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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 August 2014 (21.08.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/124492 A1

(51) International Patent Classification:
G06Q 20/40 (2012.01)

(21) International Application Number:
PCT/AU2014/000121

(22) International Filing Date:
13 February 2014 (13.02.2014)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2013900513 14 February 2013 (14.02.2013) AU

(71) Applicant: **MICHAEL HILL GROUP SERVICES PTY LTD** [AU/AU]; c/-Fisher Adams Kelly, Level 29, 12 Creek Street, Brisbane, Queensland 4000 (AU).

(72) Inventor: **MCKINNON, Ross**; c/- Fisher Adams Kelly, Level 29, 12 Creek Street, Brisbane, Queensland 4000 (AU).

(74) Agent: **FISHER ADAMS KELLY**; Level 29, 12 Creek Street, Brisbane, Queensland 4001 (AU).

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

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

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

(54) Title: PAYMENT SYSTEM AND METHOD

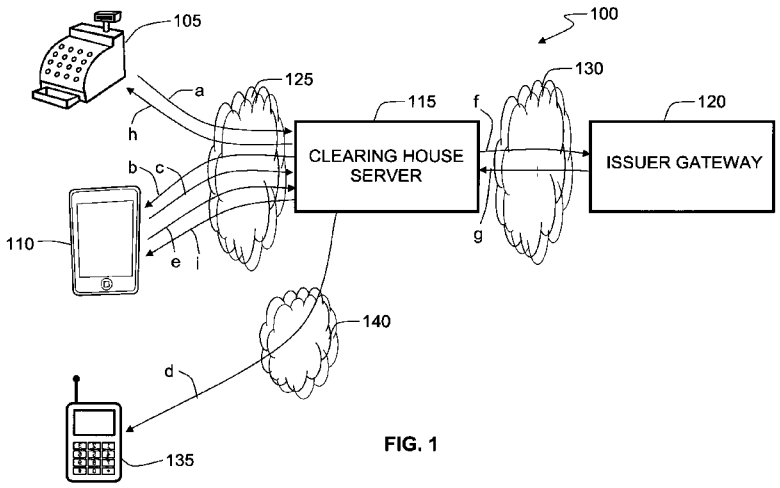

FIG. 1

(57) Abstract: A payment method enables improved payment security. The payment method includes receiving, from a merchant, a request for payment, the request for payment including a transaction amount and customer details. In response a first merchant payment threshold is retrieved from a data store, the first merchant payment threshold corresponding to a threshold transaction amount associated with the merchant and a first security measure. If the transaction amount is then determined to be greater than the first merchant payment threshold, a first security measure in the form of a one-time identifier associated with the transaction is generated by a processor. The one-time identifier is then sent to a customer mobile phone. On the data interface, security information associated with the one-time identifier is then received, and the transaction is approved based upon at least the security information and the customer details.

WO 2014/124492 A1

TITLE

PAYMENT SYSTEM AND METHOD

FIELD OF THE INVENTION

The present invention relates to financial transactions. In particular, although not exclusively, the invention relates to a payment system and method.

BACKGROUND TO THE INVENTION

Payment for goods and services has traditionally involved a transfer of a physical item of value between parties, in return for the goods and services. Today, such transactions are still common in the form of cash transactions, especially for small, fast payments.

A problem with cash is that it can easily be lost or stolen and is then very difficult to trace and/or recover. Furthermore, cash is costly to securely print and manage, and becomes dirty and damaged with use.

Cashless payment methods have thus become more popular, including credit and debit card payments. In the case of credit cards, a bank will typically grant a customer a revolving line of credit, which is available to merchants when the customer makes purchases. The customer can then pay a credit card bill, long after the merchant has received money relating to the transaction.

Credit and debit card payment is popular among merchants, as the merchant does not take a risk associated with the customer not paying off a line of credit, or risk the delayed payment associated with maintaining a line of credit. Furthermore, a theft risk is reduced when lower volumes of cash are handled by the merchant.

However, a problem with such credit card payment systems is that payment involves multiple entities, and includes multiple steps, each of which is associated with a risk, and thus fees are in total generally high. In particular, a payment is first authorized by a card issuer, and at a later time final transaction data is sent from an acquirer to the issuer for

settlement, where an actual exchange of funds takes place. These steps are performed using a payment gateway or system, further complicating the transaction.

Furthermore, credit card payment systems of the prior art are prone to fraudulent use, wherein a stolen or duplicate credit card is used without the owner's consent. Such fraudulent use ultimately results in higher costs for consumers and merchants.

Accordingly, there is a need for an improved payment system and method.

OBJECT OF THE INVENTION

It is an object of some embodiments of the present invention to provide consumers with improvements and advantages over the above described prior art, and/or overcome and alleviate one or more of the above described disadvantages of the prior art, and/or provide a useful commercial choice.

SUMMARY OF THE INVENTION

According to one aspect, the invention resides in a payment method, the payment method including:

receiving, from a merchant, a request for payment, the request for payment including a transaction amount and customer details;

retrieving, from a data store, a first merchant payment threshold, the first merchant payment threshold corresponding to a threshold transaction amount associated with the merchant and a first security measure;

determining that the transaction amount is greater than the first merchant payment threshold;

generating, by a processor, a first security measure in the form of a one-time identifier associated with the transaction;

sending the one-time identifier to a customer mobile phone;

receiving, on the data interface, security information associated with the one-time identifier; and

approving the transaction based upon at least the security information and the customer details.

Preferably, the method further comprises retrieving details of the customer mobile phone from a data store.

Preferably, approving the transaction further comprises obtaining authorisation of the transaction from an issuer associated with the customer details.

Preferably, the method further comprises:

retrieving, from a data store, a second merchant payment threshold, the second merchant payment threshold corresponding to a threshold transaction amount associated with the merchant and a second security measure;

determining that the transaction amount is greater than the second merchant payment threshold; and

receiving, on the data interface, further security information associated with the second security measure and the request for payment;

wherein approving the transaction is further based upon the further security information.

Preferably, the further security information associated with the second security measure comprises an image of the customer captured by the merchant.

Preferably, approving the transaction comprises automatically comparing the image of the customer with an image associated with the customer details.

Preferably, the method further comprises:

receiving, on the data interface and from the merchant, the first merchant payment threshold;

storing, on the data store, the first merchant payment threshold; and

associating, by a processor, the first merchant payment threshold with the merchant and the first security measure.

Preferably, the one-time identifier is a character string code or a security question having a clearly defined answer.

Preferably, the one-time identifier is a server-generated security token.

According to another aspect, the invention resides in a payment system, accessible by a plurality of merchants and a plurality of customers, the payment system including:

a data store, the data store including a plurality of merchant managed rules, each merchant managed rule associated with a merchant and associated with a fraud risk;

a server including:

a processor;

a data interface coupled to the processor; and

a memory coupled to the processor, the memory including instruction code executable by the processor for:

receiving, on the data interface and from a merchant, a request for payment, the request for payment including a transaction amount and customer details;

retrieving, from the data store, a first merchant payment threshold, the first merchant payment threshold corresponding to a threshold transaction amount associated with the merchant and a first security measure;

determining that the transaction amount is greater than the first merchant payment threshold;

generating, by a processor, a first security measure in the form of a one-time identifier associated with the transaction;

sending the one-time identifier to a customer mobile phone, for entry by a customer into a merchant device;

receiving, on the data interface, security information associated with the one-time identifier; and

approving the transaction, by the processer, based upon at least the security information and the customer details.

BRIEF DESCRIPTION OF THE DRAWINGS

To assist in understanding the invention and to enable a person skilled in the art to put the invention into practical effect, preferred embodiments of the invention are described below by way of example only with reference to the accompanying drawings, in which:

FIG. 1 illustrates a payment system, according to an embodiment of the present invention;

FIG. 2 illustrates a payment system, similar to the payment system of FIG. 1, but without a dedicated point-of-sale device, according to an embodiment of the present invention;

FIG. 3 illustrates a payment system, similar to the payment systems of FIG. 1 and FIG. 2, adapted for e-commerce, according to an embodiment of the present invention;

FIG. 4 illustrates a mobile transaction device, according to an embodiment of the present invention;

FIG. 5 illustrates a screenshot of a primary purchase approval screen, according to an embodiment of the present invention;

FIG. 6 illustrates a screenshot of a secondary purchase approval screen, according to an embodiment of the present invention;

FIG. 7 illustrates a screenshot of a purchase approval screen, according to an embodiment of the present invention;

FIG. 8 illustrates a payment system, according to an embodiment of the present invention;

FIG. 9 diagrammatically illustrates a computing device, according to an embodiment of the present invention; and

FIG. 10 illustrates a payment method, according to an embodiment of the present invention.

Those skilled in the art will appreciate that minor deviations from the layout of components as illustrated in the drawings will not detract

from the proper functioning of the disclosed embodiments of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

Embodiments of the present invention comprise payment systems and methods. Elements of the invention are illustrated in concise outline form in the drawings, showing only those specific details that are necessary to the understanding of the embodiments of the present invention, but so as not to clutter the disclosure with excessive detail that will be obvious to those of ordinary skill in the art in light of the present description.

In this patent specification, adjectives such as first and second, left and right, front and back, top and bottom, etc., are used solely to define one element or method step from another element or method step without necessarily requiring a specific relative position or sequence that is described by the adjectives. Words such as "comprises" or "includes" are not used to define an exclusive set of elements or method steps. Rather, such words merely define a minimum set of elements or method steps included in a particular embodiment of the present invention.

According to one aspect, the invention resides in a payment method, the payment method including: receiving, from a merchant, a request for payment, the request for payment including a transaction amount and customer details; retrieving, from a data store, a first merchant payment threshold, the first merchant payment threshold corresponding to a threshold transaction amount associated with the merchant and a first security measure; determining that the transaction amount is greater than the first merchant payment threshold; generating, by a processor, a first security measure in the form of a one-time identifier associated with the transaction; sending the one-time identifier to a customer mobile phone, for entry by a customer into a merchant device; receiving, on the data interface, security information associated with the

one-time identifier; and approving the transaction based upon at least the security information and the customer details.

Advantages of some embodiments of the present invention include an ability to provide improved payment security, which can in turn reduce cost relating to managing payments. Fraud management is merchant based, and each merchant can manage a risk they are willing to take in a transaction, thus preventing excessive fees by third parties having to cover these risks without specific knowledge of the industry in which the merchant operates, or the merchant's fraud management practices.

By using facial images from a customer account, text messaging of one-time-passwords to a customer telephone, and/or server based facial recognition of customers, a risk of fraud can be greatly minimised by the merchant.

Additionally, certain embodiments involve 'bidding' among issuers, thus ensuring that consumers receive low interest rates and/or better conditions associated with a transaction.

FIG. 1 illustrates a payment system 100, according to an embodiment of the present invention. The payment system 100 is accessible by a plurality of merchants and for a plurality of customers, and enables fast and secure transactions.

The payment system 100 includes a point-of-sale device 105, and a mobile transaction device 110, which are typically located at a shop of a merchant. The point-of-sale device 105 and the mobile transaction device 110 are used by the merchant to initiate, authenticate and complete payment transactions.

The payment system 100 further includes a clearing house server 115 and an issuer gateway 120. The clearing house server 115 is in communication with the point-of-sale device 105 and the mobile transaction device 110 by a data communication network 125, such as the Internet. The clearing house server 115 manages funds transfers.

The issuer gateway 120 is connected to the clearing house server 115 by a data communication network 130, which can be similar or

identical to the data communication network 125. The issuer gateway 120 corresponds to a card issuer of the customers, and includes details of the customers' accounts.

The payment system 100 is in communication with a customer mobile phone 135 by a mobile network 140, such as a Global System for Mobile Communications (GSM) telecommunication network. The customer mobile phone 135 is used for added security, as it is unlikely that a fraudster will obtain access to both a customer's credit card, and their mobile phone.

In use, a transaction is initiated at the point-of-sale device 105. Details of the transaction, including a transaction amount, are sent from the point-of-sale device 105 to the clearing house server 115, as illustrated by message 'a'.

The clearing house server 115 then sends transaction details to the mobile transaction device 110, as illustrated by message 'b', which are then presented on the mobile transaction device 110, for approval by the customer.

The customer then taps a customer card against the mobile transaction device 110 to approve the purchase, upon which details of the customer card are captured and sent to the clearing house server 115, as illustrated by message 'c'. As will be readily understood by the skilled addressee, the customer card and the mobile transaction device 110 can, for example, transfer data by near field communication (NFC) and radio-frequency identification (RFID), by scanning an image or barcode on the card, or by reading a magnetic strip of the card.

The clearing house server 115 processes the details of the transaction to determine if further authentication is required. In this case, the further authentication is achieved using security information in the form of a one-time identifier. For example, such a one-time identifier can be a character string code, a security question having a clearly defined answer, or another form of server-generated security token. The clearing house server 115 processes the details of the customer card, and retrieves

details of the customer mobile phone 135. This can be achieved using a database including details of customer cards and customer mobile phone numbers. The one-time identifier is generated and sent to the customer mobile phone 135, as illustrated by message 'd'.

The customer, upon receipt of the one-time identifier on the customer mobile phone 135, enters the one-time identifier or data associated with the one-time identifier, such as an answer to a security question, onto the mobile transaction device 110. The one-time identifier is then sent from the mobile transaction device 110 to the clearing house server 115, as illustrated by message 'e'.

The one-time identifier is then verified by the clearing house server 115. After verification of the one-time identifier, transaction details are sent from the clearing house server 115 to the issuer gateway 120, as illustrated by message 'f'. The issuer gateway 120 processes the transaction details and sends a transaction approval to the clearing house server 115, as illustrated by message 'g'.

The clearing house server 115 then finalises the transaction, and sends approval confirmations to the point-of-sale device 105 and the mobile transaction device 110.

As will be understood by the skilled addressee, FIG. 1 illustrates a valid transaction where all approval, authentication and verification has been successful. If, for example, an authentication, verification or approval step is not successful, the transaction is stopped, and error messages are sent to the point-of-sale device 105 and the mobile transaction device 110 respectively.

According to certain embodiments, an image of the customer is retrieved by the clearing house server 115 and transmitted to the mobile transaction device 110 as part of the approval confirmation message. The merchant can then compare the image of the customer to the actual customer. The merchant is able to cancel and reverse the transaction if the customer does not match the image provided by the clearing house server.

FIG. 2 illustrates a payment system 200, similar to the payment system 100, but without a dedicated point-of-sale device. The payment system 200 is particularly suited for on-site services, such as home electrical services, where portability is desirable. Similarly, the payment system 200 is suited to new shops, where there is not a need to integrate with existing point-of-sale equipment.

The payment system 200 includes a mobile point-of-sale device 210, which is similar to a combination of the point-of-sale device 105 and mobile transaction device 110 of FIG. 1. The mobile point-of-sale device 210 is connected to a clearing house server 215, which is similar to the clearing house server 115 of FIG. 1.

In use, a transaction is initiated at the mobile point-of-sale device 210. As part of initiating the transaction, the customer taps a customer card against the mobile point-of-sale device 210, upon which details of the customer card are read.

Details of the transaction, including a transaction amount and the details of the customer card, are sent from the mobile point-of-sale device 210 to the clearing house server 215, as illustrated by message 'a1'.

The clearing house server 215 processes the details of the transaction to determine if further authentication, in the form of a one-time identifier, is required. The clearing house server 215 then sends details of the further authentication required to the mobile point-of-sale device 210, as illustrated by message 'b1'. At approximately the same time, the clearing house server 215 automatically generates the one-time identifier, processes the details of the customer card, retrieves details of the customer mobile phone 135, and sends the one-time identifier to the customer mobile phone 135, as illustrated by message 'c1'.

The mobile point-of-sale device 210 displays a graphical user interface enabling the customer to enter the one-time-pin into the mobile point-of-sale device 210. Upon receipt of the one-time identifier, the customer enters the one-time identifier onto the mobile point-of-sale device 210 using, for example, a virtual keypad. The one-time identifier is

then sent from the mobile point-of-sale device 210 to the clearing house server 215, as illustrated by message 'd1'.

The one-time identifier is then verified by the clearing house server 215, after which transaction details are sent from the clearing house server 215 to the issuer gateway 120, as illustrated by message 'e1'. The issuer gateway 120 processes the transaction details returns a transaction approval to the clearing house server 215, as illustrated by message 'f1'.

The clearing house server 215 then finalises the transaction, and sends approval confirmation to the mobile point-of-sale device 210, as illustrated by message 'g1'. As discussed earlier, the approval confirmation can include an image of the customer, for verification by the merchant.

FIG. 3 illustrates a payment system 300, similar to the payment systems 100, 200 of FIG. 1 and FIG. 2, adapted for e-commerce. The payment system 300 is particularly suited for online sales and bookings, and/or when payment is made online.

The payment system 300 includes an e-commerce server 305, which provides an e-commerce web page to a plurality of customer computers 310. The e-commerce web page can, for example, comprise a traditional e-commerce store, including goods available for purchase using a shopping cart, or an online auction site. The payment system 300 also includes a clearing house server 315, similar to the clearing house server 115 of FIG. 1.

In use, a transaction is initiated at the customer computer 310, by entering details of a customer card into a website provided by the e-commerce server 305. The details of the customer card can include, for example, a card number, and an expiry date.

Details of the transaction, including the details of the customer card, are sent from the customer computer 310 to the e-commerce server 305, as illustrated by message 'a2'.

The e-commerce server 305 then sends details of the transaction, including the details of the customer card and a transaction amount, to the clearing house server 315, as illustrated by message 'b2'.

The clearing house server 315 processes the details of the transaction to determine the details of the customer mobile phone 135, automatically generates a one-time identifier, and sends the one-time identifier to the customer mobile phone 135, as illustrated by message 'c2'. As there is no direct contact between a merchant and the customer when a transaction is performed online, the one-time identifier form of verification is used for all such transactions.

The customer computer 310 displays a graphical user interface enabling the customer to enter the one-time-pin into the device. Upon receipt of the one-time identifier, the customer enters the one-time identifier into the customer computer 310, upon which the one-time identifier is sent to the e-commerce server 305, as illustrated by message 'd2'.

The e-commerce server 305 then sends the one-time identifier to the clearing house server 315, as illustrated by message 'e2'.

The one-time identifier is then verified by the clearing house server 315, after which transaction details are sent from the clearing house server 315 to the issuer gateway 120, as illustrated by message 'f2'. The issuer gateway 120 processes the transaction details returns a transaction approval to the clearing house server 315, as illustrated by message 'g2'.

The clearing house server 315 then finalises the transaction, and sends approval confirmation to the e-commerce server 305, as illustrated by message 'h2'. The e-commerce server 305 can then finalise the transaction, and can, for example, send an email confirmation to the customer.

FIG. 4 illustrates a mobile transaction device 400, according to an embodiment of the present invention. The mobile transaction device 400 can be similar or identical to the mobile transaction device 105 of FIG. 1.

Alternatively, the mobile transaction device 400 can be similar or identical to the mobile point-of-sale device 210 of FIG. 2

The mobile transaction device 400 includes a capacitive touch screen 405, a user interaction button 410, and a camera 415, all attached to a body 420. The body 420 is substantially rectangular in shape, and is sized to enable portable operation.

The merchant and customer interact with the mobile transaction device 400 primarily through the capacitive touch screen 405, where icons, buttons and other selectable elements are displayed, as discussed further below. The user interaction button 410 can, however, be user for certain interaction in the system, such as navigating between applications ('apps') on the mobile transaction device 400.

The mobile transaction device 400 has a processor and memory (not shown), the memory including program code executable by the processor. The program code can comprise operating system code, such as Android operating system code, by Google Inc. of Mountain View, California.

The mobile transaction device 400 further includes a wireless network adapter (not shown), which enables the mobile transaction device 400 to communicate with other devices and entities. The wireless adapter can communicate with a local base, such as a particular wireless hotspot, or more advantageously connect to a cellular network.

Furthermore, the camera 415 enables the mobile transaction device 400 to capture images of the user, for example the customer. As discussed above, this enables a user to capture an image of a card of the customer, such as a barcode, Quick Response (QR) code printed on the card, or to capture an image of the customer for security reasons.

FIG. 5 illustrates a screenshot 500 of a primary purchase approval screen, according to an embodiment of the present invention.

The primary purchase screen is typically the first screen that a customer will see after choosing to purchase an item. The primary purchase screen includes a merchant logo 505, which is customisable by

the merchant. This will typically comprise a general trade mark of the merchant, but can comprise any image.

The primary purchase screen further includes a purchase total 510, which corresponds to an amount that the merchant is requesting from the customer in payment. The purchase total 510 does not need to correspond directly to a purchase amount of an item or service, as vouchers, cash or other payment forms can be used for part payment.

Finally, the primary purchase screen includes purchase approval instructions 515, which indicate that the customer should tap their card against the device. As will be readily understood by the skilled addressee, purchase approval instructions 515 are configured specifically for NFC based card communications, however, the purchase approval instructions 515 can be modified to suit any purchase approval method, including scanning a card using other means, and entering card details manually.

After the customer taps the card against the device, details of the purchase and card are sent to a server, such as a clearing house server, for processing, as discussed above.

FIG. 6 illustrates a screenshot 600 of a secondary purchase approval screen, according to an embodiment of the present invention. The secondary purchase approval screen can be used when, for example, a threshold purchase amount is reached, in order to provide extra security.

The secondary purchase approval screen includes a merchant logo 605, preferably similar or identical to the merchant logo 505 of FIG. 5. The secondary purchase screen also includes a purchase total 610, similar to the purchase total 510 of FIG. 5.

The secondary purchase approval screen further includes secondary purchase approval instructions 615, a one-time-pin entry field 620, and a confirmation button 625. The secondary purchase approval instructions 615 indicate to the customer that the customer should enter their one-time-pin into the device. As discussed earlier, the one-time-pin can be sent to the customers mobile phone by text messaging.

The customer can, for example, enter the one-time-pin into the one-time-pin entry field 620 using a data entry apparatus, such as a keyboard, associated with the device, or by using a virtual keyboard and a touch screen. Upon selection of the confirmation button 625, the one-time-pin is sent to the server for verification and approval of the purchase, as discussed above.

FIG. 7 illustrates a screenshot 700 of a purchase approval screen, according to an embodiment of the present invention. The purchase approval screen is displayed to the merchant upon approval of the purchase.

The purchase approval screen includes a merchant logo 705, similar to the merchant logo 505 of FIG. 5, and a purchase approval indication 710. As will be readily understood by the skilled address, a purchase denial message (not shown) can be displayed in place of the purchase approval indication 710 if the purchase is not approved.

Furthermore, the purchase approval screen includes purchase approval instructions 715, an accountholder photo 720, an approve transaction button 725 and a cancel transaction button 730. The accountholder photo 720 has been retrieved from a database, and corresponds to an official image of the accountholder.

The merchant compares the customer with the accountholder photo 720, for security purposes. This prevents use of a lost or stolen card, even if access to the accountholders telephone is available.

If the customer matches the accountholder photo 720, the merchant selects the approve transaction button 725. The transaction is then finalised. Alternatively, a cancel transaction button 730 is selected, upon which the transaction is cancelled.

FIG. 8 illustrates a payment system 800, according to an embodiment of the present invention. The payment system 800 is similar to the payment system 200 of FIG. 2, but with the addition of several issuer gateways 820.

The payment system 800 includes the mobile point-of-sale device 210, which is connected to a clearing house server 815, which is similar to the clearing house server 215 of FIG. 2.

In use, a transaction is initiated at the mobile point-of-sale device 210, as discussed earlier, and the mobile point-of-sale device 210 interacts with the clearing house server 815 in the same way as illustrated with reference to FIG. 2 and in particular as illustrated by messages 'a1', 'b1', 'g1' and 'd1'.

After the one-time identifier is verified by the clearing house server 815, authorisation requests are sent from the clearing house server 815 to the issuer gateways 820, as illustrated by messages 'x1'-'xn'. The issuer gateways 820 process the authorisation requests and return transaction approval information, as illustrated by messages 'y1'-'yn'.

The transaction approval information includes, in addition to information regarding whether or not the transaction has been approved, details of conditions associated with the transaction, such as interest rates, payment terms and/or other conditions.

The clearing house server 815 then selects an issuer based upon the transaction approval information provided by each of the issuer gateways 820. According to certain embodiments, the issuer is selected based upon a lowest interest rate offered, a highest reward, or most favourable conditions otherwise.

The approval confirmation, which is sent to the mobile point-of-sale device 210, can include details of the selected issuer as well as an image of the customer.

A settlement request can later be initiated with the selected issuer, in order to initiate settlement with the merchant.

FIG. 9 diagrammatically illustrates a computing device 900, according to an embodiment of the present invention. The mobile transaction device 110, the clearing house server 115, 215, 315, 815, the mobile point-of-sale device 210, the e-commerce server 305, and the

mobile transaction device 400 can be similar or identical to the computing device 900.

The computing device 900 includes a central processor 902, a system memory 904 and a system bus 906 that couples various system components, including coupling the system memory 904 to the central processor 902. The system bus 906 may be any of several types of bus structures including a memory bus or memory controller, a peripheral bus, and a local bus using any of a variety of bus architectures. The structure of system memory 904 is well known to those skilled in the art and may include a basic input/output system (BIOS) stored in a read only memory (ROM) and one or more program modules such as operating systems, application programs and program data stored in random access memory (RAM).

The computing device 900 may also include a variety of interface units and drives for reading and writing data. In particular, the computing device 900 includes a hard disk interface 908 and a removable memory interface 910, respectively coupling a hard disk drive 912 and a removable memory drive 914 to the system bus 906. Examples of removable memory drives 914 include magnetic disk drives and optical disk drives. The drives and their associated computer-readable media, such as a Digital Versatile Disc (DVD) 916 provide non-volatile storage of computer readable instructions, data structures, program modules and other data for the computer system 900. A single hard disk drive 912 and a single removable memory drive 914 are shown for illustration purposes only and with the understanding that the computing device 900 may include several similar drives. Furthermore, the computing device 900 may include drives for interfacing with other types of computer readable media.

The computing device 900 may include additional interfaces for connecting devices to the system bus 906. FIG. 9 shows a universal serial bus (USB) interface 918 which may be used to couple a device to the system bus 906. For example, an IEEE 1394 interface 920 may be used to couple additional devices to the computing device 900.

The computing device 900 can operate in a networked environment using logical connections to one or more remote computers or other devices, such as a server, a router, a network personal computer, a peer device or other common network node, a wireless telephone or wireless personal digital assistant. The computing device 900 includes a network interface 922 that couples the system bus 906 to a local area network (LAN) 924. Networking environments are commonplace in offices, enterprise-wide computer networks and home computer systems.

A wide area network (WAN), such as the Internet, can also be accessed by the computing device 900, for example via a modem unit connected to a serial port interface 926 or via the LAN 924.

It will be appreciated that the network connections shown and described are exemplary and other ways of establishing a communications link between computers can be used. The existence of any of various well-known protocols, such as TCP/IP, Frame Relay, Ethernet, FTP, HTTP and the like, is presumed, and the computing device 900 can be operated in a client-server configuration to permit a user to retrieve web pages from a web-based server. Furthermore, any of various conventional web browsers can be used to display and manipulate data on web pages.

The operation of the computing device 900 can be controlled by a variety of different program modules. Examples of program modules are routines, programs, objects, components, and data structures that perform particular tasks or implement particular abstract data types. The present invention may also be practiced with other computer system configurations, including hand-held devices, multiprocessor systems, microprocessor-based or programmable consumer electronics, network PCs, minicomputers, mainframe computers, personal digital assistants and the like. Furthermore, the invention may also be practiced in distributed computing environments where tasks are performed by remote processing devices that are linked through a communications network. In

a distributed computing environment, program modules may be located in both local and remote memory storage devices.

FIG. 10 illustrates a payment method, according to an embodiment of the present invention.

At step 1005, a request for payment is received from a merchant. The request for payment includes a transaction amount and customer details. The customer details can include, for example, details of a customer card.

At step 1010, a first merchant payment threshold is retrieved from a data store. The first merchant payment threshold corresponds to a threshold transaction amount associated with the merchant and a first additional security measure. Each merchant is able to set different payment thresholds for security measures, based upon the nature of the business the merchant operates, or the level of risk the merchant is willing to take.

For example, an address based subscription service may have a high payment threshold for security measures, as it can both be easily determined who (i.e. which address) is receiving the service, and the subscription can be cancelled if needed. Foreign exchange services, for example, may have low payment thresholds, as the cash provided in such a service is often at a relatively low profit, and is virtually untraceable after a transaction is made.

In step 1015, it is determined that the transaction amount is greater than the first merchant payment threshold. Therefore, as an added security measure, a one-time identifier is sent to a customer's mobile phone.

In step 1020, security information associated with the additional security measure and the request for payment is received on the data interface. This can, for example, comprise receiving data on a web form, or receiving a message including security information associated with the one-time identifier that was sent to the customer's mobile phone.

In step 1025, the transaction is approved based upon at least the security information and the customer details. According to certain embodiments, the transaction is approved based upon a credit authorisation.

In summary, advantages of some embodiments of the present invention include an ability to provide improved payment security, which can in turn reduce cost relating to managing the payments. Fraud management is merchant based, and each merchant can manage a risk they are willing to take in a transaction, thus preventing excessive fees by third parties having to cover these risks without specific knowledge of the industry in which the merchant operates, or the merchant's fraud management practices.

By using facial images from a customer account, text messaging of one-time-passwords to a customer telephone, and/or server based facial recognition of customers, a risk of fraud can be greatly minimised.

Certain embodiments involve 'bidding' among issuers, thus ensuring that consumers receive low interest rates and/or better conditions associated with a transaction.

The above description of various embodiments of the present invention is provided for purposes of description to one of ordinary skill in the related art. It is not intended to be exhaustive or to limit the invention to a single disclosed embodiment. As mentioned above, numerous alternatives and variations to the present invention will be apparent to those skilled in the art of the above teaching. Accordingly, while some alternative embodiments have been discussed specifically, other embodiments will be apparent or relatively easily developed by those of ordinary skill in the art. Accordingly, this patent specification is intended to embrace all alternatives, modifications and variations of the present invention that have been discussed herein, and other embodiments that fall within the spirit and scope of the above described invention.

Claims

1. A payment method, the payment method including:

receiving, from a merchant, a request for payment, the request for payment including a transaction amount and customer details;

retrieving, from a data store, a first merchant payment threshold, the first merchant payment threshold corresponding to a threshold transaction amount associated with the merchant and a first security measure;

determining that the transaction amount is greater than the first merchant payment threshold;

generating, by a processor, a first security measure in the form of a one-time identifier associated with the transaction;

sending the one-time identifier to a customer mobile phone;

receiving, on the data interface, security information associated with the one-time identifier; and

approving the transaction based upon at least the security information and the customer details.

2. The payment method of claim 1, the method further comprising retrieving details of the customer mobile phone from a data store.

3. The payment method of claim 1, wherein approving the transaction further comprises obtaining authorisation of the transaction from an issuer associated with the customer details.

4. The payment method of claim 1, the method further comprising:

retrieving, from a data store, a second merchant payment threshold, the second merchant payment threshold corresponding to a threshold transaction amount associated with the merchant and a second security measure;

determining that the transaction amount is greater than the second merchant payment threshold; and

receiving, on the data interface, further security information associated with the second security measure and the request for payment;

wherein approving the transaction is further based upon the further security information.

5. The payment method of claim 4, wherein the further security information associated with the second security measure comprises an image of the customer captured by the merchant.

6. The payment method of claim 5, wherein approving the transaction comprises automatically comparing the image of the customer with an image associated with the customer details.

7. The payment method of claim 1, the method further comprising:

receiving, on the data interface and from the merchant, the first merchant payment threshold;

storing, on the data store, the first merchant payment threshold; and

associating, by a processor, the first merchant payment threshold with the merchant and the first security measure.

8. The payment method of claim 1, wherein the one-time identifier is a character string code or a security question having a clearly defined answer

9. The payment method of claim 1, wherein the one-time identifier is a server-generated security token.

10. A payment system, accessible by a plurality of merchants and a plurality of customers, the payment system including:

a data store, the data store including a plurality of merchant managed rules, each merchant managed rule associated with a merchant and associated with a fraud risk;

a server including:

a processor;

a data interface coupled to the processor; and

a memory coupled to the processor, the memory including instruction code executable by the processor for:

receiving, on the data interface and from a merchant, a request for payment, the request for payment including a transaction amount and customer details;

retrieving, from the data store, a first merchant payment threshold, the first merchant payment threshold corresponding to a threshold transaction amount associated with the merchant and a first security measure;

determining that the transaction amount is greater than the first merchant payment threshold;

generating, by a processor, a first security measure in the form of a one-time identifier associated with the transaction;

sending the one-time identifier to a customer mobile phone;

receiving, on the data interface, security information associated with the one-time identifier; and

approving the transaction, by the processer, based upon at least the security information and the customer details.

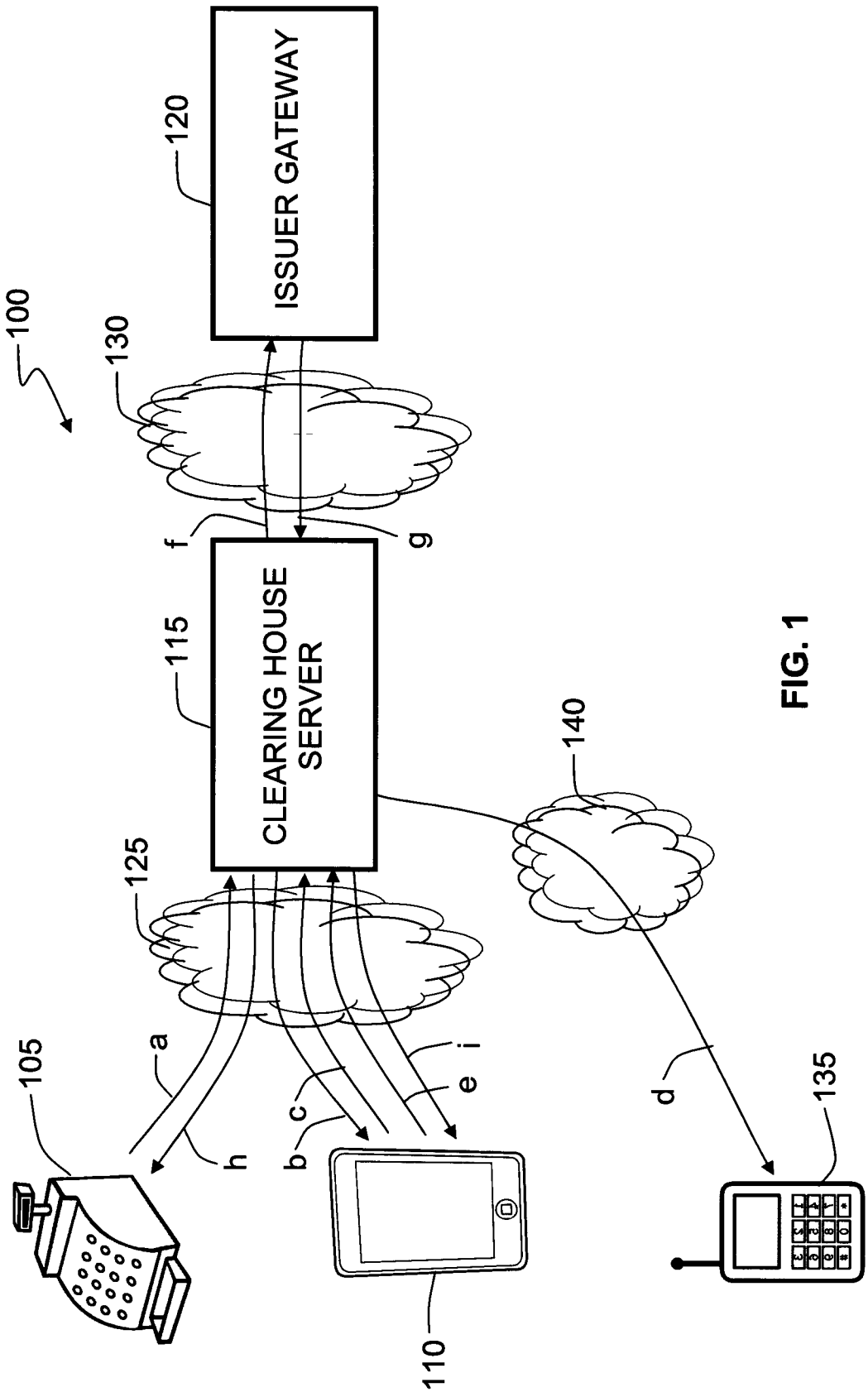
100
ISSUER GATEWAY
120
130
f
g
CLEARING HOUSE SERVER
115
140
125
105
a
h
b
c
e
i
d
135
110

FIG. 1

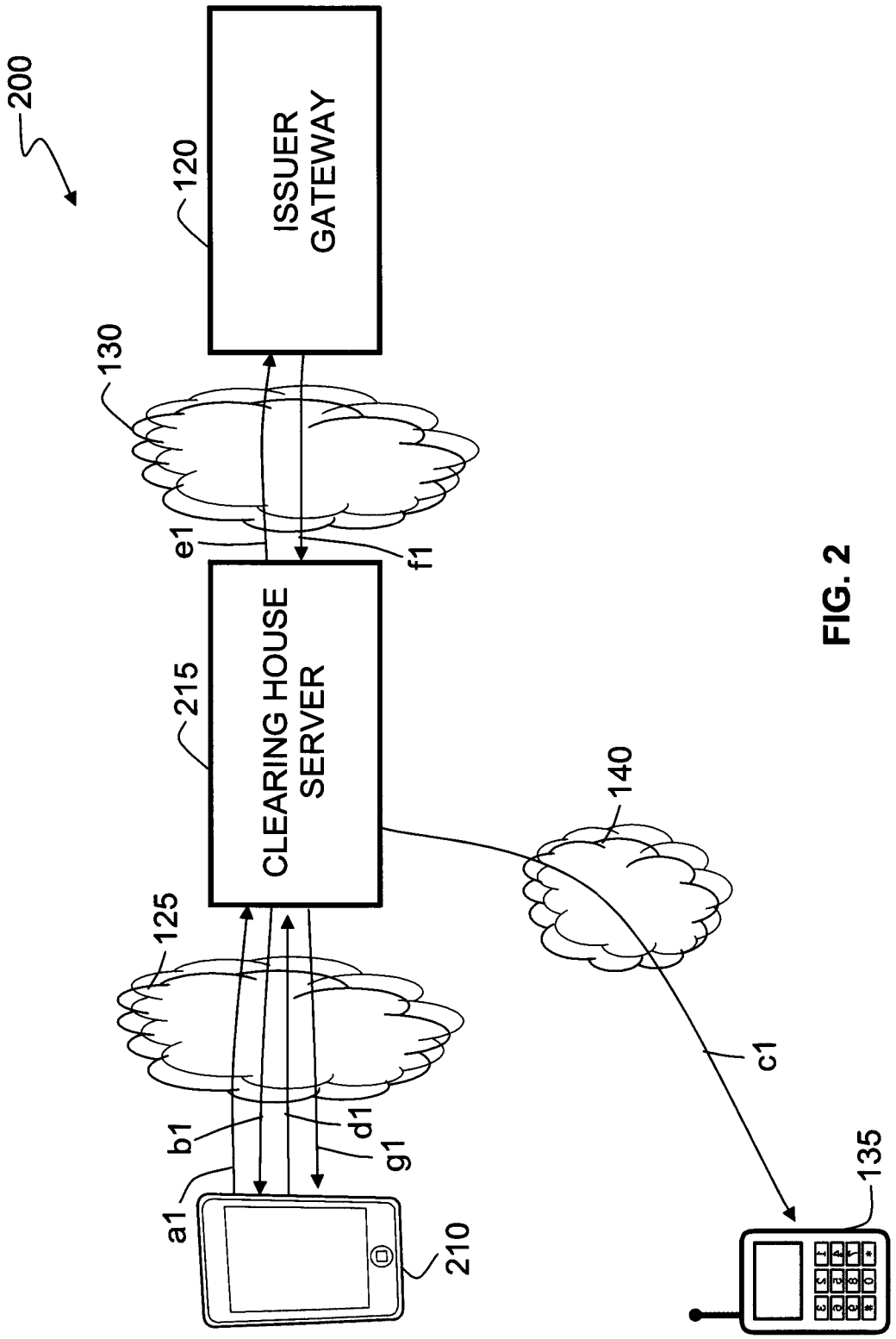
200
ISSUER GATEWAY
120
130
e1
f1
CLEARING HOUSE SERVER
215
140
125
b1
d1
g1
a1
210
c1
135

FIG. 2

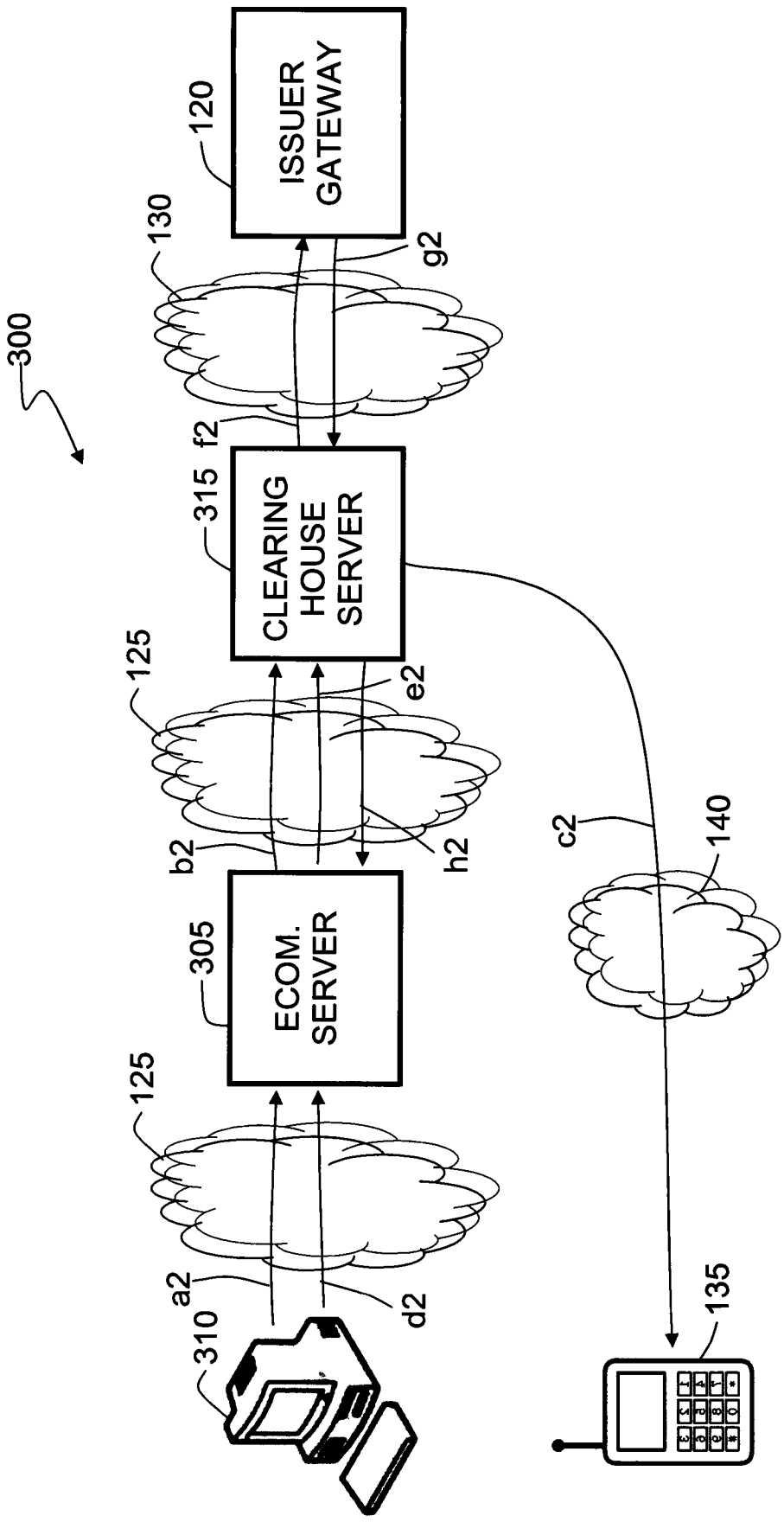
300
ISSUER GATEWAY
120
130
g2
f2
315
CLEARING HOUSE SERVER
125
e2
b2
h2
305
ECOM. SERVER
125
a2
d2
310
c2
140
135

FIG. 3

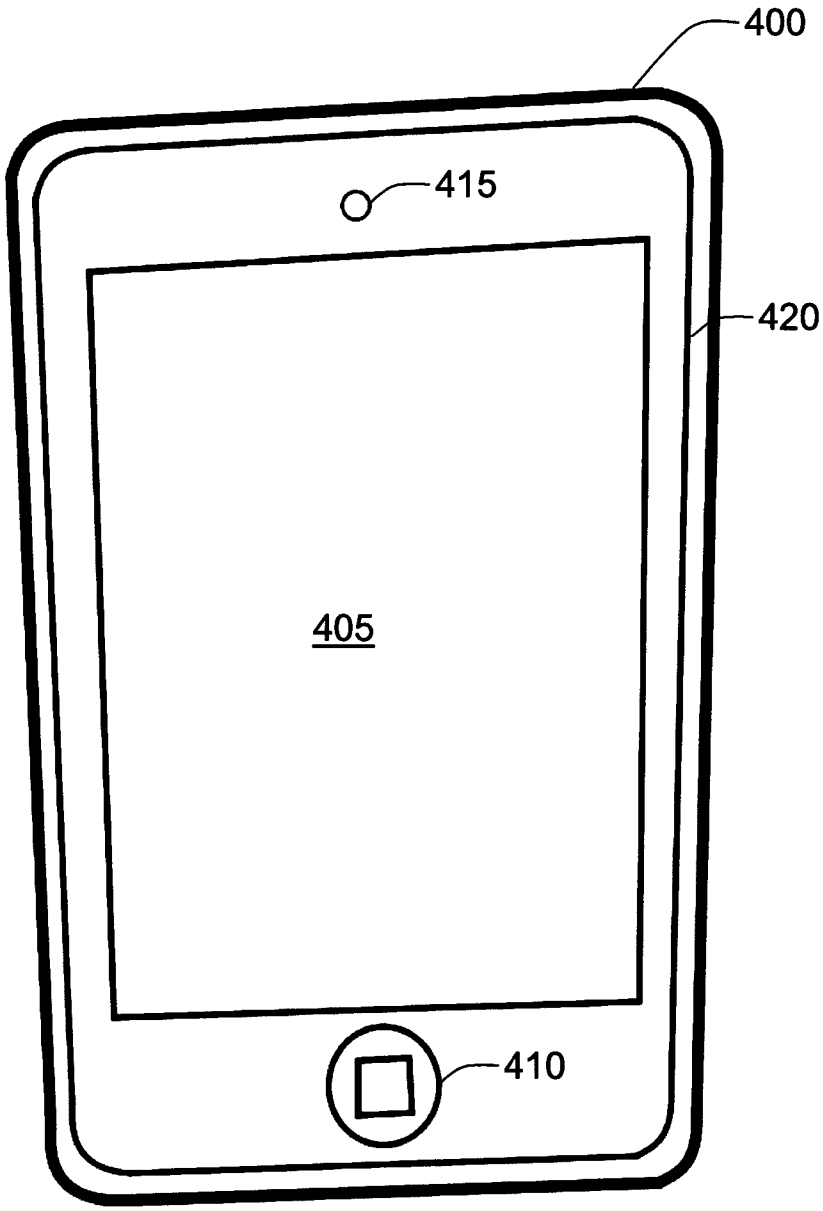

FIG. 4

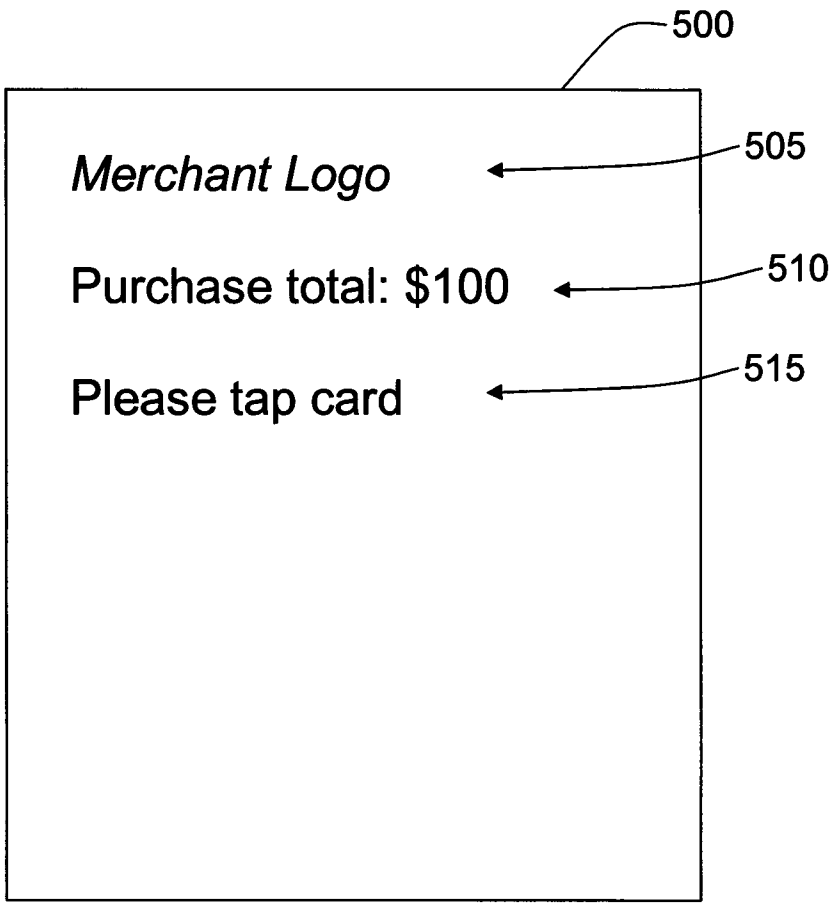
500
Merchant Logo
505
Purchase total: $100
510
Please tap card
515

FIG. 5

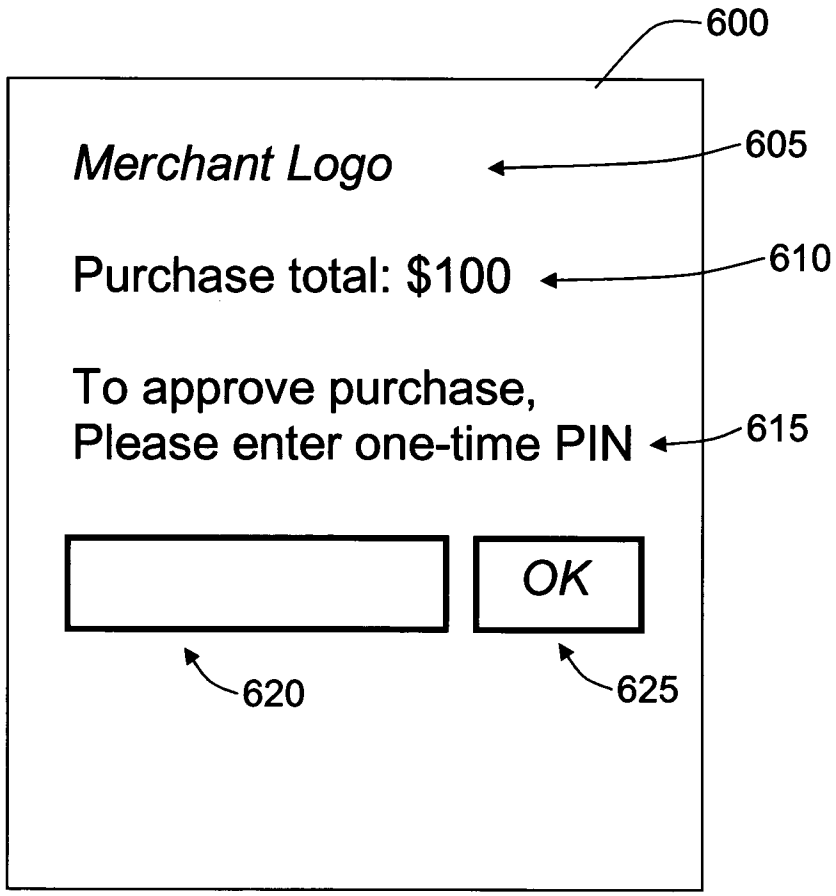
600
Merchant Logo
605
Purchase total: $100
610
To approve purchase,
Please enter one-time PIN
615
OK
620
625

FIG. 6

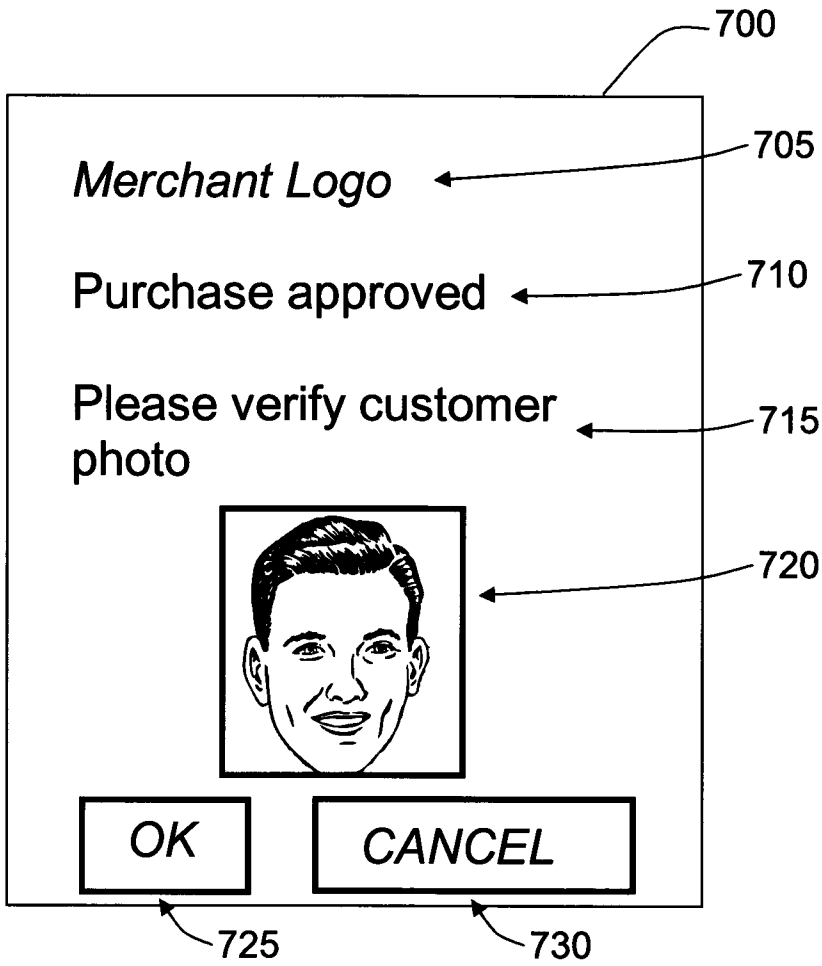
700
Merchant Logo
705
Purchase approved
710
Please verify customer photo
715
720
OK
CANCEL
725
730

FIG. 7

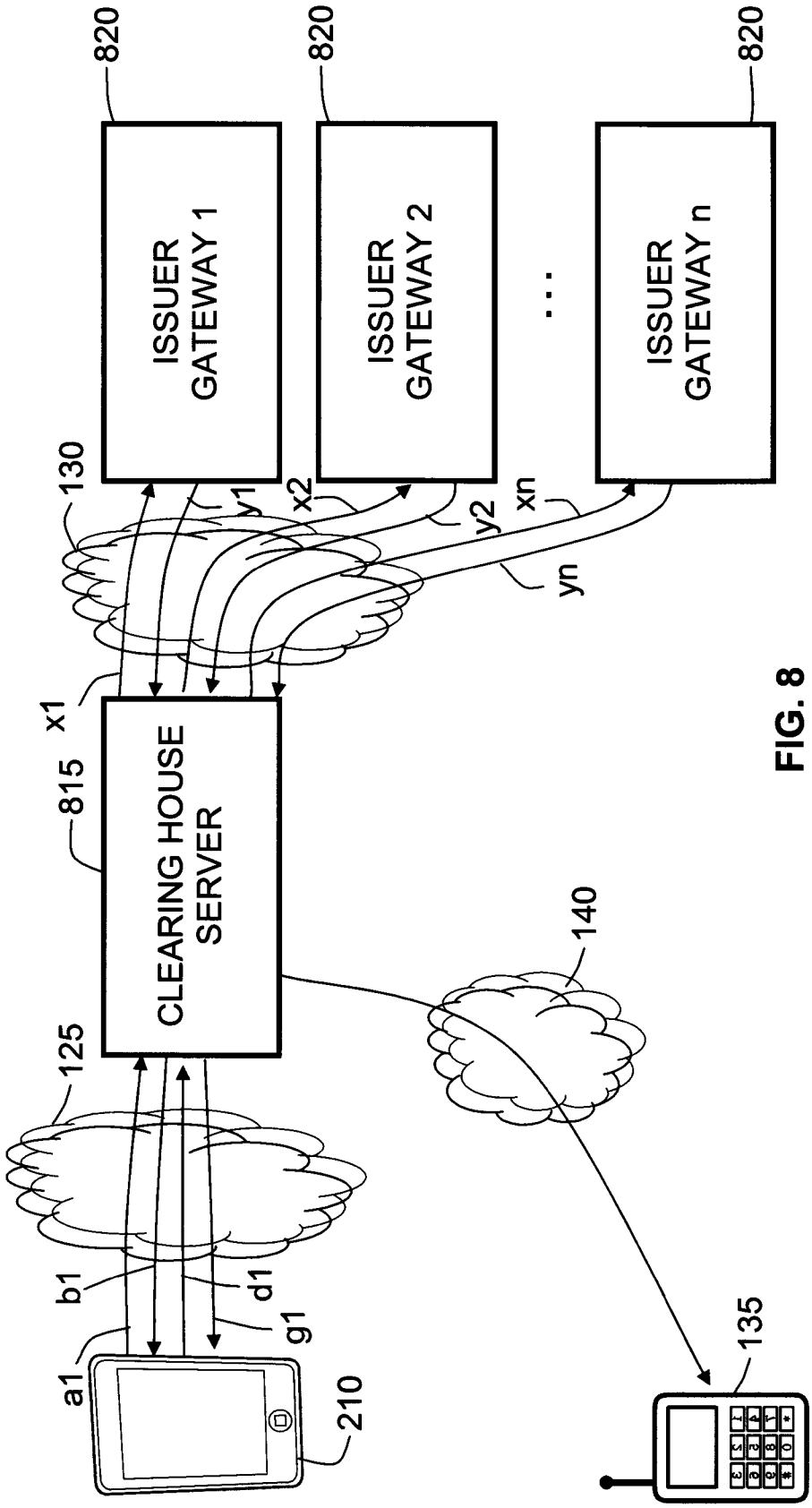
820
820
820
ISSUER GATEWAY 1
ISSUER GATEWAY 2
ISSUER GATEWAY n
130
y1
x2
y2
xn
yn
x1
815
CLEARING HOUSE SERVER
140
125
b1
d1
g1
a1
210
135

FIG. 8

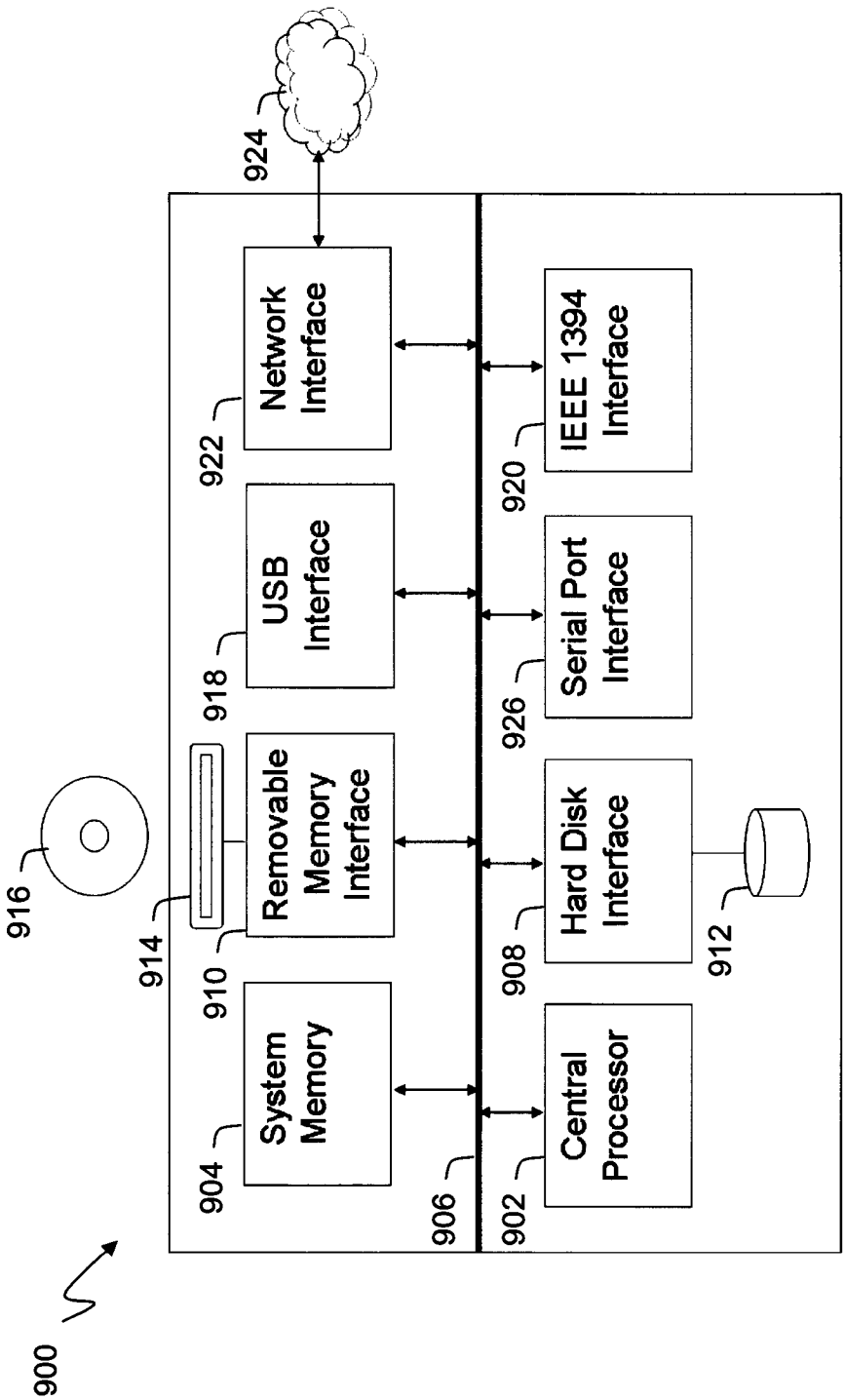
900
916
914
910
904
906
902
908
912
926
918
922
920
924
System Memory
Removable Memory Interface
USB Interface
Network Interface
Central Processor
Hard Disk Interface
Serial Port Interface
IEEE 1394 Interface

FIG. 9

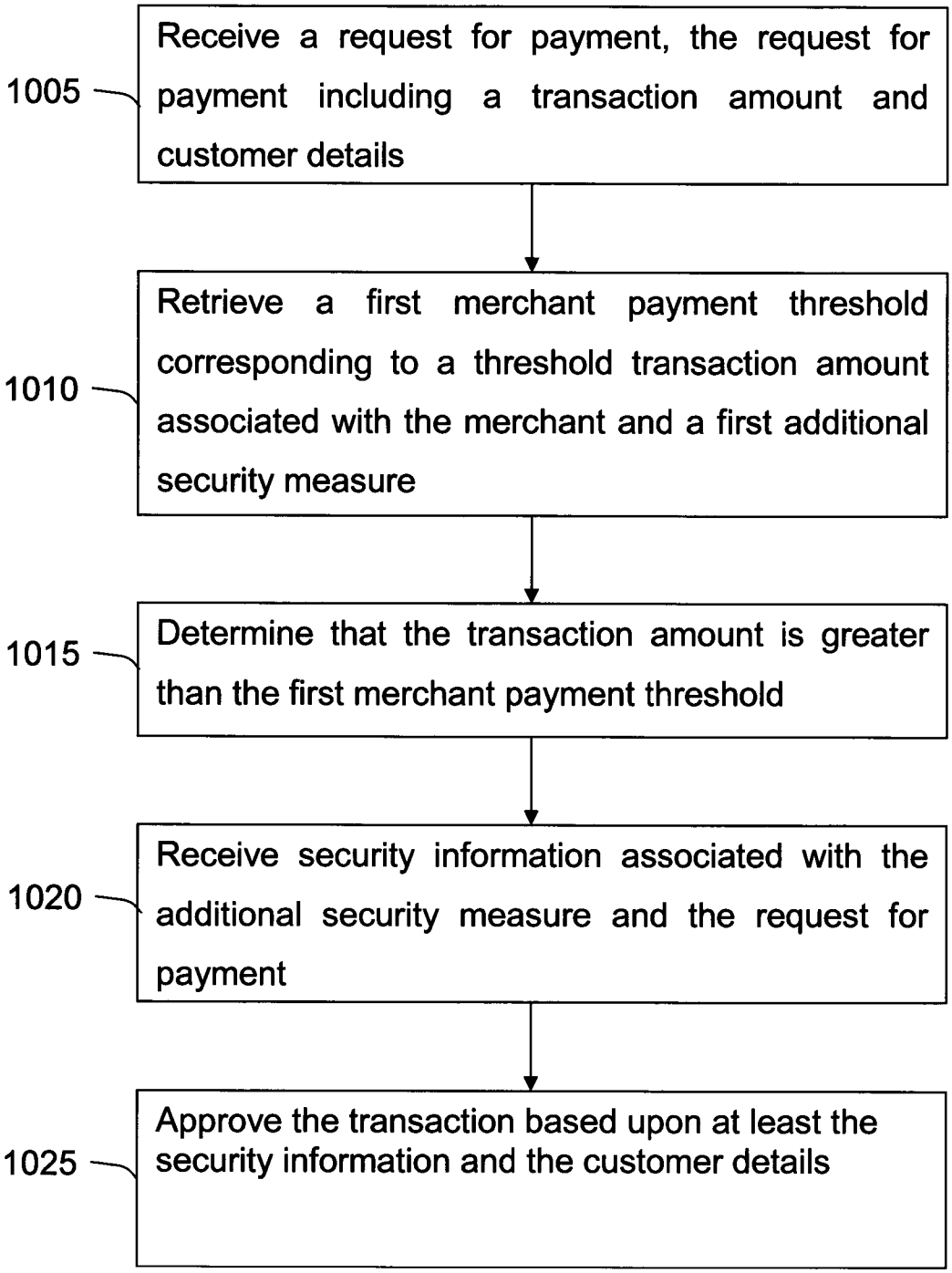
1005
Receive a request for payment, the request for payment including a transaction amount and customer details
1010
Retrieve a first merchant payment threshold corresponding to a threshold transaction amount associated with the merchant and a first additional security measure
1015
Determine that the transaction amount is greater than the first merchant payment threshold
1020
Receive security information associated with the additional security measure and the request for payment
1025
Approve the transaction based upon at least the security information and the customer details

FIG. 10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU2014/000121

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/40 (2012.01)

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI, EPODOC: IPC G06Q20/40 & keywords (multi, first, second, threshold, level, photo, camera, customer, purchaser) & like terms. Patentscope, Espacenet: keywords (one, time, identifier, phone).

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	Documents are listed in the continuation of Box C	

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

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
31 March 2014	31 March 2014

Name and mailing address of the ISA/AU	**Authorised officer**
AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA Email address: pct@ipaustralia.gov.au Facsimile No.: +61 2 6283 7999	Cathy Rees AUSTRALIAN PATENT OFFICE (ISO 9001 Quality Certified Service) Telephone No. 0262832811

INTERNATIONAL SEARCH REPORT		International application No.
C (Continuation).	DOCUMENTS CONSIDERED TO BE RELEVANT	**PCT/AU2014/000121**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	GB 2463299 A (eTRANZACT GLOBAL LIMITED) 10 March 2010	
X	Abstract, Paragraph 8, 19, 20, 25, 27, 28	1 - 3, 8 - 10
Y	Paragraph 28	4 - 7
	US 2005/0224573 A1 (YOSHIZANE et al.) 13 October 2005	
Y	Paragraphs 12, 16, 177, 211	4 - 7

INTERNATIONAL SEARCH REPORT Information on patent family members	International application No. **PCT/AU2014/000121**

This Annex lists known patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document/s Cited in Search Report		**Patent Family Member/s**	
Publication Number	**Publication Date**	**Publication Number**	**Publication Date**
GB 2463299 A	10 Mar 2010	KR 100945475 B1	05 Mar 2010
		US 2010051686 A1	04 Mar 2010
US 2005/0224573 A1	13 Oct 2005	CN 101447110 A	03 Jun 2009
		JP 2005301539 A	27 Oct 2005
		US 2005224573 A1	13 Oct 2005
		US 7258272 B2	21 Aug 2007

End of Annex

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.