contactless reader reads the credential and completes the transaction. Before doing so, however, the reader is initialized.

[0042] On mobile device 110, PPSE is an application used to maintain a list of payment applications stored on secure element 112, and provides accessibility to each payment application stored on the mobile device 112 by making them visible or not visible (*i.e.*, accessible) to systems or devices.

Reader Initialization

[0043] Initialization of the reader 120 will now be described in more detail. In one embodiment, reader 120 implements a function referred to as an Entry Point Manager (EPM) to control which application in a mobile device is selected. In this embodiment, EPM controls whether reader 120 sends a command to mobile device 110 to select an application that performs a commerce transaction or a command that performs a payment transaction. A command to select a commerce application is referred to herein as "Select Commerce." A command to select a payment application is referred to herein as "PPSE Select."

[0044] EPM also controls the start mode for the reader 120 and subsequent application switching during a checkout process. EPM thus facilitates switching (at reader 120) between the Select Commerce command for a commerce transaction and the PPSE Select command for payment transactions.

Commencing a Commerce Transaction on a Reader

[0045] A reader can be configured to initiate a commerce transaction on a reader according to several modes, which are described below in further detail. In one mode, referred to as "auto start", reader application 121 is the default application

on the reader 120. Being the default application allows reader application 121 to be available to the consumer as a first tap option (*i.e.*, upon an initial coupling communication between the mobile device 110 and contactless reader 120).

[0046] Another mode, referred to as "manual start," allows manual intervention to be used to initiate reader commerce application 121. Manual intervention can be in the form of a command from POS terminal 130 (*e.g.*, initiated by using a POS terminal interface) or from a consumer selecting a commerce application on a mobile device by using commerce widget 115.

[0047] Another mode, referred to as "payment with post transaction data," involves controlling how payments are handled in an activity stream. If a merchant supports the provisioning of post transaction data, for example, then payment and receipt of merchant data can be accomplished by the same tap event, such as after the final total for a transaction has been calculated.

[0048] Another mode is referred to as "payment first," The payment first option works in conjunction with the auto start mode and/or the manual start mode to initiate a PPSE Select command for payment and then a Select Commerce command to obtain commerce data (*e.g.*, loyalty data, offer data, reward data, and the like). Commerce data is interchangeably referred to herein as "commerce elements."

Auto Start Mode

[0049] Referring to FIG. 1, auto start mode provides commerce functionality on reader 120 at the beginning of a POS checkout process. When mobile device 110 taps reader 120, reader application 121 causes reader 120 to send a "Select Commerce" message to mobile device 110 including the AID corresponding to the commerce application to be used to execute a contactless transaction. If the message is accepted by mobile device 110 it sends a positive response message in return. Next, reader 120 sends mobile device 110 a "Get Commerce Data" command. The Get Commerce Data command contains merchant specific data that secure element 112 uses to perform a commerce transaction. Also, control passes to the mobile device 110 upon successful completion of the Get Commerce Data transaction. If reader 120 receives a negative response to "Select Commerce" message it passes control back to the EPM.

Manual Start Mode

[0050] Referring still to FIG. 1, in manual startup mode, reader 120 starts reader application 121 in response to a request from either the consumer or the POS terminal 140. In this manual start mode, at the beginning of a checkout process, reader 120 is in a PPSE select state. For a consumer initiated commerce transaction, the consumer selects the commerce application at the customer facing device (*e.g.*, commerce widget 115). The customer facing device then sends a command to reader 120 to start the reader application 121 via the EPM. For a POS terminal initiated commerce transaction, POS terminal 140 commands reader 120 to initialize the reader application 121. In one embodiment, this is initiated by a cashier via an interface on the POS terminal 140.

[0051] Once reader commerce application 121 has been started on reader 120, the commerce application will function as described in the auto start mode above.

Payment with Post Transaction Data

[0052] In payment with post transaction data mode, a payment transaction can be made such that post transaction data is communicated between POS terminal 140, reader 120, and secure element 112. This option allows the commerce protocol to start at the beginning of the consumer checkout, but payment is not requested by the reader 120 until the final transaction total has been calculated.

[0053] POS terminal 140 sends a "Post Transaction" command to reader 120 with, for example, a transaction identifier (ID) and redeemed coupon IDs. Reader 120 then transmits a request for a tap for payment. The tap allows reader 120 to first request payment credentials from secure element 112 and then cause the reader application 121 to send commerce data (*e.g.*, coupon data) to secure element 112. Both functions are performed in a single tap by the mobile device 110 at reader 120.

Payment First

[0054] In payment first mode, a payment can be made first, prior to a commerce transaction. This option accommodates a situation where the payment/PPSE process must precede any commerce processing. Payment first mode works in

conjunction with both auto and the manual start modes discussed above. Payment and commerce processing is accomplished in a single tap.

EXEMPLARY COMMERCE PROCESS FLOWS

Normal Commerce Process Flow (Single Tap)

[0055] FIG. 2 illustrates a single tap timing diagram 200 according to an exemplary embodiment. The following process flow can commence as items being purchased are being scanned at a POS. For convenience, reader 120 (FIG. 1) and POS terminal 140 (FIG. 1) are illustrated as a single component and collectively referred to as payment terminal 201. Each component (*i.e.*, reader 120 or POS terminal 140) is referred to individually when applicable.

[0056] A merchant POS system 202 can be a merchant server operated by a merchant which controls the operation of payment terminal 201. In an exemplary embodiment, merchant POS system 202 commands payment terminal 201 to activate the reader ("Activate Reader") before items are being scanned, as items are being scanned, or after the items are scanned. In each case, reader 120 requests a user (or consumer) to place a mobile device 110 in proximity of reader 120, as shown in step 250 ("Request 'tap'"). In response to a request for the user to place a mobile device 110 in proximity of reader 120 (step 250), a consumer taps mobile device 110 onto reader 120, as shown in step 251.

[0057] Once a NFC connection has been established between mobile device 110 and reader 120, the following command exchanges are initiated for service initialization and processing of both a payment transaction and a commerce transaction. Payment transaction initialization and processing exchanges between secure element 112 and reader 120 include steps 260 and commerce transaction initialization and processing exchanges between secure element 112 and reader 120 include steps 262. Steps 260 may be performed before steps 262, afterward, or substantially simultaneously.

[0058] Referring first to steps 262, after a mobile device has tapped reader 120, reader 120 sends to secure element 112 a Select Commerce command along with a particular commerce AID ("Select Commerce AID") indicating which commerce applet within secure element 112 it seeks to cooperate with (*e.g.*,

commerce applet 113). In response, secure element 112 sends a positive or negative response. A negative response (not shown) results in reader 120 terminating reader application 121 (FIG. 1) and passing control to the EPM (not shown). If the response is positive ("Positive Response"), then reader 120 sends a command ("Get Commerce Data") to secure element 112 specifying identifying information, such as a merchant/store identifier, and any additional loyalty, offer or reward schemes supported by that location, date and time information, the version of reader commerce application 121 supported by reader 120, and any merchant capability data.

[0059] Secure element 112 returns corresponding commerce elements (*e.g.*, loyalty data, offer data, reward data) to reader 120 ("Loyalty & Offers Data") based on the fields in the Get Commerce Data command received from reader 120. In one embodiment, commerce applet 113 builds a package containing the commerce data (*e.g.*, a buffer or set of buffers including loyalty data, offer data, or rewards data). In another embodiment, the buffer is pre-built using memory space in the secure element 112.

[0060] Referring to steps 260, in one embodiment, reader 120 begins payment processing by sending a PPSE request ("PPSE Select") to secure element 112.

[0061] If the Select Commerce AID and PPSE Select requests are successful, as shown in step 264 ("Read Success Indication"), payment terminal 201 forwards the commerce application data and payment credentials it has received to the merchant POS system 202 for processing ("Payment & Commerce Data"). Merchant POS system 202, in turn, records the loyalty identifier and offers (not shown) and applies any applicable discounts as product scanning continues as shown in step 266. This concludes the commerce application process and the payment processing proceeds.

[0062] Once scanning has completed and a transaction amount has been approved for payment, a payment authorization request to a payment platform 203 is made ("Payment Auth Request"). In turn, payment platform 203 returns an authorization result ("Authorization Result") indicating whether or not the payment has been authorized.

[0063] Referring again to steps 260, in one embodiment, a PPSE Select request by reader 120 to secure element 112 causes secure element 112 to return a PPSE payment AID indicating which payment applet (and hence which corresponding payment network) should be used to perform the payment transaction ("PPSE Payment AID"). In response, reader 120 sends a Select AID indicating that it supports the particular applet ("Select AID"). File control information (FCI) associated with the payment applet (*e.g.*, FIG 1, 117) is sent by secure element 112 to reader 120. Similarly, other payment and card information is sent by secure element 112 to reader 120 ("Payment/Card Data").

[0064] FIG. 3 shows a timing diagram 300 illustrating a commerce process flow including a double tap and post transaction data transmission according to an exemplary embodiment. This embodiment can be used when a merchant has data to communicate back to a mobile device. For convenience, reader 120 (FIG. 1) and POS terminal 140 (FIG. 1) are illustrated as a single component and collectively referred to as payment terminal 301. Each component (*i.e.*, reader 120 or POS terminal 140) is referred to individually when applicable. Generally, POS terminal 140 (FIG. 1) initiates a request for a second tap by sending a command, "Post Transaction Command", to reader 120. Reader 120, in turn requests a second tap from the consumer.

[0065] A merchant POS system 302 can be a merchant server operated by a merchant which controls the operation of payment terminal 301. In an exemplary embodiment, merchant POS system 302 commands payment terminal 301 to activate reader 120 ("Activate Reader") before items are being scanned, as items are being scanned, or after the items are scanned. In each case, reader 120 requests a user to place a mobile device 110 in proximity of reader 120, as shown in step 350 ("Request 'tap'"). In response to a request for the user to place a mobile device 110 in proximity of reader 120 (step 350), a consumer taps mobile device 110 onto reader 120, as shown in step 351.

[0066] Once a NFC connection has been established between mobile device 110 and reader 120, the following command exchanges are initiated for service initialization and processing of both a payment transaction and a commerce transaction. Payment transaction initialization and processing exchanges between

secure element 112 and reader 120 include steps 360 and commerce transaction initialization and processing exchanges between secure element 112 and reader 120 include steps 362. Steps 360 may be performed before steps 362, afterward, or substantially simultaneously.

[0067] Referring first to steps 362, after mobile device 110 has tapped reader 120, reader 120 sends to secure element 112 a Select Commerce command along with a particular commerce AID ("Select Commerce AID") indicating which commerce applet within secure element 112 it seeks to cooperate with (*e.g.*, commerce applet 113). In response, secure element 112 sends a positive or negative response. A negative response (not shown) results in reader 120 terminating reader application 121 (FIG. 1) and passing control to the EPM (not shown). If the response is positive ("Positive Response"), then reader 120 sends a command to the secure element 112 specifying identifying information, such as a merchant/store identifier, and any additional loyalty and offer schemes supported by that location, date and time information, the version of reader commerce application 121 supported by reader 120 and any merchant capability data ("Get Commerce Data"). Secure element 112 returns corresponding commerce elements (*e.g.*, loyalty and offers data) to reader 120 ("Loyalty & Offers Data") based on the fields in the Get Commerce Data command received from reader 120. In one embodiment, this is accomplished by commerce applet 113, which builds a package of data (essentially a buffer or set of buffers including offers and loyalty data). In another embodiment, the buffer can be pre-built using memory space in the secure element 112.

[0068] Referring next to steps 360, in one embodiment, a PPSE Select request by reader 120 to secure element 112 causes secure element 112 to return a PPSE payment AID indicating which payment applet (and hence payment network) should be used to perform the payment transaction ("PPSE Payment AID"). In response, reader 120 sends a Select AID indicating that it supports the particular applet ("Select AID"). FCI associated with the payment applet (*e.g.*, 117) is sent by secure element 112 to reader 120. Similarly, other payment and card information is sent by secure element 112 to reader 120 ("Payment/Card Data").If the Select Commerce AID and PPSE Select requests are successful, as

shown in step 364, payment terminal 301 forwards the commerce application data and payment credentials it has received to the merchant POS system 302 for processing ("Payment & Commerce Data"). Merchant POS system 302, in turn, records the loyalty identifier and offers (not shown) and applies any applicable discounts as product scanning continues as shown in step 366.

[0069] Once scanning has completed and a transaction amount has been approved for payment, a payment authorization request to a payment platform 303 is made ("Payment Auth Request"). In turn, payment platform 303 returns an authorization result ("Authorization Result") indicating whether or not the payment has been made.

[0070]

[0071] If there is data to send back to payment terminal 301, merchant POS system creates a command, "Post Transaction Data", with correctly formatted TLVs and forwards the data to reader 120. Upon receipt of a Post Transaction command payment terminal 301 will request a second tap from the consumer, as shown in step 368 ("Request 2nd 'tap'").

[0072] Referring to step 369 and steps 370, when the mobile device 110 is placed within proximity of reader 120 for the second time as shown in step 369, reader 120 sends a secure element 112 a Select Commerce command along with a particular commerce AID ("Select Commerce AID") indicating which commerce applet within secure element 112 it seeks to cooperate with (*e.g.*, commerce applet 113).

[0073] If a negative response is received reader 120 terminates the reader commerce application 121. If a positive response is received, then reader 120 forwards to secure element 112 the data received in the Post Transaction Data command from the POS terminal 140 ("Post Transaction Data"). This concludes commerce processing for this transaction.

[0074] FIG. 4 shows a timing diagram 400 illustrating a commerce process flow including a double tap, and post transaction data and payment transmissions according to an exemplary embodiment. In this scenario the payment and post transaction data are processed after a basket has been totaled and all discounts

have been applied. Usage of this flow is controlled by a reader start mode data element with a particular bit (*e.g.*, "Payment with Post Transaction") set on.

[0075] For convenience, reader 120 (FIG. 1) and POS terminal 140 (FIG. 1) are illustrated as a single component and collectively referred to as payment terminal 401. Each component (*i.e.*, reader 120 or POS terminal 140) is referred to individually when applicable. Generally, merchant POS system 402 initiates a request for a second tap by sending a post transaction data command to reader 120. Reader 120, in turn requests a second tap from the consumer.

[0076] A merchant POS system 402 can be a merchant server operated by a merchant which controls the operation of payment terminal 401. In an exemplary embodiment, merchant POS system 402 commands payment terminal 401 to activate the reader ("Activate Reader") before items are being scanned, as items are being scanned, or after the items are scanned. In each case, reader 120 requests a user to place a mobile device 110 in proximity of reader 120, as shown in step 450 ("Request 'tap'"). In response to a request for the user to place a mobile device 110 in proximity of reader 120 (step 450), a consumer taps mobile device 110 onto reader 120, as shown in step 451.

[0077] Once a NFC connection has been established between mobile device 110 and reader 120, the following command exchanges are initiated. The command exchanges are performed for service initialization and processing of both a payment transaction and a commerce transaction. Payment transaction initialization and processing exchanges between secure element 112 and reader 120 include steps 472, and commerce transaction initialization and processing exchanges between secure element 112 and reader 120 include steps 462 and 474.

[0078] Referring first to steps 462, after a mobile device has tapped reader 120, reader 120 sends to secure element 112 a Select Commerce command along with a particular commerce AID ("Select Commerce AID") indicating which commerce applet within secure element 112 to cooperate with (*e.g.*, commerce applet 113). In response, secure element 112 sends a positive or negative response. A negative response (not shown) results in reader 120 terminating reader application 121 (FIG. 1) and passing control to the EPM (not shown). If the response is positive ("Positive Response"), then reader 120 sends a command

to the secure element 112 specifying identifying information, such as a merchant/store identifier, and any additional loyalty and offer schemes supported by that location, date and time information, the version of reader commerce application 121 supported by reader 120 and any merchant capability data ("Get Commerce Data"). Secure element 112 returns corresponding commerce elements (*e.g.*, loyalty and offers data) to reader 120 ("Loyalty & Offers Data") based on the fields in the Get Commerce Data command received from reader 120. In one embodiment, this is accomplished by commerce applet 113, which builds a package of data (*e.g.*, a buffer or set of buffers including offers and loyalty data). In another embodiment, the buffer can be pre-built using memory space in the secure element 112.

[0079] At step 464, reader 120 indicates to the consumer that the transaction is complete and that the handset can be removed from payment terminal 401, which causes reader 120 to forward the commerce application data to the POS terminal 140 and, in turn, merchant POS system for processing ("Loyalty & Offers Data"). A clerk may continue to process the shopping basket.

[0080] Merchant POS system 402, records the loyalty identifier and offers (not shown) and applies any applicable discounts as product scanning continues as shown in step 466. After the basket total has been calculated, merchant POS system 402 sends a request for payment to payment terminal 401 and sends post transaction data to payment terminal 401 (if data is available to send) ("Send Post Transaction Data and Payment Req").

[0081] At step 468, payment terminal 140 requests a tap for payment. Reader 120, in turn, activates the reader field. When mobile device 110 is detected in the field of reader 120, payment processing is performed as shown in steps 472. Particularly, a PPSE Select request is made by reader 120 to secure element 112 to cause secure element 112 to return a PPSE payment AID indicating which payment applet (and hence payment network) should be used to perform the payment transaction ("PPSE Payment AID"). In response, reader 120 sends a Select AID command indicating that it supports the particular applet ("Select AID"). FCI associated with the payment applet (*e.g.*, FIG. 1, 117) is sent by

secure element 112 to reader 120. Similarly, other payment and card information is sent by secure element 112 to reader 120 ("Payment/Card Data").

[0082] Referring to steps 474, if payment terminal 401 has received post transaction data from merchant POS system 402, reader 120 starts the commerce application 121 (FIG. 1) and sends secure element 112 the Select Commerce command along with a particular commerce AID ("Select Commerce AID") after a mobile device has tapped reader 120 a second time. The Select Commerce AID identifies which commerce applet within secure element 112 should be used to cooperate with reader 120. In response, secure element 112 sends a positive or negative response. A negative response (not shown) results in reader 120 terminating reader application 121 (FIG. 1) and passing control to the EPM (not shown). If the response is positive ("Positive Response"), then reader 120 sends post transaction data to the secure element 112 ("Post Transaction Data"), with correctly formatted TLVs. This concludes commerce processing for this transaction.

[0083] If the Select Commerce AID and PPSE Select requests are successful, payment terminal 401 forwards the payment application data and payment credentials it has received to the merchant POS system 402 for processing ("Payment/Card Data"). In turn, merchant POS system sends a payment authorization request to a payment platform 403 ("Payment Auth Request"). In turn, payment platform 403 returns an authorization result (Authorization Result) indicating whether or not the payment has been authorized.

[0084] If the commerce and payment credentials and information have been successfully read, reader 120 can provide a notification either through an interface on payment terminal 140, commerce widget 115 (FIG. 1) or payment widget 119 (FIG. 1), as shown in step 478 ("Read Success Indication").

Commerce Message Specifications

Data Encoding

[0085] In one embodiment, all command/response data is encoded using BER-TLV (ISO 7816-4 Annex D) format. In some cases, the TLV (Tag, Length,Value) may be nested (embedded TLV). Due to the flexible nature of the

TLV encoding format, the tagged data may be placed in any order. This is true when formatting the data for both incoming and outgoing payloads. In addition, this data is stored in record oriented tables. The order of the TLV encoded data elements stored therein is not critical; however, some data may be placed at the beginning of the record to enhance index/search performance. Thus, the record data tables provided in this document are supplied as samples for reference purposes.

[0086] A tag is encoded using a "private" tag class and a tag type representing a primitive data object encoded on one or more subsequent bytes. Therefore, the first byte (tag class) is set to 0xDF. In all cases, the data element tag is defined on a single byte. Therefore, the second tag byte has the most significant bit (b8) set to 0. This allows up to 128 valid tag values (0x00 – 0x7F).

[0087] Length encoding supports both the short or long forms. When the length is less that (<) 128 bytes, the most significant bit (b8) is set to 0 and the actual length is specified in the remaining bits (b7 – b1). When the length is greater than (>) 128 bytes, the most significant bit (b8) is set to 1 (length mask = 0x80) and the remaining bits (b7-b1) define the number of subsequent bytes in the length field. Those subsequent bytes encode an integer equal to the number of bytes in the value field.

BER-TLV Example

[0088] Assuming the incoming data uses a tag value of 0x21 (Consumer ID) with a length of 8 bytes and a value of (0x1122334455667788), the data is encoded as shown in Table 1:

TABLE 1

Tag	Length	Value
DF 21	08	11 22 33 44 55 66 77 88
DF 21	81 08	11 22 33 44 55 66 77 88
DF 21	82 00 08	11 22 33 44 55 66 77 88

[0089] TLV encoding allows for the length indicator to be expressed in multiple bytes. Preferably multi-byte length is supported. In short form, the length field consists of a single byte where bit 8 is set to 0 and bits 7 to 1 encode the number

of bytes in the value field. One byte can thus encode any number from zero to 127. Any number from one to 127 is encoded in the same way in BER-TLV length field as in Lc and Le fields. The encoding differs for zero, 128 and more. See, for example, the coding of data objects in the Get Commerce Data command described below.

[0090] In long form, the length field consists of two or more bytes. Bit 8 of the first byte is set to 1 and bits 7 to 1 are not all equal, thus encoding the number of subsequent bytes in the length field. Those subsequent bytes encode the number of bytes in the value field. ISO/IEC 7816 does not use the "indefinite length" specified by the basic encoding rules of ASNI ISO/IEC 7816, which supports length fields of one, two, ... up to five bytes (Table 2). In ISO/IEC 7816, the values '80' and '85' to 'FF' are invalid for the first byte of length fields.

TABLE 2 – BER-TLV length fields in ISO/IEC 7816

	1st byte	2nd byte	3rd byte	4th byte	5th byte	N
1 byte	'00' to '7F'	-	-	-	-	0 to 127
2 bytes	'81'	'00' to 'FF'	-	-	-	0 to 255
3 bytes	'82'	'0000' to 'FFFF'		-	-	0 to 65 535
4 bytes	'83'	'000000' to 'FFFFFF'			-	0 to 16 777 215
5 bytes	'84'	'00000000' to 'FFFFFFFF'				0 to 4 294 967 295

Select Commerce Applet

[0091] In one embodiment, the processing starts when reader 120 detects a mobile device 110 in the field of reader 120 and NFC communications have commenced. At that time, reader 120 sends a command to secure element 112 to select a commerce applet, particularly a "Select Commerce" command. The Select Commerce command (also referred to as a "Select Commerce Applet" command) is standardized as defined in the ISO 78016-3 specification. An example Select Commerce command structure is shown in Table 3:

TABLE 3 – Select Commerce Applet

CLA	INS	P1	P2	Lc	Data	Le
00	A4	04	00	09	A00000048510010101	00

[0092] Secure element 112 in mobile device 110 validates the "Select Commerce" command and sends back an appropriate response. Example responses (also referred to as "Status Codes") are shown in Table 4:

TABLE 4 – Status Codes

SW1	SW2	Description
90	00	Successful execution of command
67	00	Wrong data length
69	01	Application ID not supported
69	99	Application not available
6A	82	Application not installed

[0093] All responses other than '90 00' ("Successful execution of command") cause commerce application 121 (FIG. 1) to terminate in reader 120 and pass control to the EPM.

Get Commerce Data

[0094] Upon commencement of the reader application 121 and communications between reader 120 and secure element 112 initiating, reader 120 sends a command to mobile device 110 to obtain commerce data, "Get Commerce Data." An exemplary Get Commerce Data command is defined below in Tables 5 and 6. In this example, specific loyalty and offers data is being requested. The "Merchant Capability" field is utilized by reader 120 to determine which fields need to be present in the request and response data.

[0095] Date and time stamp information are optional. In one embodiment, the date time is in synchronization with the POS. In the event that this information is not available from the POS, the date/time from the POS terminal 140 can be used. If date and time is not available, reader 120 will not send the date time stamp data element.

[0096] In an exemplary embodiment, the data elements contained in the Get Commerce Data request are preconfigured in the reader 120 or POS terminal 140 at setup time. The data may be modified after the reader 120 has been installed and configured.

TABLE 5 – Get Commerce Data

CLA	INS	P1	P2	Lc	Data	Le
90	50	00	00	xx	Merchant ID/ Store ID [+ Loyalty IDs +Coupon Types + Date/Time-Stamp +Application Version + Merchant Capability]	00

TABLE 6 – Command Data

Data Element	Byte Size	Value	Req
Merchant Identifier Tag	2	0xDF 31	Y
Identifier Length	1	xx	
Merchant Identifier	xx	[MerchantID]	
MerchantStore_ID Tag	2	0xDF 32	Y
Merchant_Store_ID Length	1	xx	
Merchant_Store_ID	xx	(StoreID/Location)	
Loyalty_ID Tag #1 For Secondary loyalty	2	0xDF 41	Opt
Identifier Length #1	1	xx	
LoyaltyID #1	xx	[Loyalty ID] (Hex)	
…….			
Loyalty_IDr Tag #X For Secondary loyalty	2	0xDF 41	Opt
Loyalty Identifier Length #X	1	xx	
LoyaltyID #X	xx	Loyalty ID (Hex)	
Date_Time_Stamp Tag	2	0xDF 11	Opt
Date_Time_Stamp Length	1	0x07	
Date_Time_Stamp	7	BCD (yyyymmddhhmmss)	
Commerce_App_Version Tag	2	0xDF 12	Y
Commerce_App_Version Length	1	0x02	
Commerce_App_Version Data	2	[Major + Minor] Hex	
Merchant_Capability Tag	2	0xDF 33	Y
Merchant_Capability Length	1	0x02	
Merchant_Capability Data	2	2 Bytes Hex	
Terminal_Startup_Mode Tag	2	0xDF 34	Opt
Terminal_Startup_Mode Length	1	0x02	
Terminal_Startup_Mode Data	1	1 Bytes Hex	
Total:	<var>		

[0097] Table 7 defines the possible Status Word values that may be returned by the Get Commerce Data command.

TABLE 7 – Status Codes

SW1	SW2	Description
90	00	Successful Execution of Command
61	xx	More data to follow
67	00	Wrong Data Length
69	09	Internal Error

[0098] Any response other than'61 xx' or '90 00' will result in reader 120 terminating commerce application 121 and passing control to the EPM, after recording the error and storing the data for forwarding to commerce widget 115.

[0100] If the Get Commerce Data request is correctly formatted, commerce applet 113 on secure element 112 filters the data based on the merchant identifier ("Merchant_ID"), loyalty identifier ("Loyalty_ID") and offer type code ("Offer_Type_Code") to format a response data for reader 120 based on the version number in the request. Commerce applet 113 may return more than one Loyalty ID and multiple Offers messages based on the configuration in the wallet. Table 8 lists exemplary response data:

TABLE 8 – Example Response Data

Data Element	Byte Size	Value
Consumer_ID Tag	2	0XDF21
Consumer_ID Length	1	0x10
Consumer_ID Data	16	[Consumer ID]
Loyalty_ID Tag #1	2	0xDF41
Loyalty_ID Length #1	1	xx
Loyalty Identifier #1	xx	[Loyalty ID]
Loyalty_Account_Code Tag #1	2	0xDF43
Loyalty_Account_Code Length #1	1	xx
Loyalty_Account_Code #1	xx	[Acct Code]
Loyalty_ID Tag #2	2	0xDF 41
Loyalty_ID Length #2	1	xx
Loyalty_ID Data #2	xx	[Loyalty ID]
Loyalty_Account_Code Tag #2	2	0xDF43
Loyalty_Account_Code Length #2	1	xx
Loyalty_Account_Code Code #2	xx	[Acct Code]
.....		
Offer_ID Tag #1	2	0xDF51
Offer_ID #1 ID Length	2	X'81 xx'

Data Element	Byte Size	Value
Offer_ID #1 ID Value	xx	[Coupon ID]
Offer_Code #1 Code Tag	2	0xDF53
Offer_Code #1 Code Length	2	0x'81xx'
Offer_Code #1 Code Value	xx	[Coupon Code]
Offer_ID Tag #2	2	0xDF51
Offer_ID #2 ID Length	2	0x'81xx'
Offer_ID #2 ID Value	xx	[Coupon ID]
Offer_Code #2 Code Tag	2	0xDF53
Offer_Code #2 Code Length	2	0x'81xx'
Offer_Code #2 Code Value	xx	[Coupon Code]
.....		
Total:	<var>	

[0101] The following is an exemplary response data parsing sample. The NFC reader (or POS terminal) delivers this commerce data to a POS system in a string of data that may contain consumer, loyalty and/or offer data. The merchant POS system can then parse the data to obtain the loyalty and offer data, and process the data per the merchant's specifications.

```
DF 21 10 00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF DF 41 06
18 DB 6E 23 F4 0B DF 43 0D 02 31 38 44 42 36 45 32 33 46 34 30 42
DF 51 08 88 77 66 55 44 33 22 05 DF 53 09 02 42 41 31 38 37 36 35
34 DF 51 08 88 77 66 55 44 33 22 06 DF 53 0C 02 41 39 39 39 39 31
33 33 35 37 38 DF 51 08 88 77 66 55 44 33 22 07 DF 53 10 02 5A 58
31 37 39 35 36 37 35 34 38 33 31 43 46 DF 51 08 88 77 66 55 44 33
22 08 DF 53 0C 02 31 38 30 30 38 37 32 30 30 30 31 DF 51 08 88 77
66 55 44 33 22 09 DF 53 33 02 57 4B 52 50 31 32 33 34 35 36 37 38
39 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D 4E 4F 50 50 57 50 57 50
57 50 57 50 57 50 57 50 57 50 57 50 57 50 40 A1

Data parsing example

DF 21 10 00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF
(Consumer ID)

DF 41 06 18 DB 6E 23 F4 0B            (MoCom Loyalty ID)

DF 43 0D 02 31 38 44 42 36 45 32 33 46 34 30 42
(Consumer Loyalty Code)

DF 51 08 88 77 66 55 44 33 22 05      (MoCom Offer ID)  #1

DF 53 09 02 42 41 31 38 37 36 35 34   (Merchant Offer Code)  #1

DF 51 08 88 77 66 55 44 33 22
```

Post Transaction Data

[0102] As explained above, a Post Transaction Data command provides a mechanism to receive data back from a merchant POS system (MPOS). This command is initiated by the merchant POS terminal 140 and preferably is supported in the merchant capability field. In an exemplary embodiment, this command consists of a single frame of data with a maximum data size of 255 bytes. The contents of the data use standard TLV formatting but may also be variable. This command enables dynamic reconciliation or post transaction data consolidation. Additional data tags may be defined for the transmission of additional data from the POS terminal/MPOS to the secure element 112 in mobile device 110. An exemplary post transaction data command ("Post Transaction Data") is illustrated in tables 9 and 10:

TABLE 9 – Post Transaction Data Command

CLA	INS	P1	P2	Lc	Data	Le
90	52	00	00	xx	<TLV Encoded Post Transaction Data>	00

TABLE 10 – Command Data

Data Element	Byte Size	Value	Req
Transaction ID	2	0x DF 61	Opt
Transaction ID Length	1	xx	
Transaction ID Data	xx	Merchant generated Transaction ID	
Offer_ID Code #1	2	0XDF 51	Opt
Offer_ID Length #1	1	xx	
Offer_ID Data #1	xx	Coupon ID	
…….			
Offer_ID Code #X	2	0xDF 51	Opt
Offer_ID Length #X	1	xx	
Offer_ID Data #X	xx	Coupon ID	
Total:	<var>		

Multi-block data handling

[0103] FIG. 5 illustrates an exemplary multi-block data flow according to an example embodiment. When secure element 112 has more than 255 bytes of data to send, a Get Response command (C0) is used to retrieve the remaining response

data. Particularly, this command is used to obtain the remaining data when the commerce applet 113 must send more than, for example, 255 bytes of response data.

[0104] Referring to FIG. 5, after a user taps a commerce-enabled mobile device 110 to reader 120, reader 120 sends a Select Commerce command to the secure element 112 of the mobile device 110. A positive response ('90 00') causes reader 120 to send a Get Commerce Data command. In response, secure element 112 returns loyalty and offers data. As shown in FIG. 5, the Get Commerce Data response status SW1 flag is set to '61' and the SW2 flag is set to '00'.

[0105] A Get Response command is triggered when the SW1 flag in the Get Commerce Data response is set to '61'. In this example, the SW2 flag is set to '00' because commerce applet 113 on mobile device 110 may not know how much data is left to send. The subsequent response to the Get Response command also contains an SW1 flag set to '61', causing a second Get Response command to be sent by reader 120 to mobile device 110.

[0106] This sequence will terminate when the SW1 flag of the Get Commerce Data response is set to any value other than '61'. For example, an SW1 value of '90' in response to a Get Response command as shown in FIG. 5 will indicate normal completion. Any other SW1 value can be logged as an error.

[0107] Table 11 defines exemplary settings for the Get Response Data APDU command:

TABLE 11 – Get Response Data

CLA	INS	P1	P2	Lc	Data	Le
90	C0	00	00	00	<none>	00

[0108] The actual length of the remaining data is variable. Therefore, the Le data length can be 0x00; allowing the commerce applet 113 to manage a variable length response.

[0109] Table 12 defines possible status word values ("Status Codes") that may be returned by the Get Response Data APDU command.

TABLE 12 – Status Codes

SW1	SW2	Description
90	00	Successful execution of command
61	xx	More data to follow
67	00	Wrong data length
69	09	Internal error

Reader Configuration Data

[0110] In one embodiment, during the installation and configuration of reader 120 certain merchant and commerce specific data are loaded and saved in reader 120. This data is used by reader 120 to fill in the Get Commerce Data command from reader 120. These data elements can be updated as new features and functions become available.

Commerce AID

[0111] As explained above, a commerce AID is sent in the Select Commerce command. If the command is accepted by mobile device 110, commerce applet 113 is started and APDU command / response flows will start between reader 120 and secure element 112. In an exemplary embodiment, the commerce AID value is A00000048510010101. This value can be hardcoded on reader 120. In one embodiment, reader 120 is not required to support partial selection.

Merchant_ID

[0112] A merchant identifier (Merchant_ID (DF31)) can be loaded onto reader 120. Merchant ID is a value assigned by a service provider. In one embodiment, this value is assigned by the MoCom platform operator. This is required to allow commerce applet 113 to filter the loyalty and coupon data, and send the appropriate items to the reader 120.

Merchant_Store_ID

[0113] A merchant store identifier value (Merchant_store_ID (DF32)) is loaded to the reader 120 and is a value assigned by a service provider. This value can be used, for example, for reporting purposes.

Loyalty_ID

[0114] A loyalty identifier value (Loyalty_ID (DF41)) is used when multiple Loyalty IDs are being requested during a tap. This is accomplished by setting the Secondary Loyalty in Merchant Capabilities (DF33). This allows commerce applet 113 to return additional loyalty numbers in the response to a Get Commerce Data command. Multiple (*e.g.*, 5) additional Loyalty_IDs may be coded in the Get Commerce Data request.

Offer_Type_Codes

[0115] Offer type codes (Offer Type Codes (DF54)) are loaded onto reader 120. Values assigned to Offer Type Codes are assigned by a service provider. This value is used by the commerce applet 113 to filter offers and send only the appropriate items to reader 120. Multiple Offer_Type_Codes can be defined and sent to the secure element 112 in the Get Commerce Data command.

Commerce_Application_Version

[0116] A commerce application version number (Commerce_Application_Version) can be loaded onto reader 120 to represent the version of the commerce reader specification that the application on reader 120 is coded to and certified for.

Merchant_Capabilities

[0117] The Merchant Capabilities value represents the Commerce features supported by a particular merchant. This data element can also be used by reader 120 to format the Get Commerce Data command.

Terminal_Startup_Mode

[0118] A terminal start mode command (Terminal Start Mode (DF34)) commands reader 120 to provide the mechanism used to start commerce application 121. This data element is not sent to the secure element 112. This data element will also be used to define processing flows between reader 120 and secure element 112 on the handset.

Get Commerce Data Fields

[0119] Table 13 provides an exemplary definition of data required by reader 120 to format the Select Commerce and Get Commerce Services commands:

TABLE 13

Data Element	Tag	Max Size Bytes	Data Format
Commerce AID		09	Hex
Merchant ID	DF 31	8	Hex
Merchant Store ID	DF 32	32	ASCCI
Loyalty Identifier #1 thru X	DF 41	8	BCD
Date and Time Stamp	DF 11	7	BCD
Specification Version (Major/Minor)	DF 12	2	Hex
Merchant Capabilities	DF 33	2	Binary
Commerce Start Mode	DF 34	2	Binary

Commerce Applet Version Format

[0120] A Commerce Applet Version value is a two-byte hex field the first byte containing the major version (xx) and the second byte contains the minor version (xx). These fields are updated in accordance to the specific version of the reader commerce technical specification that is implemented on reader 120. In an exemplary embodiment, the first official release of the commerce application 121 is 0x0100.

Merchant Capabilities

[0121] A merchant capabilities field (Merchant Capabilities Field (DF 33)) determines which commerce functions are being implemented by the merchant. Reader 120 can pass this field to mobile device 110, and mobile device 110 uses the information to build a response frame, referred to as Commerce Data Response frame. Table 14 illustrates exemplary merchant capabilities:

TABLE 14 – Merchant Capability Data

Commerce Start Mode Format

Byte	Bit	Value	NFC reader function
1	8 MSB	1=Merchant Loyalty Support	If Bit 8 is on the reader will send the required Merchant ID and optionally a

		0=No	Loyalty ID for the merchant
1	7	1=Secondary Loyalty 0=No	Bit 8 must be on. Additional Loyalty ID's is included in the Get Commerce Data request
1	6	1=Offers Support 0=No	Offer Type fields is included in Get Commerce Data request
1	5	1=Additional Offer support 0=No	The merchant can request additional offers in the Get Commerce request
1	4	1=Contactless Payment support 0=No	Some merchants may choose to only accept Commerce but not contactless payments. This bit setting is information only. It will not stop the PPSE process from happening.
1	3	1=Enterprise Merch ID 0=No	
1	2	1=Cloud Based Offer 0=No	Indicates that the merchant can support cloud based offers (Future)
1	2	0	Reserved for Future Use
1	1	1=Post Transaction Data support 0=No	The reader will receive redemption data from the POS and forward it to the handset
2	8-1	0	Reserved for Future Use

Commerce Start Mode Format

[0122] A commerce start mode format value (Commerce Start Mode (DF34)) indicates to reader 120 what mechanism is to be used to start commerce application 121 on reader 120. In one embodiment, this data element is not sent to the mobile device 110 in the Get Commerce Data command. In another embodiment, this data element is optional. Table 15 illustrates exemplary start modes can be used to commence commerce application 121. In an exemplary embodiment, bits 7 and 8 are exclusive and only one bit is turned on at a time:

TABLE 15 – Commerce Start Mode

Byte	Bit	Value	Reader function
1	8 MSB	1=Auto Start 0=No	At the start of the check the reader will quest Commerce AID at the first TAP
1	7	1=Manual Start 0=No	The reader will only select Commerce AID after some user intervention.
1	6	1=Payment with	Payment and Post Transaction Data will

		Post Transaction Data 0=No	occur on TAP 2
1	5	Payment First	Payment PPSE will precede in Auto or Manual start modes
1	4-1	0	Reserved for Future Use
2	8-1	0	Reserved for Future Use

Reader Message Forwarding

[0123] While reading commerce application data from the mobile device 110, reader 120 forwards the data to a merchant POS system or POS application resident on a POS terminal 140. Reader 120 strips off the APDU headers and un-blocks the data from the mobile device 110. The Tagged TLV frames are then wrapped in the appropriate protocol and forwarded to the merchant POS system or POS application running on the POS terminal for processing.

Commerce Response Data Description

[0124] During a successful interaction with a reader 120, data will be returned to the POS merchant system (or POS terminal). This information will typically be composed of a consumer loyalty number and/or some number of offers that the merchant defined and loaded to the consumer's wallet.

Consumer ID

[0125] A consumer identifier (Consumer ID) is a unique identifier that is assigned to a consumer during the wallet activation process. Typically, Consumer ID will stay with a consumer even if the consumer moves her wallet to a new mobile device or different mobile network. In a preferred embodiment, Consumer ID is sent from the mobile device to the reader on every commerce-related interaction, even if the handset has no loyalty or offers data to send. The presentation of Consumer ID can be used by the merchant POS system to trigger specific actions related to a payment-only tap.

Loyalty ID

[0126] A loyalty identifier (Loyalty ID) is sent along with each consumer loyalty number requested during a tap event. Loyalty ID is a unique value assigned to

each merchant loyalty program assigned by the MoCom platform. In most cases the Loyalty ID received by the reader will match the Merchant ID that was configured by the Get Commerce data command. Use of this information by a merchant system is optional.

Consumer Loyalty Code

[0127] A consumer loyalty code (Consumer Loyalty Code) matches the loyalty number assigned to the consumer for a specific merchant loyalty program. Wallet application 114 allows for multiple loyalty numbers to be presented at the tap. If the system is set up for multiple consumer loyalty codes, each consumer loyalty code will be preceded by its unique loyalty ID.

Offer ID

[0128] A mobile commerce offer identifier (Offer ID) is sent along with each consumer offer number sent during a commerce-related session. The Offer ID is a unique value assigned to each offer delivered to a consumer wallet. In one embodiment, no two Offer IDs generated by the MoCom platform will have the same value.

Merchant Offer Code

[0129] A merchant offer code ("Merchant Offer Code" or "Offer Number") is generated by the merchant and loaded to the consumer's wallet application through various means. This number matches the same offer that is defined on the merchant POS system for processing. There can be multiple merchant offers (*e.g.*, 10) presented during a single commerce transaction. The merchant system parses the incoming data to extract the individual merchant offers.

Commerce Response Data Fields

[0130] Table 16 defines exemplary data elements that may be returned to the merchant POS system after a successful commerce transaction:

TABLE 16

Data Element	Tag	Max Size Bytes	Data Format
Consumer ID	DF 21	16	BCD
Loyalty ID	DF 41	8	Hex
Consumer Loyalty Code	DF 43	32	ASCII, Hex, BCD
Offer ID	DF 51	8	BCD
Merchant Offer Code	DF 53	48	ASCII, Hex, BCD

[0131] In one embodiment, a data element "Terminal Start Mode" is passed to reader 120 but will not be passed to the secure element 112. Reader 120 uses this information to control when Select Commerce and Select PPSE commands are sent to the secure element 112.

Reader Commerce Application Functionality

[0132] The following section provides a list of functions that the Commerce application within reader 120 performs. Some of these functions are automated, while others are triggered via an API call from the POS terminal or merchant POS.

Select Commerce AID Command

[0133] After the Commerce application is started on reader 120 and a device is detected in the field of reader 120, the first command sent is Select Commerce AID. The command will contain the RID value assigned by ISO and a PIX value generated by a commerce service provider. The Commerce AID value is A00000048510010101. This value should be hard coded on reader 120.

Get Commerce Data Command

[0134] The Get Commerce Services Data command is a general data request to the secure element 112. The Get Commerce Data has a number of required and optional fields that communicate information to commerce applet 113. Commerce applet 113 uses this information to build the data elements that need to be sent to reader 120. Reader 120 uses the fields in the Merchant Capability records to determine which optional fields need to be included in the request to the handset.

Post Transaction Data

[0135] The Post Transaction Data command was created to provide a mechanism to receive data back from the MPOS. This command consists of a single frame of data with a maximum data size of 255 bytes. The contents of the data use standard TLV formatting, but the contents may be variable. Additional data tags may be defined for the transmission of additional data from the POS Terminal/MPOS to secure element 112 in mobile device 110.

NFC Error recovery

[0136] In a preferred embodiment, reader 120 is able to recover from a reader error generated when the handset is prematurely removed from the NFC field. Reader 120 signals the read error to the consumer via a failure interface such as a speaker that outputs a "beep" or display that provides an optical indication such as via lights. The consumer is asked to tap again and the transaction that was in progress during the error is restarted. In the case where multiple transactions are being processed, such as a commerce transaction and a PPSE transaction, reader 120 will try to recover the last process being executed.

Large Data block support

[0137] In an exemplary embodiment, reader 120 reads and writes multiple 255-byte blocks of data to and from mobile device 112 in a single tap process.

Date and time stamp support

[0138] When reader 120 has connectivity to the merchant POS system, the date and time can be retrieved from the POS terminal at the start of the transaction.

TLV Master Tag List

[0139] Table 17 defines the data elements and corresponding tag values and target/max byte sizes used by commerce based applications. Additional values have been provided for those elements with a limited/fixed value range.

TABLE 17 – APDU Commands

Commerce Services			
Shared Data Elements			
Data Element	Tag	Max	Description

		Size	
DATE_TIME_STAMP	0xDF11	7	Date/Time stamp (yyyymmddhhmmss)
COMMERCE_APP_VERSION	0xDF12	2	Supported Commerce application Version Number
Consumer Data Elements			
Data Element	Tag	Max Size	Description
CONSUMER_ID	0XDF21	16	MoCom Platform specific consumer identifier
CONSUMER_KEY	0xDF22	16	MoCom Platform generated consumer specific 3DES key
CONSUMER_CERT	0xDF23	8	MoCom Platform generated consumer signature/ certificate
Merchant Data Elements			
Data Element	Tag	Max Size	Description
MERCHANT_ID	0xDF31	8	MoCom Platform specific merchant identifier
MERCHANT_STORE_ID	0xDF32	32	MoCom Platform specific merchant store identifier ASCII character data
MERCHANT_CAPABILITY	0xDF33	2	Supported Commerce application Services
NFC READER_START_MODE	0xDF34	2	NFC enabled payment terminal startup mode (provided by Merchant POS System during initialization)
Merchant Capabilities			
Data Element	Value	Max Size	Description
MERCAP_MERCHANT_ LOYALTY	0x80	1	The Get Commerce Data request includes a valid merchant identifier used to determine the Loyalty data received by the applet.
MERCAP_ADDITIONAL_ LOYALTY	0x40	1	The Get Commerce Data request includes additional Loyalty Identifiers. Additional Loyalty data is determined by the specified Loyalty ID(s).
MERCAP_MERCHANT_ OFFERS	0x20	1	Offer type fields are included in Get Commerce Data request

MERCAP_ADDITIONAL_ OFFERS	0x10	1	The Get Commerce Data request includes a valid merchant identifier used to determine the offers data received by the applet.
MERCAP_PAYMENT	0x08	1	Indicates merchant supports contactless payment.
MERCAP_ENTERPRISE	0x04	1	Indicates support for Enterprise Merchant ID
MERCAP_CLOUD	0x02	1	Indicates support for cloud based offers and Loyalty
MERCAP_REDEMPTION	0x01	1	The NFC reader supports the transmission of offer redemption data (from the POS) to the applet via the Redeem Offer command.
Service Provider Platform Data Elements			
PLATFORM_SIGNATURE	0x71	8	MoCom Platform generated MAC/Signature appended to command/data originating from the platform for remote verification purposes (data integrity/ authenticity).
PLATFORM_KEY	0x72	16	MoCom Platform Key
PLATFORM_CERT	0x73	8	MoCom Platform Certificate

Loyalty			
Loyalty Data Elements			
Data Element	Tag	Max Size	Description
EMBEDDED_TLV_ LOYALTY_DATA	0xDF40	xx	Embedded TLV loyalty data tag
LOYALTY_ID	0xDF41	8	MoCom Platform specific loyalty identifier
LOYALTY_STATUS	0xDF42	1	Loyalty card/account status (see below)
LOYALTY_ACCOUNT_ CODE	0xDF43	32	Loyalty account (barcode data)
LOYALTY_MAC_ SIGNATURE	0xDF44	8	MoCom Platform specific MAC/Signature for integrity/ authenticity verification

Transaction Log			
Transaction Data Elements			
Data Element	Tag	Max	Description

		Size	
EMBEDDED_TLV_ TRANSACTION_LOG	0xDF60	xx	Transaction log record data tag
TRANSACTION_ID	0xDF61	16	Transaction ID (assigned by POS)
TRANSACTION_STATUS	0xDF62	3	Transaction log record data tag

Offers			
Offer Data Elements			
Data Element	Tag	Max Size	Description
EMBEDDED_TLV_ OFFER_DATA	0xDF50	xx	Embedded TLV offer data tag
OFFER_ID	0xDF51	8	MoCom Platform specific offer identifier
OFFER_STATUS	0xDF52	1	Offer status (see below)
OFFER_CODE	0xDF53	130	Offer (UPC/EPC/GS1 Databar) barcode data
OFFER_TYPE_CODE	0xDF54	9	Offer Type (see below)
OFFER_MAC_ SIGNATURE	0xDF55	8	MoCom Platform specific data security signature
OFFER_UPDATE_FLAG	0xDF56	1	Update flag (synchronization status)

[0140] Table 18 provides a master list of exemplary APDU commands supported by the Commerce Applet 113.

TABLE 18

Command	CLA	INS	P1	P2	Lc	Data	Le
Get Commerce Data	90	50	00	00	xx	Date/Time Stamp + Merchant ID + Store ID [+ Commerce application Version + Merchant Capabilities + Transaction ID + Loyalty IDs + Offer Codes]	00
Post Transaction Data	90	52	00	00	xx	<TLV-Encoded Transaction Data>	00
Get Remaining Data	90	C0	00	00	xx	None	

Specially Formatted Data Elements

[0141] Data elements included in the commerce data payload may include a format byte that identifies the data encoding used for that element. The data encoding is specified by the merchant to ensure compatibility at the point of sale. The formatted data value is supplied by the commerce platform to the wallet application 114. Thus, no additional interpreting/formatting is necessary between the platform 130, wallet 114, secure element 112, and reader 120/POS terminal 140 (collectively referred to as "payment terminal"). It is the role of the payment terminal (or merchant POS system) to properly interpret the data and supply it to the merchant system for processing.

[0142] In an exemplary embodiment, the following data elements include the following format value:

- Loyalty Account Code (DF 43)
- Offer Code (DF 53)

[0143] Table 19 defines possible format byte values and their corresponding encoding rule:

TABLE 19

Format Byte	Encoding Rule	Description
0x00	Hexadecimal	Each byte of data is encoded in (raw) hexadecimal format.
0x01	Binary Coded Decimal (BCD)	Each nibble represents a single digit. Thus, only decimal values are specified. A data stream containing an odd number (length) of digits includes the hex value 'F' in the first nibble of the data stream.
0x02	ASCII	Each byte represents an ACII value that is interpreted as such and handled as its corresponding CHAR value. In most cases, these data streams are converted into a String before being passed to the merchant POS system for processing.

[0144] A BCD encoded data value that includes the hexadecimal value 'F' in the first nibble shall identify a data stream containing an odd number of digits. Thus, the BCD data stream *12345* is encoded in 3 byte buffer as follows: *0xF12345*.

Exemplary Implementations

[0145] FIG. 6 illustrates windows or screen shots generated by the graphical user interface for a wallet application in accordance with an example embodiment of the present invention. For purposes of this exemplary implementation, the mobile device 110 has some redeemable offers and loyalty cards stored in memory 111b.

[0146] The wallet home screen 601 features a strip of merchant tiles 604. A tile is present for every merchant that has a redeemable object (*e.g.*, a redeemable offer or loyalty card) present in the mobile wallet. The user may, for example, swipe through the tiles, left and right, to find a particular merchant. Once the particular merchant is found, the tile is selected to open a merchant offer view 602. This can be done prior to making a transaction or immediately prior to making the transaction, such as while waiting in line, or earlier (*e.g.*, while browsing through a store.).

[0147] The merchant offer view 602 presents a list of redeemable offers 603 available in the wallet. Non-redeemable promotions may be presented as well. If present, a loyalty card 605 is also presented and made accessible from the merchant offer view 602.

[0148] If the selected merchant is not a commerce-enabled merchant, there is no option presented to load offers for a commerce transaction. If the merchant is a commerce-enabled merchant, however, one or more buttons or icons 606a, 606b are presented allowing offers to be loaded for a commerce transaction.

[0149] The user may select an offer (*e.g.*, 606a), and then select the "Done" bar at the bottom of the screen.

[0150] In an exemplary embodiment, a limit as to the number of offers can be enforced by secure element 112 (*e.g.*, 10 offers), and the user interface of commerce widget 115 enforces this limit while the user is activating offers. The "Done" bar is the trigger to load the selected offers into secure element 112. If there are offers from another merchant in the secure element 112, they can be removed at the same time as the new offers are loaded – this ensures that there are only offers from one merchant present in the 112 at any given time.

[0151] When the secure element load is complete, the user taps the mobile device 110 to reader 120. What happens next depends on a few factors. If the reader that is tapped is not capable of processing commerce elements, the selected payment card is sent, but no commerce elements (*e.g.*, offers or loyalty credentials) are sent. A post-tap message is presented through the reader interface indicating that payment credentials were sent, with no other information.

[0152] If the reader that is tapped is capable of processing commerce elements, but the merchant-ID does not match the selected merchant, offers will not be sent. Commerce applet 113 in secure element 112 can search for a loyalty card for this merchant-ID and transmit loyalty credentials, if present. A post-tap message is presented through an interface indicating that an event took place, identifying the merchant and reporting that loyalty credentials were sent (if they were available) as well as the payment credentials.

[0153] If the reader that is tapped is a commerce-enabled reader and the merchant-ID matches the selected merchant, selected offers and (if present) the loyalty card credentials for the merchant are sent. Mobile device 110 can present a post-tap message through the commerce widget 115 user interface confirming that offers and loyalty (if present) were sent, along with payments.

[0154] Following the tap, offers that were loaded into the secure element 112 are left in secure element 112 until the user removes them or selects offers from another merchant. Alternatively, if the offers expire, it is removed from the secure element 112 when wallet maintenance is performed. In an exemplary embodiment, the selected merchant will remain the "active" merchant on the wallet home page until the user selects a different merchant.

Instant Offer Implementation

[0155] FIG. 7 illustrates a flow diagram illustrating an exemplary instant offer implementation according to an embodiment of the present invention. In this embodiment, a mobile commerce (MoCom) platform can be integrated with merchant POS system to implement a mechanism for users to select offers by using a wallet application and/or instant offers merchants make available to consumers.

[0156] A wallet application running on a mobile device can be used to allow consumers to pay for purchases and present loyalty and offers via a payment terminal. One way a consumer can redeem an offer is by selecting the offer via the wallet application to be presented at checkout.

[0157] Consumers can also be provided with offers that can be instantly redeemed through the wallet application. Such offers are referred to herein as "instant offers". This feature allows merchants to reward consumers who use a mobile device running the wallet application to make purchases. Consumers benefit from the instant offer because, among other reasons, they do not need to specifically select an offer via the wallet application. Depending on the implementation, an instant offer can be used along with an offer explicitly selected by the consumer from the wallet application. Whether an offer is selected by the consumer or provided "instantly," a consumer identifier ("Consumer ID") value retrieved from the mobile device (*e.g.,* from secure element 112) is used as the key for retrieving and redeeming an instant offer.

[0158] Referring to FIG. 7, in one embodiment, a consumer selects offers from the wallet application to be presented at the checkout. At block 702, a payment is requested at a POS. If at block 704, it is determined that the payment is not a contactless payment, then at block 706 the payment process is completed via alternative means (*e.g.*, by using cash) and the checkout process is completed. If it is determined at block 704 that the payment will be a contactless payment, then the mobile device user is asked to tap his or her mobile device to the reader (*e.g.*, reader 120 described above).

[0159] In response, the mobile device is tapped to the reader. During the tap event, a number of data elements can be passed between the reader and a secure element on the mobile device as described above. In one embodiment, the payment card data, Consumer ID, loyalty number, and offer codes are passed to the reader during the tap of the reader. In this embodiment, Consumer ID is sent to the reader even if the tap is for a payment only transaction with no offers selected.

[0160] If at block 708 it is determined that a MoCom Consumer ID is not present, then at block 706 the payment process is completed and the checkout process is completed by processing the payment.

[0161] If it is determined at block 708 that a MoCom Consumer ID is present, then at block 710 a determination is made as to whether a MoCom offer is present (*e.g.*, an offer selected by the user via a wallet application). If at block 710 a determination is made that a MoCom offer is present, then a determination is made at block 712 as to whether a MoCom instant offer has been defined as well. If at block 712 it is determined that a MoCom instant offer has been defined, both the MoCom offer (*i.e.*, an offer selected by a user via a wallet application interface) and MoCom instant offer are processed, as shown in block 714. Once the MoCom offer and/or MoCom instant offer are processed, the payment associated with those offers is processed as shown at step 706.

[0162] If at block 710 a determination is made that a MoCom Offer is not present, then at block 716 a determination is made as to whether a MoCom instant offer has been defined. If not, the payment is completed as shown at step 706. If a determination is made at block 716 that the MoCom instant offer is present, the MoCom instant offer is processed as shown at block 718 and the payment associated with the MoCom instant offer processed as shown at block 706.

[0163] If a determination is made at block 712 that a MoCom instant offer has not been defined, then a standard MoCom offer is processed, as shown at block 720 and at block 706 the payment processed is completed.

[0164] The merchant POS system can use the presence of the ConsumerID to trigger the use of an instant offer. The offer could be, for example, a cents off or percentage off type offer that a merchant using the MoCom system defines. This can be, for example, applied for the purchase of a specific item. In an exemplary implementation, the merchant is provided an option of turning instant offer functionality off or on when a wallet offer is presented during the tap.

[0165] The instant offer can be defined by a merchant and then distributed to its retail locations. The offer can also have an associated specific start and end date.

The ability to distribute instant offers to different geographical areas can be taken into account as well.

Commerce Applet Package/Applet/Instance Management

[0166] The following section defines the AID values and application specific parameters used during download/installation of commerce applet 113 (FIG. 1). Table 20 defines AIDs.

TABLE 20 – AIDs

Description	AID
Package AID	A0 00 00 04 85 10 01 01
Applet AID	A0 00 00 04 85 10 01 01 00
Instance AID	A0 00 00 04 85 10 01 01 01

Applet-Specific Installation Parameters

[0167] The commerce applet's initial commerce services data characteristics may be provisioned via applet-specific installation parameters. This data follows the standard JavaCard AID and installation parameters.

These parameters must be coded as shown in Table 21:

TABLE 21 – Applet Installation Parameters

Provisioning Data	Byte Size	Default Value
Maximum Number of Loyalty Records	2	20
Maximum Number of Pre-Load Merchant Records	2	1
Maximum Number of Transaction Records	2	3
Total:	6	

Memory Requirements

[0168] Exemplary memory specifications are listed in Table 22 below. The first memory specification, "Package Download," indicates the approximate amount of non-volatile (EEPROM) memory space required to download the commerce applet package. The second memory specification, "Instantiation," indicates the amount of memory required to instantiate a new instance of the commerce applet.

The final memory requirement, "Transient Data Space," indicates the amount of volatile (RAM) memory that is used by each instance of the commerce applet.

TABLE 22 – Applet Memory Requirements

Memory	Byte Size
Package Download	9396
Instantiation	6260
Transient Data Space	518

Data Management

[0169] The available commerce (*e.g.*, loyalty, offers, rewards, etc.) data is stored within the commerce applet 113 onboard the secure element 112. All of the relevant commerce data is stored in three separate data tables. These data tables are managed by the commerce applet 113. Additional commerce data may be stored/managed within a corresponding commerce widget 115 onboard the handset.

[0170] In one embodiment, the data elements defined herein have a variable length. Therefore, all elements (included those with a fixed length) will be assigned a maximum length. As a result, all lengths and byte size references should be interpreted as maximum values.

Commerce Data

[0171] Commerce applet 113 manages a few data fields that are shared by all commerce service applications. These data fields are stored in persistent data variables. An exemplary data element, Consumer ID, is defined in Table 23. Additional elements may be stored as well, such as consumer/platform keys and certificates.

TABLE 23

Variable	Type	Description
ConsumerID	byte[]	Unique consumer ID assigned to a specific MoCom consumer/user.

Loyalty Data Table

[0172] Commerce applet 113 also includes loyalty data tables enabling the storage/management of all consumer loyalty data.

[0173] Table 24 defines the data elements (and their corresponding tag values used during TLV encoding) that are included in the loyalty data table.

TABLE 24 – Loyalty Data

Data Element	Tag Value	Byte Size	TLV Encoding Overhead
LOYALTY_PROGRAM_ID	0xDF41	8	3
LOYALTY_ACCOUNT_CODE	0xDF43	32	3
Total:		40	6
Minimum TLV Encoded Record Size:		46	

[0174] The data is stored in a record oriented data buffer, where the loyalty identifier ("Loyalty ID") is utilized as the key field for search/retrieval tasks.

[0175] In an exemplary embodiment, TLV Data Overhead includes a (maximum) of five bytes per element data overhead (2-byte tag and 3-byte length) as required by the BER-TLV encoding format.

[0176] In an alternative embodiment, an index (or hash table) may be created internally to speed up the Loyalty ID search task.

Cached Merchant Data Table

[0177] Commerce applet 113 also includes a merchant cached data table enabling the storage/management of all data related to a given merchant. This feature allows the commerce data for a given merchant to be pre-loaded by the wallet application 114 in order to improve performance.

[0178] Table 25 defines the data elements (and their corresponding tag values used during TLV encoding) that are included in the cached merchant data table.

TABLE 25 – Cached Merchant Data

Data Element	Tag Value	Byte Size	TLV Encoding Overhead
MERCHANT_ID	0xDF31	8	3
LOYALTY_PROGRAM_ID	0xDF41	8	3
LOYALTY_ACCOUNT_CODE	0xDF43	32	3

OFFER_ID	0xDF51	8	3
OFFER_CODE	0xDF53	130	3
.....			
Maximum		104	6
Minimum TLV Encoded Record Size:		110	

[0179] The data is stored in a record oriented data buffer, where the merchant identifier ("Merchant ID") is utilized as the key field for search/retrieval tasks. An index (or hash table) may be created internally to speed up the Merchant ID search task.

[0180] In an exemplary embodiment, TLV Data Overhead includes a (maximum) of five bytes per element data overhead (2-byte tag and 3-byte length) as required by the BER-TLV encoding format.

Transaction Log

[0181] Commerce applet 113 includes a transaction log that is used to track usage within the MoCom platform at the merchant point-of-sale. During commerce widget 115 and secure element 112 synchronization tasks, this transaction log is transmitted up to the commerce widget 115 for later over-the-air ("OTA") synchronization with the MoCom platform.

[0182] The actual content of the transaction log depends upon the Get Commerce Data command data/parameters provided by reader 120 during the transaction process at the merchant point-of-sale. An exact copy of the data payload sent to the commerce applet 113 by reader 120 via the Get Commerce Data APDU command is stored within that commerce transaction's record.

[0183] The transaction status is determined based on the logical result of the commerce data processing. If a data/processing error is detected within the commerce applet 113, the corresponding internal error code can be appended to the transaction log.

[0184] The following table defines the data elements (and their corresponding tag values used during TLV encoding) that are included in the transaction log.

TABLE 26 – Transaction Log Data

Data Element	Tag Value	Byte Size	TLV Encoding Overhead

Get Commerce Data command parameter(s)/data	xx	255	4
TRANSACTION_STATUS	0xDF62	3	3
Total:		266	7
Maximum TLV Encoded Record Size:		273	

[0185] The data is stored in a record oriented data buffer. A variable Get Commerce Data command data size is supported.

[0186] TLV Data Overhead includes a (maximum) of five bytes per element data overhead (2-byte tag and 3-byte length) as required by the BER-TLV encoding format.

Error Management

[0187] In an exemplary embodiment, error detection and management is handled at two levels. First, the response of the APDU command includes a two-byte Status Word result value. These responses are standardized and dictated by ISO 7816-4. However, a second level of error handling is managed internally by the Commerce Services applet. The second level of management includes the issuance of a standard 0x6909 status word in the response to the APDU command. Following this response, the client may issue a second command ("Get Internal Error Code") to obtain a two-byte internal error code. This code may be cross-referenced to Table 27. Table 27 provides details on where and why the error occurred within the applet.

[0188] Particularly, Table 27 provides a master list of all possible internal error codes returned by the Get Internal Error Code APDU command supported by the commerce applet.

TABLE 27 – Internal Error Codes

Error Code	Error Description
0x0101	SSE_INTERNAL_ERROR_APPLET_NOT_PROVISION
0x0102	SSE_INTERNAL_ERROR_COMMAND_NOT_ALLOWED_VIA_CONTACTLESS_INTERFACE
0x0103	SSE_INTERNAL_ERROR_COMMAND_NOT_ALLOWED_INVALID_CONTEXT
0x0201	SSE_INSTALL_INVALID_INSTALLATION_PARAMETER_LENGTH
0x0301	SSE_PARSE_COMMAND_DATA_INVALID_COMMERCE_TAG
0x0302	SSE_PARSE_COMMAND_DATA_INVALID_CONSUMER_ID_LENGTH

0x0302	SSE_PARSE_COMMAND_DATA_INVALID_MERCHANT_ID_LENGTH
0x0302	SSE_PARSE_COMMAND_DATA_INVALID_MERCHANT_LOCATION_LENGTH
0x0303	SSE_PARSE_COMMAND_DATA_INVALID_DATE_TIME_STAMP_LENGTH
0x0304	SSE_PARSE_COMMAND_DATA_INVALID_MERCHANT_COMMERCE_APP_ VERSION_LENGTH
0x0305	SSE_PARSE_COMMAND_DATA_INVALID_MERCHANT_CAPABILITIES_ LENGTH
0x0306	SSE_PARSE_COMMAND_DATA_INVALID_LOYALTY_ID_LENGTH
0x0307	SSE_PARSE_COMMAND_DATA_INVALID_LOYALTY_ACCOUNT_CODE_ LENGTH
0x0308	SSE_PARSE_COMMAND_DATA_INVALID_OFFER_ID_LENGTH
0x0309	SSE_PARSE_COMMAND_DATA_INVALID_OFFER_TYPE_CODE_LENGTH
0x030A	SSE_PARSE_COMMAND_DATA_INVALID_TRANSACTION_ID_LENGTH
0x030B	SSE_PARSE_COMMAND_DATA_INVALID_CACHED_MERCHANT_DATA_ OFFER_COUNT_LENGTH
0x030C	SSE_PARSE_COMMAND_DATA_INVALID_CACHED_MERCHANT_DATA_ LENGTH
0x030D	SSE_PARSE_COMMAND_DATA_INVALID_COMMERCE_TAG
0x0A01	SSE_GET_RESPONSE_REMAINING_DATA_INVALID_RESUME_STATE
0x0B01	SSE_VERIFY_REQUIRED_PARAMETERS_INVALID_PARAMETER_TAG
0x0B02	SSE_VERIFY_REQUIRED_PARAMETERS_DATE_TIME_STAMP_NOT_ PRESENT
0x0B03	SSE_VERIFY_REQUIRED_PARAMETERS_MERCHANT_ID_NOT_PRESENT
0x0B04	SSE_VERIFY_REQUIRED_PARAMETERS_MERCHANT_STORE_ID_NOT_ PRESENT
0x0B05	SSE_VERIFY_REQUIRED_PARAMETERS_MERCHANT_COMMERCE_APP_ VERSION_NOT_PRESENT
0x0B06	SSE_VERIFY_REQUIRED_PARAMETERS_MERCHANT_CAPABILITIES_NOT_ PRESENT
0x0B07	SSE_VERIFY_REQUIRED_PARAMETERS_LOYALTY_ID_NOT_PRESENT
0x0B08	SSE_VERIFY_REQUIRED_PARAMETERS_LOYALTY_ACCOUNT_CODE_NOT_ PRESENT
0x0B0A	SSE_VERIFY_REQUIRED_PARAMETERS_CONSUMER_ID_NOT_PRESENT
0x0B0B	SSE_VERIFY_REQUIRED_PARAMETERS_CACHED_MERCHANT_DATA_ OFFER_COUNT_NOT_PRESENT
0x0B0C	SSE_VERIFY_REQUIRED_PARAMETERS_EMBEDDED_TLV_CACHED_ MERCHANT_DATA_NOT_PRESENT
0x0C01	SSE_GET_COMMERCE_DATA_INVALID_WALLET_STATE
0x0E01	SSE_UPDATE_CACHED_MERCHANT_DATA_FAILED_CMD_BUFFER_ LENGTH_EXCEEDED
0x1101	LME_INVALID_LOYALTY_TAG
0x1102	LME_INVALID_LOYALTY_ID_LENGTH
0x1103	LME_INVALID_LOYALTY_ACCOUNT_CODE_LENGTH
0x1201	LME_GET_LOYALTY_DATA_RECORD_NOT_FOUND
0x1202	LME_GET_LOYALTY_DATA_INSUFFICIENT_BUFFER_LENGTH
0x1301	LME_UPDATE_LOYALTY_ID_NOT_SPECIFIED
0x1401	LME_DELETE_LOYALTY_ID_NOT_SPECIFIED
0x1402	LME_DELETE_LOYALTY_DATA_RECORD_NOT_FOUND

0x1501	LME_GET_LOYALTY_RECORD_INSUFFICIENT_BUFFER_LENGTH
0x3101	TLVME_MAX_DATA_LENGTH_EXCEEDED
0x3201	TLVME_APPEND_FAILED_INVALID_LENGTH
0x3301	TLVME_GET_NEXT_TAG_FAILED_INVALID_CONTEXT_NO_CURRENT_TAG
0x3401	TLVME_GET_TLV_OBJECT_FAILED_INVALID_TAG_CLASS
0x3402	TLVME_GET_TLV_OBJECT_FAILED_INVALID_LENGTH
0x3403	TLVME_GET_TLV_OBJECT_FAILED_TLV_LENGTH_NOT_SUPPORTED
0x3501	TLVME_GET_NEXT_ELEMENT_FAILED_INVALID_TAG_CLASS
0x3502	TLVME_GET_NEXT_ELEMENT_FAILED_TLV_LENGTH_NOT_SUPPORTED
0x3503	TLVME_GET_NEXT_ELEMENT_FAILED_INVALID_LENGTH
0x3504	TLVME_GET_NEXT_ELEMENT_FAILED_BUFFER_LENGTH_EXCEEDED
0x4101	DME_DATAMANAGER_INVALID_RECORD_NUMBER
0x4102	DME_DATAMANAGER_INVALID_RECORD_LENGTH
0x4103	DME_DATAMANAGER_RECORD_NOT_INITIALIZED
0x4104	DME_DATAMANAGER_RECORD_STORE_FULL
0x4105	DME_DATAMANAGER_INVALID_DATA_LENGTH
0x4106	DME_DATAMANAGER_INSUFFICIENT_BUFFER_SIZE
0x4201	DME_DATAMANAGER_PRIMARY_INDEX_NOT_ACTIVE
0x4202	DME_DATAMANAGER_PRIMARY_INDEX_KEY_NOT_SPECIFIED
0x4203	DME_DATAMANAGER_INVALID_PRIMARY_INDEX_KEY_LENGTH
0xA201	SUE_NO_INSTALL_PARAMETERS_FOUND
0xA202	SUE_INSUFFICIENT_APPLICATION_PARAMETER_BUFFER_LENGTH
0xA203	SUE_NO_APPLICATION_SPECIFIC_INSTALL_PARAMETERS_FOUND
0xD101	SSE_SECURITY_AUTHENTICATION_FAILED
0xD102	SSE_SECURITY_INVALID_CIPHER_DATA_LENGTH
0xD103	SSE_SECURITY_INVALID_KEY_DATA_LENGTH
0xD104	SSE_SECURITY_INVALID_DIVERSIFICATION_DATA_LENGTH
0xDC00	SSE_SECURITY_CRYPTO_EXCEPTION_UNDEFINED_REASON
0xDC01	SSE_SECURITY_CRYPTO_EXCEPTION_ILLEGAL_VALUE
0xDC02	SSE_SECURITY_CRYPTO_EXCEPTION_UNINITIALIZED_KEY
0xDC03	SSE_SECURITY_CRYPTO_EXCEPTION_NO_SUCH_ALGORITHM
0xDC04	SSE_SECURITY_CRYPTO_EXCEPTION_INVALID_INIT
0xDC05	SSE_SECURITY_CRYPTO_EXCEPTION_ILLEGAL_USE

Commerce Services

[0189] The following section provides a detailed description of the APDU commands available via the commerce applet 113.

APDU Commands

[0190] All communications/data exchanges with the commerce applet 113 will be performed via APDU commands as defined in the ISO 7816 standards. Additional restrictions and data handling are described below.

Command Usage Restrictions

[0191] For security reasons, a subset of the available commerce service commands can be restricted to specific connection modes. In one embodiment, referred to as "contact (wallet) mode," all of the APDU commands defined in Table 18 above are available. However, in contactless mode, the following commands are allowed:

- Get Version
- Get Internal Error Code
- Get Response (Remaining Data)
- Get Commerce Data

[0192] If any other APDU command is sent in contactless mode, an exception is thrown and the Internal Error Code is set to the corresponding invalid command mode value (0x0102).

[0193] In one embodiment, the Get Commerce Data command may only be successfully executed when wallet application 114 is open. When the wallet application 114 is either started or terminated by the consumer, it is the responsibility of the wallet application 114 to notify a wallet companion applet (WCAp) so that it can perform monitoring, management and/or security functions. The WCAp applet, in turn, notifies the commerce applet of the wallet application state via a shared interface. WCAp applets are discussed in U.S. Pat. Appln. No. 13/857,400 entitled "Systems, Methods, and Computer Program Products For Securing And Managing Applications On Secure Elements," which is hereby incorporated by reference in its entirety.

Data Payload Management

[0194] Commerce applet 113 validates that all required parameters have been included in the data payload. However, in most cases all non-relevant data elements can be ignored and a command will still process normally. In one

embodiment, the length expected (Le) value is not verified by the commerce applet 113. It can be assumed to be the value zero, allowing the commerce applet 113 to send all available data via the response.

Get Version

[0195] The Get Version command is used to obtain the version information of the currently loaded commerce applet 113. The version will be stored in three bytes (xx.yy.zz), where xx = release version, yy = major version (Wave) number, and zz = minor version number. This information is assigned by, for example, a MoCom platform system, specified during applet development or packaging, or stored as a static value within the code, and cannot be changed.

[0196] Table 28 defines the settings for the Get Version APDU command:

TABLE 28 – Internal Get Version

CLA	INS	P1	P2	Lc	Data	Le
90	10	00	00	00	*<none>*	3

[0197] In one embodiment, no data is sent to the commerce applet. The Lc data length is 0x00.

[0198] The version information is contained within a three-byte response. The Le data length is 0x03. A length of 0x00 is also allowed. Exemplary response data elements are defined in Table 29:

TABLE 29 – Response Data

Data Element	Byte Size	Value
Commerce Specification Version Tag	1	0xDF12
Commerce Specification Version Length	1	3
Commerce Specification Version Value	3	[Version (xx.yy.zz)]
Total:	5	

[0199] Table 30 defines the possible Status Word values that may be returned by this command.

TABLE 30 – Status Codes

SW1	SW2	Description

90	00	Successful Execution of Command
67	00	Wrong Data Length
69	09	Internal Error

Provision Applet

[0200] An applet provisional command, "Provision Applet," allows the provisioning (or update) of the consumer related data, including the consumer ID and optionally related security data (key value and certificates). The new/updated data values are specified via the command data. In an exemplary embodiment, the Provision Applet command may only be used to update the Consumer ID.

[0201] Tables 31 and 32 define the settings for the Provision Applet APDU command:

TABLE 31 – Provision Applet

CLA	INS	P1	P2	Lc	Data	Le
90	12	00	00	XX	TLV-Encoded Provisioning Data	00

[0202] The incoming data, illustrated in table 31, consists of the TLV encoded provisioning data. Therefore, the Lc data length is variable.

[0203] In one embodiment, no data is returned by the commerce applet 113. The Le data length is 0x00.

TABLE 32 – Command Data

Data Element	Byte Size*	Value
Provisioning Data Element Tag	1	[Element Tag]
Element Data Length	1	xx
Element Data Value	xx	[Data]
…….		
Total:	<var>	

[0204] Table 33 defines the possible Status Word values that may be returned by Provision Applet command

TABLE 33 – Status Codes

SW1	SW2	Description
90	00	Successful Execution of Command
67	00	Wrong Data Length

69	09	Internal Error

Get Consumer Info

[0205] The Get Consumer Info command is used to obtain a subset of static data related to the token owner (*i.e.*, consumer). This data includes the following:

Consumer Identifier

[0206] Table 34 defines the settings for the Get Consumer Info APDU command:

TABLE 34 – Get Consumer Info

CLA	INS	P1	P2	Lc	Data	Le
90	14	00	00	00	*<none>*	00

[0207] No data is sent to the commerce applet 113. The Lc data length is, for example, 0x00. The actual length of the requested consumer information returned by the applet is variable, specific to the available consumer data. Therefore, the Le data length is 0x00, allowing the applet to manage a variable length response.

[0208] The response data is returned as a TLV formatted data steam. The Consumer ID may also be returned.

TABLE 35 – Response Data

Data Element	Byte Size	Value
Consumer ID Tag	1	0XDF21
Consumer ID Length	1	16
Consumer ID	16	[Consumer ID]
Total:	<var>	

[0209] Table 36 defines the possible Status Word values that may be returned by this command.

TABLE 36 – Status Codes

SW1	SW2	Description
90	00	Successful Execution of Command
67	00	Wrong Data Length
69	09	Internal Error

Get Commerce Data

[0210] The Get Commerce Data command provides commerce information (*e.g.*, loyalty, offers and rewards) for a specified merchant (or set of merchants), based on the specified merchant/loyalty identifiers and supported offer types. This command provides a single point of contact for reader 120 attached to the merchant POS system (*e.g.*, POS terminal).

[0211] A date/time stamp, merchant ID, store ID, commerce protocol version, and merchant capabilities byte can be sent as part of the incoming data. Additional loyalty identifiers may also be sent in order to specify (filter) the loyalty information requested. The applet shall search a loyalty data table (Table 5), for the specified merchant/loyalty program ID(s) and retrieve the corresponding loyalty data. Additional offer type codes may be also sent as part of the incoming data in order to specify the type of offer information requested. The commerce applet 113 searches the cached merchant data table (Table 25) for the specified merchant identifier/offer code(s) and retrieves the corresponding offer data.

Required Parameters include:

- Date/Time Stamp
- Merchant ID
- Store ID
- App Version

[0212] Once transmission has been successfully completed, the applet shall create an entry in its transaction log recording the commerce data request.

[0213] Tables 37 and 38 define the settings for the Get Commerce Data APDU command:

TABLE 37 – Get Commerce Data

CLA	INS	P1	P2	Lc	Data	Le
90	50	00	00	xx		00

[0214] The incoming data consists of a date/time stamp (used for transaction logging), merchant identifier, store identifier, merchant capabilities byte, and an optional set of additional data elements, including one or more additional loyalty identifiers (indicating loyalty programs supported by the merchant location), and additional offer codes (indicating the type of offers supported by the merchant location). In one embodiment, if a merchant does not specify a Merchant Capability parameter, a default mode supporting only merchant based loyalty and offers is used.

[0215] The actual length of the requested commerce data returned by the applet is variable specific to the available loyalty/offers related data. Therefore, the Le data length is 0x00, allowing the applet to manage a variable length response.

TABLE 38 – Command Data

Data Element	Byte Size	Value
Date/Time Stamp Tag	1	0xDF11
Date/Time Stamp Length	1	7
Date/Time Stamp	7	[Date/Time Stamp]
Merchant ID Tag	1	0xDF31
Merchant ID Length	1	8
Merchant ID	8	[Merchant ID]
Store ID Tag	1	0x32
Store ID Length	1	32
Store ID	32	[Store ID]
Commerce Version Tag	1	0xDF12
Commerce Version Length	1	3
Commerce Version Data	2	[Commerce App Version]
Merchant Capability Tag	1	0xDF33
Merchant Capability Length	1	2
Merchant Capability Data	1	[Merchant Capability Code]
Transaction ID Tag	1	0xDF61
Transaction ID Length	1	16
Transaction ID	16	[Transaction ID]
Additional Loyalty ID Tag	1	0xDF41
Additional Loyalty ID Length	1	8
Additional Loyalty ID	8	[Loyalty ID]
…….		
Additional Offer Type Tag	1	0xDF54
Additional Offer Type Length	1	9
Additional Offer Type Code	9	[Offer Type Code]

.....		
Total:	<var>	

[0216] The response data is returned as a TLV formatted data steam. The MoCom platform-specific consumer identifier and all relevant loyalty/offers data are returned in a single data payload.

Consumer ID

[0217] The Consumer ID is sent in TLV format, where the data is sent using the tag CONSUMER_ID (0XDF21). In one embodiment, unless an error is detected, the consumer ID shall always be returned.

Loyalty

[0218] In one embodiment, each instance of loyalty data shall consist of the following TLV encoded data elements:

- Loyalty Identifier
- Loyalty Account Code

[0219] Within this data stream, the first tag shall contain the Loyalty Identifier tag (*T*) byte (0xDF41). The length (*L*) byte shall specify the length of the Loyalty Identifier. The value (*V*) shall contain the actual Loyalty Identifier of *L* length for the corresponding Loyalty Data that will immediately follow.

[0220] The second tag should contain the Loyalty Account Code tag (*T*) byte (0xDF43). The length (*L*) byte shall specify the total length of the account code data linked to the previous Loyalty Identifier. The value (*V*) shall contain the actual loyalty data of *L* length.

[0221] Any additional loyalty identifiers found within the loyalty data table are appended to the TLV encoded data payload using this same format.

Offers

[0222] Each instance of offer data shall consist of the following TLV encoded data elements:

- Offer ID
- Offer Code

[0223] Within this data stream, the first tag contains the Offer ID tag (*T*) byte (0xDF51). The length (*L*) byte specifies the length of the Offer ID. The value (*V*) contains the Offer ID for the corresponding offer data that will immediately follow.

[0224] The second tag preferably contains the Offer Code tag (*T*) byte value (0xDF53). The length (*L*) byte specifies the length of the Offer Type Code. The value (*V*) contains the Offer Code data for the corresponding Offer ID.

[0225] Any additional offer identifiers found within the offer data table are appended to the TLV encoded data payload using this same format. Exemplary response data is defined in Table 39.

TABLE 39 – Response Data

Data Element	Byte Size	Value
Consumer Identifier Tag	1	0XDF21
Consumer Identifier Length	1	16
Consumer Identifier	16	[Consumer ID]
Loyalty Identifier Tag	1	0xDF41
Identifier Length	1	8
Loyalty Identifier	8	[Loyalty ID]
Loyalty Account Code Tag	1	0xDF43
Account Code Length	1	32
Loyalty Account Code	32	[Acct Code]
…….		
Offer ID Tag	1	0xDF51
Offer ID Length	1	8
Offer ID Value	8	[Offer ID]
Offer Code Tag	1	0xDF53
Offer Code Length	1	130
Offer Code Value	130	[Offer Code]
…….		
Total:	<var>	

[0226] Commerce applet 113 manages the transmission of multiple response packets (using the Get Response command) when the total data length exceeds 256 bytes. Table 40 defines the possible Status Word values that may be returned by the Get Response command.

TABLE 40 – Status Codes

SW1	SW2	Description

90	00	Successful Execution of Command
61	00	Successful Execution of Command w/ Additional data available via Get Response
67	00	Wrong Data Length
69	09	Internal Error

Post Transaction Data

[0227] The Post Transaction Data command provides a method through which the Merchant PoS system or payment terminal may return post-transaction data, including redeemed coupons, new offers, e-receipts, or other enhanced commerce data.

[0228] Tables 41 and 42 define the settings for the Post Transaction Data APDU command:

TABLE 41 – Post Transaction Data

CLA	INS	P1	P2	Lc	Data	Lc
90	52	00	00	xx	<TLV-Encoded Transaction Data>	00

[0229] The incoming data consists of the TLV encoded provisioning data and a platform signature for authenticity purposes. Therefore, the Lc data length is variable.

[0230] Data need not be returned by commerce applet 113. The Le data length is 0x00.

TABLE 42 – Command Data

Data Element	Byte Size	Value
Post Transaction Data Element Tag	1	[Element Tag]
Element Data Length	1	xx
Element Data Value	xx	[Data]
.....		
Total:	<var>	

[0231] Table 43 defines the possible Status Word values that may be returned by the Post Transaction Data command.

TABLE 43 – Status Codes

SW1	SW2	Description

90	00	Successful Execution of Command
67	00	Wrong Data Length
69	09	Internal Error

Get Transaction Log

[0232] The Get Transaction Log is used to obtain all data stored in the transaction log. This command is typically used by the commerce widget for the purpose of widget and secure element data synchronization tasks.

[0233] Table 44 defines the settings for the Get Transaction Log APDU command:

TABLE 44 – Get Transaction Log

CLA	INS	P1	P2	Lc	Data	Le
90	54	00	0x	00	*<none>*	

P2 Value	Applet Behavior
0x00	Normal processing.
0x01	Clear transaction log. No data transmitted.
0x02	Get Transaction Log Status

[0234] In one embodiment, no data is sent to the commerce applet. The Lc data length is 0x00. The actual length of the transaction data returned by the applet is variable, depending on the number of transaction records and the variable length of the corresponding transaction log data. Therefore, the Le data length can be 0x00, allowing commerce applet 113 to manage variable length response.

[0235] Preferably, response data is returned as a TLV formatted data steam.

Transaction Log Response Data

[0236] Each transaction log record shall consist of an Embedded-TLV Transaction Log tag followed by all related data elements. The data elements included in the transaction record are a mirror of those provided during the corresponding Get Commerce Data command requested by the Commerce-enabled payment terminal (NFC reader) at the merchant point-of-sale. Additional transaction log records are appended to the data using the same format. Table 45 illustrates exemplary response data.

TABLE 45 – Response Data

Data Element	Byte Size	Value
Embedded TLV Transaction Record Tag	1	0xDF60
Embedded TLV Transaction Record Length	3	xx
TLV-encoded transaction data	xx	xx
…….		
Total:	<var>	

[0237] In one embodiment, commerce applet 113 manages the transmission of multiple response packets using the Get Response command when the total data length exceeds 256 bytes.

Transaction Log Status Response Data

[0238] When the transaction log status is requested, the commerce applet responds with status information within an embedded TLV data payload. This data includes the number of available transaction log records, loyalty and offer records sent during the last transaction. This is the same data payload provided to WCAp via the shared interface. Table 46 illustrates exemplary response data.

TABLE 46 – Response Data

Data Element	Byte Size	Value
Embedded TLV Transaction Status Tag	1	0xE4
Embedded TLV Transaction Record Length	1	0x0C
Transaction Record Count Tag	1	0xDB
Transaction Record Count Length	1	0x02
Transaction Record Count Value	2	xx
Last Transaction Loyalty Count Tag	1	0xDC
Last Transaction Loyalty Count Length	1	0x02
Last Transaction Loyalty Count Value	2	xx
Last Transaction Offer Count Tag	1	0xDD
Last Transaction Offer Count Length	1	0x02
Last Transaction Offer Count Value	2	xx
Total:	14	

[0239] Table 47 defines possible Status Word values that may be returned by the Get Transaction Log command.

TABLE 47 – Status Codes

SW1	SW2	Description
90	00	Successful Execution of Command

61	00	Successful Execution of Command w/ Additional data available via Get Response
67	00	Wrong Data Length
6B	00	Wrong P1/P2 Parameter
69	09	Internal Error

Get Internal Error Code

[0240] The Get Internal Error Code command is used to retrieve the last internal error code generated by the Commerce Services applet. This code provides a value that can be cross-referenced with the Internal Error Codes table (Table 26), providing a more specific description of the error. This command is used for more detailed diagnostic and error resolution.

[0241] Table 48 defines the settings for the Get Internal Error Code APDU command:

TABLE 48 – Get Internal Error Code

CLA	INS	P1	P2	Lc	Data	Le
90	70	00	00	00	*<none>*	02

[0242] In one embodiment, no data is sent to the applet. The Lc data length is 0x00. The error code is contained within a two-byte response. Therefore, the Le data length is 0x02.

[0243] The following table defines the possible Status Word values that may be returned by this command.

TABLE 49 – Status Codes

SW1	SW2	Description
90	00	Successful Execution of Command
67	00	Wrong Data Length
69	09	Internal Error

Loyalty Services

Get Loyalty Data

[0244] The Get Loyalty Data command defined in Tables 50 and 51 is used to obtain the stored loyalty information based on a specified loyalty identifier. The

two-byte loyalty identifier may be sent as part of the incoming data in order to specify the loyalty information requested. Commerce applet 113 searches a table of loyalty data for the specified merchant/loyalty ID and retrieves all of the corresponding loyalty data.

TABLE 50 – Get Loyalty Data

CLA	INS	P1	P2	Lc	Data	Le
90	30	00	00	xx	[TLV-Encoded Loyalty ID]	00

[0245] The (optional) incoming data shall consist of a TLV encoded loyalty identifier indicating the loyalty information requested. If Lc is set to 0x00 (no data incoming data is specified), all available loyalty identifiers are returned.

[0246] The actual length of the requested loyalty data returned by the applet is variable specific to the requested/available loyalty data. Therefore, the Lc data length is 0x00, allowing the applet to manage a variable length response.

TABLE 51 - Command Data

Data Element	Byte Size	Value
Loyalty Identifier Tag	1	0xDF41
Loyalty Identifier Length	1	8
Loyalty Identifier	8	[Loyalty ID]
Total:	<var>	

[0247] The response data (Table 51) is returned as a TLV formatted data stream. All of the relevant loyalty data is returned in a single data payload.

[0248] In one embodiment, if a loyalty data dump is requested (Lc = 0x00), a list of all Loyalty Identifiers is returned in LV (no tag) format. Thus, only the Loyalty Identifier for each entry is included in the data payload.

[0249] Each instance of loyalty data includes the following data elements:

- Loyalty Identifier
- Loyalty Account Code

TABLE 52 – Response Data

Data Element	Byte Size	Value
Loyalty Identifier Tag	1	0xDF41

Identifier Length	1	8
Loyalty Identifier	8	[Loyalty ID]
Loyalty Account Code Tag	1	0xDF43
Account Code Length	1	xx
Loyalty Account Code	xx	[Acct Code]
Total (Max):	<var>	

[0250] Table 53 defines the possible Status Word values that may be returned by this command.

TABLE 53 – Status Codes

SW1	SW2	Description
90	00	Successful Execution of Command
61	00	Successful Execution of Command w/ Additional data available via Get Response
67	00	Wrong Data Length
69	09	Internal Error

Update Loyalty Data

[0251] The Update Loyalty Data command is used to add or update the specified merchant loyalty data. The data is sent as TLV formatted data stream. If the specified loyalty identifier exists, the corresponding loyalty data elements are updated. If the loyalty identifier does not exist, a new data record is created in the loyalty data table. Tables 54 and 55 define the settings for the Update Loyalty Data APDU command:

TABLE 54 – Update Loyalty Data

CLA	INS	P1	P2	Lc	Data	Le
90	32	00	00	xx	TLV-Encoded Loyalty Data	00

[0252] The incoming data shall consist of TLV encoded loyalty data. Therefore, the Lc data length is variable. In one embodiment, no data is returned by the applet. The Le data length is be 0x00.

TABLE 55 – Command Data

Data Element	Byte Size	Value
Loyalty Identifier Tag	1	0xDF41
Identifier Length	1	8

Loyalty Identifier	8	[Loyalty ID]
Loyalty Account Code Tag	1	0xDF43
Account Code Length	1	xx
Loyalty Account Code	Xx	[Acct Code]
Total:	<var>	

[0253] Table 56 defines the possible Status Word values that may be returned by this command.

TABLE 56 – Status Codes

SW1	SW2	Description
90	00	Successful Execution of Command
67	00	Wrong Data Length
69	09	Internal Error

Delete Loyalty Data

[0254] The Delete Loyalty Data command is used to delete the specified merchant loyalty data. The one-byte merchant code is specified via the command data. Alternatively, the P2 byte may be used to purge all existing offers. If P2 is set to 0xFF, the entire offer data store is deleted.

[0255] Tables 57 and 58 define the settings for the Delete Loyalty Data APDU command:

TABLE 57 – Delete Loyalty Data

CLA	INS	P1	P2	Lc	Data	Le
90	34	00	xx	xx	TLV-Encoded Loyalty ID	00

[0256] The incoming data consists of a TLV-encoded loyalty identifier. Therefore, the Lc data length is variable.

[0257] In one embodiment, no data is returned by commerce applet 113. The Le data length is 0x00.

TABLE 58 – Command Data

Data Element	Byte Size	Value
Loyalty Identifier Tag	1	0xDF41
Loyalty Identifier Length	1	xx
Loyalty Identifier	Xx	[Loyalty ID]
Total:	<var>	

P2 Value	Applet Behavior
0x00	Normal processing.
0xFF	Purge loyalty table (delete all records)

[0258] Table 59 defines the possible Status Word values that may be returned by the Delete Loyalty Data command.

TABLE 59 – Status Codes

SW1	SW2	Description
90	00	Successful Execution of Command
67	00	Wrong Data Length
69	09	Internal Error

Merchant Cached Data Services

Get Cached Merchant Data

[0259] The Get Cached Merchant Data command is used to obtain all previously loaded data pertaining to a specific merchant. The merchant identifier may be sent as part of the incoming data in order to specify the pre-loaded data requested. If provided, the commerce applet searches a table of cached merchant data for the specified merchant ID and retrieves all of the corresponding data. This command may also be used to obtain information on all cached merchants stored within the Commerce Services applet.

[0260] Table 60 defines the settings for the Get Cached Merchant Data APDU command:

TABLE 60 – Get Cached Merchant Data

CLA	INS	P1	P2	Lc	Data	Le
90	56	00	00	xx	<none>	00

[0261] In one embodiment, no data is sent to the applet. The Lc data length is 0x00. The actual length of the requested cached merchant data returned by the applet is variable, specific to the requested/available cached merchant data. Therefore, the Le data length is 0x00; allowing the applet to manage a variable length response.

[0262] The response data (Table 61) may be returned as a TLV formatted data stream. All of the cached data is returned in a single data payload. Each instance of cached merchant data includes the following corresponding cached merchant data elements (if available):

- Merchant Identifier
- Loyalty Identifier
- Loyalty Account Code
- Offer Identifier(s)
- Offer Code(s)

TABLE 61 – Response Data

Data Element	Byte Size	Value
Merchant ID Tag	1	0xDF31
Merchant ID Length	1	8
Merchant ID	8	[Merchant ID]
Loyalty ID Tag	1	0xDF41
Loyalty ID Length	1	8
Loyalty ID Value	8	[Loyalty ID]
Loyalty Account Code Tag	1	0xDF43
Loyalty Account Code Length	1	32
Loyalty Account Code Value	32	[Loyalty Account Code]
…….		
Offer ID Tag	1	0xDF51
Offer ID Length	1	xx
Offer ID Value	Xx	[Offer ID]
Offer Code Tag	1	0xDF53
Offer Code Length	1	xx
Offer Code Value	Xx	[Offer Code]
…….		
Total:	<var>	

[0263] In an exemplary embodiment, the cached merchant data will be loaded/managed by the wallet application and may include multiple offer IDs/codes pertaining to that specific merchant. However, the applet shall prefix the consumer identifier to the response data and append any additional loyalty/offer data requested by the Get Commerce Data command.

[0264] Table 62 defines the possible Status Word values that may be returned by this command.

TABLE 62 – Status Codes

SW1	SW2	Description
90	00	Successful Execution of Command
67	00	Wrong Data Length
69	09	Internal Error

Update Cached Merchant Data

[0265] The Update Cached Merchant Data command is used to update the cached (quick-response) data for a specified merchant. The data is sent as TLV formatted data stream, similar to the response data returned by the Get Commerce Data command. This command is used to pre-load a given merchant's Get Commerce Data response.

[0266] Tables 63 and 64 define the settings for the Update Cached Merchant Data APDU command:

TABLE 63 – Update Cached Merchant Data

CLA	INS	P1	P2	Lc	Data	Le
90	58	00	0x	xx	TLV-Encoded Cached Merchant Data]	02

P2 Value	Applet Behavior
0x00	Normal processing.
0x01	APDU Chain (data will be appended to CMD buffer)
0Xff	Delete cached merchant data [Lc = 0]

[0267] The incoming data consists of embedded TLV encoded cached merchant data. Therefore, the Lc data length is variable.

[0268] Commerce applet returns a two byte response containing the number of available bytes remaining in the cached merchant data buffer. Therefore, the Le data length is 0x02 (or 0x00).

TABLE 64 – Command Data

Data Element	Byte Size	Value
Merchant ID Tag	1	0xDF31
Merchant ID Length	1	8
Merchant ID Value	8	[Merchant ID]
Cached Merchant Data Offer Count Tag	1	0x57
Cached Merchant Data Offer Count Length	1	1
Cached Merchant Data Offer Count Value	1	[CMD Offer Count]
Embedded TLV Cached Merchant Data Tag	1	0x58
Embedded TLV Cached Merchant Data Length	Xx	xx
Offer ID Tag	1	0xDF51
Offer ID Length	1	xx
Offer ID Value	Xx	[Offer ID]
Offer Code Tag	1	0xDF53
Offer Code Length	1	xx
Offer Code Value	Xx	[Offer Code]
…….		
Total:	<var>	

[0269] The response data (Table 65) returned by the command consists of a 2-byte (short) value representing the number of remaining bytes available in the cached merchant data buffer. This allows the wallet application 114 to manage how many cached offers can "fit" into the Commerce Services applet.

TABLE 65 – Response Data

Data Element	Byte Size	Value
Available Cached Merchant Data Buffer (bytes) Size	2	xx
Total:	2	

[0270] Table 66 defines the possible Status Word values that may be returned by this command.

TABLE 66 – Status Codes

SW1	SW2	Description
90	00	Successful Execution of Command
67	00	Wrong Data Length
69	09	Internal Error

[0271] Table 67 defines the data elements and corresponding tag values and target/max byte sizes used by commerce based applications according to the example aspects described herein. Additional values have been provided for those elements with a limited/fixed value range.

TABLE 67

Commerce Services			
Shared Data Elements			
Data Element	Tag	Max Size	Description
DATE_TIME_STAMP	0x11	7	Date/Time stamp
COMMERCE_APP_VERSION	0x12	3	Supported Commerce App Version Number
Consumer Data Elements			
Data Element	Tag	Max Size	Description
CONSUMER_ID	0x21	16	MoCom Platform specific consumer identifier
CONSUMER_KEY	0x22	16	MoCom Platform generated consumer specific 3DES key
CONSUMER_CERT	0x23	8	MoCom Platform generated consumer signature/ certificate
Merchant Data Elements			
Data Element	Tag	Max Size	Description
MERCHANT_ID	0x31	8	MoCom Platform specific merchant identifier
MERCHANT_STORE_ID	0x32	32	MoCom Platform specific merchant store identifier
MERCHANT_CAPABILITY	0x33	2	Supported Commerce App Services
READER_START_MODE	0x34	2	NFC enabled payment terminal startup mode (provided by Merchant POS System during init)
Merchant Capabilities			
Data Element	Value	Max Size	Description
MERCAP_MERCHANT_LOYALTY	0x80	1	The Get Commerce Data includes a valid merchant identifier used to determine the Loyalty data received by the applet.
MERCAP_ADDITIONAL_	0x40	1	The Get Commerce Data request

LOYALTY			includes additional Loyalty Identifiers. Additional Loyalty data is determined by the specified Loyalty ID(s).
MERCAP_MERCHANT_ OFFERS	0x20	1	Offer type fields aincluded in Get Commerce Data request
MERCAP_ADDITIONAL_ OFFERS	0x10	1	The Get Commerce Data includes a valid merchant identifier used to determine the offers data received by the applet.
MERCAP_PAYMENT	0x08	1	Merchant supports contactless payment.
MERCAP_CLOUD	0x02	1	The merchant supports cloud redemption. Only the Consumer ID will be returned by the applet for resolution in the cloud.
MERCAP_REDEMPTION	0x01	1	The Merchant & Payment Terminal support the transmission of offer redemption data (from the ECR) to the applet via the Post Transaction command.
MoCom Platform Data Elements			
PLATFORM_SIGNATURE	0x71	8	MoCom Platform generated MAC/Signature appended to command/data originating from the platform for remote verification purposes (data integrity/ authenticity).
PLATFORM_KEY	0x72	16	MoCom Platform Key
PLATFORM_CERT	0x73	8	MoCom Platform Certificate

Loyalty			
Loyalty Data Elements			
Data Element	Tag	Max Size	Description
EMBEDDED_TLV_ LOYALTY_DATA	0x40	xx	Embedded TLV loyalty data tag
LOYALTY_ID	0x41	8	MoCom Platform specific loyalty identifier
LOYALTY_STATUS	0x42	1	Loyalty card/account status (see below)
LOYALTY_ACCOUNT_ CODE	0x43	32	Loyalty account (barcode data)
LOYALTY_MAC_ SIGNATURE	0x44	8	MoCom Platform specific MAC/Signature for integrity/

			authenticity verification
Loyalty Status			
Data Element	Value	Max Size	Description
LOYALTY_STATUS_ DEACTIVATED	0x00	1	Loyalty account inactive. Not available.
LOYALTY_STATUS_ ACTIVE	0x01	1	Loyalty account active. Available for use.

Transaction Log			
Transaction Data Elements			
Data Element	Tag	Max Size	Description
EMBEDDED_TLV_ TRANSACTION_LOG	0x60	xx	Transaction log record data tag
TRANSACTION_ID	0x61	16	Transaction ID (assigned by ECR)
TRANSACTION_STATUS	0x62	11	Transaction status; including status byte (see below), 2-byte status word, 2-byte internal error code, 2-byte number of available transaction records, 2-byte last transaction loyalty count, 2-byte last transaction offer count
Transaction Status			
Data Element	Value	Max Size	Description
TRANSACTION_STATUS_SU CCESSFUL	0x00	1	Commerce data received. Result pending.
TRANSACTION_STATUS_FA ILED	0x01	1	Error detected. Internal error code appended.

Offers			
Offer Data Elements			
Data Element	Tag	Max Size	Description
EMBEDDED_TLV_ OFFER_DATA	0x50	xx	Embedded TLV offer data tag
OFFER_ID	0x51	8	MoCom Platform specific offer identifier
OFFER_STATUS	0x52	1	Offer status (see below)
OFFER_CODE	0x53	48	Offer (UPC/EPC/GS1 Databar) barcode data
OFFER_TYPE_CODE	0x54	9	Offer Type (see below)
OFFER_MAC_ SIGNATURE	0x55	8	MoCom Platform specific data security signature

OFFER_UPDATE_FLAG	0x56	1	Update flag (synchronization status)
CACHED_MERCHANT_ DATA_OFFER_COUNT	0x57	1	Offer Count within Cached Merchant Data
EMBEDDED_TLV_ CACHED_MERCHANT_ DATA	0x58	xx	Embedded TLV Cached Merchant (Offer) Data
Offer Status			
Data Element	Value	Max Size	Description
OFFER_STATUS_ DEACTIVATED	0x00	1	Offer present in data store, but not available for redemption.
OFFER_STATUS_ ACTIVE	0x01	1	Offer present in data store. Available for redemption.
OFFER_STATUS_ EXPIRED	0x10	1	Expired Offer
OFFER_STATUS_ SUBMITTED	0x20	1	Offer has been presented for redemption. Result pending.
OFFER_STATUS_ REDEEMED	0x40	1	Offer has been redeemed.
Offer Type			
Data Element	Value	Max Size	Description
OFFER_TYPE_CLASS_01	0x01	1	Offer Class: Merchant Specific (merchant ID appended)
OFFER_TYPE_CLASS_02	0x02	1	Offer Class: CPG
OFFER_TYPE_CLASS_03	0x03	1	Offer Class: Misc

Specially Formatted Data Elements

[0272] A few of the data elements included in the commerce data payload include a format byte that identifies the data encoding used for that element. The data encoding is specified by the merchant to ensure compatibility at the point of sale. The formatted data value is supplied by the MoCom platform to the wallet application. Thus, no additional interpreting/formatting is necessary between the platform, wallet, secure element, and payment terminal. It is the role of the payment terminal (or merchant POS system) to properly interpret the data and supply it to the merchant system for processing.

[0273] The following data elements shall include the format byte:

- Loyalty Account Code
- Offer Code

[0274] Table 68 defines the possible format byte values and their corresponding encoding rule:

TABLE 68

Format Byte	Encoding Rule	Description
0x00	Hexadecimal	Each byte of data is encoded in (raw) hexadecimal format.
0x01	Binary Coded Decimal (BCD)	Each nibble represents a single digit. Thus, only decimal values are specified. A data stream containing an odd number (length) of digits includes the hex value 'F' in the first nibble of the data stream.
0x02	ASCII	Each byte represents an ACII value that is interpreted as such and handled as its corresponding CHAR value. In most cases, these data streams will be converted into a String before being passed to the merchant POS system for processing.

[0275] A BCD encoded data value that includes the hexadecimal value 'F' in the first nibble shall identify a data stream containing an odd number of digits. Thus, the BCD data stream *12345* is encoded in 3 byte buffer as follows: *0xF12345*.

Computer Readable Medium Implementation

[0276] The example embodiments described above such as, for example, the systems and procedures depicted in or discussed in connection with FIGs. 1- 7 or any part or function thereof, may be implemented by using hardware, software or a combination of the two. The implementation may be in one or more computers or other processing systems. While manipulations performed by these example embodiments may have been referred to in terms commonly associated with mental operations performed by a human operator, no human operator is needed to perform any of the operations described herein. In other words, the operations may be completely implemented with machine operations. Useful machines for performing the operation of the example embodiments presented herein include general purpose digital computers or similar devices.