(12) UK Patent Application (19) GB (11) 2506867 (13) A

(43) Date of A Publication 16.04.2014

(21) Application No: 1218090.7

(22) Date of Filing: 09.10.2012

(71) Applicant(s):
**Barclays Bank PLC**
**(Incorporated in the United Kingdom)**
**1 Churchill Place, LONDON, E14 5HP, United Kingdom**

(72) Inventor(s):
**James Gardiner**
**Colin McSkeane**

(74) Agent and/or Address for Service:
**R G C Jenkins & Co**
**26 Caxton Street, London, SW1H 0RJ,**
**United Kingdom**

(51) INT CL:
***G06Q 20/40*** (2012.01)

(56) Documents Cited:
**US 6269348 B1**
**US 20080267456 A1**
**US 20050127161 A1**
**US 20030015583 A1**
**US 20120154296 A1**
**US 20070136198 A1**
**US 20040044606 A1**

(58) Field of Search:
INT CL **G06Q**
Other: **EPODOC, WPI**

(54) Title of the Invention: **System and method for authenticating a payment transaction**
Abstract Title: **System and method for authenticating a payment transaction**

(57) In an electronic payment transaction, a mobile merchant device captures customer card details using an integrated camera. The customer enters card security details on a touch-screen of the mobile merchant device, which also captures fingerprint data from the customer. The fingerprint data are stored in a transaction record, for non-repudiation purposes.


FIG. 3

GB 2506867 A

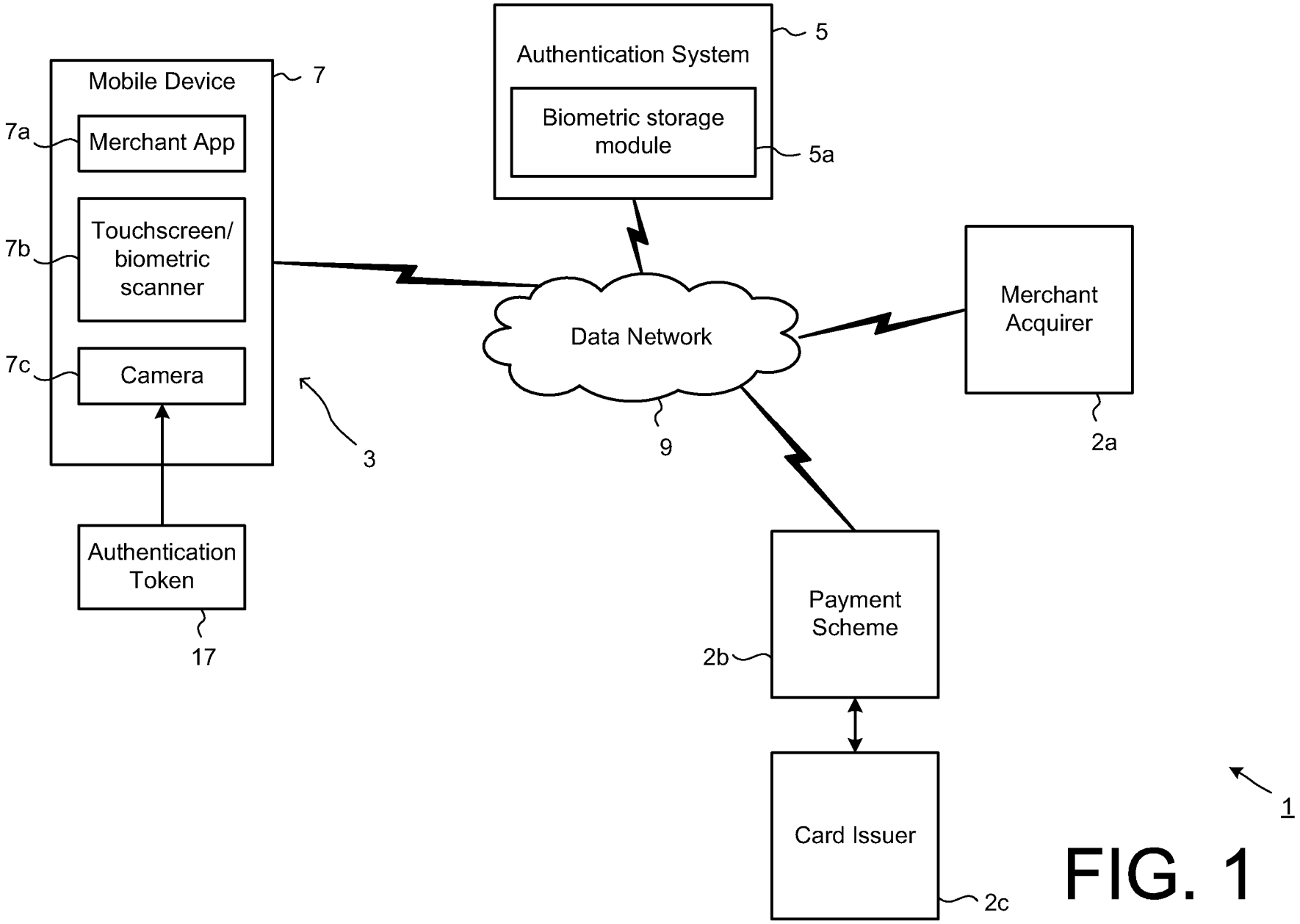
Authentication System
5
Biometric storage module
5a
Mobile Device
7
7a
Merchant App
7b
Touchscreen/ biometric scanner
7c
Camera
Data Network
Merchant Acquirer
2a
9
3
Authentication Token
17
Payment Scheme
2b
Card Issuer
2c
1

FIG. 1

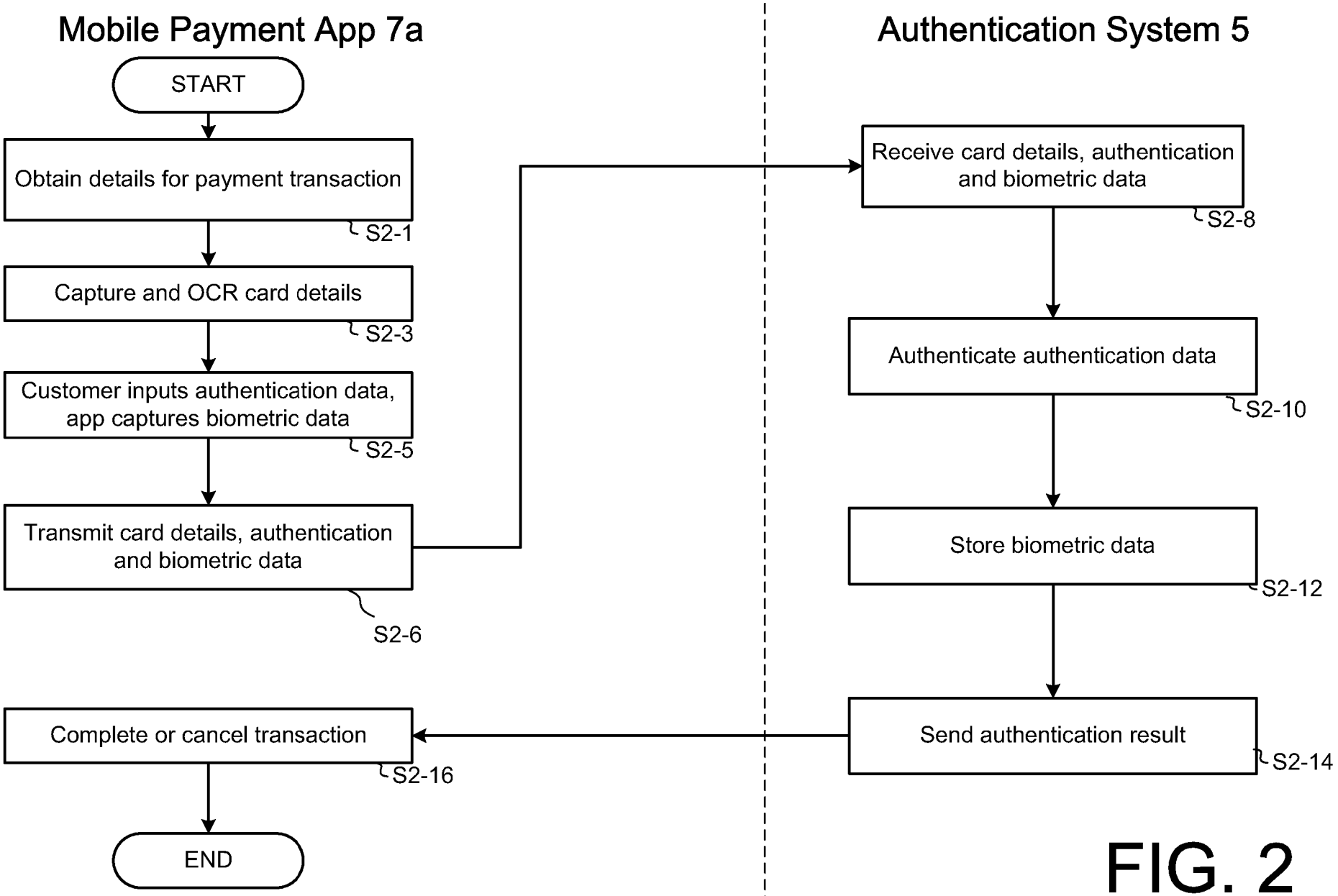
Mobile Payment App 7a
Authentication System 5
START
Obtain details for payment transaction
S2-1
Capture and OCR card details
S2-3
Customer inputs authentication data, app captures biometric data
S2-5
Transmit card details, authentication and biometric data
S2-6
Receive card details, authentication and biometric data
S2-8
Authenticate authentication data
S2-10
Store biometric data
S2-12
Send authentication result
S2-14
Complete or cancel transaction
S2-16
END

FIG. 2

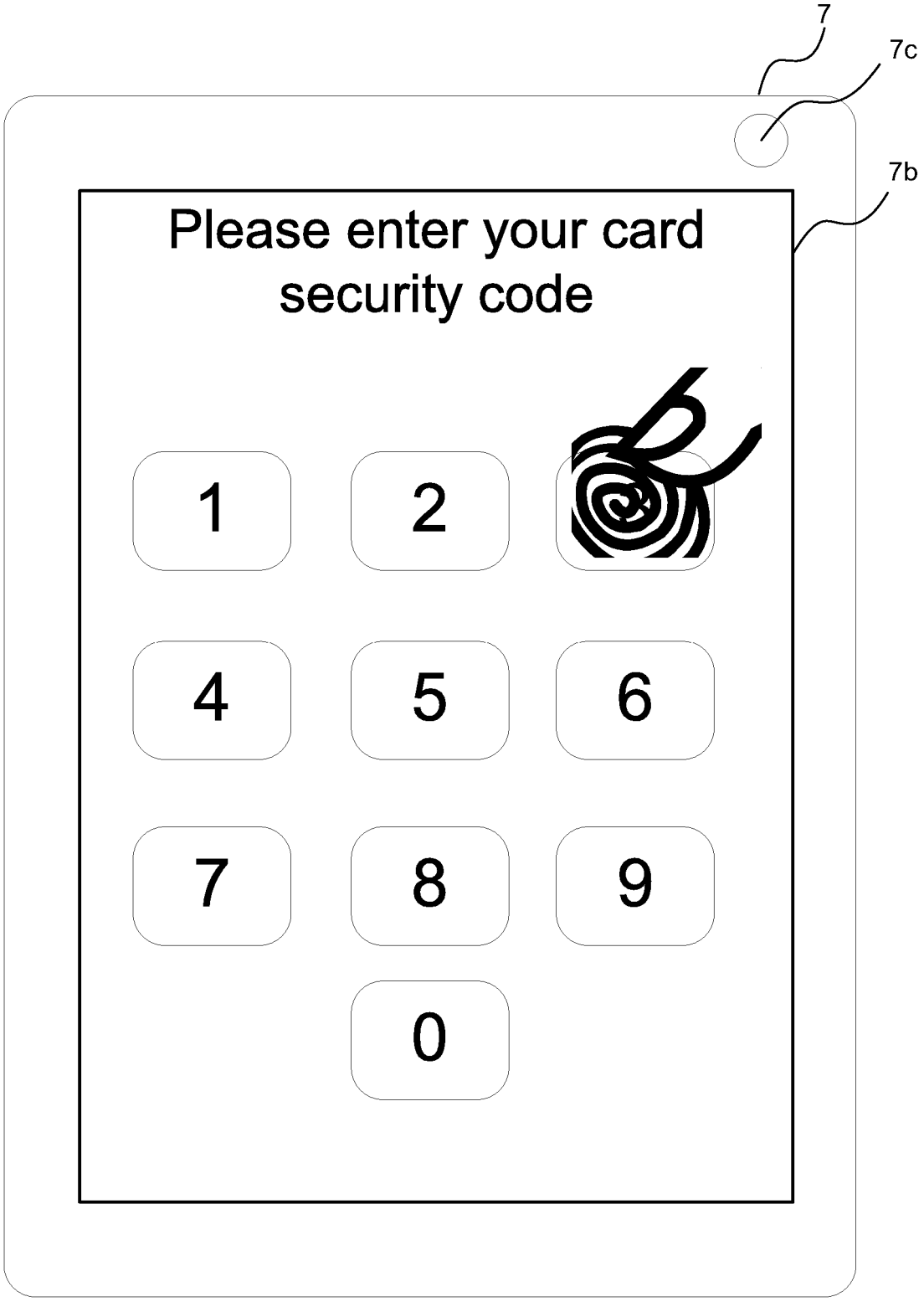


FIG. 3

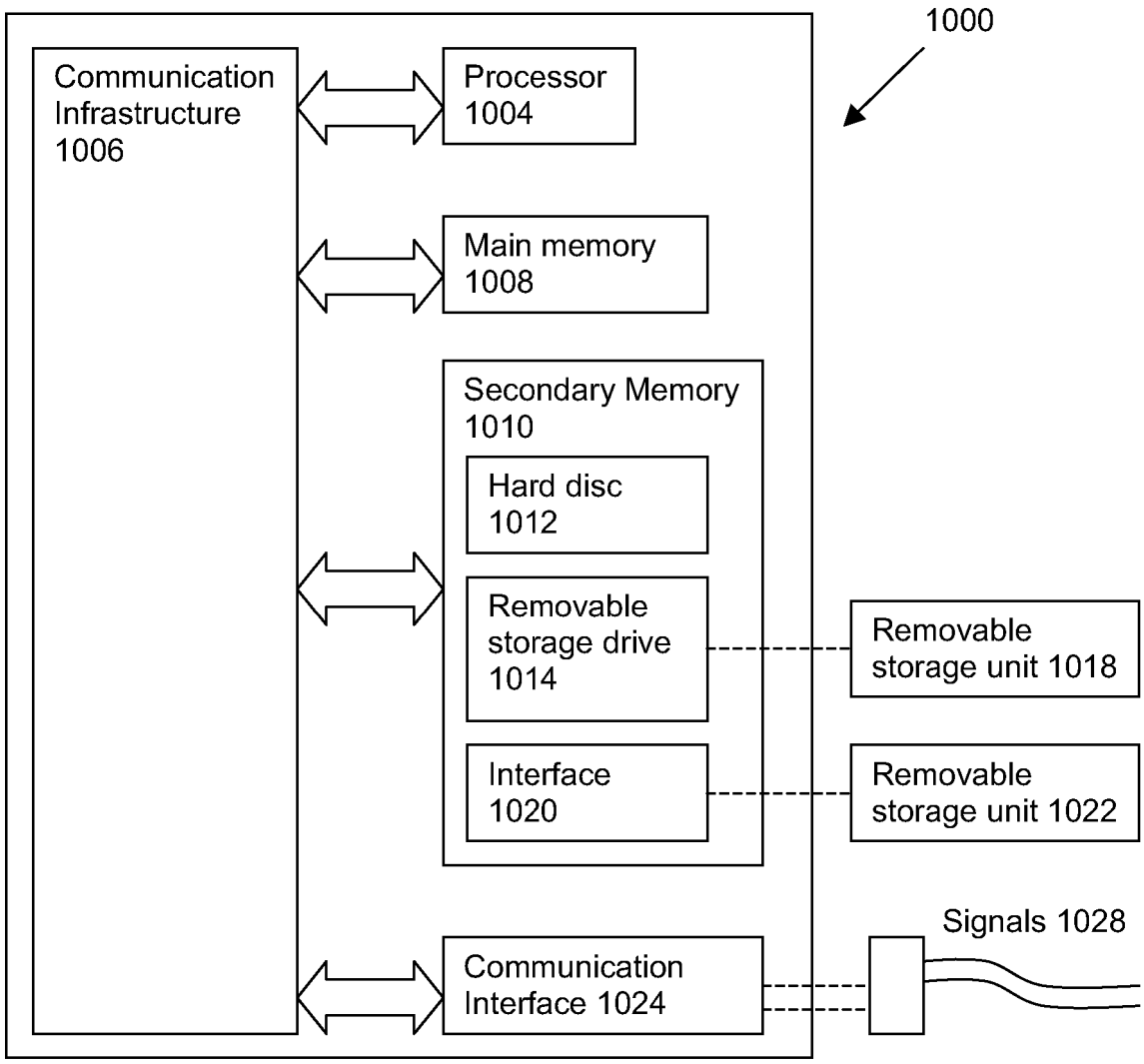
1000
Communication Infrastructure 1006
Processor 1004
Main memory 1008
Secondary Memory 1010
Hard disc 1012
Removable storage drive 1014
Interface 1020
Removable storage unit 1018
Removable storage unit 1022
Signals 1028
Communication Interface 1024

FIG. 4

# System and Method for Authenticating a Payment Transaction

## Field of the Invention

**[0001]** This invention relates to a transaction payment system, and more particularly to a system and method for providing enhanced authentication of card payment transactions.

## Background of the Invention

**[0002]** Payment transaction systems that use a mobile data terminal to handle 'Point of Sale' (POS) credit/debit card transactions for a merchant are known. Typically, the merchant's data terminal can be a mobile smartphone, tablet computer or portable computing device with cellular data communication capabilities, such as GPRS, EDGE or 3G, and capable of running a payment application. The payment application preferably provides accounting functions for the merchant, such as calculating a total bill, printing receipts, providing summaries of transactions etc. and can communicate electronically with a transaction processing back-end server to process and settle the transactions.

**[0003]** A payment card reader may be provided as a peripheral device in communication with the data terminal. Alternatively, the merchant's data terminal may capture the customer's card details using a scanner or camera, for example as disclosed in US-A-2010/0008535 (Jumio). This technique does not require a card reader, so may be implemented on a standard smartphone with an integrated camera, but is inherently less secure than the commonly used 'Chip and PIN' card reader.

**[0004]** As such card payment systems become more prevalent, there is a need for improved systems and techniques to provide greater security for transactions and reduce the risk of fraudulent use.

## Statements of the Invention

**[0005]** Aspects of the present invention are set out in the accompanying claims.

**[0006]** According to one aspect of the present invention, there is provided a method and system for authenticating a payment transaction at a merchant device, in which the customer is required to enter authentication data, and biometric data is captured

from that entry. The biometric data is stored in a transaction record for later use in the case of attempted repudiation.

**[0007]** The authentication data may be entered on a touch-sensitive screen which is able to capture fingerprint data from the entry of the authentication data. Advantageously, the customer is not required to provide fingerprint or other biometric data as a separate step.

**[0008]** Preferably, the merchant device captures card details for the transaction without the need for a dedicated card reader. For example, a camera integrated with the merchant device may be used to capture an image of the card, from which card details are extracted by OCR.

**[0009]** In a further aspect of the present invention there is provided a mobile device, an authentication system, and associated computer programs arranged to carry out the above method.

## Brief Description of the Drawings

**[0010]** There now follows, by way of example only, a detailed description of embodiments of the present invention, with references to the figures identified below.

**[0011]** Figure 1 is a block diagram showing the main components of a payment processing system according to an embodiment of the invention.

**[0012]** Figure 2 is a flow diagram illustrating the main processing steps performed by the system of Figure 1 according to an embodiment.

**[0013]** Figure 3 is a schematic diagram of a display screen for authentication data entry.

**[0014]** Figure 4 is a diagram of an example of a computer system on which one or more of the functions of the embodiment may be implemented.

## Detailed Description of Embodiments of the Invention

### Card Payment Background

**[0015]** Card payments are a way of paying for goods and services without cash changing hands; the presentation of the card details and appropriate card holder authentication guarantee the merchant payment. A conventional card payment system

is made up of a number of components: card holder, merchant, acquirer, scheme and issuer.

**[0016]** In the normal process the card holder presents his card (or token) to the merchant in order to pay for goods or services rendered; this transaction may take place over any one of a number of channels (in store or via the Internet, for example). The merchant, through his acquirer, is set up to accept different card types by scheme (Visa$^{RTM}$, MasterCard$^{RTM}$, Amex$^{RTM}$, credit, debit, for example). When a card is presented, the card holder is authenticated (by Personal Identification Number, PIN, passcode, or Card Verification Value, CV2, for example), subject to channel and merchant capability, and the transaction is submitted to the merchant's acquirer for authorisation. Authorisation and authentication of the merchant and/or card holder may instead or additionally be handled through a trusted third party authentication system that is known to the merchant acquirer.

**[0017]** Once the transaction is received, the acquirer routes the authorisation transaction, in real time, to the relevant scheme based upon card type. The scheme provides isolation between acquirers and issuers for routing of authorisations, settlements and funds movement. The acquirer doesn't need to know who the issuer is, just which scheme to route it to which is determined by Bank Identification Number (BIN).

**[0018]** The issuer authorises the transaction based upon the card holder's balance and other risk/fraud criteria and returns an authorised message and authorisation code to the scheme, which routes it back to the acquirer who sends it to the merchant. The merchant then confirms the sale, which posts a settlement transaction to the acquirer; this is a mandate to make the payment and move funds. The settlement transaction is routed between acquirers and issuers via the scheme.

**Technical Architecture**

**[0019]** Referring to Figure 1, a payment transaction system 1 according to an embodiment of the invention comprises a merchant system 3 for handling payment transactions, such as credit/debit card transactions, through a merchant application 7a running on a mobile device 7. In a typical payment transaction process, the merchant

application 7a can receive data identifying goods and/or services associated with the payment transaction, apply discounts or vouchers, determine the total amount due for payment, and initiate authentication of an payment token 17 presented by the customer. The merchant application 7a must obtain details of the payment token 17 before the payment transaction can be settled and completed.

**[0020]** In the present embodiment, the payment token 17 is a credit or debit card of conventional type, carrying at least a card number, expiry date and cardholder name on the front side and a card security code on the reverse side.

**[0021]** The mobile device 7 can be a mobile smartphone, tablet computer or portable computing device, or the like, and communicates with a transaction processing module 5 via a data network 9. The merchant application 7a can be secured by means of a passcode and information associated with a payment transaction can be provided via the secured merchant application 7a running on the mobile device 7. Electronic data communication by the merchant application 7a may be encrypted.

**[0022]** The data network 9 may be any suitable data communication network such as a wireless network, a local- or wide-area network including a corporate intranet or the Internet, using for example the TCP/IP protocol, or a cellular communication network such as GPRS, EDGE or 3G, for example. Such communication protocols are of a type that are known *per se* in data networks and need not be described further.

**[0023]** Components of the merchant system 3 are also in communication with a merchant acquirer 2a, payment scheme 2b and card issuer 2c components over the data network 9, which are typically provided for authorizing and settling card payment transactions as described in the section above, and need not be described further.

**[0024]** In this embodiment, additional authentication is handled through an authentication system 5 hosted by a trusted third party that is known to the merchant acquirer 2a. Alternatively, the authentication system 5 may be provided as a component of the merchant acquirer 2a. As will be described below, this authentication system 5 provides an authentication security check prior to authorisation processing of a payment transaction, and additionally stores biometric

information captured from the customer during the authentication security check, in a biometric storage module 5a.

**[0025]** The mobile device 7 includes a digital camera 7c for scanning or imaging the payment token 17 so as to capture the card details at least from the front side of the card. The digital camera 7c is controlled by the merchant app 7a to capture a digital still or moving image of the front side of the card. The merchant app 7a obtains the card details from the digital image using an Optical Character Recognition (OCR) process.

**[0026]** The mobile device 7 also includes a touch-sensitive screen 7b that is able to retrieve biometric information such as fingerprint information from a user as the user touches the screen. Examples of such screens are disclosed in US-A-2012/0154296 (Microsoft) and US2012/0092127 (Qualcomm). Preferably, at least part of the touch-sensitive screen 7b has sufficient sensing resolution to detect the pattern of the user's fingerprint as the user touches the screen. An advantage of such a screen is that the user's fingerprint can be captured without requiring a specific fingerprint scanning step; instead, fingerprint information can be captured while the user performs another type of interaction with the touch-sensitive screen 7b. Partial fingerprint information may be captured from each of multiple touch interactions, and merged to form more complete fingerprint information.

**Payment Authentication Process**

**[0027]** An embodiment of a process of payment authentication will now be described with reference to Figure 2, to illustrate the technical advantage of the payment transaction system embodiment described above.

**[0028]** The process begins at step S2-1 where details for a new payment transaction are obtained by the merchant application 7a running on the mobile device 7. The transaction details typically include a payment amount to be transferred and data identifying the transaction, such as the time and date of the transaction and a description of the associated goods or services. The merchant application 7a may scan codes (such as 1D barcodes or 2D QR codes) associated with the goods or services to obtain details of the transaction.

**[0029]** At step S2-3, the merchant application 7a captures a digital image of the front side of a card presented by the customer and obtains the card details using an OCR process on the digital image, as described above. This conveniently avoids the customer or merchant having to enter the card number and other details manually.

**[0030]** At step S2-5, the merchant application 7a displays a data entry screen to the customer, prompting the customer to enter their card security code, such as the CV2 code. An example of the data entry screen is shown in Figure 3, in which virtual numeric keys are displayed. As represented by the finger and fingerprint, the screen 7b captures at least a partial fingerprint when the customer touches the screen 7b with a finger, as well as recording the number pressed. Since the customer is required to enter multiple numbers for the card security code, the screen 7b may capture multiple partial or complete fingerprints.

**[0031]** In this embodiment, the merchant application 7a does not attempt to authenticate the captured fingerprints, since there is no authentic fingerprint data available for the customer. In particular, any authentic fingerprint data stored on a chip on the customer's card cannot be read, since the mobile device 7 does not include a chip reader. Instead, the merchant application 7a records the captured fingerprint data for storage as part of a payment transaction record, as will be explained below. The merchant application 7a may however determine whether no significant fingerprint data has been captured, for example as a result of the customer using a stylus, and may then prompt the customer to re-enter the authentication data using a finger.

**[0032]** The merchant application 7a may encode and/or compress the captured fingerprint data using a standard format for fingerprint data, such as disclosed in ANSI/NIST-ITL 1-2011 Special Publication 500-290, 'Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information'.

**[0033]** The merchant application 7a may request input of alternative or additional authentication information, such as the cardholder's postal (zip) code for comparison with the cardholder's registered billing address.

**[0034]** At step S2-6, the merchant application 7a transmits the captured authentication and biometric (e.g. fingerprint) data together with the captured card details, to the authentication system 5 where the data is received, at step S2-8. At step S2-10, the authentication system 5 uses the card details to access a corresponding cardholder record and authenticate the authentication data against the cardholder record. The cardholder record is typically held by the card issuer 2c, so the authentication system 5 may delegate the authentication step to the card issuer 2c, via the payment scheme 2b, and receive an authentication response from the card issuer 2c. Alternatively, the merchant application 7a may send the authentication data to the merchant acquirer 2a for authentication, and send the biometric data to the authentication system 5.

**[0035]** At step S2-12, the authentication system 5 stores the received biometric data in a cardholder transaction record. The cardholder transaction record may subsequently be retrieved if the cardholder seeks to repudiate the transaction i.e. denies that the cardholder authorised the transaction. The cardholder may then be required to provide a fingerprint scan for comparison with the biometric data in the cardholder transaction record.

**[0036]** The authentication system 5 may optionally validate the biometric data to ensure that it corresponds to one or more valid fingerprints. In a case where the authentication system 5 has access to cardholder records including authentic fingerprint data, the authentication system 5 may authenticate the received biometric data against the cardholder records. Alternatively, the authentication system 5 may store previously received biometric data from previously authenticated transactions in a card or cardholder record, and authenticate the received biometric data for the current transaction against the previously received biometric data.

**[0037]** At step S2-14, the authentication system 5 sends an authentication result to the merchant application 7a, dependent on the authentication of the authentication data and optionally on the validation/authentication of the biometric data. At step S2-16, the merchant application 7a may complete or cancel the transaction, depending on the received authentication result.

**[0038]** Optionally, if the authentication system 5 fails to authenticate the authentication data and/or the biometric data, it may send an alert message to an address registered in the cardholder record. The address may be a mobile number for sending a text or multimedia message, an email address, or a postal address.

**[0039]** In this way, acquirers and merchants in the payment transaction system are provided with enhanced security and non-repudiation of payment transactions.

**Alternative Embodiments**

**[0040]** It will be understood that embodiments of the present invention are described herein by way of example only, and that various changes and modifications may be made without departing from the scope of the invention.

**[0041]** For example, in the exemplary embodiment described above, the biometric data comprises fingerprint data and the authentication data entry means comprises a touch-sensitive screen. Other combinations may be envisaged which nevertheless allow biometric data to be captured during authentication data entry. In one alternative, the customer may be required to speak authentication data into a microphone of the mobile device; the authentication data is captured using a speech recognition process, and the biometric data is captured as a voiceprint characteristic of the speaker. In another alternative, the authentication data entry means may be a touchpad separate from any display screen, the touchpad also being able to capture fingerprint data.

**[0042]** The card details may be captured by means other than a digital image. For example, the card or other payment token may include an NFC or RFID tag which can be read by the mobile device 7. Alternatively, but less preferably, the customer or merchant may be required to enter the card details manually on the mobile device 7.

**[0043]** The division of operations between the merchant application 7a and the authentication system 5 may differ from that described in the embodiment above. For example, the digital image of the card may be sent to the authentication system 5 for OCR processing. The fingerprint data may be sent to the authentication system 5 for encoding. In either case, less processing is required by the merchant application 7a, at

the expense of greater bandwidth requirements between the merchant application 7a and the authentication system 5a.

**[0044]** Alternative embodiments may be envisaged, which nevertheless fall within the scope of the following claims.

**Computer Systems**

**[0045]** The entities described herein, such as the mobile device 7 or authentication system 5, may be implemented by computer systems such as computer system 1000 as shown in Figure 4. Embodiments of the present invention may be implemented as programmable code for execution by such computer systems 1000. After reading this description, it will become apparent to a person skilled in the art how to implement the invention using other computer systems and/or computer architectures.

**[0046]** Computer system 1000 includes one or more processors, such as processor 1004. Processor 1004 may be any type of processor, including but not limited to a special purpose or a general-purpose digital signal processor. Processor 1004 is connected to a communication infrastructure 1006 (for example, a bus or network). Various software implementations are described in terms of this exemplary computer system. After reading this description, it will become apparent to a person skilled in the art how to implement the invention using other computer systems and/or computer architectures.

**[0047]** Computer system 1000 also includes a main memory 1008, preferably random access memory (RAM), and may also include a secondary memory 610. Secondary memory 1010 may include, for example, a hard disk drive 1012 and/or a removable storage drive 1014, representing a floppy disk drive, a magnetic tape drive, an optical disk drive, etc. Removable storage drive 1014 reads from and/or writes to a removable storage unit 1018 in a well-known manner. Removable storage unit 1018 represents a floppy disk, magnetic tape, optical disk, etc., which is read by and written to by removable storage drive 1014. As will be appreciated, removable storage unit 618 includes a computer usable storage medium having stored therein computer software and/or data.

**[0048]** In alternative implementations, secondary memory 1010 may include other similar means for allowing computer programs or other instructions to be loaded into computer system 1000. Such means may include, for example, a removable storage unit 1022 and an interface 1020. Examples of such means may include a program cartridge and cartridge interface (such as that previously found in video game devices), a removable memory chip (such as an EPROM, or PROM, or flash memory) and associated socket, and other removable storage units 1022 and interfaces 1020 which allow software and data to be transferred from removable storage unit 1022 to computer system 1000. Alternatively, the program may be executed and/or the data accessed from the removable storage unit 1022, using the processor 1004 of the computer system 1000.

**[0049]** Computer system 1000 may also include a communication interface 1024. Communication interface 1024 allows software and data to be transferred between computer system 1000 and external devices. Examples of communication interface 1024 may include a modem, a network interface (such as an Ethernet card), a communication port, a Personal Computer Memory Card International Association (PCMCIA) slot and card, etc. Software and data transferred via communication interface 1024 are in the form of signals 1028, which may be electronic, electromagnetic, optical, or other signals capable of being received by communication interface 1024. These signals 1028 are provided to communication interface 1024 via a communication path 1026. Communication path 1026 carries signals 1028 and may be implemented using wire or cable, fibre optics, a phone line, a wireless link, a cellular phone link, a radio frequency link, or any other suitable communication channel. For instance, communication path 1026 may be implemented using a combination of channels.

**[0050]** The terms "computer program medium" and "computer usable medium" are used generally to refer to media such as removable storage drive 1014, a hard disk installed in hard disk drive 1012, and signals 1028. These computer program products are means for providing software to computer system 1000. However, these terms

may also include signals (such as electrical, optical or electromagnetic signals) that embody the computer program disclosed herein.

**[0051]** Computer programs (also called computer control logic) are stored in main memory 1008 and/or secondary memory 1010. Computer programs may also be received via communication interface 1024. Such computer programs, when executed, enable computer system 1000 to implement embodiments of the present invention as discussed herein. Accordingly, such computer programs represent controllers of computer system 1000. Where the embodiment is implemented using software, the software may be stored in a computer program product and loaded into computer system 1000 using removable storage drive 1014, hard disk drive 1012, or communication interface 1024, to provide some examples.

**[0052]** Alternative embodiments may be implemented as control logic in hardware, firmware, or software or any combination thereof.

**CLAIMS**

1. A computer-implemented method of authenticating a payment transaction between a merchant and a customer in an electronic payment system, comprising:
    a. initiating a transaction at a merchant device;
    b. capturing biometric data from the customer while receiving authentication data as input from the customer at the merchant device;
    c. storing the biometric data in a payment transaction record; and
    d. authenticating the transaction by means of the authentication data.
2. The method of claim 1, wherein the transaction is further authenticated by means of the biometric data.
3. The method of claim 1 or claim 2, wherein the merchant device includes a touch-sensitive surface on which the authentication data is input by the customer, the touch sensitive surface being arranged to capture fingerprint data from said input by the customer.
4. The method of claim 3, wherein the touch-sensitive surface comprises a touch-sensitive display screen.
5. The method of claim 1 or claim 2, wherein the authentication data is input as speech, and the biometric data is derived from the speech.
6. The method of any preceding claim, further including receiving payment token data from a payment token presented by the customer.
7. The method of claim 6, wherein the payment token comprises a bank card.
8. The method of claim 6 or 7, wherein the payment token data is captured from a digital image of the payment token.
9. The method of claim 8, wherein the digital image is obtained using a camera integrated with the merchant device.
10. The method of claim 8 or claim 9, wherein the authentication data comprises a security code displayed on the payment token.

11. The method of any preceding claim, wherein the merchant device comprises a mobile device.

12. A system comprising means for performing the method of any preceding claim.

13. A storage medium comprising machine readable instructions stored thereon for causing a computer system to perform a method in accordance with any one of claims 1 to 11.

14. A method substantially as herein described with reference to the accompanying drawings.

15. A system substantially as herein described with reference to the accompanying drawings.

**CLAIMS**

1. A computer-implemented method of processing a payment transaction between a merchant and a customer in an electronic payment system by means of a merchant device having a touch-sensitive surface arranged for input of authentication data by the customer and for capture of fingerprint data from said input, the method comprising, at the merchant device:

    a. initiating the payment transaction;

    b. capturing fingerprint data from the customer while receiving customer authentication data as input from the customer from the touch-sensitive surface;

    c. sending the authentication data and fingerprint data to a transaction authentication system;

    d. receiving an authentication result from the authentication system, dependent at least on the authentication data; and

    e. completing or cancelling the payment transaction dependent on the authentication result.

2. The method of claim 1, wherein the authentication result is further dependent on authentication or validation of the fingerprint data.

3. The method of claim 1 or 2, wherein the touch-sensitive surface comprises a touch-sensitive display screen.

4. The method of any preceding claim, further including receiving payment token data at the merchant device from a payment token presented by the customer.

5. The method of claim 4, wherein the payment token comprises a bank card.

6. The method of claim 4 or 5, wherein the payment token data is captured from a digital image of the payment token.

7. The method of claim 6, wherein the digital image is obtained using a camera integrated with the merchant device.

8. The method of claim 6 or claim 7, wherein the authentication data comprises a security code displayed on the payment token.

9. The method of any preceding claim, wherein the merchant device comprises a mobile device.

10. The method of any preceding claim, further comprising, in the event of the customer seeking to repudiate the transaction: receiving a fingerprint scan from the customer and comparing the fingerprint scan to the fingerprint data.

11. A system comprising means for performing the method of any preceding claim.

12. A storage medium comprising machine readable instructions stored thereon for causing a computer system to perform a method in accordance with any one of claims 1 to 9.

13. A method substantially as herein described with reference to the accompanying drawings.

14. A system substantially as herein described with reference to the accompanying drawings.

**Application No:** GB1218090.7 **Examiner:** Mr Martin Price

**Claims searched:** 1-15 **Date of search:** 30 January 2013

# Patents Act 1977: Search Report under Section 17

**Documents considered to be relevant:**

| Category | Relevant to claims | Identity of document and passage or figure of particular relevance |
|---|---|---|
| X,Y | X: 1 at least; Y: 3 | US 2007/0136198 A1 Foth - see e.g. claim 1 and paragraph 0019 |
| X,Y | X: 1 at least; Y: 3 | US 2005/0127161 A1 Smith - see e.g. claim 1 and figure 5a |
| X,Y | X: 1 at least; Y: 3 | US 2004/0044606 A1 Buttridge - see e.g. claim 1 and paragraphs 0038, 0040, 0050, 0055 |
| X,Y | X: 1 at least; Y: 3 | US 2003/0015583 A1 Abdi - see e.g. claims 1, 3 |
| X,Y | X: 1 at least; Y: 3 | US 6269348 B1 Pare - see e.g. the abstract |
| Y | 3 | US 2012/0154296 A1 Hinckley - see e.g. the abstract and figures |
| Y | 3 | US 2008/0267456 A1 Anderson - see e.g. the abstract and figures |

Categories:

| | | | |
|---|---|---|---|
| X | Document indicating lack of novelty or inventive step | A | Document indicating technological background and/or state of the art. |
| Y | Document indicating lack of inventive step if combined with one or more other documents of same category. | P | Document published on or after the declared priority date but before the filing date of this invention. |
| & | Member of the same patent family | E | Patent document published on or after, but with priority date earlier than, the filing date of this application. |

## Field of Search:

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC$^{X}$ :

Worldwide search of patent documents classified in the following areas of the IPC

G06Q

The following online and other databases have been used in the preparation of this search report

EPODOC, WPI

**International Classification:**

| Subclass | Subgroup | Valid From |
|---|---|---|
| G06Q | 0020/40 | 01/01/2012 |