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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 June 2008 (05.06.2008)

PCT

(10) International Publication Number
WO 2008/067313 A2

(51) International Patent Classification:
H04L 9/00 (2006.01)

(21) International Application Number:
PCT/US2007/085643

(22) International Filing Date:
27 November 2007 (27.11.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/605,203 27 November 2006 (27.11.2006) US

(71) Applicant *(for all designated States except US)*: **SMS.AC** [US/US]; 741 F Street, San Diego, CA 92101 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **POUSTI, Michael** [US/US]; 255 G Street #723, San Diego, CA 92101 (US).

(74) Agent: **GILLESPIE, Noel, C.**; Baker & Mckenzie LLP, 2001 Ross Avenue, Suite 2300, Dallas, TX 75201 (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*

WO 2008/067313 A2

(54) Title: SYSTEM AND METHOD FOR VERIFICATION OF IDENTITY FOR TRANSACTIONS

(57) Abstract: Billing a customer through an intermediary billing system for a transaction by receiving, at the intermediary billing system, a transaction request associated with a transaction amount and a customer identification code, validating, in the intermediary billing system, the transaction request by determining whether the customer identification code corresponds to a customer that is registered with the intermediary billing system, and sending, in the case that the transaction request is valid, a billing event trigger associated with the customer identification code to an external billing mechanism, the billing event trigger representing the transaction amount.

SYSTEM AND METHOD FOR VERIFICATION OF IDENTITY FOR TRANSACTIONS

Field of the Invention

[0001] The present invention concerns the automated processing of transactions, including small transactions known as micro-transactions. In particular, the invention concerns the use of an intermediate billing system that acts on behalf of third party providers of content or services by interacting with various external billing mechanisms to effectuate transactions between such third party providers and their customers.

Background of the Invention

[0002] While credit card use and automatic credit card billing is a common way to conduct business transactions in many countries, they are not necessarily the best way in some situations. In particular, there are many users of the internet that do not have access to a credit card or do not want to use their credit card for an internet based transaction out of security concerns. Many such users most likely have a mobile phone or mobile device, and it would be more easy and efficient to have a mechanism for billing the user for transactions through the user's pre-existing account with the mobile carrier associated with the user's mobile phone number. In addition, the use of a credit card is economically viable only if the transaction amount, or a volume of such transactions, exceeds a particular amount that depends on the underlying efficiency of the billing and collecting system implemented by the merchant and by the credit card provider. Currently, mobile phone carriers routinely bill users for small transactional amounts, such as a one minute call, or portion thereof, and are able to bill and collect for these small transactions while making a profit. These small transactions are referred to as micro-transactions and, in terms of U.S. currency, can be as small as a few pennies, although larger transactions occur as well.

[0003] Retailers or vendors, such as internet commercial websites, may desire to provide their respective content or services to mobile phone users via the internet or directly through the user's mobile phone, and bill the user for such content or services as micro-transactions. Currently, a retailer or vendor will find it very difficult and inefficient to bill and collect for such a micro-transaction because the retailer/vendor would need to negotiate and enter into a contractual relationship with the mobile phone carrier in order to bill the mobile phone user subscribed to that carrier. The process is further complicated by the fact that the universe of customers with

mobile phones use different mobile phone carriers. Accordingly, the retailer/vendor would need to enter into contractual relationships with many different mobile phone carriers in order to be able to provide a mobile phone based micro-transaction billing option to the desired global market of mobile phone users. A retailer or vendor can try to use billing mechanisms other than mobile carriers, such as prepaid card services, web-based payment services, bank account and credit card billing services, and other such external billing mechanisms to support customer transactions. However, in such examples, the same problem still exists for the vendor/retailer because they would still need to have pre-existing relationships with all of the various external billing mechanisms that their various customers wish to use for payment of transactions.

[0004] Thus, there exists a need for a system and method that allows retailers/vendors to easily conduct transactions, many of which may be micro-transactions, with a global market of customers, where the transactions are easily billable through a single intermediate billing system which can effectuate the transaction through a wide variety of external billing mechanisms on behalf of the retailer/vendor, thereby eliminating the need for the retailer/vendor to individually establish a pre-existing relationship with each of the wide variety of external billing mechanisms.

Summary of the Invention

[0005] The present invention solves the foregoing problems by providing a method and system that uses a single intermediate billing system to effectuate transactions between retailers/vendors and their customers through a wide variety of external billing mechanisms, without the need for the retailer/vendor to individually establish a pre-existing relationship with each of the wide variety of external billing mechanisms.

[0006] In one embodiment, the invention is directed to a method and system for billing a customer through an intermediary billing system for a transaction, by receiving, at the intermediary billing system, a transaction request associated with a transaction amount and a customer identification code, validating, in the intermediary billing system, the transaction request by determining whether the customer identification code corresponds to a customer that is registered with the intermediary billing system, and sending, in the case that the transaction request is valid, a billing event trigger associated with the customer identification code to an external billing mechanism, the billing event trigger representing the transaction amount.

[0007] In another embodiment, the invention is directed to a method and system for billing a customer through an intermediary billing system for a transaction between the customer and a third party provider, by receiving, at the intermediary billing system, a registration request to register the customer, registering the customer in the intermediary billing system by providing a mobile phone number of the customer to the intermediary billing system, assigning a customer identification code to the customer, the customer identification code being shared with the third party provider, and associating the mobile phone number of the customer with the customer identification code assigned to the customer, receiving, at the intermediary billing system, a billing request from the third party provider, the billing request including a product identification code corresponding to a product associated with the transaction between the customer and the third party provider, a customer identification code assigned to the customer and a provider identification code corresponding to the third party provider, validating, in the intermediary billing system, the billing request by determining whether the customer identification code corresponds to a customer that is registered with the intermediary billing system, and by determining whether the provider identification code corresponds to a valid third party provider, and sending, in the case that the billing request is validated, at least one message from the intermediary billing system to a mobile phone number associated with the customer identification code, the at least one message representing a billing value that corresponds to the product identification code.

[0008] In another embodiment of the invention, a method and system is provided for billing a customer through an intermediary billing system for a transaction between the customer and a third party provider, by receiving, at the intermediary billing system, a transaction activation request from the third party provider to activate a customer for the transaction associated with a product offered by the third party provider, the customer being automatically directed from the third party provider to the intermediary billing system, prompting, by the intermediary billing system, the customer to confirm an instruction to proceed with the transaction, sending, in the case that the customer confirms the instruction to proceed with the transaction, at least one message from the intermediary billing system to a mobile phone number associated with a customer identification code for the customer, the at least one message representing a billing value that corresponds to the product, generating, in the intermediary billing system, an encrypted verification code in association with the customer identification code for the customer,

installing the encrypted verification code on a web browser application of the customer (for browsing web pages on the internet), and automatically directing the customer from the intermediary billing system to the third party provider, receiving, at the intermediary billing system, a verification code validation request containing a returned encrypted verification code and a customer identification code from the third party provider, and validating, in the intermediary billing system, whether the returned encrypted verification code is the same as the encrypted verification code sent from the intermediary billing system to the third party provider for that customer identification code, and sending, from the intermediary billing system, a validation response to the third party provider, the validation response containing an error code in the case that the returned encrypted verification code is not valid, and containing a valid confirmation code in the case that the returned encrypted verification code is valid, wherein the third party provider enables the customer to access the product on the basis of the validation response received by from the intermediary billing system.

[0009] In this manner, the present invention provides that an efficient and timely billing system that utilizes mobile text messages to bill customers for transactions between the customers and third-party providers of content or services, without the need for a third-party provider to have any relationship or interaction with the mobile phone carrier of the customer.

[0010] This brief summary has been provided so that the general nature of the invention may be understood quickly. A more complete understanding of the invention can be obtained by reference to the following detailed description thereof in connection with the attached drawings. It is to be understood that embodiments of the invention other than that provided in the description below and the accompanying drawings may be utilized and that changes may be made without departing from the scope of the present invention.

Brief Description of the Drawings

[0011] Figure 1 is a block diagram of a computer system with which the present invention may be practiced, according to one embodiment of the invention;

[0012] Figure 2 is a block diagram of a mobile community environment in which the invention may be practiced, according to one embodiment of the invention;

[0013] Figure 3 is a block diagram providing a detailed view of the mobile community platform shown in Figure 2;

[0014] Figure 4 is a flowchart for explaining the registration and activation of a customer for transaction billing, according to one embodiment of the invention;

[0015] Figure 5 is a flowchart for explaining the processing of a billing request for a transaction, according to one embodiment of the invention;

[0016] Figure 6 is a flowchart for explaining the processing of a transaction, according to another embodiment of the invention;

[0017] Figure 7 is a flowchart for explaining the processing of a billing request for a transaction, according to another embodiment of the invention;

[0018] Figure 8 is a flowchart for explaining how transaction requests may be initiated;

[0019] Figure 9 is a flowchart for explaining the processing of a transaction request by a third party provider, according to another embodiment of the invention;

[0020] Figure 10 is a flowchart for explaining a "white label" verification and/or billing process; and

[0021] Figure 11 is a diagram depicting use of certain embodiments of the invention to allow transactions across compatible networks.

Detailed Description of the Invention

[0022] As mentioned above, the present invention is a method and system that utilizes an intermediary billing system in conjunction with one or more external billing mechanisms for supporting transactions between customers and third-party providers of content or services, without the need for a third-party provider to have a relationship or interaction with any of the external billing mechanisms.

[0023] Figure 1 is a block diagram of an exemplary computer system with which one embodiment of the present invention may be practiced. As seen in Figure l, computer system 100 includes a bus 102 or other communication mechanism for communicating information, and a processor 104 coupled with bus 102 for processing information. Computer system 100 also includes a main memory 106, such as a random access memory (RAM) or other dynamic storage device, coupled to bus 102 for storing information and instructions to be executed by processor 104. Main memory 106 also may be used for storing temporary variables or other intermediate information during execution of instructions to be executed by processor 104. Computer system 100 further includes a read only memory (ROM) 108 or other static storage device coupled to

bus 102 for storing static information and instructions for processor 104. A storage device 110, such as a magnetic disk or optical disk, is provided and coupled to bus 102 for storing information and instructions.

[0024] Computer system 100 may be coupled via bus 102 to a display 112, such as a cathode ray tube (CRT), for displaying information to a computer user. An input device 114, including alphanumeric and other keys, is coupled to bus 102 for communicating information and command selections to processor 104. Another type of user input device is cursor control 116, such as a mouse, a trackball, or cursor direction keys for communicating direction information and command selections to processor 104 and for controlling cursor movement on display 112. This input device typically has two degrees of freedom in two axes, a first axis (e.g., x) and a second axis (e.g., y), that allows the device to specify positions in a plane.

[0025] Computer system 100 operates in response to processor 104 executing one or more sequences of one or more instructions contained in main memory 106. Such instructions may be read into main memory 106 from another computer-readable medium, such as storage device 110. Execution of the sequences of instructions contained in main memory 106 causes processor 104 to perform the process steps described herein. In alternative embodiments, hard-wired circuitry may be used in place of or in combination with software instructions to implement the invention. Thus, embodiments of the invention are not limited to any specific combination of hardware circuitry and software.

[0026] The term "computer-readable medium" as used herein refers to any medium that participates in providing instructions to processor 104 for execution. Such a medium may take many forms, including but not limited to, non-volatile media, volatile media, and transmission media. Non-volatile media includes, for example, optical or magnetic disks, such as storage device 110. Volatile media includes dynamic memory, such as main memory 106. Transmission media includes coaxial cables, copper wire and fiber optics, including the wires that comprise bus 102. Transmission media can also take the form of acoustic or light waves, such as those generated during radio-wave and infra-red data communications.

[0027] Common forms of computer-readable media include, for example, a floppy disk, a flexible disk, hard disk, magnetic tape, or any other magnetic medium, a CD-ROM, any other optical medium, punchcards, papertape, any other physical medium with patterns of holes a

RAM, a PROM, and EPROM, a FLASH-EPROM, any other memory chip or cartridge, a carrier wave as described hereinafter, or any other medium from which a computer can read.

[0028] Various forms of computer readable media may be involved in carrying one or more sequences of one or more instructions to processor 104 for execution. For example, the instructions may initially be carried on a magnetic disk of a remote computer. The remote computer can load the instructions into its dynamic memory and send the instructions over a telephone line using a modem. A modem local to computer system 100 can receive the data on the telephone line and use an infra-red transmitter to convert the data to an infra-red signal. An infra-red detector can receive the data carried in the infra-red signal and appropriate circuitry can place the data on bus 102. Bus 102 carries the data to main memory 106, from which processor 104 retrieves and executes the instructions. The instructions received by main memory 106 may optionally be stored on storage device 110 either before or after execution by processor 104.

[0029] Computer system 100 also includes a communication interface 118 coupled to bus 102. Communication interface 118 provides a two-way data communication coupling to a network link 120 that is connected to a local network 122. For example, communication interface 118 may be an integrated services digital network (ISDN) card or a modem to provide a data communication connection to a corresponding type of telephone line. As another example, communication interface 118 may be a local area network (LAN) card to provide a data communication connection to a compatible LAN. Wireless links may also be implemented. In any such implementation, communication interface 118 sends and receives electrical, electromagnetic or optical signals that carry digital data streams representing various types of information.

[0030] Network link 120 typically provides data communication through one or more networks to other data devices. For example, network link 120 may provide a connection through local network 122 to a host computer 124 or to data equipment operated by an Internet Service Provider (ISP) 126. ISP 126 in turn provides data communication services through the world wide packet data communication network now commonly referred to as the "Internet" 128. Local network 122 and Internet 128 both use electrical, electromagnetic or optical signals that carry digital data streams. The signals through the various networks and the signals on network link 120 and through communication interface 118, which carry the digital data to and from computer system 100, are exemplary forms of carrier waves transporting the information.

[0031] Computer system 100 can send messages and receive data, including program code, through the network(s), network link 120 and communication interface 118. In the Internet example, a server 130 might transmit a requested code for an application program through Internet 128, ISP 126, local network 122 and communication interface 118. The received code may be executed by processor 104 as it is received, and/or stored in storage device 110, or other non-volatile storage for later execution. In this manner, computer system 100 may obtain application code in the form of a carrier wave. Of course, other forms of computing systems may be used to implement the present invention.

[0032] Figure 2 is a block diagram of a mobile community environment in which the invention may be practiced according to an exemplary embodiment. Figure 2 depicts a block diagram of a computer-based mobile community platform 202. Mobile community platform 202 can be implemented in the computing system show in Figure 1, or some other form of computing system. As seen in Figure 2, users 212, 214, 216 can connect to the mobile community platform 202 via a network or similar communications channel 210. In an exemplary embodiment, network 210 is the internet by which users 212, 214 and 216 can access internet-enabled applications and websites, such as third party providers 231, 232 and 233. In this regard, third party providers 231, 232 and 233 can be websites that provide only information, or may be commercial websites that offer a product, such as access to premium content or services, for purchase by the user, whereby the user is provided with access to the product after opting-in (purchasing) the product from that particular website. In addition, third party providers 231, 232 and 233 can be internet-enabled applications such as a software application that is enabled to access the internet and that can provide content or services to the user of the software application for a price. For example, a software game being executed on a user's computer, or an internet-enabled game device, may allow the user to access the internet in order to purchase additional features of the game to be downloaded or "premium" information about how to play the game for a price. It can be appreciated that a third party provider can be any type of application, game, product or service that is internet-enabled and that offers additional product (software, content, information, or services) to the user for a price. Any such third party provider can maintain a website to which the user is directed when the user elects to purchase a product from the third party provider.

[0033] Third party providers 231, 232 and 233 are maintained and operated by known means and can be implemented in a computing system such as that shown in Figure 1, or other known types of networked computing environments, such as a server, or combination of computers and servers. By means of the connection with mobile community platform 202, a user (e.g., 212) may create a profile page or "home page" supported and maintained by mobile community platform 202 that the user can personalize. This profile page can include various files and content that the user wants to share with other members of the mobile community platform 202.

[0034] The user's profile page may include a hierarchy of pages, some of which are for public view and some of which have restrictions on viewing. For example, the mobile community platform 202 can be logically organized into neighborhoods such as "friends", "family", "workplace", "dog owners", etc. Users 212, 214, 216 can belong to these different neighborhoods and share different pages with the members of the different neighborhoods.

[0035] As seen in Figure 2, mobile community platform 202 connects with various mobile carrier systems 204, 206, 208, each of which has an associated community of mobile phone subscribers, 224, 226 and 228. In this regard, each of mobile carrier systems 204, 206, 208 is a carrier network and system for supporting mobile devices including mobile phones and other mobile devices such as personal device assistants (pda). Each mobile carrier system is generally a wireless network provider, which can be cellular, PCS, or other wireless spectrum. Users 212, 214, 216 of the mobile community platform 202 are also subscribers of one or more of the various mobile carriers, which support the mobile phones, or other mobile devices, of users 212, 214, 216. In this way, users 212, 214, 216 of mobile community platform 202 can access other users' profile pages through the computer-based platform of mobile community platform 202, and they can also access the subscribers 224, 226 and 228 of the various mobile carrier systems 204, 206, and 208 who also belong to mobile community platform 202.

[0036] A significant benefit of the architecture depicted in Figure 2, is that the mobile community platform 202 has pre-existing contractual relationships with the various mobile carrier systems 204, 206, 208 for accessing subscribers through each carrier systems and for billing subscribers through their respective carrier system for content and services purchased by the subscriber through mobile community platform 202. As is known in the art, the mobile carrier systems 204, 206, 208 provide text messaging and also premium text message functionality. Such messages are sent via the mobile carrier's infrastructure to its mobile

subscribers and, internal to the mobile carrier's infrastructure, the sending of such a message generates a billing event according to a particular tariff rate, which then is added to the subscriber's bill from that mobile carrier.

[0037] When mobile community platform 202 sends a message via a mobile carrier system (e.g., 204), it is billing the subscriber-recipient of the message using the existing billing system of that mobile carrier. The billing event is often a micro-transaction of a small monetary amount (e.g., less than one dollar). Thus, a user (e.g., 212) of the mobile community platform may purchase a service or content within mobile community platform 202 and be billed for those transactions through that user's mobile carrier service account. The present invention provides for such micro-transaction billing support through mobile community platform 202 for a transaction between a user (e.g., 212) and a third party provider (e.g., 231) which is external to mobile community platform 202. In this manner, a third party provider need only communicate with mobile community platform 202 to conduct transactions with users, and does not require any affiliation or agreement with the various mobile carrier systems of the users.

[0038] Figure 3 depicts a more detailed view of mobile community platform 202. As mentioned above, mobile community platform 202 can be used to conduct micro-transactions in which a mobile carrier's billing system is used by mobile community platform 202 to automatically bill the user for each micro-transactions with a third party provider, without the need for a negotiation or contract between the third party provider and the mobile carrier. An example of this feature is a third party provider that operates a website which offers sports score updates to users of mobile community platform 202 for a predetermined price, while taking advantage of the billing arrangements already in place between mobile community platform 202 and the mobile carriers 204, 206, 208. Of course, a third party provider may provide other types of content, products and services to users of mobile community platform 202.

[0039] Turning to Figure 3, mobile community platform 202 includes multimedia messaging system 302, user area 304, which supports content, community and commerce functions for the users, including website interface for users to mobile community platform 202, and intermediary billing interface 306. The details of these different components are more fully explained below.

[0040] As noted earlier, users 212, 214, 216 can visit user area 304 of mobile community platform 202 in order to participate in an online-based community of users that includes various communication, content and commerce opportunities. The user accesses a website of user area

304 through the user's web browser that may be hosted on a laptop or desktop computer, or, in the alternative, even on the user's mobile device such as a PDA or mobile phone. In this regard, user area 304 includes a web server that communicates with users 212, 214, 216 and includes a data store (database) of user information and other content. With these resources, mobile community platform 202 is able to present a profile page ("home page") to a user (e.g., 212) that reflects a set of content, information and products associated with, and desired by, that particular user. This set of content, information and products is not maintained on the local computer being used by the user 212 but, rather, is maintained and managed by the computing environment of mobile community platform 202. Although not explicitly depicted in Figure 3, one of ordinary skill will recognize that there are numerous functionally equivalent techniques to create, manage, store and serve user information, user profiles, user content, software tools and other resources within the user area 304. Included in these techniques are methods to ensure security, data integrity, data availability and quality of service metrics.

[0041] Multimedia messaging system (MMS) 302 includes applications for connecting with and communicating with the multiple different mobile carriers 204, 206, 208 that have been partnered with mobile community platform 202. MMS 302 is configured to generate message requests in the appropriate format for each of the mobile carriers 204, 206, 208 including tariff information that determines the amount for which the recipient of the message will be charged. Upon receipt of the message request, the mobile carriers 204, 206, 208 will use the information in the request to generate an appropriate message to the intended recipient/subscriber of the mobile carrier and then bill the recipient/subscriber's mobile service account for that specified amount. In this manner, mobile community platform 202 uses the mobile carriers to bill user/subscribers of the mobile carriers for transactions conducted through mobile community platform 202.

[0042] The MMS 302 communicates with the user area 304, such that users of mobile community platform 202 can advantageously use the connectivity between MMS 302 and the mobile carriers 204, 206 and 208 in order to send messages to subscribers of any of the mobile carriers 204, 206, 208. The messages may be SMS messages, MMS messages, or other known message formats or subsequently developed message formats. Some of these messages may have zero tariff and, therefore do not generate a bill to the recipient/subscriber (other than the

underlying charges implemented by the mobile carrier) and others may have non-zero tariffs resulting in a billing event for the recipient/ subscriber.

[0043] Intermediary billing interface 306 provides an interface between third party providers 231, 232 and 233 and mobile community platform 202 for enabling transactions between such third party providers and users 212, 214 and 216, through the use of sending messages to the users as a billing mechanism. In this regard, intermediary billing interface 306 is accessed by the third party providers via network connection 210 (internet). As seen in Figure 3, intermediary billing interface 306 is in communication with user area 304, both of which are in communication with MMS 302. Accordingly, intermediary billing interface 306 can access user information from user area 304, such as whether the user is registered and verified for billing through their mobile phone number, as discussed more fully below. Intermediary billing interface 306 can interface with user area 304 to communicate with a user, such as via webpages supported by user area 304, for purposes of registering the user with mobile community platform 202 and verifying the user for billing of transactions related to a product offered through a third party provider, as also discussed in more detail below.

[0044] As seen in Figure 3, intermediary billing interface 306 also includes local database 310 which is used by intermediary billing interface 306 to store customer identification codes, third party provider identification codes, and other information for implementing the present invention. Accordingly, third party providers 231, 232 and 233 can interact with all users of the mobile community platform 202 whereby billable transactions with users 212, 214, 216 are automatically billed to the users via the billing systems of their mobile carriers 204, 206, 208. Furthermore, and importantly, this capability is available to the third party providers without requiring them to negotiate or contract with any of the mobile carriers for billing arrangements, or to worry about how to communicate with a particular mobile carrier's systems and resources. The third party providers seamlessly take advantage of the unified set of connectivity and billing arrangements that exist between mobile community platform 202 and the mobile carriers 204, 206, 208. As a result, the third party providers may conduct transactions with users/subscribers of any of a variety of different mobile carriers without easily and efficiently through mobile community platform 202.

[0045] Figure 4 is a flowchart that provides an exemplary depiction of the registration and activation of a customer for transaction billing in one embodiment of the invention. The process

starts in Figure 4 and proceeds to step 401 in which it is determined whether the customer (e.g. one of users 212, 214 and 216) is initiating a transaction for a product at a third party provider, such as one of third party providers 231, 232 and 233, or is initiating a transaction for a product offered by the third party provider at mobile community platform 202, which acts as the intermediary billing system in either case. If the customer is initiating the transaction at mobile community platform 202, then the process proceeds to step 405 which is discussed further below. On the other hand, if the customer is initiating the transaction at the third party provider, then the process proceeds to step 402 in which the third party provider determines if the customer is already registered as a customer with the third party provider. If the customer is already registered with the third party provider, then the process proceeds to step 404. If not, then the process proceeds to step 403 in which the customer registers with the third party provider, such as by providing the customer's name and contact information, and in which the third party provider generates a unique customer identification code corresponding to that customer. Of course, it should be appreciated that the third party provider can use any form of registration process and may not necessarily require the customer to provide any specific information, in which case the third party provider simply generates and assigns a unique customer identification code to that customer. In this regard, the third party provider maintains a database of its registered customers, and their corresponding customer identification numbers and information. The customer identification number will be used in the invention for common tracking of the same customer between the third party provider and the intermediary billing system of mobile community platform 202

[0046] In step 404, the third party provider directs the customer to mobile community platform 202 along with a registration request to register and activate the customer, the request including the customer identification code for the customer. Next, in step 405, the registration and activation steps for the customer begin by the mobile community platform 202 (intermediary billing system) determining if the customer is already registered as a member of mobile community platform 202. If the customer is already registered with mobile community platform 202, then the process proceeds to step 407. If not, then the process proceeds to step 406 in which the customer registers with mobile community platform 202, such as by providing the customer's name and contact information, including the customer's mobile phone number, which is used by mobile community platform 202 in the invention to bill the customer for the transaction.

[0047] If it was determined in step 401 that the customer is originating the transaction at mobile community platform 202, then mobile community platform 202 also generates a unique customer identification code for the customer. Also in the registration process, mobile community platform 202 stores the customer identification code for the customer in a database of registered customers, along with related information, maintained in mobile community platform 202, and activates the customer's mobile phone number for transaction billing as described below.

[0048] Continuing with the registration and activation process, the mobile community platform 202 generates a verification code for the registration/activation of the customer, and directs the customer back to the third party provider along with the verification code, the customer identification code, and possibly other information, in step 407. Next, in step 408, the third party provider sends a verification code validation request to mobile community platform 202, the request including the verification code for the customer, to make sure that the third party provider and mobile community platform 202 are in agreement on the customer identification code to be used for the customer, and that the customer is registered and activated for the transaction in both the third party provider and the mobile community platform 202. In this regard, the term "activated" means that the mobile community platform 202 has enabled the customer associated with the assigned customer identification code to be billed for transactions, such as through the customer's mobile phone number, or through some other external billing mechanism used by mobile community platform 202.

[0049] In step 409, mobile community platform 202 determines whether the verification code received in the verification code validation request from the third party provider is valid by comparing it to the verification code stored in the database of mobile community platform 202 for that customer identification code. If the two codes match, then the verification code is valid, and mobile community platform 202 sends a confirmation reply to the third party provider in step 411 to confirm that the verification code is valid. If the two codes do not match, then the verification code is not valid, and mobile community platform 202 sends an error reply to the third party provider in step 410 to advise that the verification code is not valid. The registration and activation process for the customer between the third party provider and mobile community platform 202 is then complete and ends.

[0050] In an exemplary embodiment of the invention, HTTP and XML are used to communicate between the third party provider and intermediary billing system of mobile community platform

202 in the steps described above. In particular, the registration request in step 404 is implemented with an HTTP POST, and can be passed with the following parameters:

[0051] ActionCode: 1 means to activate the customer;

[0052] 2 means to confirm the verification code;

[0053] PartnerID: Assigned by mobile community platform to uniquely identify the third party provider (partner);

[0054] ProductID: Assigned by mobile community platform to uniquely identify the particular product involved in the transaction;

[0055] CustomerID: Customer identification code for the customer;

[0056] FirstName: First name of customer;

[0057] LastName: Last name of customer;

[0058] EmailAddress: Email address of customer;

[0059] Birthdate: Birthdate of customer;

[0060] Gender: Gender of customer;

[0061] Preferably, the ActionCode, PartnerID, ProductID, and CustomerID are required parameters.

[0062] An example of HTML for the registration request is shown below in Table 1:

```
<html>
<head>
    <script type="text/javascript">
        function frmSubmit() {window.document.form1.submito();}
    </script>
</head>
    <!-- Auto submit when body loads. -->
    <body LANGUAGE="Javascript" onload="return frmSubmit()">
    <form
        id="form1"
        name="form1"
        action="http://www.sms.ac/Directory/ppcoptin.aspx"
        method="POST">
        <input type="hidden" name="action" value="1">
        <input type="hidden" name="PartnerId" value="1234">
        <input type="hidden" name="ProductId" value="5678">
        <input type="hidden" name="CustomerId" value="test_user_01">
        <input type="hidden" name="FirstName" value="John">
        <input type="hidden" name="Lastname" value="Smith">
        <input type="hidden" name="EmailAddress" value="js@ExampleEmail.com">
        <input type="hidden" name="BirthDate" value="05/21/1977">
```

```
        <input type="hidden" name="Gender" value="M">
    </form>
</body>
</html>
```

Table 1

[0063] Similarly, an HTTP POST is used in step 407 in which mobile community platform 202 directs the customer back to the third party provider along with the verification code, and the same parameter fields as discussed above. The URL to which the customer is directed back to is specified by the third party provider. An example of HTML for the redirect of step 407 is shown below in Table 2:

```
<html>
<head>
    <script type="text/javascript">
        function frmSubmit() (window.document.form1.submit () ;}
    </script>
</head>
    <!-- Auto submit when body loads. -->
    <body LANGUAGE="Javascript" onload="return frmSubmit()">
    <form
        id="form1"
        name="form1"
        action-"http://www.MobilePartner.com/CustomerLandingPage.html"
        method="POST">
        <input type="hidden" name="vc"
            value="EXAMPLE_VERIFICATION_CODE">
        <input type="hidden" name="PartnerId" value="1234">
        <input type=" hidden" name="ProductId" value="5678">
        <input type="hidden" name="CustomerId" value="test_user_01">
        <input type="hidden" name="FirstName" value="john">
        <input type="hidden" name=" LastName" value="Smith">
        <input type="hidden" name="EmailAddress" value="js@ExampleEmail.com">
        <input type="hidden" name="BirthDate" value="05/21/1977">
        <input type="hidden" name="Gender" value="M">
    </form>
</body>
</html>
```

Table 2

[0064] In the same manner, the confirmation request of the verification code in step 408 is sent from the third party provider using an HTTP POST or an HTTP GET directly between the third party provider and mobile community platform 202, without involving the customer's browser.

The parameter for ActionCode is set to "2" for customer confirmation. An example of HTML for the confirmation request of step 408 is shown below in Table 3:

```
<html>
<head>
    <script type="text/javascript">
        function frmSubmit() {window.document.form1.submit();}
    </script>
</head>
    <!-- auto submit when body loads. -->
    <body LANGUAGE=" JavaScript" onload="return frmsubmit()">
    <form
        id="form1"
        name="forml"
        action="http://www.sms.ac/Directory/ppcoptin.aspx"
        method=" POST">
        <input type="hidden" name="action" value="2">
        <input type="hidden" name="vc"
            value="EXAMPLE_VERIFICATION_CODE">
        <input type="hidden" name=" PartnerId" value="1234">
        <input type="hidden" name="CustomerId" value="test_user_01">
    </form>
</body>
</html>
```

Table 3

[0065] In this regard, the result for the confirmation request is written by mobile community platform 202 as plain text to the output stream, and the possible return values for the result of the confirmation request are:

[0066] "Success: #CustomerID# has been verified"

[0067] "Error: bad 'CustomerID': #CID#"

[0068] "Error: bad 'vc': #VC#"

[0069] "Error: bad 'PartnerID': #PID#"

[0070] "Error: could not verify 'CustomerID': #CID#" or 'PartnerID': #PID#"

[0071] Figure 5 is a flowchart that depicts the processing of a billing request for a transaction according to an exemplary embodiment, after the registration and activation process described above has been completed successfully. In Figure 5, the process starts and proceeds to step 501 in which the customer initiates a billing event by requesting the product, such as premium content or services, for which the third party was registered and/or activated as described above with respect to Figure 4. In step 502, the third party provider generates a billing request that

includes the customer identification code, a product identification code for the product that is the subject of the transaction, and a provider identification code of the third party provider. Other parameters may also be included in the billing request.

[0072] Next, in step 503, mobile community platform 202 (intermediary billing system) receives the billing request described above and then performs validation of the billing request in step 504. The validation of the billing request is performed by determining whether the customer identification code in the billing request corresponds to a customer in the database of mobile community platform 202, and by determining whether the provider identification code in the billing request corresponds to a valid third party provider in the database of mobile community platform 202. If it is determined in step 505 that the billing request validation result is not valid, then the process proceeds to step 506 in which mobile community platform 202 sends an error reply to the third party provider, upon which the third party provider may refuse access to the product by the customer.

[0073] On the other hand, if it is determined in step 505 that the billing request validation result is valid, then the process proceeds to step 507 in which mobile community platform 202 sends at least one message, such as a premium SMS or other type of billable message, to the mobile phone number associated with the customer identification code in the database of mobile community platform 202. The message is sent from mobile community platform 202 through the carrier for the customer's mobile phone number, so that a billable amount associated with the message is billed to the customer's account with the carrier. In this manner, the transaction for a product between the customer and the third party provider is easily supported by mobile community platform 202 through the use of billable messages sent to the customer. The billing request from the third party provider may include a message text string which is then included in the message sent from mobile community platform 202 to the customer's mobile phone number. Such a text string may be used by the third party provider to thank the customer for the purchase, and possibly to confirm the details of the purchase, such as the product identification, the transaction price, etc.

[0074] In step 508, mobile community platform 202 sends a confirmation to the third party provider that the customer was billed, upon which the third party provider may enable access to the product by the customer. The billing process of Figure 5 then ends.

[0075] Similar to the registration and activation process, the billing request of the invention may be formatted as XML and transmitted via an HTTP POST to a target URL set by mobile community platform 202. The POST parameter name is 'XML', which is an XML string that contains the following fields:

[0076]	CommunityID:	Root XML tag;
[0077]	Authentication:	Tag denotes the authentication section of the document;
[0078]	TransmissionID:	Unique identifier for the transmission;
[0079]	PartnerID:	Unique identifier for the third party provider (partner);
[0080]	UserID:	Community member name;
[0081]	Password:	Password of community member;
[0082]	ProductID:	Unique identifier for the product;
[0083]	MessageText:	Text to be included in premium message; and
[0084]	CustomerID:	Customer identification code for the customer.

[0085] Preferably, all of the above fields are required. An example of the XML for the billing request is shown below in Table 4:

```
<?xml version="1.0" encoding="utf-16"?>
<SMSac xmlns="http://tempuri.org/SMSacXMLSample.xsd">
    <TransmissionId>234032832</Transmissionid>
    <Authentication>
        <MobilePartnerId>TestMPID</MobilePartnerId>
        <!--Required; Mobile Partner username -->
        <UserId>TestUserID</UserId>
        <!--Required; SMs.ac Member Name -->
        <Password>Password1</Password>
        <!--Required:  Password of your sms.ac account -->
    </Authentication>
    <UserOriginatedMessages>
        <Useroriginatedmessage>

            <ProductId>5678</ProductId>
            <!--Required; The ID of the mobile Product -->

            <MessageText>
                Thank you for using www.MobilePartner.com
            </MessageText>
            <!--Required; The Text of the Message -->
```

```
            <CustomerI>test_user_01</CustomerId>
            <!--Required; The customer that is to be charged -->

        </UserOriginatedMessage>
    </UserOriginatedMessages>
</SMSac>
```

Table 4

[0086] and an example XSD for the request is shown below in Table 5:

```
<?xml version="1.0"?>
<xs:schema id="NewDataSet" targetNamespace="sms.ac"
    xmlns:mstns="sms.ac"
    xmlns="sms.ac" xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:msdata="urn:schemas-microsoft-com:xml-msdata"
    attributeFormDefault="qualified" elementFormDefault="qualified">
    <xs:element name="SMSac">
        <xs:complexT'ype>
            <xs:sequence>
                <xs:element name="TransmissionId" type="xs:int" minoccurs="1"
                    minoccurs="i"/>
                <xs:element name="Authentication" minoccurs="1" minoccurs="1">
                    <xs:complextype>
                        <xs:sequence>
                            <xs:element name=" MobilePartnerId" type="xs:int"
                                minoccurs="1" maxoccurs="1" />
                            <xs:element name="userId" type="xs:string" minoccurs="1"
                                maxoccurs="1" />
                            <xs:element name="Password" type="xs:string"
                                minoccurs="1" maxoccurs="1" />
                        </xs:sequence>
                    </xs:complexType>
                </xs:element>
            <xs:element name="UserOriginatedMessages" minoccurs="0"
                maxoccurs="1">
                        <xs:complexType>
                            <xs:sequence>
                                <xs:element name="UserOriginatedMessage"
                                    minoccurs="0" maxoccurs="unbounded">
                                    <xs:complexType>
                                    <xs:sequence>
                                        <xs:element name="ProductId" type="xs:int"
                                            minoccurs="1" />
                                        <xs:element name="MessageText" type="xs:string"
                                            minoccurs="1" />
```

```
                                    <xs:element name="CustomerId" type="xs:string"
                                        minoccurs="1" />
                                    <xs:element name="ChargeType"
                                        default="Premium">
                                        <xs:simpleType>
                                        <xs:restriction base="xs:string">
                                            <xs:enumeration value="Premium"/>
                                            <xs:enumeration value="Standard"/>
                                        </xs:restriction>
                                        </xs:simpleType>
                                    </xs:element>
                                </xs:sequence>
                            </xs:complexType>
                        </xs:element>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
        </xs:sequence>
    </xs:complexType>
</xs:element>
<xs:element name="NewDataSet" msdata:ISDataset="true"
    msdata:Enforceconstraints="False">
    <xs:complexType>
        <xs:choice maxoccurs="unbounded">
            <xs:element ref="SMSac" />
        </xs:choice>
    </xs:complexType>
</xs:element>
</xs:schema>
```

Table 5

[0087] The possible response code for the billing request, include the error reply of step 506 and the confirmation of step 508 in Figure 5. In this regard, the response codes are indicated of these replies are indicated by a "1" for success, and a "0" for failure (error). The response of "0" for failure can also include a failure message that provides a brief explanation of why the billing request failed.

[0088] Figure 6 is a flowchart which provides another exemplary embodiment of processing a billing transaction according to the invention. As seen in Figure 6, the process starts and proceeds to step 601 in which a customer initiates a billing event by selecting a product, such as premium content or services, offered through the third party provider. Then, in step 602, the third party provider directs the customer to mobile community platform 202 (intermediary billing system), along with a provider identification code for the third party provider and a product

identification code for the product. This initiates the transaction activation process. In a particular embodiment, the customer is directed to mobile community platform 202 through the use of a hyperlink.

[0089] In step 603, mobile community platform 202 determines whether the customer needs to login, and register if not already registered. The customer does not need to login if the customer is registered and has previously been successfully through this process for the same product. If the login or registration is required, the process proceeds to step 605. On the other hand, if the login or registration is required, the process proceeds to step 604 in which the customer logs in to mobile community platform 202, or registers with mobile community platform 202 as described above in the embodiment of Figure 4. Next, in step 605, mobile community platform 202 prompts the customer for a confirmation of an instruction to proceed with the transaction, and displays a description of the product (service or content) along with the price and possibly other information. Assuming the customer confirms the transaction, the process proceeds to step 606, in which mobile community platform 202 generates an encrypted cookie that indicates the customer has "opted in" (purchased) the product, and can therefore skip steps 603 to 606 in the future for transactions involving this particular product. The encrypted cookie is then placed in the customer's browser application.

[0090] In step 607, mobile community platform 202 bills the customer for the product by sending a premium message to the mobile phone number associated with the customer identification code for this customer in the database of mobile community platform 202. The billing value of the premium message corresponds to the transaction price for the product. In this manner, mobile community platform 202 easily handles the billing, which may often be a micro-transaction, for third party provider through the use of premium messages and the existing relationships between various mobile carrier systems and mobile community platform 202. Next, in step 608, mobile community platform 202 generates a verification code that indicates the customer has been billed for the transaction, encrypts the verification code, and places the encrypted verification code in a cookie on the customer's browser application. The verification code is also stored in the database of mobile community platform 202 in association with the customer identification code for this customer. Then customer is then directed back to the third party provider location (such as a website page) associated with the product of the transaction (this URL is specified by the third party provider).

[0091] The third party provider then accesses the cookie from the customer's browser application and obtains the encrypted verification code. In step 609, mobile community platform 202 receives a validation request from the third party provider, the validation request including a returned encrypted verification code that the third party provider obtained from the cookie in the user's browser, along with the customer identification code for this customer. Then, in step 610, mobile community platform 202 performs validation on the returned encrypted verification code by decrypting it and comparing it against the encrypted verification code that was previously generated by mobile community platform 202 for this transaction, and confirming that the customer has been successfully billed for this transaction. If the verification code is validated by mobile community platform 202, then flow passes to step 612 in which mobile community platform 202 sends a valid response to the third party provider. If, on the other hand, the verification code is not validated by mobile community platform 202, then flow passes to step 611 in which mobile community platform 202 sends an error response to the third party provider. The third party provider then determines whether to provide the customer with access to the product based on the validation response received from mobile community platform 202 (intermediary billing system). The process of Figure 6 then ends.

[0092] It can be appreciated that the invention may be carried out in various embodiments, in which some of the above described aspects may not be included. In this regard, Figure 7 depicts a billing process according to another embodiment of the invention, in which the intermediary billing system may be standalone and can process transaction requests from any source for a customer and transaction amount, by using various types of external billing mechanisms and billing event triggers. In Figure 7, the process begins at step 701 in which mobile community platform 202 (intermediary billing system) receives a transaction request, from any source internal or external to mobile community platform 202, that is associated with a customer identification code and a predetermined transaction amount. Mobile community platform 202 then performs validation of the transaction request in step 702. The validation of the transaction request is performed by determining whether the customer identification code in the transaction request corresponds to a previously-registered and activated customer in the database of mobile community platform 202. If it is determined in step 703 that the transaction request validation result is not valid, then the process proceeds to step 704 in which mobile community platform 202 denies the transaction request, the customer is not billed, and the process ends.

[0093] On the other hand, if it is determined in step 703 that the transaction request validation result is valid, then the process proceeds to step 705 in which mobile community platform 202 sends a billing event trigger to an external billing mechanism in order to effectuate billing of the customer for the transaction amount. The billing event trigger is associated with the customer identification code, and may actually contain the customer identification code, so that the external billing mechanism bills the correct customer for the transaction amount. The external billing mechanism can be any type of mechanism or system for billing the customer, such as the billing system of a mobile carrier for the customer's mobile phone (as discussed above), a credit card billing system, a prepaid card billing system, a web-based payment system, a bank account billing system, or any other billing system or mechanism to which mobile community platform 202 can interface and direct a billing event trigger for a customer. Mobile community platform 202 can simultaneously use several different external billing mechanisms, and may use one or several of them for each customer depending on the type of third party providers with which the customer conducts transactions. Accordingly, mobile community platform 202 acts as a virtual point-of-sale for third party providers to enable the payment for transactions through the use of one or more external billing mechanisms with which mobile community platform 202 has a pre-existing relationship for authorized use of the external billing mechanisms.

[0094] Similarly, the billing event trigger can be one of many different types and formats, depending on the external billing mechanism to which the billing event trigger is sent for the customer, and the pre-existing arrangement (if any) that mobile community platform 202 has with the external billing mechanism. For example, in the case that the external billing mechanism is the billing system of the mobile carrier corresponding to the customer's mobile phone number, then the billing event trigger can be a message, such as a premium SMS, MMS, or other type of billable message, that is sent from mobile community platform 202 to the customer's mobile phone number through the mobile carrier. In the alternative, other types of billing event triggers can be used with the external billing mechanism. For example, the billing event trigger sent to the mobile carrier billing system can be a billing record file which contains the transactions for a customer that will then be added to the customer's carver bill by the mobile carrier billing system. As mentioned above, other types and forms of billing event triggers that can be used by mobile community platform 202 include messages such as SMS, MMS, email,

file transfers, XML, HTTP, billing record transfers, or any other type of communication supported by the internet, encrypted or unencrypted.

[0095] The transaction request from the third party provider may include a message text string which is then included in the message sent from mobile community platform 202 to the customer's mobile phone number. Such a text string may be used to thank the customer for the purchase, and possibly to confirm the details of the purchase, such as the product identification, the transaction price, etc. The process of Figure 7 then ends. It can be appreciated that the general billing system depicted in Figure 7 provides a powerful, efficient and convenient way with which to bill customers for various types of transactions by using an existing interface between mobile community platform 202 and one or more external billing mechanisms.

[0096] Once a number of transactions have been accomplished, the third party provider will have funds present in the mobile community platform 202. In this description, a third party provider may be any user or company that can accrue value such that currency or funds may be sent from the user or company to another user or company. These funds can stay within the mobile community when users transfer such funds from one account to another. In fact, the mobile community platform or network can act as the processor of funds that are held within the community. However, at some point, users may wish to transfer these funds out of the community, e.g., to receive cash, make a purchase, etc.

[0097] To obtain access to these funds, the third party provider may request a check, electronic transfer, or other such payment mechanism to be initiated. Referring to Figures 8 and 9, an embodiment is shown of a method of providing a transaction, in particular a "cashout" or "payout" transaction, to a third party provider registered with the mobile community platform.

[0098] It is noted at this point that the mobile community platform refers to a network in which each user has a handset or other wireless device with embedded software which interfaces with software that may be embedded in a web site, a cash register, a television (e.g., to allow viewer voting contexts within television programming), or other product-dispensing devices, e.g., vending machines. The mobile community platform need not specifically be a web site: it can be software connected to a point of sale device. The mobile community platform can exist as a feature of common electronic devices or via a connected device such as a cash register or a broadband two-way device such as a television. In this way, and as described in greater detail below, the handset or other wireless device acts as a remote control enabling the user to conduct

a variety of functions. The user is, thus, enabled to utilize a free environment, namely, the sending of no-charge text messages, to conduct a variety of transactions. One skilled in the art can envision future technologies replacing text messages to effectuate such transactions. The mobile wireless device is a device the user possesses, but other devices serving as a remote control can also be employed, including a television, a cash register in a store, and so on.

[0099] The method begins when a user, such as a customer, merchant, vendor, or indeed any holder of currency, either by the mobile community platform or otherwise, either initiates a transaction request (step 714) or is asked about a potential transaction request (step 715). In the first case, a user initiates the transaction request in order to perform a purchase or receive a cash-out, and this is termed a mobile-originated (MO) transaction request. In the second case, the mobile community platform, third-party vendor, or other non-user asks the user if a transaction request is desired. This is termed a mobile-terminated (MT) transaction request. This may pertain to the case where a user wishes to purchase a good: then in response to a third-party message to the mobile community platform, the user may receive an MT verification or confirmation of the user's request. The former may be to ensure the user intended to request the transaction. The latter may be to give confirmation to the user that the transaction has occurred. In another case, in response to the user receiving money in their account, such as a deposit or other positive cash flow transaction, the user may be asked if a transaction request is desired. In either case, the user may send the MO request or may concur with the MT verification or confirmation of the user's request and the transaction proceeds with the mobile community platform receiving the request (step 706).

[0100] Referring in particular to Figure 9, the method 721 continues when the mobile community platform receives the transaction request associated with a transaction amount by the third party provider (step 706). It is particularly envisioned here that a cashout transaction is requested, where the third party provider requests a check or other transfer of an amount certain. However, numerous other transactions may also be contemplated within the scope of the invention. The third party provider may typically send this transaction request via the mobile community platform website and via a first computing system. However, in alternative embodiments, the transaction request may be sent via a wireless communication device.

[0101] There are several possible embodiments of the mobile community platform. There can be software on the network, such as the Internet, interacting with a product via a browser or other

type of world wide web. One embodiment utilizes a WAP link, a WAP site or a mobile web site. In the case of a mobile web site, messages maybe retained on the handset, allowing the same to be utilized as a constant reference similar to a benchmark. Another possibility is to have handset applications with "on deck" software installed that recreates the mobile community network product experience, functioning similar to other familiar application experiences on the handset, from a software perspective, but also enabling data transfers from the web. The software may be similar to an email client installed on a machine, but once opened up to access emails originating from another source, allowing access to the mobile community network and accompanying mobile community network applications through the installed software. Another embodiment includes enablement of interaction with hardware such as in the case of a consumer's physical interaction with the device. This interaction may occur through a single button imbedded on a device which when clicked will access the community for the user. Further details of this embodiment are provided below.

[0102] Following the request, the mobile community transmits an identity verification code to the third party provider (step 707) via a mobile network to a wireless communication device. In alternative embodiments, the code may be sent via a wired network, or to a wired communication device, or both. The wireless communication device serves an important function in this embodiment, however. The physical possession by the requester of the wireless communication device, to which, e.g., an SMS is sent, serves as an effective check on the identity of the requester, because if the requester lacks physical possession of their wireless communication device, the transaction cannot be completed. The code may be sent in the form of an SMS, which may be encrypted or otherwise protected, or via similar means.

[0103] An added level of protection is provided by requiring the user to identify a personally identifiable number, e.g., a mobile PIN, that has been assigned to that user, much like an ATM PIN number. By way of example only, by entering the mobile PIN, the handset can be used like a keypad and can achieve the functionality equivalent to a "portable ATM". Once a key on the handset is pressed, the user accesses an interface (which may be just the handset's native messaging functionality, a user interface associated with the mobile community platform, or indeed any other way of sending a signal) and is then queried as to what they desire to do. The user can respond with the selection such as to send cash, as an example. The user is then asked to enter the mobile PIN. The platform confirms and executes the user's requested transaction.

By pressing a button on the wireless device, the user has achieved the same transaction as walking to a bank or to an ATM. Other types of protection can also be provided, e.g., by text-messaging, etc.

[0104] Following receipt of the identify verification code, the third party provider transmits the same to the mobile community platform (step 708). The transmission may be by way of a wired or wireless communication device or computing device, but may be typically accomplished by way of the World Wide Web and the code input on the mobile community platform website itself. The mobile community platform then receives the transmitted identity code (step 709), and compares the code transmitted by the mobile community platform to the one received by the same (step 710).

[0105] The codes are compared to determine if they match (step 711). If they do, the YES branch of the decision is followed and the mobile community platform sends a transaction trigger associated with the third party provider code to an external payment mechanism for the transaction amount (step 712). In the case exemplified here, if the codes match then the mobile community platform sends a check or other transfer to the third party provider to, e.g., "cash them out". If the codes do not match, then the transaction request is denied (step 713), further securing the transaction against fraud or other deleterious activity.

[0106] Various implementation details of the method are now discussed. It is noted that the embodiment of Figure 8 is with respect to a third party provider; however, any user or customer of the mobile community platform who desires a transaction may be caused to perform the same steps to enable verification. For example, if a user has accumulated funds, through any method, the same may request a check or transfer of those funds using the above method. Also, in this method, the transaction requested may be different than a cashout request, e.g., a transfer request to transfer funds to another account, either within the mobile community platform or outside of the same. In the latter case, e.g., a transaction may be made across a compatible network, such as Cirrus, Star, PayPal, etc., in communication with a bank or other credit provider account. The transfer may also be for purchase of goods, and the identity code may be input on a point-of-sale terminal or other mode of communication, such as on the wireless device itself, to enable verification prior to purchase (in this case, the third party provider or other user is considered a "purchaser"). The subsequent verification is to confirm that the user wishes to complete the transaction, further securing the billing transaction. Such a system is shown in Figure 11, where

mobile community platform 719 is shown interfacing with non-mobile community platform networks 720 through the verification method 721 according to an embodiment of the invention.

[0107] Moreover, the term "wireless communication device" may apply to cell phones, mobile phones, satellite phones, personal digital assistants with wireless capabilities, computing devices with wireless capabilities, or indeed any device that can transmit and receive signals, etc.

[0108] An alternative embodiment includes wireless communication devices such as handsets having built-in a special button keyed to a code transmitter to enable transmission of a special code associated with that handset, to prevent spurious or illegal code generation intended to impersonate the handset and circumvent the security procedures therein. In this way, the handset may act as a "remote control". As detailed above, the remote control can interface with the software on a web site, cash register, television, vending machine or with any other device selling products. The remote control functions much like a point of sale terminal with the added advantage of being mobile. The button on such a "remote control" not only triggers the billing event but also represents an inherent verification mechanism. Such functionality may be particularly important where the transacted funds are located and are sent to accounts within the mobile community platform.

[0109] In a further alternative embodiment, the special button may be specifically for purchases or other such transactions, and the use of the same in conjunction with a transaction amount may be employed to automatically connect to (or contact via a WAP communication through the handset) the mobile community platform to automatically debit the third party provider or user's account for the transaction amount. In this way, the handset may be used in a way similar to a wallet - holding funds secure until a user wishes to disburse the same. An advantage of this embodiment is that the handset may be significantly more secure than a wallet, in that a wallet can be stolen while use of the handset as a purchasing mechanism is contingent upon the user entering the proper code. Purchases made in this way may be charged on the user's billing system as described in detail above, or may be debited to a bank or other credit provider, mobile phone or carrier as described above and below.

[0110] In a similar fashion, the system may be employed to enable purchases on online shopping sites or other purchasing venues (collectively "third party vendors"). In one embodiment, the charge for the purchase or transaction can be applied to the mobile account, i.e., the billing system described above. In this embodiment, the third party vendor, if an online shopping site,

may be provided a button to link to the mobile community platform. Clicking on this button during checkout may then result in the user being charged through the billing system described above and receiving the goods purchased in due course. In more detail, referring to Figure 10, a user may desire to purchase goods from a third party vendor (step 716). In so doing, the third party vendor may employ the mobile community platform billing system to receive payment (step 717). To accomplish this, the third party vendor or user may cause an MT to be sent to the user's handset, the third party vendor may cause a transaction request via another technique, or the user may send an MO transaction request to the mobile community platform (collectively step 718). The flow of the transaction may then continue at step 706 as described above. In certain cases, the user may sign into their account on the third party vendor site and identify items of purchase in a shopping cart. The system may know the user's payment preferences, either via billing using the mobile community platform or via another system. The mobile community platform can provide verification and confirmation of payment in either system, and may also provide payment if the user's payment preference is via billing employing the mobile community platform.

[0111] In another embodiment, the system may be used for online shopping or other purchases, including at physical point-of-sale storefronts, in conjunction with another account for payment, e.g., a separate bank account, PayPal, carrier, etc. In this embodiment, the user would, during check-out, identify a bank account to use to purchase the goods in their shopping cart. Of course, the online shopping site or storefront may also pre-identify such accounts preferred by the user on the basis of use history. Once identified, the bank or other holder of the account sends a verification code via the mobile community network to the purchaser or user to allow verification of the identity of the same. Alternatively, the mobile community platform may also send a verification code on behalf of the bank to the purchaser, customer, or user via their wireless communications device. Return of the code to the mobile community platform, either via the wireless communication device, a computing system associated with the purchaser, a computing system associated with the online shopping site or physical storefront, or otherwise, then allows a degree of protection against fraud. Upon code receipt and verification, the mobile community platform may direct the bank or other credit provider to debit the user's account appropriately. Alternatively, as noted above, the mobile community platform may cause the user's mobile account to be charged appropriately for the purchase or other transaction. In any

case, the purchaser is protected by the physical possession of the handset and knowledge of their unique PIN and the built in security requirements of the platform's software.

[0112] As may be seen from the above disclosure, certain embodied systems may combine billing and verification functions to accomplish cash-outs, purchasing, security and permissions, e.g., to allow downloading or uploading of protected content. In particular, such verification ensures that there is a secure identification mechanism in place for the uploading process.

[0113] While the present invention has been particularly described above with reference to the various figures and embodiments, it should be understood that the invention is not limited to the above-described embodiments. Various changes and modifications may be made to the invention by those of ordinary skill in the art without departing from the spirit and scope of the invention.

WHAT IS CLAIMED IS:

1. A method for performing a secure transaction, the method including:
   a. a customer transaction request step of transmitting, from a first computing system to an intermediary billing system, a request for a secure transaction;
   b. a verification code step of generating, in the intermediary billing system, a verification code, and transmitting, from the intermediary billing system to a wireless communication device associated with the customer, the verification code;
   c. a customer confirmation step of transmitting, from a second computing system, the verification code to the intermediary billing system;
   d. a validation step of receiving, at the intermediary billing system, the verification code sent in the customer confirmation step and comparing the verification code sent in the customer confirmation step to the verification code generated in the verification code step;
   e. a response step of allowing the customer transaction request, at the intermediary billing system, if the verification code sent in the customer confirmation step matches the verification code generated in the verification code step, and denying the customer transaction request, at the intermediary billing system, if the verification code sent in the customer confirmation step does not match the verification code generated in the verification code step.
2. The method of claim 1, wherein the customer is a user.
3. The method of claim 1, wherein the intermediary billing system is part of a mobile community platform.
4. The method of claim 2, wherein the user is requesting a transaction selected from the group consisting of: a cash-out transaction, a transfer transaction, a purchase transaction, and an account replenishment transaction.
5. The method of claim 1, wherein the first computing system is the same as the second computing system.

6. The method of claim 1, wherein the first and second computing systems are selected from the group consisting of: a wireless communication device and a wired communication device.
7. The method of claim l, wherein the customer is a third party provider.
8. The method of claim 7, wherein the third party provider is requesting a transaction selected from the group consisting of: a cash-out transaction, a transfer transaction, and an account replenishment transaction.
9. The method of claim 1, wherein the first computing device is associated with the customer.
10. The method of claim 1, wherein the first computing device is associated with a third party vendor.
11. The method of claim 10, wherein the third party vendor is an online shopping website or a point-of-purchase retail store.
12. The method of claim 11, further comprising a validation response step of transmitting, from the intermediary billing system, a validation response code to the online shopping website or the point-of-purchase retail store.
13. The method of claim 1, wherein the second computing device is associated with the customer.
14. The method of claim 1, wherein the second computing device is associated with a third party vendor.
15. The method of claim 14, wherein the third party vendor is an online shopping website or a point-of-purchase retail store.
16. The method of claim 15, further comprising a validation response step of transmitting, from the intermediary billing system, a validation response code to the online shopping website or the point-of-purchase retail store.
17. The method of claim 1, wherein the customer is associated with a bank or other credit provider, and the method further including a bank or other credit provider notification step of transmitting, from the intermediary billing system to the bank or other credit provider, notification of the customer transaction request if the same has been allowed in the response step.

18. The method of claim 17, wherein the notification of the customer transaction request includes a request to debit an account of the customer in the bank or other credit provider for an amount corresponding to the customer transaction request step.

19. A computer readable medium carrying one or more sequences of instructions for carrying out the method of claim 1.

20. An intermediary billing system for performing a secure transaction, comprising:

    a. at least one processor;

    b. an interface having access to the internet; and

    c. a computer readable medium carrying one or more sequences of instructions for performing a secure transaction, wherein execution of the one or more sequences of instructions by the at least one processor causes the at least one processor to perform the steps of:

        i. a customer transaction request step of receiving, from a first computing system to the intermediary billing system, a request for a secure transaction;

        ii. a verification code step of generating, in the intermediary billing system, a verification code, and transmitting, from the intermediary billing system to a wireless communication device associated with the customer, the verification code;

        iii. a validation step of receiving, at the intermediary billing system, the verification code sent in the customer confirmation step and comparing the verification code sent in the customer confirmation step to the verification code generated in the verification code step;

        iv. a response step of allowing the customer transaction request, at the intermediary billing system, if the verification code sent in the customer confirmation step matches the verification code generated in the verification code step, and denying the customer transaction request, at the intermediary billing system, if the verification code sent in the customer confirmation step does not match the verification code generated in the verification code step.

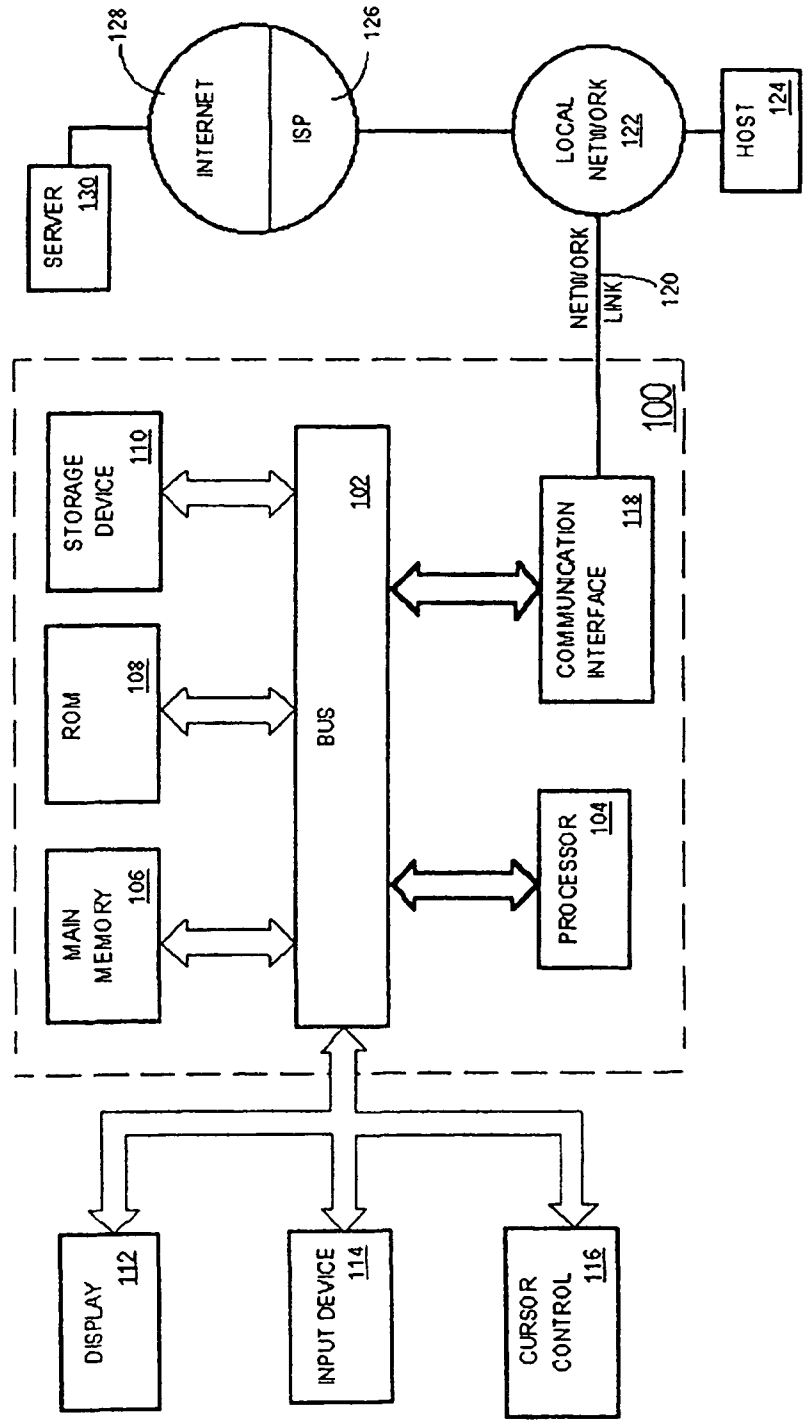

128
126
INTERNET
ISP
LOCAL NETWORK 122
HOST 124
SERVER 130
NETWORK LINK 120
100
STORAGE DEVICE 110
ROM 108
MAIN MEMORY 106
BUS 102
COMMUNICATION INTERFACE 118
PROCESSOR 104
DISPLAY 112
INPUT DEVICE 114
CURSOR CONTROL 116

FIG. 1

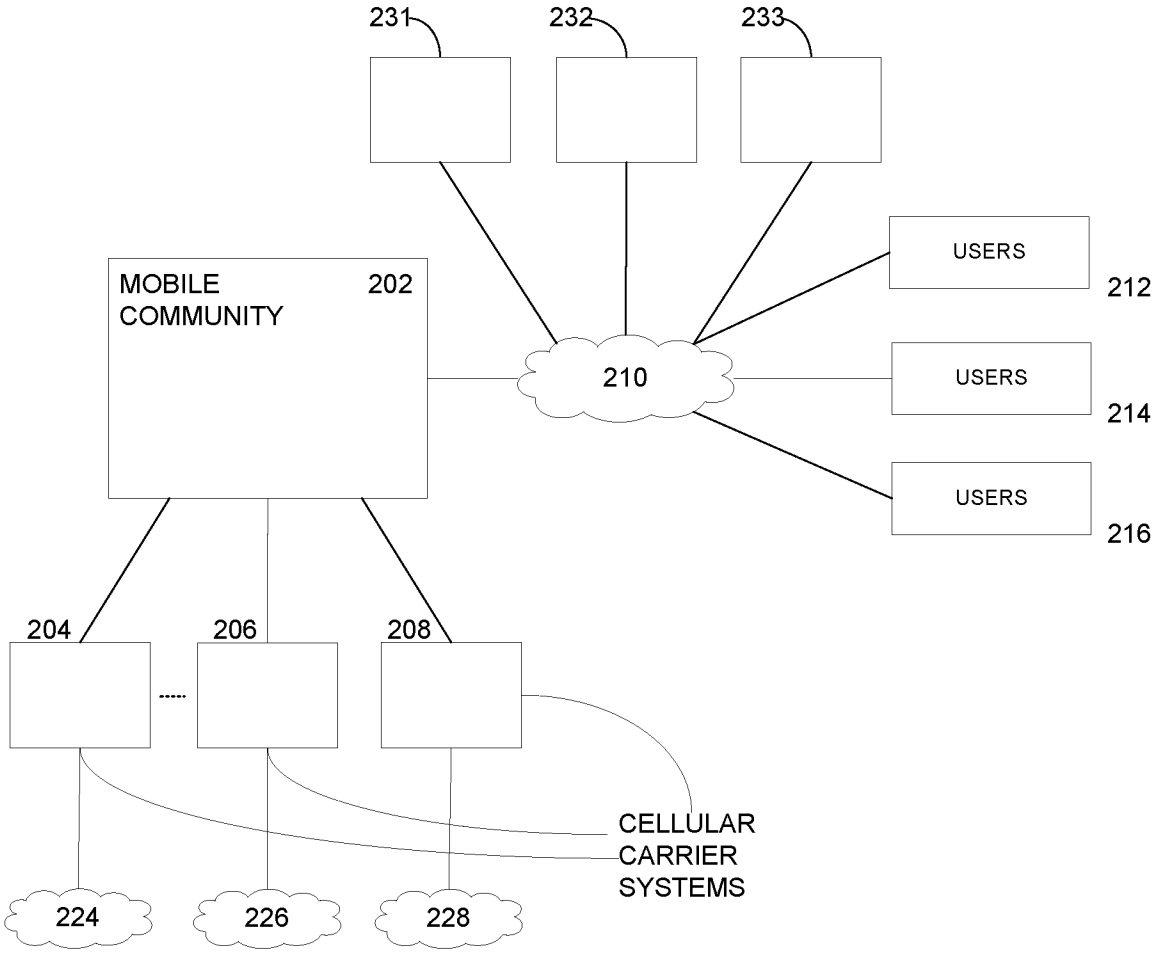

231
232
233
USERS
212
MOBILE
COMMUNITY
202
210
USERS
214
USERS
216
204
206
208
CELLULAR
CARRIER
SYSTEMS
224
226
228

FIG. 2

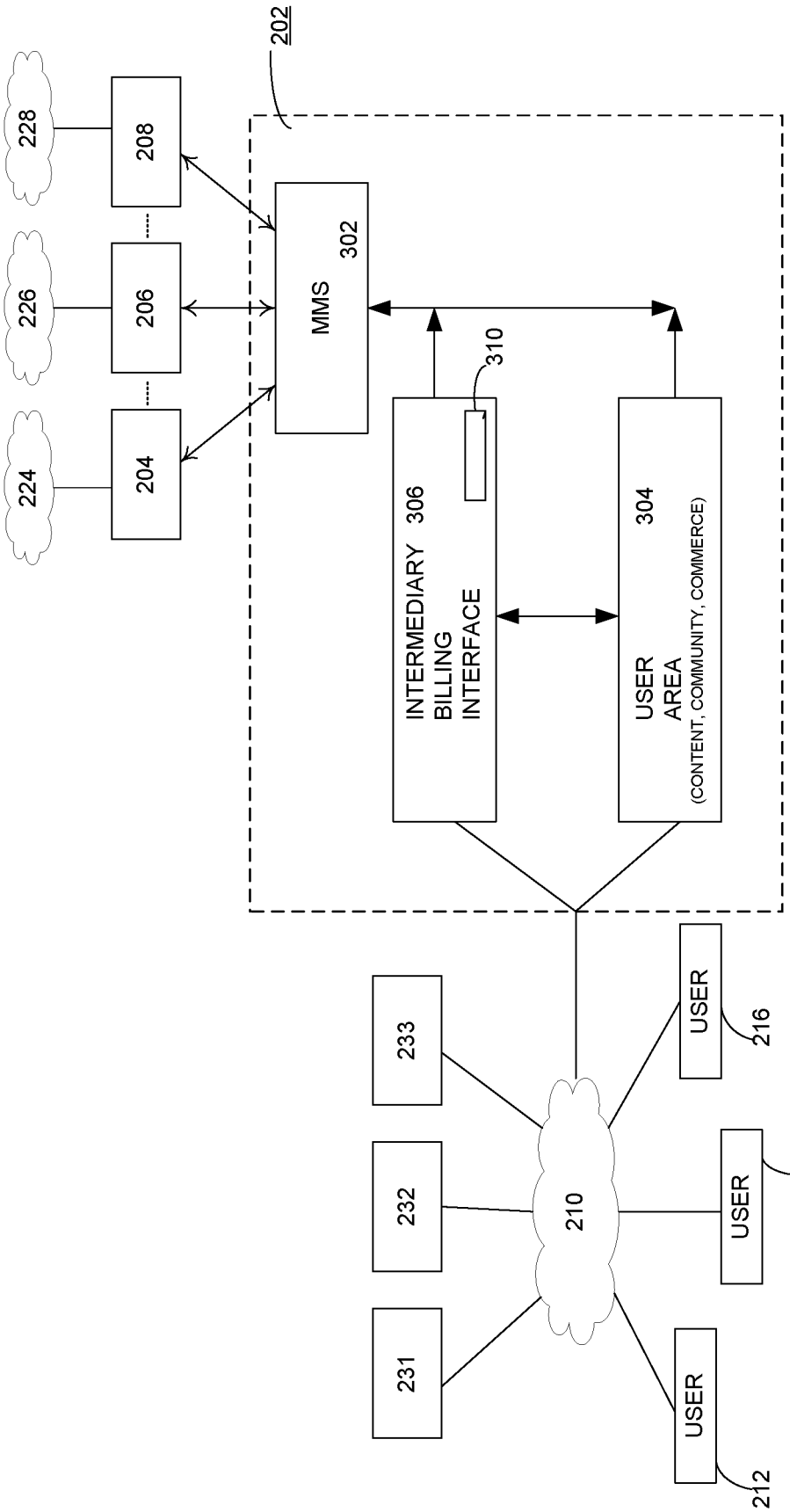

202
228
208
226
206
224
204
MMS
302
310
INTERMEDIARY
306
BILLING
INTERFACE
USER
AREA
304
(CONTENT, COMMUNITY, COMMERCE)
233
232
231
210
USER
216
USER
214
USER
212

FIG. 3

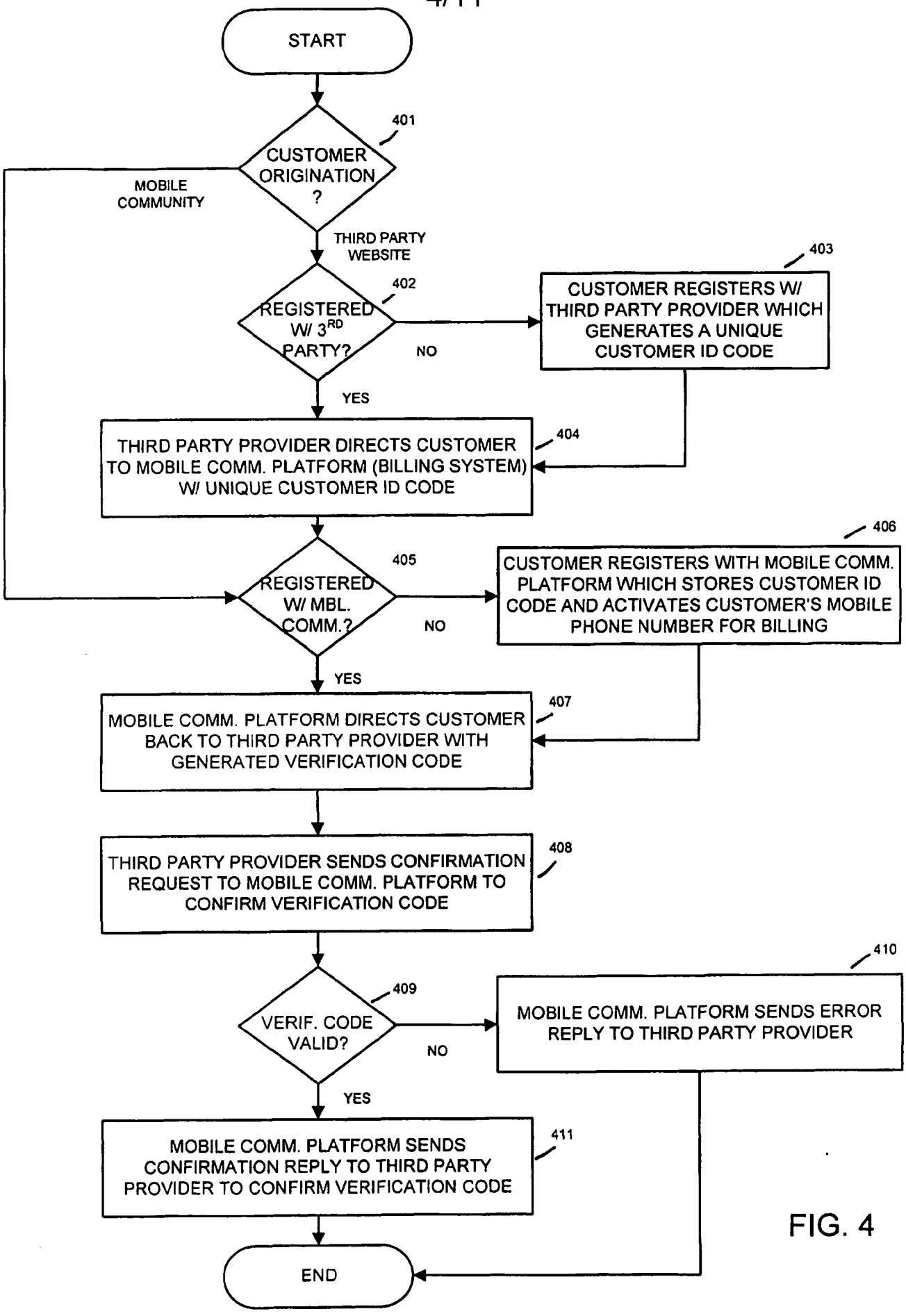

START
401
CUSTOMER ORIGINATION ?
MOBILE COMMUNITY
THIRD PARTY WEBSITE
402
REGISTERED W/ 3RD PARTY?
NO
403
CUSTOMER REGISTERS W/ THIRD PARTY PROVIDER WHICH GENERATES A UNIQUE CUSTOMER ID CODE
YES
404
THIRD PARTY PROVIDER DIRECTS CUSTOMER TO MOBILE COMM. PLATFORM (BILLING SYSTEM) W/ UNIQUE CUSTOMER ID CODE
405
REGISTERED W/ MBL. COMM.?
NO
406
CUSTOMER REGISTERS WITH MOBILE COMM. PLATFORM WHICH STORES CUSTOMER ID CODE AND ACTIVATES CUSTOMER'S MOBILE PHONE NUMBER FOR BILLING
YES
407
MOBILE COMM. PLATFORM DIRECTS CUSTOMER BACK TO THIRD PARTY PROVIDER WITH GENERATED VERIFICATION CODE
408
THIRD PARTY PROVIDER SENDS CONFIRMATION REQUEST TO MOBILE COMM. PLATFORM TO CONFIRM VERIFICATION CODE
409
VERIF. CODE VALID?
NO
410
MOBILE COMM. PLATFORM SENDS ERROR REPLY TO THIRD PARTY PROVIDER
YES
411
MOBILE COMM. PLATFORM SENDS CONFIRMATION REPLY TO THIRD PARTY PROVIDER TO CONFIRM VERIFICATION CODE
END

FIG. 4

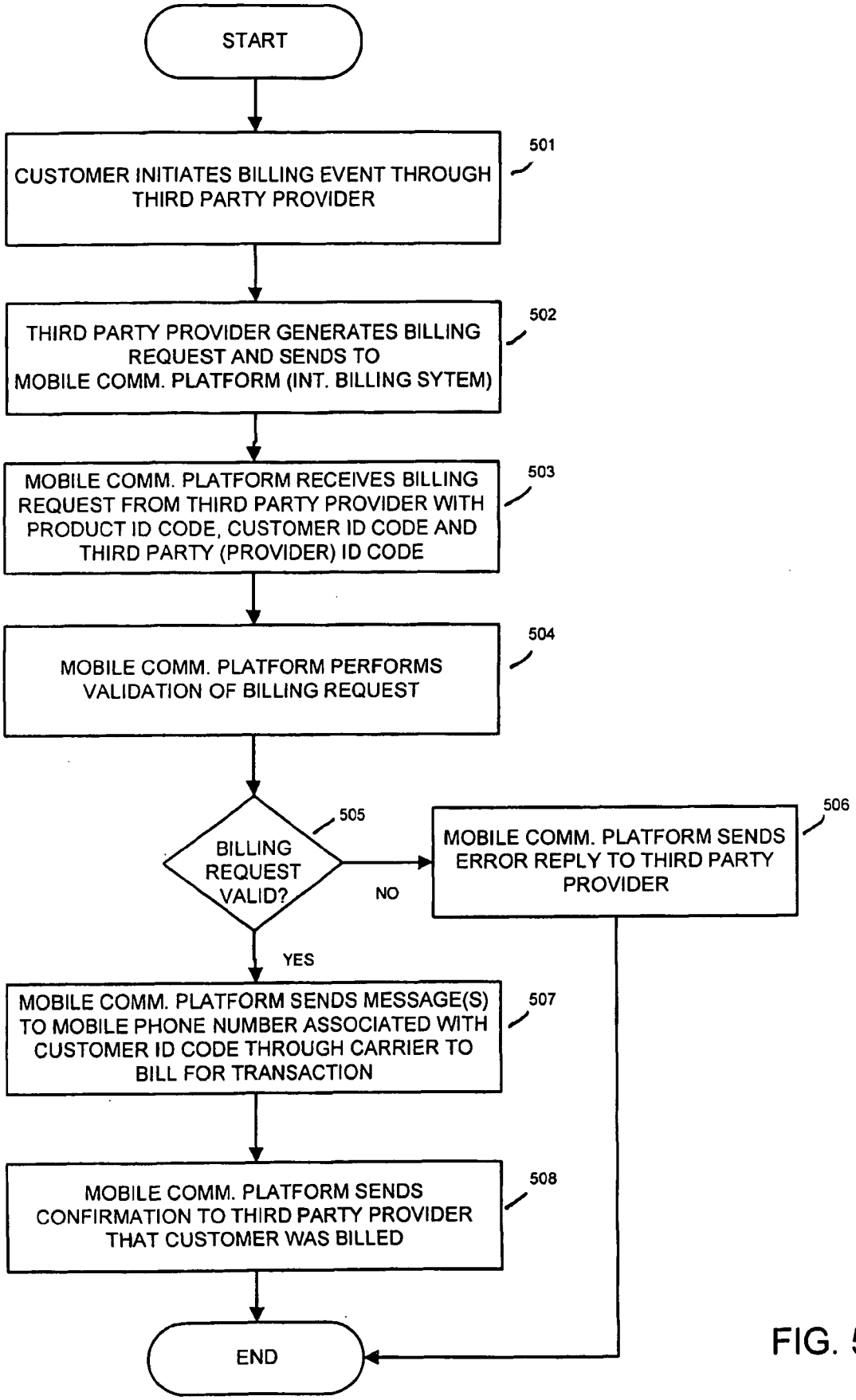

START
CUSTOMER INITIATES BILLING EVENT THROUGH THIRD PARTY PROVIDER
501
THIRD PARTY PROVIDER GENERATES BILLING REQUEST AND SENDS TO MOBILE COMM. PLATFORM (INT. BILLING SYTEM)
502
MOBILE COMM. PLATFORM RECEIVES BILLING REQUEST FROM THIRD PARTY PROVIDER WITH PRODUCT ID CODE, CUSTOMER ID CODE AND THIRD PARTY (PROVIDER) ID CODE
503
MOBILE COMM. PLATFORM PERFORMS VALIDATION OF BILLING REQUEST
504
BILLING REQUEST VALID?
505
NO
MOBILE COMM. PLATFORM SENDS ERROR REPLY TO THIRD PARTY PROVIDER
506
YES
MOBILE COMM. PLATFORM SENDS MESSAGE(S) TO MOBILE PHONE NUMBER ASSOCIATED WITH CUSTOMER ID CODE THROUGH CARRIER TO BILL FOR TRANSACTION
507
MOBILE COMM. PLATFORM SENDS CONFIRMATION TO THIRD PARTY PROVIDER THAT CUSTOMER WAS BILLED
508
END

FIG. 5

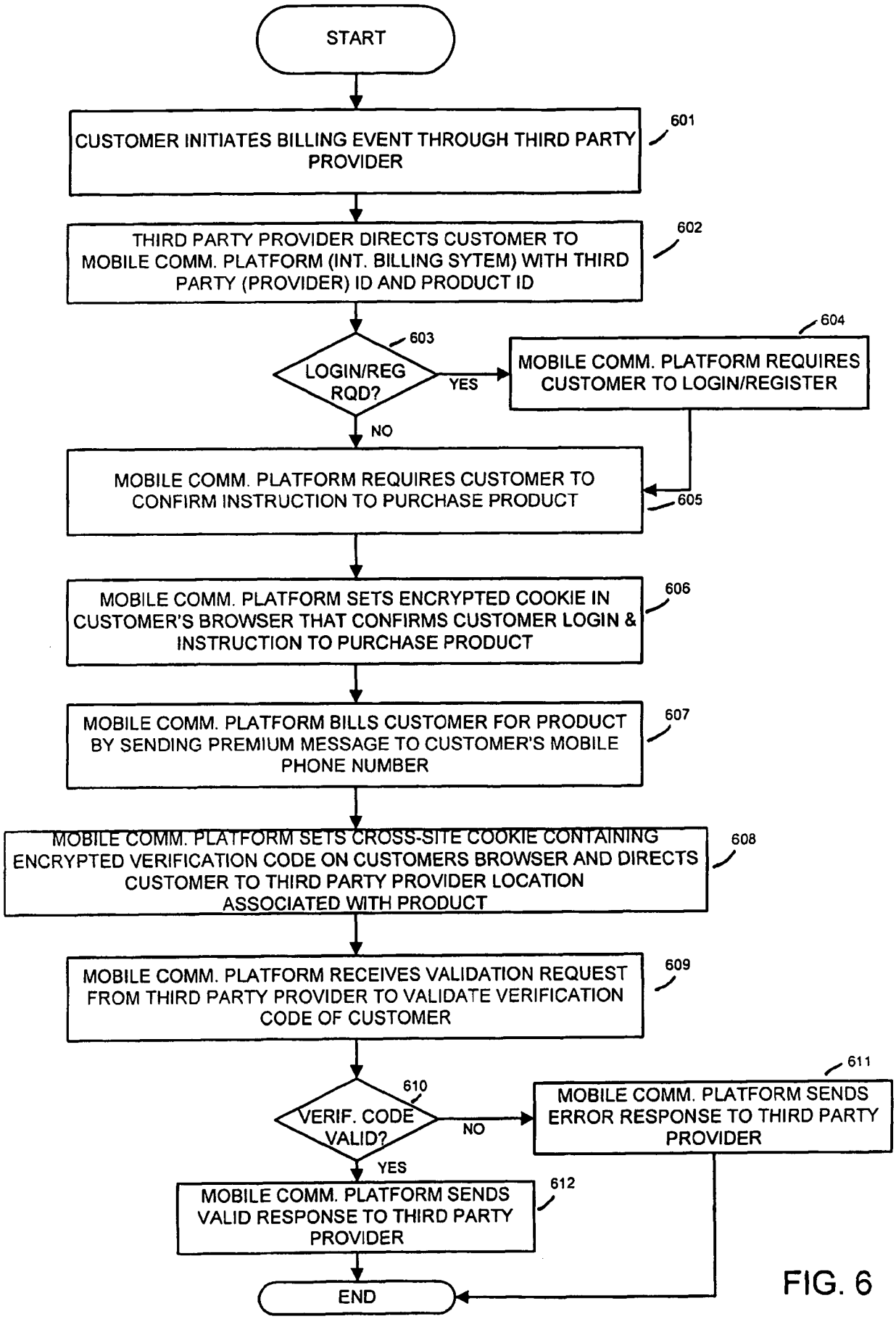

START
CUSTOMER INITIATES BILLING EVENT THROUGH THIRD PARTY PROVIDER
601
THIRD PARTY PROVIDER DIRECTS CUSTOMER TO MOBILE COMM. PLATFORM (INT. BILLING SYTEM) WITH THIRD PARTY (PROVIDER) ID AND PRODUCT ID
602
603
LOGIN/REG RQD?
YES
604
MOBILE COMM. PLATFORM REQUIRES CUSTOMER TO LOGIN/REGISTER
NO
MOBILE COMM. PLATFORM REQUIRES CUSTOMER TO CONFIRM INSTRUCTION TO PURCHASE PRODUCT
605
MOBILE COMM. PLATFORM SETS ENCRYPTED COOKIE IN CUSTOMER'S BROWSER THAT CONFIRMS CUSTOMER LOGIN & INSTRUCTION TO PURCHASE PRODUCT
606
MOBILE COMM. PLATFORM BILLS CUSTOMER FOR PRODUCT BY SENDING PREMIUM MESSAGE TO CUSTOMER'S MOBILE PHONE NUMBER
607
MOBILE COMM. PLATFORM SETS CROSS-SITE COOKIE CONTAINING ENCRYPTED VERIFICATION CODE ON CUSTOMERS BROWSER AND DIRECTS CUSTOMER TO THIRD PARTY PROVIDER LOCATION ASSOCIATED WITH PRODUCT
608
MOBILE COMM. PLATFORM RECEIVES VALIDATION REQUEST FROM THIRD PARTY PROVIDER TO VALIDATE VERIFICATION CODE OF CUSTOMER
609
610
VERIF. CODE VALID?
NO
611
MOBILE COMM. PLATFORM SENDS ERROR RESPONSE TO THIRD PARTY PROVIDER
YES
MOBILE COMM. PLATFORM SENDS VALID RESPONSE TO THIRD PARTY PROVIDER
612
END

FIG. 6

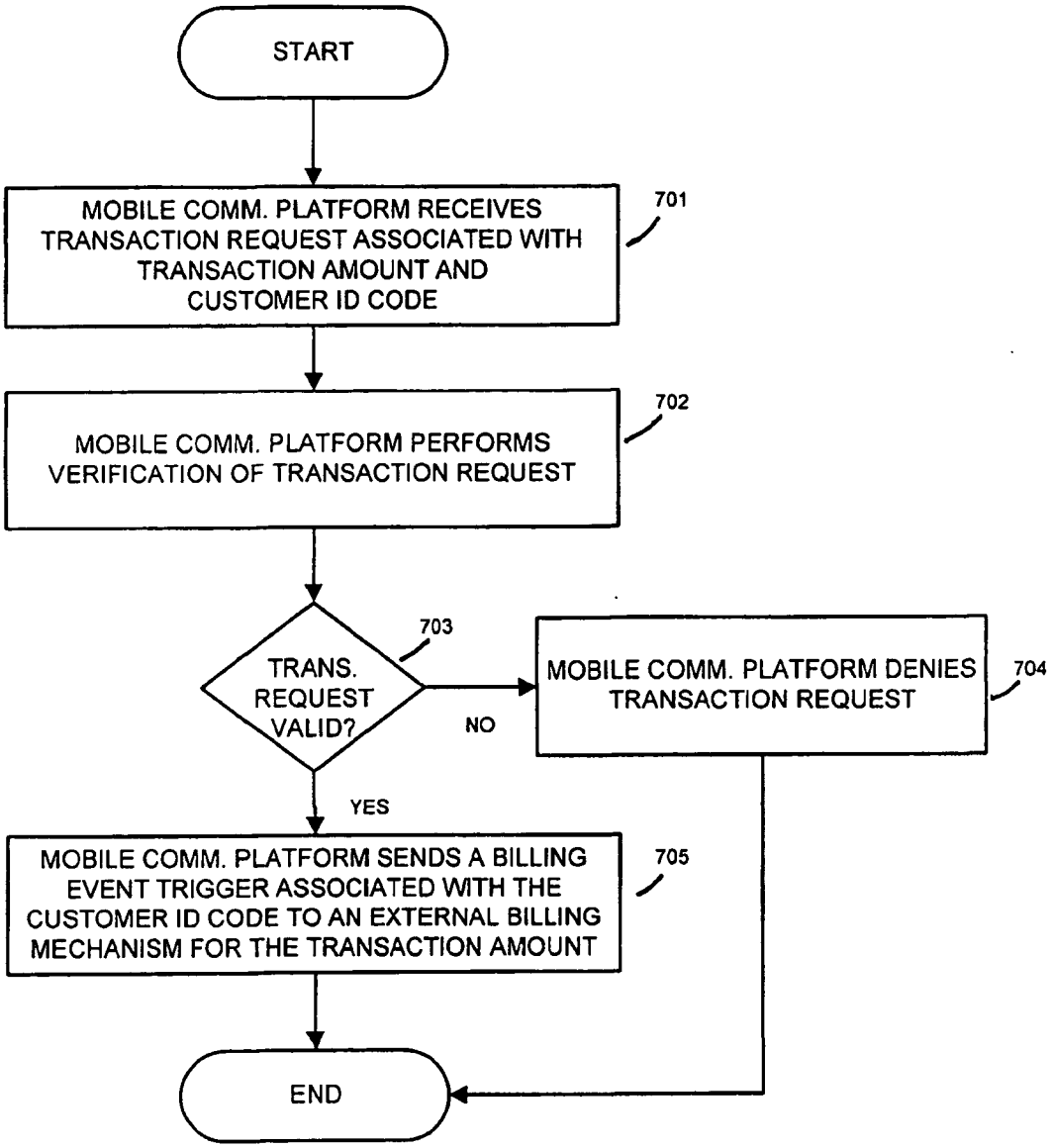
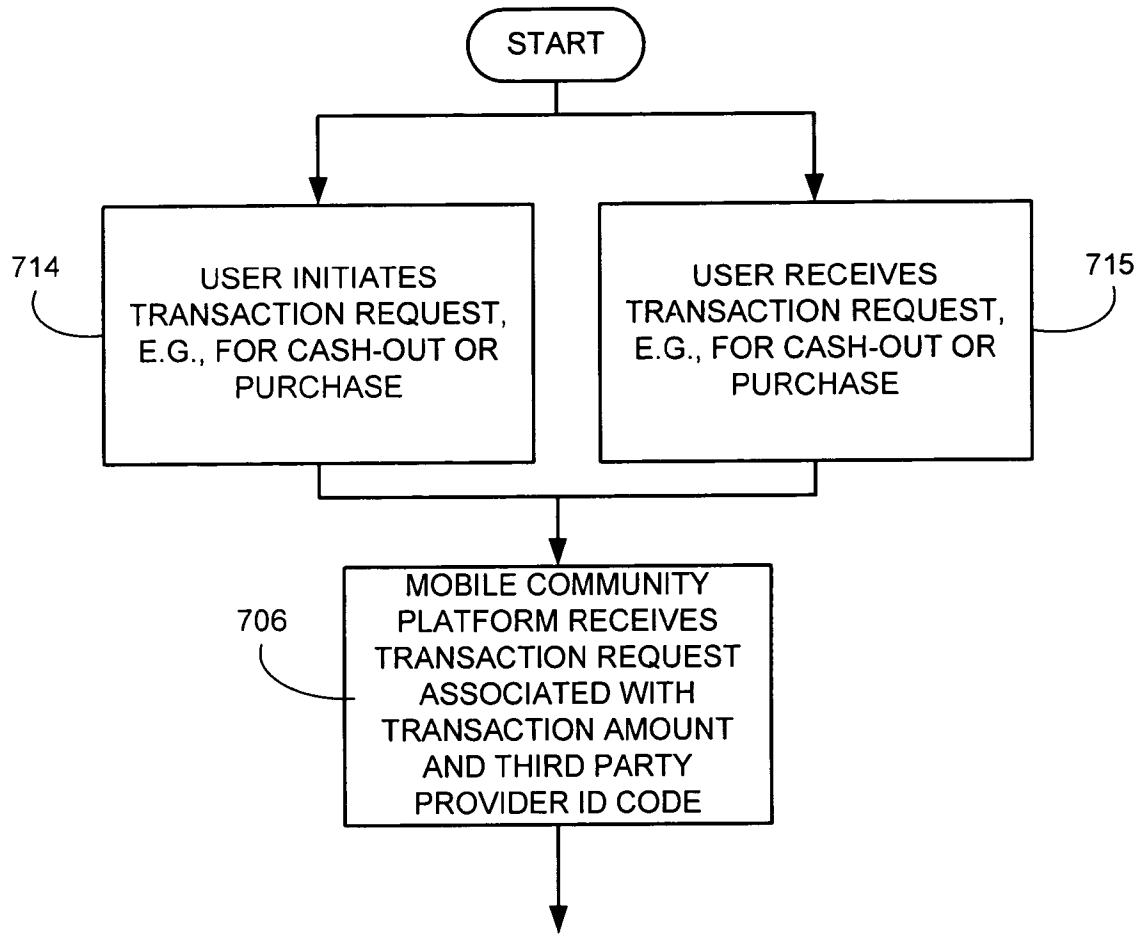

START
MOBILE COMM. PLATFORM RECEIVES TRANSACTION REQUEST ASSOCIATED WITH TRANSACTION AMOUNT AND CUSTOMER ID CODE
701
MOBILE COMM. PLATFORM PERFORMS VERIFICATION OF TRANSACTION REQUEST
702
TRANS. REQUEST VALID?
703
NO
MOBILE COMM. PLATFORM DENIES TRANSACTION REQUEST
704
YES
MOBILE COMM. PLATFORM SENDS A BILLING EVENT TRIGGER ASSOCIATED WITH THE CUSTOMER ID CODE TO AN EXTERNAL BILLING MECHANISM FOR THE TRANSACTION AMOUNT
705
END

FIG. 7



See Figure 9

Figure 8

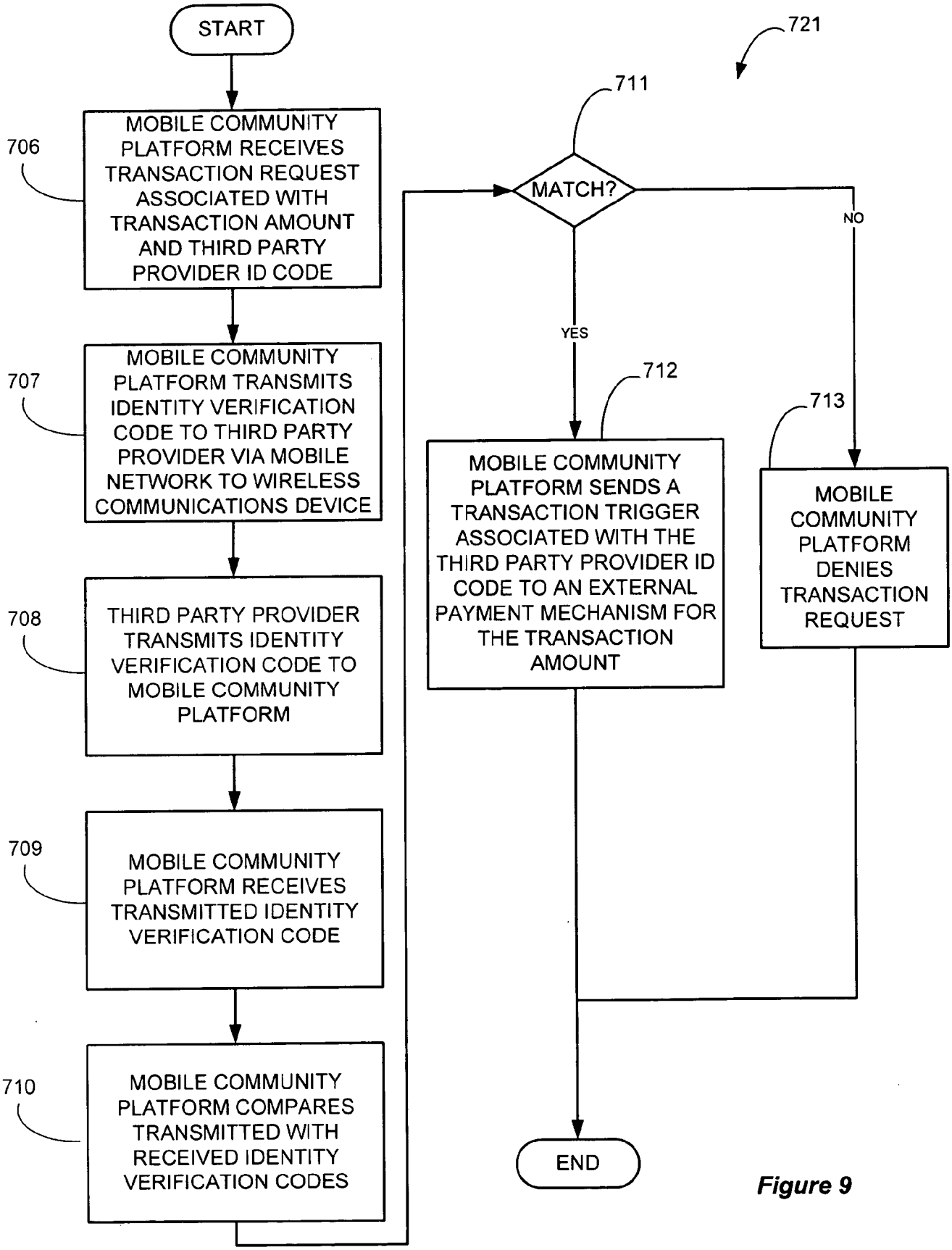

START
706
MOBILE COMMUNITY PLATFORM RECEIVES TRANSACTION REQUEST ASSOCIATED WITH TRANSACTION AMOUNT AND THIRD PARTY PROVIDER ID CODE
707
MOBILE COMMUNITY PLATFORM TRANSMITS IDENTITY VERIFICATION CODE TO THIRD PARTY PROVIDER VIA MOBILE NETWORK TO WIRELESS COMMUNICATIONS DEVICE
708
THIRD PARTY PROVIDER TRANSMITS IDENTITY VERIFICATION CODE TO MOBILE COMMUNITY PLATFORM
709
MOBILE COMMUNITY PLATFORM RECEIVES TRANSMITTED IDENTITY VERIFICATION CODE
710
MOBILE COMMUNITY PLATFORM COMPARES TRANSMITTED WITH RECEIVED IDENTITY VERIFICATION CODES
721
711
MATCH?
YES
NO
712
MOBILE COMMUNITY PLATFORM SENDS A TRANSACTION TRIGGER ASSOCIATED WITH THE THIRD PARTY PROVIDER ID CODE TO AN EXTERNAL PAYMENT MECHANISM FOR THE TRANSACTION AMOUNT
713
MOBILE COMMUNITY PLATFORM DENIES TRANSACTION REQUEST
END

Figure 9

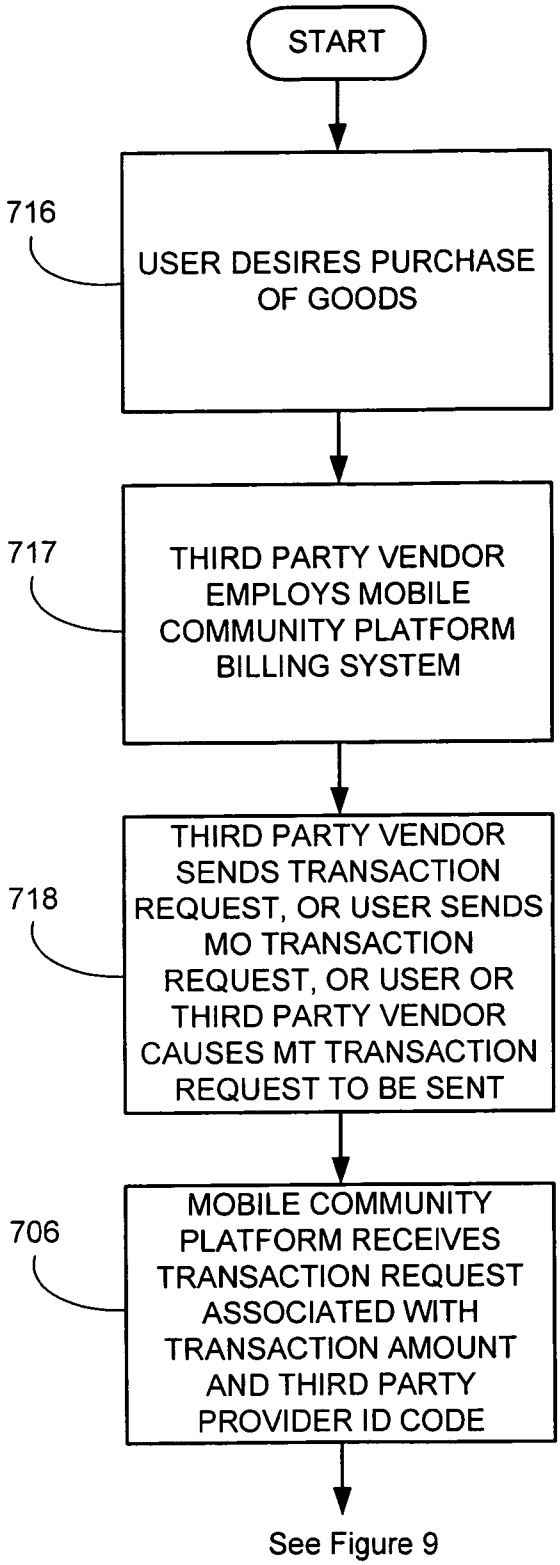

START
716
USER DESIRES PURCHASE OF GOODS
717
THIRD PARTY VENDOR EMPLOYS MOBILE COMMUNITY PLATFORM BILLING SYSTEM
718
THIRD PARTY VENDOR SENDS TRANSACTION REQUEST, OR USER SENDS MO TRANSACTION REQUEST, OR USER OR THIRD PARTY VENDOR CAUSES MT TRANSACTION REQUEST TO BE SENT
706
MOBILE COMMUNITY PLATFORM RECEIVES TRANSACTION REQUEST ASSOCIATED WITH TRANSACTION AMOUNT AND THIRD PARTY PROVIDER ID CODE
See Figure 9

Figure 10

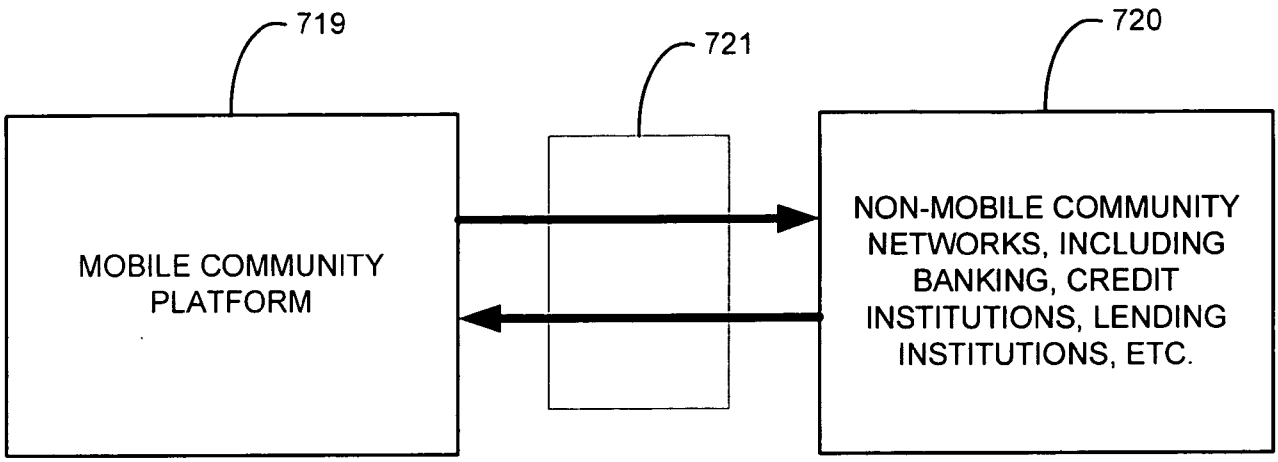

719
721
720
MOBILE COMMUNITY PLATFORM
NON-MOBILE COMMUNITY NETWORKS, INCLUDING BANKING, CREDIT INSTITUTIONS, LENDING INSTITUTIONS, ETC.

Figure 11