(12) UK Patent Application (19) GB (11) 2549245 (13) A

(43) Date of A Publication 18.10.2017

(21) Application No: 1520531.3

(22) Date of Filing: 22.11.2015

(71) Applicant(s):
Facebanx Ltd
(Incorporated in the United Kingdom)
273, Eversholt Street, London, NW1 1BA,
United Kingdom

(72) Inventor(s):
Andrew Churchill

(74) Agent and/or Address for Service:
Invicta IP Ltd
18c Fairfield Road, Petts Wood, ORPINGTON, Kent,
BR5 1JR, United Kingdom

(51) INT CL:
G06Q 20/38 (2012.01) ***G06F 21/35*** (2013.01)
G06F 21/43 (2013.01) ***G06Q 20/32*** (2012.01)
G06Q 20/36 (2012.01)

(56) Documents Cited:

WO 2014/145708 A	**US 20140279099 A**
US 20140058937 A	**US 20120265688 A**
US 20120089514 A	**US 20100131347 A**
US 20100106649 A	**US 20090254485 A**
US 20090240626 A	**US 20030080183 A**

(58) Field of Search:
INT CL **G06F, G06Q**
Other: **EPODOC, WPI.**

(54) Title of the Invention: **Out of band pre-authentication of a transaction**
Abstract Title: **Using a mobile device for out-band transaction authentication**

(57) Disclosed is a transaction security system with a merchant's terminal 7 a mobile device 2 operable by a customer 1 and authorising authority servers 4,5,6. The merchant's terminal communicates with the authorising authority on a first band 6a which may form a part of a wide area network. The customer's mobile device communicates with the authorising authority on a second independent band 9 which forms part of the wide area network. The mobile device acquires transaction data and calculates a one-time code (OTC) from the transaction and other data on the device before transmission to the authorising authority servers. If subject to conventional credit checks, the transaction is approved by the authorising authority, the transaction is pre-approved to the customer. The customer device communicates the pre-approved anonymised OTC to the merchant's terminal. The merchant's terminal then communicates the received OTC with the authorising authority over the first band. If this matches the original approved OTC received by the authorising authority the transaction is approved if not it is refused.

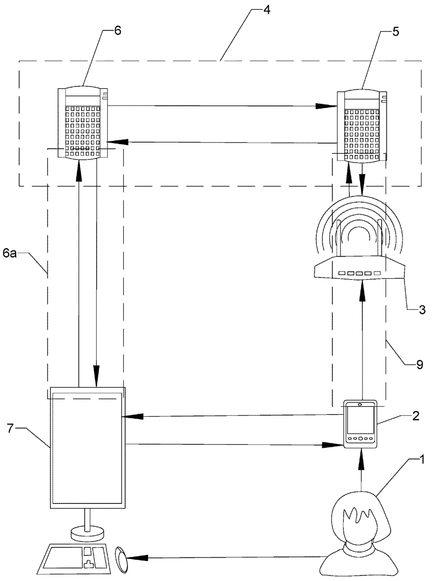

Fig 1A

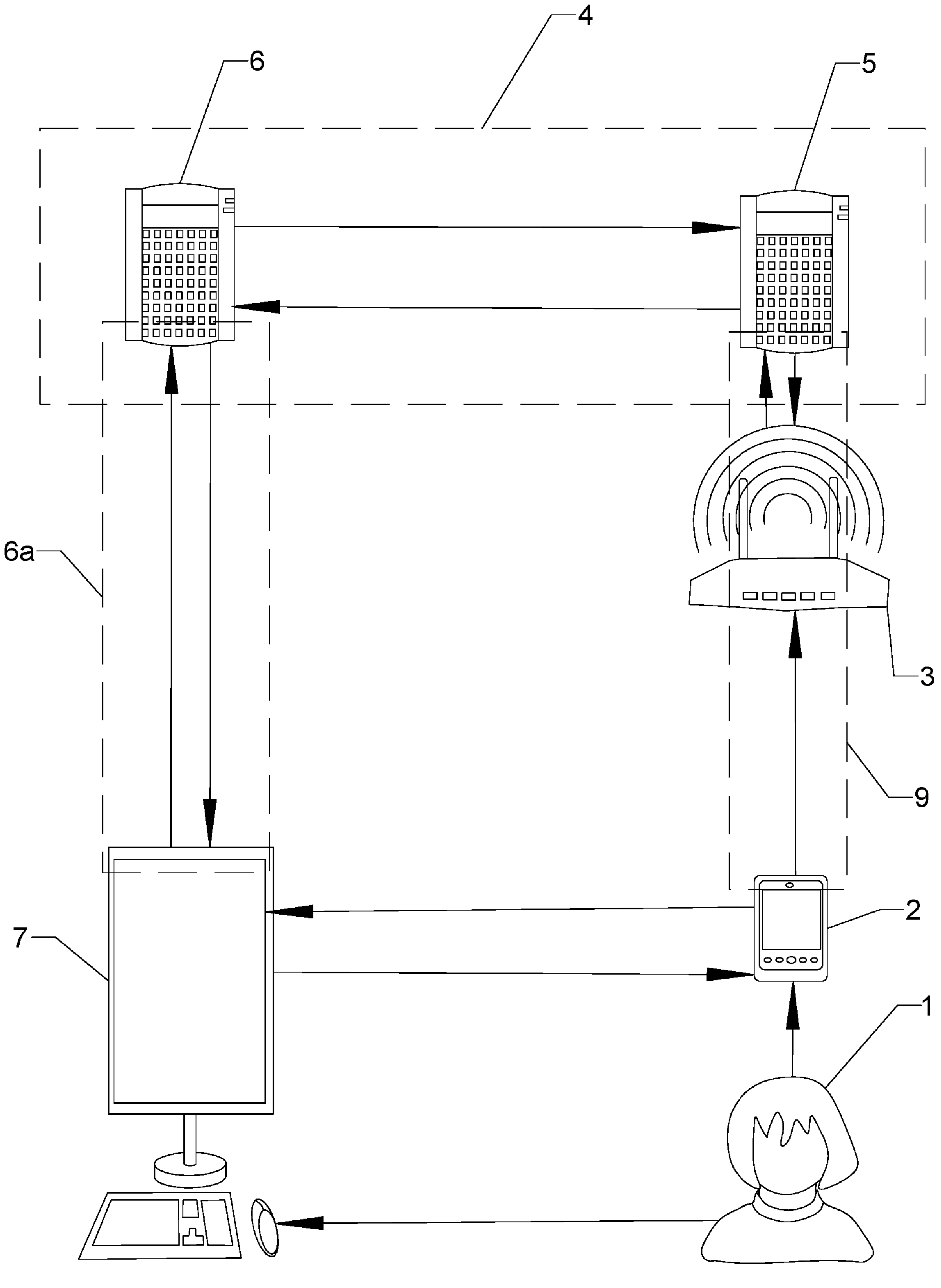

Fig 1A

04 07 17

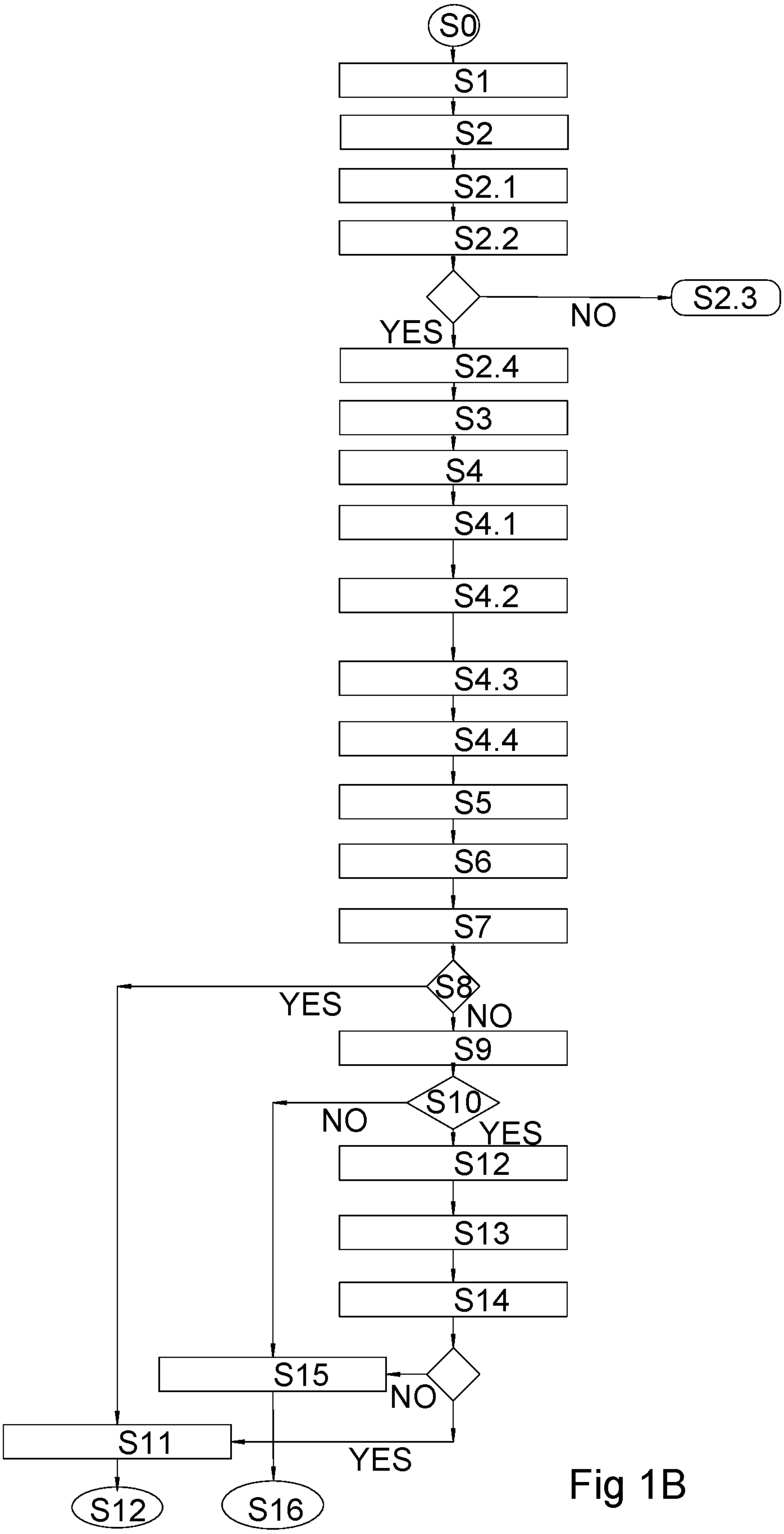

Fig 1B

04 07 17

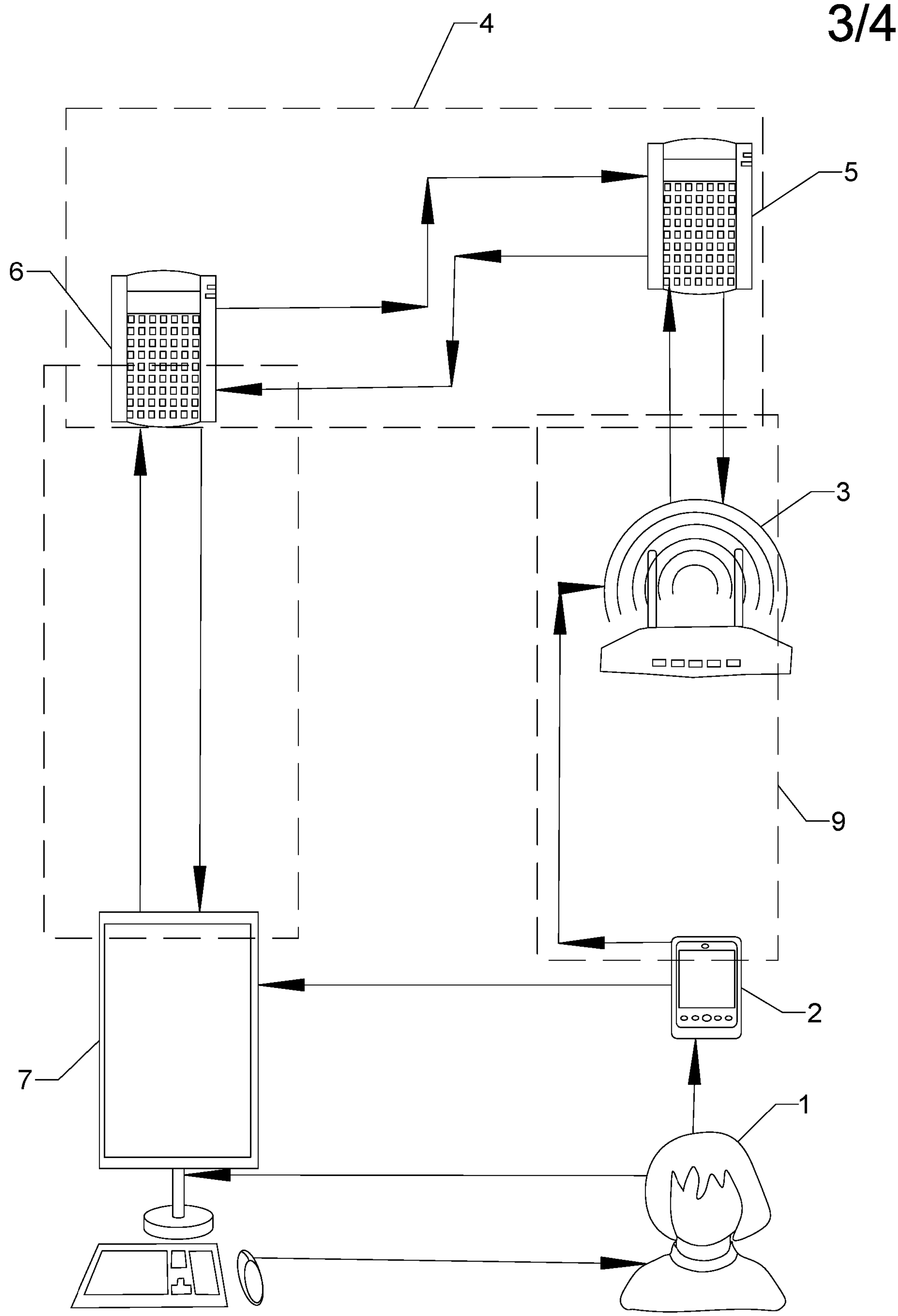

Fig 2A

04 07 17

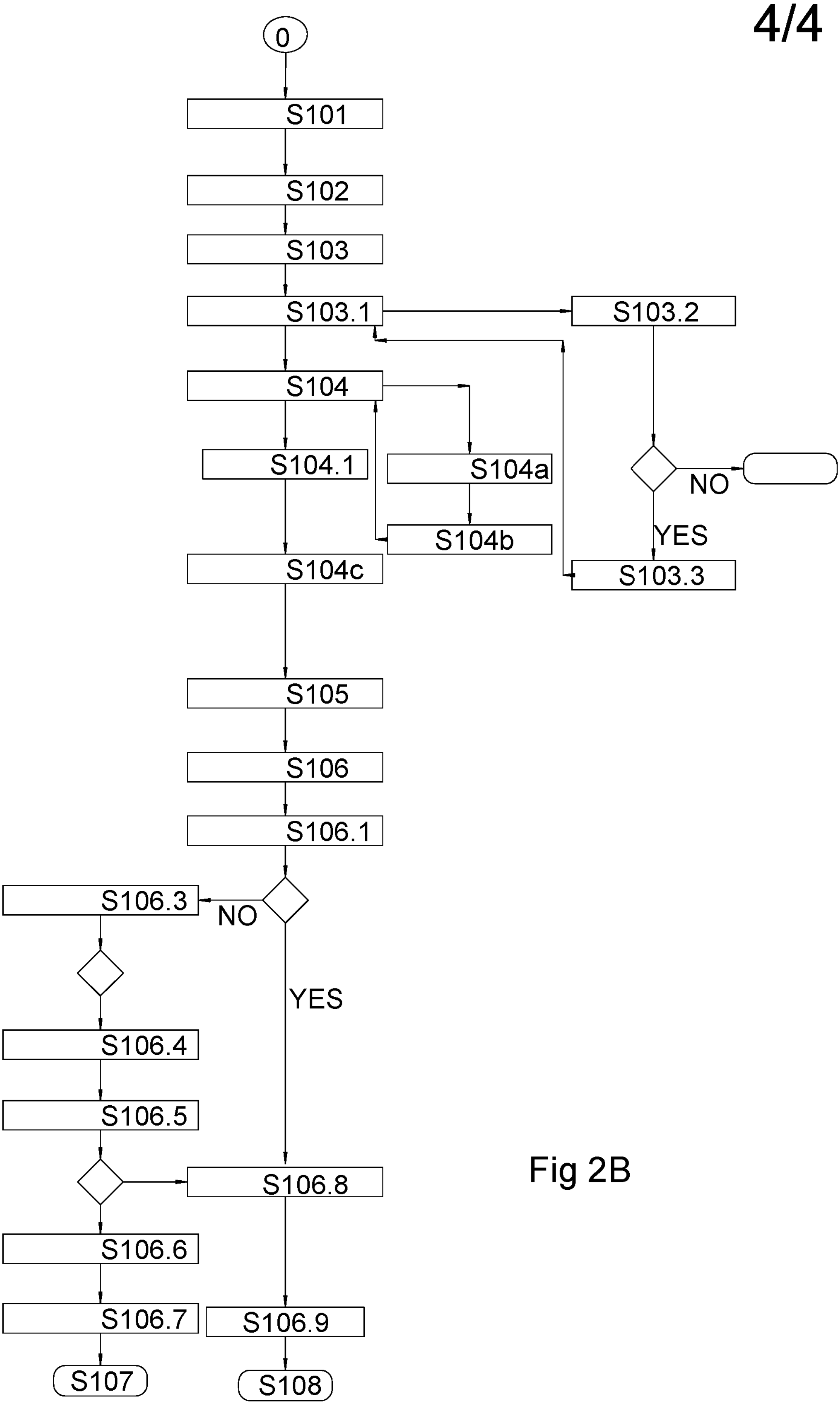

Fig 2B

Application No. GB1520531.3 RTM Date :1 June 2017

The following terms are registered trade marks and should be read as such wherever they occur in this document:

WIFI (Page 13)

Out of Band Pre-authentication of a Transaction

Technical Field

[001] The present invention relates to securing a transaction particularly but not exclusively a non-physical cash or credit financial transaction. For these purposes a transaction may be understood to mean a transaction such as the purchase of goods or services in a store, passage through a physical access barrier requiring authentication of an identity or access to a non-physical space.

Prior Art

[002] In the most basic of non-cash financial transactions a buyer presents a physical card to a merchant. The card details are recorded by the merchant and authorised by the buyer using a signature. The merchant checks the signature against a record signature on the card before proceeding with the transaction. If the signatures are a reasonable match the merchant processes the transaction. Subsequently the recorded transaction details are communicated to the merchant’s bank and reconciled with the buyer’s bank. For these purposes the term “bank” should be understood as any authorising authority providing the service of approving or disapproving a transaction in real time, and not exclusively an organisation which calls itself a bank.

[003] The only security provided by the simple form of transaction referenced above is that of possessing the card and the difficulty of fraudulently replicating a signature. Criminals now find it easy to circumvent such security and accordingly further security measures have commonly been adopted. In particular a card may be provided with a “chip” capable of being read only in response to the input of a password, commonly a four digit PIN number, input by the buyer/cardholder. The PIN substitutes for the signature and being evident only during the PIN input, cannot easily be deduced and used fraudulently, even if the card is stolen.

[004] It has become commonplace for the merchant to transmit the transaction data to the merchant’s bank, from the merchant’s card reader, over a landline or wireless communication, or some combination of the landline and wireless. The data is thus communicated on a single “band”. Larger users which implement large volumes of transactions may have a dedicated communication band for this purpose. However, smaller users will communicate this data over a general purpose band. The band is most commonly provided via a landline, mobile telephony or internet connection or a combination thereof. Transmission takes place in, the case of larger transactions (exceeding some threshold value) immediately so that the merchant’s bank can

authorise or refuse the transaction, smaller transactions e.g. those for less than a threshold sum such as GBP 30 are authorised so long as the PIN entered is valid. Smaller transactions are vulnerable to conventional fraudulent card use, for example where a card is stolen or cloned and the PIN acquired. The larger transactions are vulnerable to a “man in the middle” attack where the data is intercepted on the communication band and what appears to be the merchant’s bank ‘s response is fraudulent in approving the transaction.

[005] Commercial pressure to reduce the delay in transactions caused by the requirement to process a card transaction via signature or PIN has led to the development of so called “contactless” payment cards. These are cards containing a near field communication (NFC) enabled chip capable of transmitting cardholder account data to a near field enabled reader. Thus in a merchant environment the cardholder’s purchase details are acquired by the merchant’s terminal, the merchant’s reader is enabled and the account transaction implemented by the card holder touching the card to the reader or bringing the card into sufficiently close proximity to the reader. Security is entirely dependent on the cardholder preventing theft of their card and in ensuring that criminals are unable to clone cards or to forge fraudulent cards capable of being

accepted by a reader. Generally legislation limits the size of transaction which can be implemented via contactless cards without the use of a PIN or other security measures.

[006] The proliferation of the use of machine readable credit cards, debit cards, store cards, customer loyalty cards, identity cards and key cards has resulted in many users being overburdened with wallets and purses inconveniently encumbered with such cards, some of which will rarely be used. The theft or loss of a card may go unnoticed for a prolonged period, especially if it is rarely used, increasing the security risk.

[007] The implementation of near field communications has presented the opportunity for NFC cards to be emulated on mobile devices, particularly mobile phones. In such implementations a single mobile phone can effectively and securely store a large number of NFC enabled “virtual cards” in a device already commonly carried and thus obviate the many card encumbrance problem described above.

[008] One of the flaws with conventional or virtual card transactions is that data identifying the account and hence the buyer’s identity is invariably presented to the merchant or the merchant’s bank, unlike a conventional physical cash transaction the card holder cannot be completely anonymised.

[009] The use of wirelessly connected mobile devices to make payments presents an opportunity to enhance the security of transactions, to expedite transactions and may enable transactions to be completely anonymised.

Statement of Invention

[010] A transaction security system comprising:

a terminal capable of communicating with a first authorising authority on a first band;

a mobile device capable of communication with an authorising authority on a second band and having;

a card module capable of storing transaction card account data for one or more transaction card accounts;

wherein said mobile device is adapted to;

acquire transaction data relating to a specific transaction,

transmit said transaction data to an authorising authority via said second band in the form of a one-time code generated on the mobile device;

said authorising authority being arranged to judge the allowability of the transaction and to issue a pre-authorisation to the mobile device and to flag the transaction as allowed or disallowed;

said mobile device communicating the one time code to the terminal;

said terminal responsive to receiving the one time code to communicate the one time code to the authorising authority on the first band;

said authorising authority responding to the terminal on the first band to allow or disallow the transaction according to the flag.

[011] By allowing or disallowing the transaction before the terminal is engaged the system obviates a waste of resources. For example in a shop environment the transaction is approved before the terminal is engaged so that refusal of a transaction does not delay or cause a que or publicly embarrass the card holder. Furthermore, the one time code and approval signal from the authorising authority does not need to contain any data which can be used by the vendor to identify the card holder. Because the one time card number is generated on the mobile device first and transmitted to the authorising authority via two bands interception and re-use is extremely difficult. One problem with existing security applications is that one time codes are pre-stored in batches on a mobile device, the mobile device application which controls the visibility of the codes is responsive to a password mediated security protocol. If the password can be obtained

or the security otherwise overcome the entire set of unused one time codes can be accessed.

[012] Mobile devices are commonly provided with input devices in the form of microphones and cameras as well as keypads. Preferably access to the card account module will be mediated by at least one of, or each of; a password or biometric. Biometrics may include at least: finger print, facial recognition, voice recognition or iris recognition.

[013] A transaction may be initiated by the card holder/user causing an application to execute on the mobile device. The application will call for the input of the biometric and/or a password before offering the card holder a selection of virtual cards representing the accounts installed in the card module. Selection of the desired card will cause the application to call for transaction data. Alternatively the transaction data may be input before the selection of the card. The application will then generate the one-time code incorporating the transaction data, and account data identifying the card holder's account to the authorising authority.

[014] Communication of the approved one-time code to the terminal may be by displaying the code on a device screen in the form of text, a bar code QR code or another visible machine readable image encoding the one time code. Alternatively the code may be

communicated via near field communication. In some cases the one time code may be manually input into the terminal.

[015] According to a second aspect of the present invention there is provided A transaction security system comprising:

a terminal capable of communicating with an authorising authority on a first band;

a mobile device capable of communication with an authorising authority on a second band and having;

a card module capable of storing transaction card account data for one or more transaction card accounts;

wherein said mobile device is adapted to;

acquire transaction data relating to a specific transaction,

transmit said transaction data to an authorising authority via said second band in the form of a one-time code generated on the mobile device;

said mobile device being responsive to communicate the one-time code to the terminal;

said terminal responsive to receiving the one-time code to communicate the one-time code to the authorising authority on the first band;

said authorising authority responding to the one-time code received on the first band to seek to match with a one-time code received within a predetermined period on the second band and responsive to matching such received one time codes to judge the transaction allowable;

said authorising authority responsive to judging a transaction allowable to communicate the judgement to the merchant’s terminal.

[016] Preferably the second aspect of the invention will include an authorising authority server responsive to the matching step failing to assess the risk of the requested transaction being fraudulent and if the risk is below a threshold risk to implement a routine where the one-time card numbers which could be calculated from received transaction data are calculated by the authorising authority. The static elements of the authorising authority calculated one time card numbers are compared to the one-time card number received from the merchant’s terminal, and only if the static elements of the one-time card numbers match, the authorising authority server judges the transaction allowable and proceeds to communicate the judgement to the merchant’s terminal.

Brief Description of Figures

[017] Embodiments of the system and method will now be described, by way of example only, with reference to the accompanying figures; in which,

Figure 1 is a diagram showing the elements of a first embodiment;

Figure 2 is a flowchart illustrating the steps implemented in the first embodiment;

Figure 3 is a diagram of a second embodiment of the system; and

Figure 4 is a flowchart of the steps of the second embodiment.

Detailed Description of the Figures

[018] Figure 1 diagrammatically illustrates a first embodiment of a system having a buyer 1 provided with a mobile device such as a smart phone 2 capable of communication over various bands including at least cellular mobile telephony such as GSM, CDMA or TDMA and their successors. A smart phone will also commonly be capable of communication over WiFi, Bluetooth™ and increasingly commonly will be near field communication (NFC) enabled. Cellular communication will be transmitted over a communications network 3.

[019] The system also includes an authorising authority 4. The authorising authority in this example comprises a buyer's bank 5 and a merchant's bank 6. In this example the

buyer’s bank and merchant’s bank are described as different organisations. However, in practice there will be transactions where they are the same organisation. These systems will be largely automated so the authorising authority should be understood as servers arranged to communicate and respond in accordance with the method described in more detail below.

[020] The system also includes a merchant’s terminal 7 arranged to communicate electronically over a network with the authorising authority via the merchant’s bank 6. It is an important feature of the system that the merchant’s terminal communicates using a first communications band 8 separate from a second communications band 9 used for communication between the mobile device 2 and the authorising authority 4.

[021] In the method of the first embodiment shown in the algorithm of figure 1B the buyer 1 or card holder will have a virtual payment card enabled in a wallet application capable of executing on the mobile device 2. At step S1 the card holder will choose the goods or services to buy.

[022] At step S2 the card holder will initiate the relevant wallet application and select one of the available accounts (cards) for the transaction. This will be achieved by means of a secured access protocol which requires the card holder to verify that they are

authorised to access the wallet and make purchases, in this case the protocol advantageously uses voice recognition to identify the user. This can be achieved by means of an appropriate predetermined phrase and by comparison of characteristic elements of the buyers voice. To prevent a recording of the authorised buyers voice being used to beat the security protocol may require the buyer to recite a changeable phrase read out onto the device or to recite the current date and time or the location which can be verified by the device’s on board clock or GPS. Unlike conventional voice recognition which requires access to the internet voice recognition will be implemented on board the mobile device. This is possible because the device is only required to recognise one voice using a limited range of phrases and instructions.

[023] Alternative biometrics such as facial recognition, iris recognition or fingerprint recognition may be used. If biometric voice recognition fails for any reason, for example because of a very noisy environment or because the buyer is unwell a conventional password/PIN code may be input.

[024] When the voice recognition is accepted voice instructions to select a specific card account are input by the buyer at S2.4.

[025] At step S3 the mobile device acquires the terms of the transaction from the merchant. This may be achieved in any of many ways including, for example:

[026] the buyer inputting the terms from the merchant,

[027] scanning a bar or QR code using the mobile devices on board camera,

[028] using an NFC, or IRFID tag on the goods,

[029] WiFi or Bluetooth® enabled communication with the merchant's terminal.

[030] At step S4 the mobile device generates a one-time code number (OTCN). The OTCN will comprise at least unique elements of the transaction data acquired such as

[031] prices, time and date,

[032] biometric data

[033] GPS coordinates.

[034] At step S4.3 the OTCN is transmitted from the mobile device 2 to the authorising authority, in this example to the buyers bank 5 by way of the second band 9.

[035] At step S4.4 the OTCN is communicated from the buyers mobile device 2 to the merchant's terminal 7.

[036] At step S5 the merchant's terminal communicates the OTCN to the authorising authority, in this case the merchant's bank 6 via the first band 6a. Where the merchant's bank 6 and the buyers bank are separate enterprises the merchant's bank will communicate the OTCN to the buyer's bank 5.

[037] At step S6 the buyer's bank will judge whether or not the terms of the transaction are acceptable. The first step in this process will be for the buyer's bank to seek to match the OTCN received on the first band with an OTCN received within a predetermined limited period on the second band. Reception of matching OTCN's is a very strong indication that the identity of the buyer and merchant have not been corrupted. If the OTCN's are matched and inspection of the buyers account indicates that the transaction matches the buyer's credit limits the transaction will be approved and this judgement will be communicated to the merchant's terminal at step 11. The transaction will then be reconciled with the merchant's account being credited and the buyer's account debited in the usual way.

In the event that the OTCN's are not matched, for example because there is a failure in the second communications band the procedure proceeds to step S9 where the value of the transaction is compared to a predetermined risk threshold determined primarily based on the value of the purchase, but potentially also on the nature of the goods or services and the location. For example certain GPS or merchant data may indicate that quality of service over the second band from that location is poor. If the transaction is judged below the threshold risk value the system proceeds to step S12 where the OTCN's possible from the received transaction data are calculated. At step S13 the possible OTCN's are compared with the OTCN received from the merchant, at step S14 the static elements of the received and possible OTCN's are compared and if they match the method proceeds to step S11 where transaction approval is judged and communicated to the merchant's terminal. If the OTCN's static data does not match the transaction is judged refused and the judgement communicated to the merchant's terminal at step S15.

[038] Figures 2A and 2B illustrate a second embodiment of the method in which similar elements of figure 2A are numbered similarly to the elements of figure 1A.

[039] The process of the second embodiment starts with step s101 where the card holder chooses the goods or services desired. At step S102 the terms of offer of sale are acquired by the mobile device.

[040] At step 103 the card holder selects the wallet using a voice recognition procedure similar to the first embodiment in which the voice biometric must be matched at step S103.1 for the card selection instruction to be processed successfully at step S103.2. If the biometric is not matched the process terminates.

[041] With the card successfully selected the process goes to step S104 where an offer of sale with details of terms is acquired.

[042] At step 104 the mobile device digitally signs the transaction data at S104a and then constructs a one-time card number from:

[043] the transaction data

[044] biometric security data

[045] global positioning data

[046] elements of the card account data

[047] At step S104c the mobile device transmits the OTCN to the authorising authority over the second band.

[048] At step S104c the mobile device communicates the OTCN to the merchant’s terminal by any one of:

a. manual input;

b. presentation of a graphic encoding the data on the device screen, eg a bar code, QR code, or text data;

c. Bluetooth® or WiFi

[049] The merchant’s terminal then transmits the OTCN to the authorising authority over the first band. at step S105.

[050] At step S106 the authorising authority judges the acceptability of the transaction, in particular the authorising authority judges the credibility of the transaction request by first seeking to match the OTCN received on the first band to any OTCN received on the second band during a predetermined period. If a match is found and the card holder’s account credit rating is acceptable the transaction is judged approved at S106.8 and the approval communicated to the merchant’s terminal at step S106.9.

[051] If no matching OTCN is found the process goes from S106.1 to S106.3 where the transaction risk is assessed . Transaction risk may be assessed on factors such as the value of the transaction, the reputation of the merchant, the nature of the goods or services being transacted as derived from the terms of sale. Certain goods or services are much less attractive to criminals than others.

[052] If the transaction risk is judged by the authorising authority server to exceed a threshold value at S106.3 the transaction proceeds to step 106.6 where the transaction refusal message is communicated to the merchant’s terminal over the first band and the transaction ends unsuccessfully.

[053] If the threshold risk is judged by the authorising authority server to be below the acceptable risk the authorising server proceeds to S106.4 and calculates the possible OTCN’s or at least the relevant static elements thereof from the transaction data. If the static elements of the OTCN calculated by the authorising authority server matches the static elements received from the merchant’s terminal at step 106.5 the process moves to step 106.8 where the transaction is judged approved and the judgement communicated to the merchant’s terminal at step 106.9.

[054] If the static elements do not match at step 106.5 the process moves to S106.6 where the transaction is judged refused and step S106.7 where the refusal is communicated to the merchant’s terminal.

CLAIMS

1. A transaction security system comprising:

a merchant’s terminal capable of communicating with a first authorising authority on a first band;

a mobile device capable of communication with an authorising authority on a second band and having;

a card module capable of storing transaction card account data for one or more transaction card accounts;

wherein said mobile device is adapted to;

acquire transaction data relating to a specific transaction,

transmit said transaction data to an authorising authority via said second band in the form of a one-time code generated on the mobile device;

said authorising authority being arranged to judge the allowability of the transaction and to issue a pre authorisation to the mobile device and to flag the transaction as allowed or disallowed;

said mobile device communicating the one-time code to the terminal;

said terminal responsive to receiving the one-time code to communicate the one-time code to the authorising authority on the first band;

said authorising authority responding to the terminal on the first band to allow or disallow the transaction according to the flag.

2. A transaction security system according to claim 1 wherein the one-time code is generated to include at least one or more unique elements comprising:

- price,
- time
- date
- biometric data
- GPS coordinates.

3. A transaction security system according to claim 1 or claim 2 wherein the one-time code includes static elements.

4. A transaction security system wherein the mobile device uses a secured access protocol to verify that the user is authorized to access a wallet application containing the card module.

5. A transaction security system according to claim 4 wherein the mobile device implements voice recognition to verify the user’s identity.

6. A transaction security system according to claim 5 wherein the voice recognition requires the user to recite a changeable phrase read out from the device or to recite the current: time, date or location.

7. A transaction security system according to any one of the preceding claims wherein the authorizing authority is responsive to a mismatch in the one-time codes received on the respective first and second bands to compare the value of the transaction to a predetermined risk threshold, said authorizing authority responsive to the threshold not being exceeded to calculate the possible one time codes from the received transaction data and to compare the static elements of the possible one time codes and the one-time codes received from the merchant, said system responding to a match to authorize the transaction.

Intellectual Property Office

Application No:	GB1520531.3	**Examiner:**	Mr David Maskery
Claims searched:	1 - 7	**Date of search:**	1 June 2017

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
Y	1 - 7	US 2003/0080183 A (RAJASEKARAN et AL) See paragraphs 37 - 46 and figs 4 - 6.
Y	1 - 7	US 2010/0131347 A (SARTIPI) See paragraphs 35 - 43 and fig 1.
Y	1 - 7	US 2010/0106649 A (ANNAN) See paragraphs 55 - 60 and fig 3.
Y	1 - 7	US 2009/0240626 A (HASSON et AL) See paragraphs 41 - 50 and 58 with figs 3a and 3b.
Y	1 - 7	US 2009/0254485 A (BAENTSCH et AL) See paragraphs 16 - 28 and 30 - 45.
Y	1 - 7	US 2012/0089514 A (KRAEMLING et AL) See paragraphs 78 - 82, 85, 98 - 106, 120 - 133 and 138.
Y	1 - 7	US 2012/0265688 A (DINAN) See paragraphs 14 - 18, 21 -23 and 31 - 35 with figs.
Y	4 - 6	US 2014/0279099 A (VOS et AL) See paragraph 101 and figs.
Y	4 - 6	WO 2014/145708 A (VISA INTERNATIONAL) See paragraph 5.
Y	4 - 6	US 2014/0058937 A (WATSON) See paragraph 16.

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	P	Document published on or after the declared priority date but before the filing date of this invention.

	same category.		
&	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

G06F; 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	0020/38	01/01/2012
G06F	0021/35	01/01/2013
G06F	0021/43	01/01/2013
G06Q	0020/32	01/01/2012
G06Q	0020/36	01/01/2012