HOST SERVER FOR AUTHORISING A TRANSACTION, COMPUTER PROCESS AND NETWORK

FIELD

[0001]The present disclosure relates to a host server for authorising a transaction, a transaction authorisation computer process performed using such a host server, and a network incorporating that host server.

BACKGROUND

[0002]Transaction fraud, such as credit and debit card fraud, is an increasingly common event. Potentially fraudulent transactions can either be identified before authorising a particular transaction, or after the transaction.

[0003]Oftentimes, parties to a transaction cannot be identified retrospectively. As a result, once a past transaction is alleged to have been fraudulently made, credit and debit card companies must analyse transaction information to assess whether the transaction was in fact fraudulent. For example, a credit or debit card company may assess whether the transaction was made with a merchant from whom the cardholder does not purchase, or whether purchased products differ from those the cardholder routinely buys and, if so, assume the transaction to be fraudulent. However, credit and debit card companies typically have little recourse to positively identify parties to a particular transaction.

[0004]Additional security measures are also in place for determining, at the time of a transaction, whether the transaction is potentially fraudulent. These include requesting confirmation, for example by contacting the cardholder's smartphone, for making transactions at particular providers or where the transaction has a value above a set threshold.

[0005]Despite the above measures, there are very few mechanisms for identifying potentially fraudulent transactions at the time a transaction is made, or retrospectively upon a cardholder asserting fraud has taken place, where the relevant transaction is one it is reasonable to expect the cardholder may make. For

example, where a fraudulent transaction occurs at a merchant of a type the cardholder may occasionally visit, it is difficult to confirm its fraudulent nature.

[0006]It is desirable therefore to provide an improved system and computer process for identifying potentially fraudulent transactions, or at least to provide a useful alternative.

SUMMARY

[0007]The present disclosure provides a host server for authorising a transaction, comprising:

a processor; and

a memory device in communication with the processor and storing program instructions thereon, the processor operative with the program instructions:

to receive, from one or more transaction terminals, transaction information comprising one or more transactions and, for each said transaction:

to receive:

payment vehicle credentials of a payment vehicle used to make the transaction;

a time at which the transaction was made; and

a transaction terminal location of the transaction terminal at which the transaction was made,

and, for each transaction:

to fetch from a database, the database comprising one or more stored payment vehicle credentials associated with a respective mobile device identifier, a mobile device identifier associated with the payment vehicle credentials;

to receive, from a mobile device management server, location data for a mobile device associated with the mobile device identifier and identifying a location of the mobile device at the time at which the transaction was made; and

to determine whether the transaction terminal location matches the location of the mobile device ("**location matching**") and:

decline authorisation of the transaction if the transaction terminal location does not match the location of the mobile device; and

authorise the transaction if the transaction terminal location matches the location of the mobile device.

[0008]The present disclosure further provides a transaction authorisation computer process comprising:

receiving, at a host server and from one or more transaction terminals, transaction information comprising one or more transactions and, for each said transaction:

receiving:

payment vehicle credentials of a payment vehicle used to make the transaction;

a time at which the transaction was made; and

a transaction terminal location of the transaction terminal at which the transaction was made;

fetching, from a database comprising one or more stored payment vehicle credentials associated with a respective mobile device identifier, a mobile device identifier associated with the payment vehicle credentials;

receiving, at the host server, location data from a mobile device management server, the location data being for a mobile device associated with the mobile device identifier and identifying a location of the mobile device at the time at which the transaction was made; and

determining, at the host server, whether the transaction terminal location matches the location of the mobile device ("**location matching**") and:

declining authorisation of the transaction if the transaction terminal location does not match the location of the mobile device; and

authorising the transaction if the transaction terminal location matches the location of the mobile device.

[0009]The present disclosure also provides a network for authorising a transaction, comprising:

a host server;

one or more transaction terminals;

a database; and

a mobile device manager server,

wherein the host server comprises:

a processor; and

a memory device in communication with the processor and storing program instructions thereon, the processor operative with the program instructions:

to receive, from the one or more transaction terminals, transaction information comprising one or more transactions and, for each said transaction:

to receive:

payment vehicle credentials of a payment vehicle used to make the transaction;

a time at which the transaction was made; and

a transaction terminal location of the transaction terminal at which the transaction was made;

to fetch from the database, the database comprising one or more stored payment vehicle credentials associated with a respective mobile device identifier, a mobile device identifier associated with the payment vehicle credentials;

to receive, from the mobile device management server, location data for a mobile device associated with the mobile device identifier and identifying a location of the mobile device at the time at which the transaction was made; and

to determine whether the transaction terminal location matches the location of the mobile device ("**location matching**") and:

decline authorisation of the transaction if the transaction terminal location does not match the location of the mobile device; and

authorise the transaction if the transaction terminal location matches the location of the mobile device.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010]Some embodiments of the invention will now be described by way of non-limiting example only, with reference to the accompanying drawings in which:

[0011]Figure 1 is a method for authorising a transaction in accordance with present teachings;

[0012]Figure 2 is a schematic diagram of a distributed network architecture or network for performing methods described herein, including the methods of Figures 1, 3, 4 and 7;

[0013]Figure 3 is a method for authorising a transaction in accordance with present teachings;

[0014]Figure 4 is a method for authorising a transaction in accordance with present teachings, including steps for checking the balance of a payment vehicle;

[0015]Figure 5 is a method for deactivating location matching in accordance with present teachings;

[0016]Figure 6 is a method for authorising a transaction in accordance with present teachings, including steps for determining whether location matching should be performed;

[0017]Figure 7 is a method for authorising a transaction in accordance with present teachings, including steps for querying whether a past transaction is fraudulent or otherwise;

[0018]Figure 8 is a method for reactivating/activating location matching in accordance with present teachings;

[0019]Figure 9 is a schematic diagram of an example of a server of Figure 2;

[0020]Figure 10 is a schematic diagram of an example of a transaction system of Figure 2;

[0021]Figure 11 is a schematic diagram of an example of a mobile device of Figure 2; and

[0022]Figure 12 is a schematic diagram of an embodiment of a network for implementing the computer processes described herein.

DETAILED DESCRIPTION

[0023]An example of a method for performing a transaction will now be described with reference to Figures 1 and 3 to 8.

[0024]For the purpose of these examples, it is assumed that the transactions are performed in part utilising one or more client devices (e.g. mobile devices such as smart phones, personal digital assistants, laptops etc) that in use interact with one or more payment processing devices (e.g. transaction terminals such as EFTPOS machines, ATMs etc). The payment processing device(s) are typically part of one or more processing systems, such as one or more servers, and may form part of a payment network backend, or similar. For the following description, reference will generally be made to a single transaction terminal, but it will be appreciated that the functionality performed by the payment transaction terminal could in practice be distributed across multiple terminals and reference to a single device is not intended to be limiting.

[0025] A transaction authorisation computer process 100 in accordance with the present disclosure is represented in Figure 1. The process 100 can enable a transaction to be identified as potentially fraudulent or, alternatively, likely valid, based on a user's (i.e. a cardholder's) mobile device being in the vicinity of a terminal on which the transaction is being performed. This ensures that in the event of theft of credit card, debit card and other payment card details, the thief cannot use those details to make transactions on a terminal unless the authentic cardholder's mobile device (e.g. smart phone) is also in the vicinity of the same terminal.

[0026]Similarly, the process 100 can also be used in the event that a user contests the nature of a transaction as being fraudulent on the basis that they did not perform the transaction. In such cases, the process 100 can enable the suspect transaction

to be analysed to determine whether the user was in the vicinity of the terminal on which the transaction was performed at the time the transaction was performed.

[0027]The process 100, which may interchangeably be referred to as a method, broadly comprises:

Step 102: receiving transaction information;
Step 104: identifying a mobile device identifier;
Step 106: receiving location data;
Step 108: location matching;
Step 108a: declining authorisation of the transaction; and
Step 108b: authorising the transaction.

[0028]The process 100 commences upon initiation of a transaction – Step 101. Initiation may be a user or cardholder attempting to make a transaction at the transaction terminal, such as an ATM or EFTPOS terminal, through an online platform or through any other appropriate transaction terminal.

[0029]On initiation of a transaction, transaction information is received – Step 102. With reference to Figure 2, the transaction information is typically sent from one or more transaction terminals 202 (202a, 202b,…, 202n) to host server 204.

[0030]The transaction information itself comprises one or more transactions. In this context, a transaction, since it is sent digitally, typically comprises a plurality of data elements collectively uniquely identifying the transaction. Presently, each transaction comprises payment vehicle credentials of a payment vehicle used to make the transaction, a time at which the transaction was made, and a transaction terminal location of the transaction terminal at which the transaction was made. The one or more transactions referred to herein are transaction for which location matching is performed. The skilled person will appreciate the transaction information may further comprise one or more ‘further transactions’ for which location matching is not performed.

[0031]A "payment vehicle" may be a credit card, debit card, virtual credit or debit card, loyalty rewards card, or any other suitable payment vehicle. Similarly, "payment

vehicle credentials" are the values such as credit or debit card number, expiry date, card verification value (CVV) and other information, such as that which would typically be displayed on a physical card.

[0032]The transaction terminal location may be determined in a number of ways. In some cases, latitude and longitude coordinates are supplied with, or as part of, each transaction. In other cases, unique identification numbers may be provided. For example, International Standard Organisation (ISO) has defined a set of data elements that uniquely identify the location of an entity that can accept particular payment vehicle (e.g. card) payments. These include:

- data element (DE) 41 - card except terminal identification;
- DE 42 - card accepted identification code; and
- DE 43 - card except the name/location.

[0033]In any case, the transaction terminal location should be sufficient to uniquely identify a particular transaction terminal (such as an ATM, electronic funds transfer point of sale (EFTPOS) machine, or other relevant card-accepting device) or to identify the general location of one or more transaction terminals. For example, mobile EFTPOS machines can sometimes be transported from one place of business to another and thus uniquely identifying the particular machine is insufficient to identify the actual location of that machine. In such cases, a mobile telecommunications tower identifier, or an identifier relating to some other fixed infrastructure, may be used as the transaction terminal location. This means that transaction is made through such a card-accepting device will be authorised, per step 108b, provided the relevant mobile device is connected to the same fixed infrastructure.

[0034]In some cases, the mobile device may be connected to different fixed infrastructure to that to which the transaction terminal is connected, provided the fixed infrastructure is sufficiently near the transaction terminal that it can be assumed the user of the mobile device is in the vicinity of the transaction terminal. This may occur where, for example, a mobile device preferentially connects to a particular mobile tower operated by a first mobile telecommunications service provider, and a

transaction terminal preferentially connects to a different mobile tower operated by a second mobile telecommunications service provider that is different from the mobile tower operated by the first mobile telecommunications service provider.

[0035]Step 104 involves identifying a mobile device identifier associated with the payment vehicle credentials. Typically, a user's mobile device will be a smart phone, personal digital assistant or other readily transportable mobile device. In the case of a smart phone, the mobile device identifier will be the telephone number for that smart phone. The mobile device identifier that uniquely identifies a particular mobile device.

[0036]The mobile device identifier is fetched from a database (see 206 in Figure 2) comprising one or more stored payment vehicle credentials - it shall be taken to include individual payment vehicle credentials, such as a credit card number, and also to include sets of payment vehicle credentials such as a credit card number, associated expiry date of that credit card, CVV and so on. Each of the one or more stored payment vehicle credentials is associated with a respective mobile device identifier. Thus Step 104 can be performed by the host server 204 querying, or fetching from, the database 206 using the payment vehicle credentials in order to identify the mobile device identifier with which this payment vehicle credentials are associated.

[0037]Notably, an association between payment vehicle credentials and the mobile device identifier may be directly associated. For example, the payment vehicle credentials and the mobile device identifier may be linked, or otherwise stored together, in the database 206. Alternatively, the payment vehicle credentials and the mobile device identifier may be indirectly associated. For example, the payment vehicle credentials may be associated with other information such as a user's name, a particular address or account (such as a bank account, loyalty rewards account or other type of account), and the mobile device identifier may be associated that same other information in the database 206.

[0038]Step 106 involves receiving location data for a mobile device associated with the mobile device identifier identified at Step 104. The location data is received at all by the host server 204, and is sent from a mobile device management server 208.

[0039]The location data for the particular mobile device identifier, identifies a location of the mobile device at the time at which the transaction was made. To achieve this, a user's mobile device 210 may be in communication with the mobile device management server 208 and send to the mobile device management server 208 GPS data or other data indicating a location of the mobile device 210. The mobile device management server 208 may therefore track the location of the mobile device 210 over time.

[0040]The mobile device 210 may comprise an app used to obtain GPS or other mobile location tracking data and send it to the mobile device management server 208. Such an app may also be used to activate and deactivate the location matching functions as described with reference to Step 108.

[0041]While the host server 204 may simply receive location data for the mobile device 210 from the mobile device management server 208 in real time, the host server 204 may instead send a location capture request to the mobile device management server 208 is shown in Figure 3.

[0042]In Figure 3 Steps 301, 302, 304 and 308 (and Sub-Steps 308a and 308b) are essentially the same as Steps 101, 102, 104 and 108 (and Sub-Steps 108a and 108b) respectively, the descriptions for which are supplied with reference to Figure 1. Step 106, however, has been broken down into two Sub- Steps 306a and 306b. These Sub-Steps (which are still, of themselves, steps) are:

Step 306a – sending a location capture request; and
Step 306b – receiving the location data.

[0043]The location capture request sent at Step 306a is a request for information on the location of the mobile device at the time the transaction was made. To that end, the location capture request may comprise the mobile device identifier identified at Step 104 and the time at which the transaction was made, and/or any other information usable by the mobile device management server 208 to extract, or fetch, the relevant location data from a database 212 in which it is stored.

[0044]The host server 204 may send the location capture request to a mobile device management server 208. The mobile device management server 208 may be hosted by, and interface with, a mobile app installed on the mobile device 210, the mobile app providing mobile device location information to the mobile device management server 208. Alternatively, the mobile device management server 208 may be installed or otherwise provided on the mobile device 210 itself, or at any other appropriate location within any other appropriate device. Similarly, the host server 204 may send the location capture request to the mobile device 210, and the mobile device 210 upon receiving that request may forward it to the mobile device management server 208 which subsequently sends the relevant information to the host server 204.

[0045]In the present embodiment, in response to receiving the location capture request the host server 204 receives, from the mobile device management server 208, the location data for the mobile device, that location data including the location of the mobile device at the time at which the transaction was made.

[0046]Step 108 involves determining whether the transaction terminal location matches the location of the mobile device. This is called "location matching" and is performed at the host server. As discussed above, the mobile device 210 may be in the vicinity of the transaction terminal 202 at the time at which the transaction was made. Despite this, the mobile device 210 may nevertheless be connected to different fixed infrastructure than the transaction terminal 202. The mobile device 210 may therefore appear to be in a different location to that of the transaction terminal 202. To this end, what constitutes an acceptable "match" when performing location matching may not involve an exact one-to-one correspondence between the recorded location of the mobile device 210 and the location of the transaction terminal 202 at the time the transaction was made. In other words, a "match" may be an exact match, or may be an inexact match.

[0047]On the one hand, where the location of the mobile device 210 at the time the transaction was made, as identified in the location data, is the same as the transaction terminal location, the locations will match. On the other hand, where the location of the mobile device 210 at the time the transaction was made differs from the location of the transaction terminal 202 at the time the transaction was made, the

host server 204 may determine whether the location of the mobile device to 100 is within a predetermined range or distance of the transaction terminal location. If so, the host server will authorise the transaction per Step 208b. If not, the host server will decline authorisation of the transaction per Step 208a. The predetermined distance may also depend on the relative vicinity of fixed infrastructure. For example, the predetermined distance may be or relate to the distance between a mobile telecommunications tower to which the mobile device 210 is connected and a Wi-Fi connection to which a transaction terminal 202 is connected.

[0048]On this basis, the host server 204 declines authorisation of the transaction if the transaction terminal location does not match the location of the mobile device 210 – Step108a, and authorises the transaction if the transaction terminal location matches the location of the mobile device.

[0049]The ability for a cardholder to make a transaction may depend not only whether the cardholder is the authentic owner or holder of a particular payment card, but also on the balance of that payment card. In such cases, the payment vehicle has an available balance for use in processing the transaction. Thus authorising the transaction may comprise determining if the value of the transaction is at most equal to the available balance of the payment vehicle.

[0050]In order to perform this check, each transaction may comprise a transaction value. The transaction value may be the cost of all items in the relevant basket, may be the cost of all items plus goods and services tax or any other taxes and levies, and may include shipping and other additional costs. The cheque may be performed by the host server 204, a server of a card issuer (which may be the host server 204), or any other appropriate party that has access to the available balance of the payment vehicle and the transaction value.

[0051]Checking the balance of the payment vehicle may be performed before Step 104, after Step 108, 108a, 108b, or at any other appropriate time. This is illustrated in Figure 4 in which Steps 401, 402, 404, 406 and 408 (including Sub-Steps 408a and 408b) are essentially the same as Steps 101, 102, 104, 106 and 108 (including Sub-Steps 108a and 108b) respectively, the descriptions which are provided with reference to Figure 1.

[0052]In Figure 4 Step 410 provides for a balance check. The balanced check may be performed when the transaction is initiated at Step 401, or at any other appropriate time. If the available balance of the payment vehicle is at least sufficient, or at least as high as, the transaction value of the transaction then after Step 410 the process 400 returns back to the Steps performed as shown in Figures 1 and 3. In other words if, after Step 402, balanced check Step 410 is performed and the available balance of the payment vehicle is at least as much as the transaction value, then Step 404 is performed and process 400 continues as usual.

[0053]Figure 6 illustrates a circumstance in which the processes 100, 300, 400 and so on, as disclosed herein, may be used both for users for whom location matching should be performed when determining whether a transaction is able to be authorised, along with users for whom location matching should not be performed or is otherwise undesirable to perform. In Figure 6 Steps 601, 602, 604, 606 and 608 (including Sub-Steps 608a and 608b) are essentially the same as Steps 101, 102, 104, 106 and 108 (including Sub-Steps 108a and 108b) respectively, the descriptions which are provided with reference to Figure 1.

[0054]It may be that it is inconvenient or otherwise undesired for some people to use location matching as a security measure in the determination of whether a transaction should or should not be authorised. The host server 204 may therefore query a database, such as database 206, to determine whether location matching has been activated for a particular user per Step 605. To facilitate this, a user or cardholder may have an account. The account may be hosted by the issuer, such as a credit card or debit card account, and acquirer account such as a deposit account or credit account with a particular bank or a loyalty or awards program account with particular loyalty or awards program host, or any other relevant account.

[0055]The mobile device identifier and payment vehicle credentials may therefore be associated with the account in order to determine whether location matching has been activated for the particular user or cardholder. Again, direct or indirect association may be used. For example, the payment vehicle credentials may be directly associated with the account in the case that the account is a credit card account and the payment vehicle is the associated credit card. In this case, the

mobile device identifier may be used by, for example, providing the mobile device identifier which can then be used by the credit card issuer to identify the relevant payment vehicle and/or credit card account by identifying the user associated with that mobile device identifier. Thus the mobile device identifier may be indirectly associated with the relevant account.

[0056]Thus details ascertained at step 102 and/or 104 may be used to identify the relevant account by their association with that account. Location matching then only occurs for a council which location matching is activated. In other words, the host server 204 determines whether location matching is activated for the account at Step 605. If location matching is activated, the host of the 206 performs Step 608, and by virtue of that, Step/Sub-Step 608a or 608b. If, however, location matching is deactivated the host server 204 authorises the transaction per Step 608b. Again, authorising a transaction per Step 608b does not mean processing the transaction. Instead, authorisation simply means it passes the location matching test per Step 608 (including Sub-Step 608b) and can thus proceed for further processing such as balance checks, other security tests and so on. Moreover, in the event that a location matching has not been activated or has otherwise been deactivated, the present process 600 must automatically authorise the transaction per Step 608b. If this is not performed, it is possible that every transaction may fail Step 608. This would mean that every transaction performed by a party for whom location matching has been deactivated, or is otherwise yet to be activated, would be declined. This is clearly undesirable.

[0057]It is also often the case that telephones become broken or otherwise unworkable, lost or stolen. In these cases it would be very inconvenient for an authentic cardholder or user to be unable to perform transactions using their payment vehicle is if the telephone cannot indicate the authenticity of the cardholder or user or cannot indicate its own location.

[0058]In the event that the cardholder or user does not have their mobile device 210 with them, or it is otherwise incapable of being used to identify its own location for the sake of authorising valid transactions, the cardholder or user may use a transaction terminal to deactivate location matching. This process, process 500, is illustrated in Figure 5.

[0059]The process 500 broadly comprises:

Step 502 – sending/receiving a deactivation request;
Step 504 – deactivating location matching for the user's account.

[0060]In the present embodiment, the "transaction terminal" is the terminal used to initiate Step 502 of process 500. It is not necessarily a terminal used for making payments, such as an EFTPOS terminal or ATM, but may be a user's mobile device 210. Accordingly, the transaction terminal used for the activation may or may not be the same as a transaction terminal used to perform, for example, a purchase transaction. For example, the transaction terminal use the deactivation may be an automatic teller machine (ATM).

[0061]The account in respect of which location matching has been either activated or not activated/deactivated, may also be hosted by the mobile device management server 208. Thus, upon a deactivation request being sent by the transaction terminal in accordance with Step 502 of process 500, and thus received by the mobile device management server 208, the mobile device management server deactivate location matching for the account in accordance with Step 504.

[0062]Thus in accordance with process 500, where location matching has been activated for a particular account, the mobile device management server 208 will supply to the host server 204 the location data for the mobile device associated with the mobile device identifier. Where location matching has been deactivated, or otherwise not yet activated, for a particular account, the mobile device management server 208 will supply to the host server 204 an approval flag or other token (e.g. indicating that location matching has not been activated or is otherwise inactive for the relevant account) they can be used by the host server 204 to authorise transactions in line with Step 108b in all cases. The mobile device management server 208 may also supply a universal location or token that will prove true when location matching is performed by the host server 204 in accordance with Step 108, in all cases.

[0063]The host server 204 is therefore also capable of receiving a deactivation request from the transaction terminal. As its name suggests, the deactivation request

is a request to deactivate location matching for a particular mobile device 210. In response to receiving the deactivation request, the host server 204 deactivate location matching for the account. When the host server 204 subsequently receives a transaction, comprising the information as set out above in relation to Step 102, the transaction will automatically be authorised insofar as it will automatically pass the security test comprising location matching.

[0064]Notably, in this sense, authorising a transaction may either result in the transaction actually being processed or, alternatively, authorising a transaction may simply mean that it has passed the location matching test and is thus submitted for further processing such as further security steps, payment vehicle balance tests and any other tests. In some embodiments, any such further processing may have been performed in advance of the location matching steps.

[0065]A deactivation request may also be sent from the mobile device 210, and received by the host server 204, or from any other appropriate or authorised device for making such requests.

[0066]Conversely, Figure 8 illustrates a process for activating location matching for a particular account, or reactivating location matching where location matching has been previously deactivated. The process 800 broadly comprises:

> Step 802 – sending/receiving a activation/reactivation request;
> Step 804 – activating/reactivating location matching for the user's account.

[0067]It will be understood that there steps are essentially the same as Steps 502 and 504, with the exception that they result in the activation of location matching and thus the processes 100, 300, 400 and 600 may subsequently be performed. Notably, it may be possible to affect process 700 for accounts for which location matching is not activated. In other words, location matching may be automatically performed if location matching is activated for a particular account, at the time a transaction is sought to be made, but may be performed on request in accordance with Figure 700 on occasions where the nature of a transaction – i.e. whether or not it is potentially fraudulent – is queried.

[0068]Processes 100, 300, 400 and 600 may be performed at the time a transaction is desired to be made. In these cases, location matching will either enable the transaction to be processed or, if location matching is unsuccessful, result in declination of the transaction. In other words, the transaction will not be processed. Processes 100, 300, 400 and 600 may alternatively be performed at some future date when the validity of a transaction is brought into question. For example, a cardholder or user may assert that a transaction was fraudulently made and that they are thus not liable the funds paid to process that transaction. In these cases, it will be necessary to consult historical data to ascertain relevant information by which an assessment can be made of the nature, fraudulent or otherwise, of the transaction.

[0069]The processes 100, 300, 400 and 600 may be adapted in accordance with process 700 of Figure 7, in order to facilitate checking of the nature of a transaction at some point after the transaction has been made. For ease of illustration, process 700 uses process 100 as a base. However, any other one of processes 300, 400 and 600 may be used. Moreover, the processes, examples and embodiments described herein may be modified without departing from the scope of the present disclosure. For example, a feature may be taken will be moved from one embodiment or process and substituted for a relevant feature or features from another embodiment of process, or features from one embodiment of process may be added to those of another, without departing from the scope of the present disclosure.

[0070]In Figure 7, Steps 701 and 702 are essentially the same as steps 101 and 102 of process 100 of Figure 1. However, in process 700, rather than progressing to mobile device identification step, Step 704, the transaction information is stored per Step 703. That transaction information may be stored in a first database, such as database 206 of Figure 2. Thus the transaction information may be called upon once a transaction is brought into question in future.

[0071]Similarly, location data is sent from the mobile device 210 to the mobile device management server 208 and is thus received by the mobile device management server 208 in accordance with Step 705, and stored in a second database, such as database 212, in accordance with Step 707. The second

database may be the same as the first database. Alternatively, the second database may be a different database.

[0072]The location data may be continuously sent, such that the location data tracks the position of movement of the mobile device 210 at all times. In some cases, such as when a mobile device 210 is used for making payment, the mobile device 210 may send location data to the mobile device management server 208 at the time a transaction is made. Accordingly, the location of the mobile device 210 need not be continuously tracked. In other cases, when a transaction is made, any of the parties in a normal four-party transaction process (i.e. merchant, acquire, payment scheme and issuer) may identify the mobile device identifier in accordance with Step 104, 304, 404 or 704 and sent notice to the mobile device management server 208 but it should capture the location of the mobile device 210. Where the location data for the mobile device 210 is continuously sent from the mobile device 210 to the mobile device management server 208, the mobile device management server 208 need only store the most recent location data for the mobile device 210. Alternatively, the mobile device management server 208 may send a request for location data to the mobile device 210. The mobile device 210 then responds by providing the relevant location data to the mobile device management server 208, which then stores that data in accordance with Step 707. Where location data is sent or otherwise captured at the time a transaction is made, that location data may be stored with the transaction information in the first memory, second memory, different memories or in accordance with any other storage format or protocol.

[0073]Once a user, cardholder, issuer or any other party identifies a particular transaction as potentially fraudulent and not made by the user or cardholder, that party may question the validity of the transaction. In some cases, a user or cardholder will have legitimately not made the transaction. In other cases, the user or cardholder may have forgotten that they did indeed make the transaction, or may be attempting to fraudulently gain reimbursement for a transaction they consciously made. In such cases, it can be difficult for a payment vehicle issuer, acquirer or body for investigating fraud to determine whether or not the user or cardholder is being truthful.

[0074]Based on the relative proximity of the user or cardholder's mobile device to the location at which the transaction was made could assist in at least identifying cases where the cardholder or user was indeed near or at the transaction terminal at the time the transaction was made.

[0075]To enable a processed transaction to be retrospectively queried, process 700 additionally, broadly, comprises:

Step 709 - receiving a request for review of the transaction;
Step 711 – matching the candidate fraudulent transaction identifier to a transaction identifier;
Step 704 - identifying a mobile device identifier;
Step 706 - receiving location data;
Step 708 - performing location matching; and
Step 708a - declining the transaction; or
Step 708b - authorising the transaction.

[0076]Step 709 involves receiving a request for review of the transaction from the mobile device 210, a transaction terminal 202, or any other device or system that is authorised to question the validity or nature, fraudulent or otherwise, of transactions. The request is a request for review of a candidate fraudulent transaction. To facilitate identification of the transaction, the request comprises a candidate fraudulent transaction identifier. The candidate fraudulent transaction identifier may be a receipt number for the transaction, a combination of credit card number and date and time on which the relevant transaction was made, or any other combination of information that enables a particular transaction to be uniquely identified. Similarly, to facilitate the future identification of a transaction, each transaction, when made, will similarly comprise a transaction identifier such as a receipt number or combination of features such as a payment vehicle credentials and a time at which the transaction was made. Accordingly, each transaction comprises a transaction identifier which made the different from the payment vehicle credentials, time at which the transaction was made and transaction terminal location as discussed above, or may alternatively be a combination of one or more of those pieces of information and potentially one or more additional pieces of information.

[0077]After the candidate fraudulent transaction identifier received, the host server 204 matches the candidate fraudulent transaction identifier to the transaction identifier of a suspect transaction – Step 711. A suspect transaction is one of the one or more transactions that have been stored in database 206. Thus host server 204 queries database 206 to identify the relevant suspect transaction by comparing the fraudulent transaction identifier to transaction identifiers of transactions the information for which is stored in database 206.

[0078]Locating the relevant suspect transaction enables the additional steps of processes 100, 300, 400 to take place. In particular, after identifying the suspect transaction the host server 204 fetches, from the database 206, the mobile device identifier of a mobile device associated with the suspect transaction. With reference to Step 104, the mobile device identifier associated with the payment vehicle credentials is identified by identifying the mobile device identifier of the suspect transaction – Step 704. Inherently, the mobile device identifier of the suspect transaction will be associated with the payment vehicle credentials of the payment vehicle used to affect that transaction. Thus, the host server 204 identifies the mobile device identifier for the relevant suspect transaction in the same manner as mobile device identifiers are identified for transactions in accordance with Step 104

[0079]Location data is then received by the host server 204 from the mobile device management server 208 – Step 706. This may be achieved by the host server 20 for sending a request for location data to the mobile device management server 208, and that request may contain the suspect transaction identifier, a time at which the suspect transaction was made, and/or any other relevant information to enable the mobile device management server to respond with the necessary location data. That location data may identify the location of the mobile device over a continuous period of time, including the time at which the transaction was made, and the host server 204 will then need to identify, based on the type which the transaction was made, the relevant location of the mobile device. Alternatively, the mobile device management server 208 may identify the location of the mobile device based on the time at which the transaction was made, or based on the suspect transaction identifier in cases where the location of the mobile device is only stored at the time a transaction is made, and respond to the host server 204 with only the relevant location data.

[0080]The host server 204 then determines whether the transaction terminal location matches the location of the mobile device at the time the suspect transaction was made – Step 708. This is performed in accordance with Step 106, 306, or 406 as described above. Subsequently, the suspect transaction is either confirmed as being potentially fraudulent or potentially valid. This is achieved by performing the same process as is performed in Steps 108a, 108b, 308a, 308b, 408a, 408b. In other words, at Step 708a "declining authorisation of the transaction" comprises confirming the suspect transaction is potentially fraudulent, and at Step 708b "authorising the transaction" comprises confirming the suspect transaction is potentially valid.

[0081]As discussed above, a potentially fraudulent transaction is one in respect of which the payment vehicle and the mobile device of the cardholder or user were not co-located or within a predetermined distance of each other at the time the transaction was made. Similarly, a potentially valid transaction is one in respect of which the payment vehicle and the mobile device of the cardholder or user were co-located or within a predetermined distance of each other at the time the transaction was made.

[0082]In this example, the network 200 comprises:

a host server 204;

one or more transaction terminals 202 (comprising individual transaction terminals 202a, 202b,…, 202n where a plurality of transaction terminals are provided);

a database, comprising memory or databases 206, 212; and

a mobile device management server 208.

[0082]The network 200 is designed and configured to interact with mobile devices 210. Each of the elements 202, 204, 206, 208, 210 and 212 may be hardwired or otherwise coupled, via one or more communications networks 214, such as the internet, landline telephone network, pain old telephone services (POTS), mobile or cellular network and/or a number of local area networks (LANs).

[0083] In some examples, the mobile devices may be touchtone telephones, smart phones or any other device capable of ascertaining its location.

[0084] It will be appreciated that any number of servers 204, 208 and similarly any number transaction terminals 202 and mobile devices 210 could be provided, and the current representation is for the purpose of illustration only. Similarly, each server 204, 208 and database 206, 212 may comprise a single physical device or system, or may comprise multiple processors, servers, memories, databases and the like, co-located or distributed across multiple geographical locations, such as using a cloud based environment.

[0085] The configuration of the network 214 is also for the purpose of example only, and in practice the servers 204, 208, transaction terminals 202, databases 206, 212, mobile device manager 208 and mobile devices 210 can communicate via any appropriate mechanism, such as via wired or wireless connections, including, but not limited to mobile networks, private networks, such as an 802.11 networks, the Internet, LANs, WANs, or the like, as well as via direct or point-to-point connections, such as Bluetooth, or the like.

[0086] In use, the servers 204, 208 are adapted to be perform various data processing tasks forming part of a computer process for authorising a transaction, and the particular functionality will vary depending on the particular requirements. For example, the processing systems can be adapted to determine transaction details (e.g. payment vehicle credentials, time (including date and time) at which a transaction was made etc), determine transaction values, perform authentication, perform payments, or cause further payment processing devices (not shown), such as servers of financial institutions, payment gateways or the like, to perform payments, as will be appreciated by persons skilled in the art.

[0087] Whilst the servers 204, 208 are shown as single entities, it will be appreciated they could include a number of processing systems distributed over a number of geographically separate locations, for example as part of a cloud based environment. Thus, the above described arrangements are not essential and other suitable configurations could be used.

[0088] An example of a suitable server 204, 208 is shown in Figure 9. In this example, the server 204, 208 includes at least one microprocessor 900, a memory 906, an optional input/output device 902, such as a keyboard and/or display, and an external interface 908, interconnected via a bus 904 as shown. In this example the external interface 908 can be utilised for connecting the server 204, 208 to peripheral devices, such as the communications network 214, databases 206, 212, other storage devices, or the like. Although a single external interface 908 is shown, this is for the purpose of example only, and in practice multiple interfaces using various methods (eg. Ethernet, serial, USB, wireless or the like) may be provided.

[0089] In use, the microprocessor (or processor) 900 executes instructions in the form of applications software stored in the memory 906 to allow the required processes to be performed. The applications software may include one or more software modules, and may be executed in a suitable execution environment, such as an operating system environment, or the like.

[0090] Accordingly, it will be appreciated that the server 204, 208 may be formed from any suitable processing system, such as a suitably programmed PC, web server, network server, or the like. In one particular example, the server 204, 208 is a standard processing system such as an Intel Architecture based processing system, which executes software applications stored on non-volatile (e.g., hard disk) storage, although this is not essential. However, it will also be understood that the processing system could be any electronic processing device such as a microprocessor, microchip processor, logic gate configuration, firmware optionally associated with implementing logic such as an FPGA (Field Programmable Gate Array), or any other electronic device, system or arrangement.

[0091] In this configuration, the host server 204 thus comprises a processor 900 and a memory device 906. The memory device 206 is in communication with the processor 900 and stores program instructions. The processor 900 is thus operative with the program instructions to perform the steps of (A) receiving, from the one or more transaction terminals, transaction information comprising one or more transactions and, for each said transaction: payment vehicle credentials of a payment vehicle used to make the transaction; a time at which the transaction was made; and a transaction

terminal location of the transaction terminal at which the transaction was made. For each transaction, the processor (B) fetches from a database (e.g. database 206, 212), the database comprising one or more stored payment vehicle credentials associated with a respective mobile device identifier (this enables, e.g., identification of the mobile device identifier using the payment vehicle credentials), a mobile device identifier associated with the payment vehicle credentials, (C) receives, from a mobile device management server, location data for a mobile device associated with the mobile device identifier and identifying a location of the mobile device at the time at which the transaction was made, and (D) determines whether the transaction terminal location matches the location of the mobile device ("location matching"). The processor then (D1) declines authorisation of the transaction if the transaction terminal location does not match the location of the mobile device, or (D2) authorises the transaction if the transaction terminal location matches the location of the mobile device.

[0092] As shown in Figure 10, in one example, the transaction terminal 202 includes at least one microprocessor 1000, a memory 1006, an input/output device 1002, such as a keyboard and/or display, and an external interface 1008, interconnected via a bus 1004 as shown. In this example the external interface 1008 can be utilised for connecting the transaction terminal 202 to peripheral devices, such as the communications network 214, databases 206, 212, other storage devices, the mobile device 210 and so on. Although a single external interface 1008 is shown, this is for the purpose of example only, and in practice multiple interfaces using various methods (eg. Ethernet, serial, USB, wireless, telephone, POTS, or the like) may be provided.

[0093] In use, the microprocessor 1000 executes instructions in the form of applications software stored in the memory 1002, and to allow communication with one of the servers 204, 208.

[0094] Accordingly, it will be appreciated that the transaction terminals 202 may be formed from any suitable client device, or multiple client devices, and could include suitably programmed PCs, Internet terminal, lap-top, or hand-held PC, POS terminals, ATMs or the like, as well as a tablet, or smart phone. However, it will also be understood that the transaction terminals 202 can be any electronic processing device such as a microprocessor, microchip processor, logic gate configuration, firmware

optionally associated with implementing logic such as an FPGA (Field Programmable Gate Array), or any other electronic device, system or arrangement.

[0095] As discussed above, the transaction terminal 202 may include, or be in communication with, mobile device 210 (e.g. a smart phone). Optionally, in some examples the transaction terminal 202 includes a decoding processing device, for example a DTMF processing system, which monitors and optionally records signals to/from the mobile device 210, and automatically processes the signals. Thus, the decoding processing device may automatically decode encoded data, intentionally masking results of the decoding process from a payee. Hence, the payer's payment details are not made visible to a payee, reducing the risk of fraud. Nevertheless, a decoding processing device is not essential and similar functionality may be provided in one or more other types of transaction terminal 202.

[0096] In one example, the mobile device 210 is a handheld computer device such as a smart phone or a PDA (e.g. as manufactured by Apple™, LG™, HTC™, Research In Motion™ or Motorola™). In one particular example, the mobile device 210 includes a mobile phone or a computer such as a tablet computer. An exemplary embodiment of the mobile device 210 is shown in Figure 11. As shown, the payer client devices 210 includes the following components in electronic communication via a bus 1106:

1. a display 1102;
2. non-volatile memory 1104;
3. random access memory ("RAM") 1108;
4. N processing components 1110;
5. a transceiver component 1112 that includes N transceivers;
6. user controls 1114;
7. microphone/speaker 1116.

[0097] Although the components depicted in Figure 11 represent physical components, Figure 11 is not intended to be a hardware diagram; thus many of the components depicted in Figure 11 may be realized by common constructs or distributed among additional physical components. Moreover, it is certainly contemplated that other

existing and yet-to-be developed physical components and architectures may be utilized to implement the functional components described with reference to Figure 11.

[0098] The display 1102 generally operates to provide a presentation of content to a user, and may be realized by any of a variety of displays (e.g., CRT, LCD, HDMI, micro-projector and OLED displays). And in general, the non-volatile memory 1104 functions to store (e.g., persistently store) data and executable code including code that is associated with the functional components of a browser component and a transaction App 1118. In some embodiments, for example, the non-volatile memory 1104 includes bootloader code, modem software, operating system code, file system code, and code to facilitate the implementation of one or more portions of the transaction App 1118 as well as other components well known to those of ordinary skill in the art that are not depicted for simplicity.

[0099] In many implementations, the non-volatile memory 1104 is realized by flash memory (e.g., NAND or ONENAND memory), but it is certainly contemplated that other memory types may be utilized as well. Although it may be possible to execute the code from the non-volatile memory 1104, the executable code in the non-volatile memory 1104 is typically loaded into RAM 1108 and executed by one or more of the *N* processing components 1110.

[00100] The *N* processing components 1110 in connection with RAM 1108 generally operate to execute the instructions stored in non-volatile memory 1104 to effectuate the functional components. As one of ordinarily skill in the art will appreciate, the *N* processing components 1110 may include a video processor, modem processor, DSP, graphics processing unit (GPU), and other processing components.

[00101] The transceiver component 1112 includes *N* transceiver chains, which may be used for communicating with external devices via wireless networks. Each of the *N* transceiver chains may represent a transceiver associated with a particular communication scheme. For example, each transceiver may correspond to protocols that are specific to local area networks, cellular networks (e.g., a CDMA network, a GPRS network, a UMTS networks), and other types of communication networks.

[00102] Accordingly, it will be appreciated that the payer client devices 210 be formed from any suitably programmed processing system and could include suitably programmed PCs, Internet terminal, lap-top, or hand-held PC, a tablet, a smart phone, or the like. However, it will also be understood that the payer client devices 210 can be any electronic processing device such as a microprocessor, microchip processor, logic gate configuration, firmware optionally associated with implementing logic such as an FPGA (Field Programmable Gate Array), or any other electronic device, system or arrangement.

[00103] Examples of the processes for performing transactions have been described above. For the purpose of these examples one or both of the servers 204, 208 may be payment servers that provide payment processing functionality, and in one example provide payment network functionality including communicating with acquirers or issuers as required in order to perform transactions. The servers 204, 208 may execute processing device software, allowing relevant actions to be performed, with actions performed by the servers 204, 208 being performed by the processor 900 in accordance with instructions stored as applications software in the memory 906 and/or input commands received from a user via the I/O device 902. It will also be assumed that actions performed by the transaction terminals 202, are performed by the processor 1000 in accordance with instructions stored as applications software in the memory 1006 and/or input commands received from a user via the I/O device 1002, whilst actions performed by the mobile devices 210 are performed by the processor 1110 in accordance with instructions stored as applications software in the memory 1104 and/or input commands received from a user via the user controls 1114.

[00104] However, it will be appreciated that the above described configuration assumed for the purpose of the following examples is not essential, and numerous other configurations may be used. It will also be appreciated that the partitioning of functionality between the different processing systems may vary, depending on the particular implementation.

[00105] In addition, the transaction app 1118 may interact with a GPS logging device or other location or geolocation device or interface in the mobile device 210 in order to capture location data for the mobile device 210. The transaction app 1118 then

forwards that location data to the mobile device management server 208 as discussed above. This location data may be captured at the time a transaction is made or may be continuously monitored and stored. The app 1118 may further include means (e.g. a virtual button) for activating and deactivating location matching. Thus a user of the mobile device 210 may, via app 1118, selectively activate location matching in which case the mobile device 210 forwards an activate/reactivation request to the mobile device management server 208 (which may be the same server, or in part the same server, as host server 206) by which the location matching service is activated/reactivated, and may similarly send a deactivation request to the mobile device management server 208 by which location matching is deactivated.

[00106] A further schematic illustration of a network 1200 is shown in Figure 12, the network comprising a host server 1202 for authorising a transaction. In addition to the descriptions set out below, detailed descriptions of the network, the individual components and steps or operations performed by each of the components of the network are also given with respect to Figures 1 and 3 to 8.

[00107] The host server 1202 comprises a processor 1212 and the memory device 1214. As discussed above, the memory device 1214 is in communication with the processor 1212 and stores program instructions. The program instructions of the present embodiment implement:

an information receiver module 1216,
an account query module 18,
a deactivation module 1220,
a payment vehicle credential identifier module 1222,
a mobile device identification fetcher module 1224,
a location identifier module 1226,
a location matching module 1228 and
an approval/declination module 1230.

Other modules of program code may also be stored in the memory device 1214.

[00108] The host server 1202 comprises an I/O interface 1204 that includes a receiver 1206, transmitter 1208 and ports 1210. The functions of these components of the I/O interface 1204 will be understood. It will be appreciated that the receiver 1206

and transmitter 1208 may be a unitary transceiver and that various components of interfaces in general can be combined and separated as desired or as suitable for any particular application

[00109] The I/O interface 1204 can send and/or receive information from mobile device identifier database 1234, transaction terminal(s) 1236, accounts database 1238, mobile device management server 1240 and consumer mobile device(s) 1246. The sending and receiving of information may involve the use of MAC addresses or any other known addressing technology suitable to facilitate the sending of signals from a source to a desired destination.

[00110] The processor 1212 is operative with the program instructions stored on memory device 1214, and by acting through I/O interface 1204, to implement the various modules of program code stored in memory device 1214. In this regard, information receiver module 1216 receives transaction information from the transaction terminal(s) 1236. The transaction information comprises one or more transactions as discussed above. In one implementation, the information receiver module 1216 passes the payment vehicle credentials, of one of the transactions received in the transaction information, to the mobile device identifier fetcher module 1224. The mobile device identifier fetcher module 1224 fetches mobile device identifiers from a database 1234, and the database 1234 comprises one or more stored payment vehicle credentials each associated with a respective mobile device identifier. Thus, based on the payment vehicle credentials, mobile device identifier fetcher module 1224 fetches, from database 1234, a mobile device identifier associated with the payment vehicle credentials.

[00111] Location identifier module 1226 then generates a location capture request and sends it the to mobile device management server 1240, the location capture request comprising the mobile device identifier and the time the relevant transaction was made. The mobile device management server 1240 comprises a processor 1242 and a mobile device location database 1244, the mobile device location database 1244 storing one or more mobile device identifiers, along with the locations of the mobile devices 1246 associated with the one or more mobile device identifiers over time. The processor 1242 queries the database 1244 using the mobile device identifier, and extracts location data for the mobile device 1246 associated with that mobile device identifier. The location data may comprise a single location, being the location of the

mobile device 1246 at the time the transaction was made. The location data may instead comprise the location of the mobile device 1246 over a period of time including the time at which the transaction was made.

[00112] The location data is sent back to the host server 1202, and a location identifier module 1226 identifies the location of the mobile device 1246 at the time the transaction was made. The location matcher module 1228 then determines whether the transaction terminal location 1236 through which the transaction was made, matches the location of the mobile device 1246 at the time the transaction was made. The result of this determination is then forwarded to the approval/declination module 1230 which declines authorisation of the transaction if the transaction terminal location does not match the location of the mobile device 1246, and authorises the transaction if the transaction terminal location matches the location of the mobile device 1246.

[00113] The processor 1212 may also decline the transaction, even where the location matcher module 1228 indicates that the location of the mobile device 246 at the time the transaction was made matches the location of the transaction terminal 1236 through which the transaction was made. This may occur, for example, if the processor 1212, implementing balance query module 1248, queries accounts database 1238 and determines that an available balance for the relevant payment vehicle is less than a value of the transaction.

[00114] The processor 1212 may also only allow location matching to be performed for users of mobile devices 1246 for whose accounts location matching has been activated. In this regard, account query module 1212 may query database 1238 to determine if the location matching has been enabled for an account associated with the payment vehicle credentials for the transaction. Similarly, an account in the database 1238 may be associated with the mobile device identifier and thus the mobile device identifier may also be used in some embodiments to determine whether location matching has been activated for a particular account. If location matching has been activated for the relevant account, then the process described with reference to Figure 1 may proceed. If location matching has not been activated, or has been deactivated, for the particular account then location matching will not occur.

[00115] Accounts database 1238 has been described as containing information relevant to determining an available balance for the payment vehicle, and also for determining whether location matching has been activated for a particular account. It will be appreciated, however, that the available balance may be accessible from a different database to that on which information regarding the activation or deactivation of location matching is stored. Similarly, any database described herein may be combined with any other database or databases, or any single database may be distributed across multiple storage devices in the same or different locations.

[00116] The host server 1202 may also receive a request for deactivation of location matching. For example, during a transaction where the user has lost their mobile device 1246 or otherwise does not have it with them at the time the transaction is made, then it may be desirable to deactivate location matching so as to enable the transaction to take place. The deactivation module 1220 sends a deactivation command to database 1238 which is then updated, for the relevant account, to indicate that location matching has been deactivated. The deactivation request may be sent from the transaction terminal 1236 by the user selecting an appropriate command (e.g. pressing a physical or virtual button on a display) on the transaction terminal 1236 and inputting a code, personal identification number (PIN), biometric information or using any other known authorisation/verification technique. The transaction terminal 1236 then sends the deactivation request along with the relevant code or other information to the deactivation module 1220, which implements the deactivation command by updating the database 1238 as described above.

[00117] Using a similar process, the deactivation command may also be received by the host server 1202 from the mobile device 1246. This may occur, for example, where the cardholder of a payment card (in the present example the payment card, such as a credit or debit card, constitutes the payment vehicle) has given their payment card to another person to make purchases on their behalf. Thus the cardholder and their mobile device 1246 are not in the vicinity of the transaction terminal 1236 at the time the transaction takes place even though the transaction is valid.

[00118] Many of these processes can be performed in real-time, when the transaction is taking place, thereby authorising or declining the transaction at the time it is being made. However, it may also be desirable to assess whether a past transaction

was fraudulently made. In this regard, host server 1202 may store the transaction information in a database 1250 which may be different from, or incorporated into, one or more of the databases mentioned above. Location data may then similarly be stored in database 1244 of the mobile device management server 1240, in association with the relevant mobile device identifier. Using this stored, historical information the host server 1202 can receive a request for review of a candidate fraudulent transaction that includes a candidate fraudulent transaction identifier such as a receipt number or other unique identifier of the transaction.

[00119] Fraud query module 1252 then sends a query to database 1250 using the candidate fraudulent transaction identifier. The query attempts to match the candidate fraudulent transaction identifier to the transaction identifier of one of the transactions stored in database 1250, and thereby fetch from database 1250 the mobile device identifier associated with the payment vehicle credentials used in making the candidate fraudulent transaction. Fraud query module 1252 may also fetch, from database 1250, further information such as the time at which the suspect transaction was made. Other information, such as payment vehicle credentials, may also be fetched from database 1250 in this fetching operation.

[00120] The mobile device identifier, or payment vehicle credentials if also extracted from database 1250, may then be used in the process described above to extract location information from database 1244 – the location information indicates the location of a mobile device 1246 associated with the payment vehicle credentials at the time the transaction was made. Thereafter, as also described above, module 1228 performs the location matching operation and module 1230 approves or declines the transaction. Thus the approval/declination module 1230 will either confirm the suspect transaction as being potentially valid or potentially fraudulent.

[00121] Accordingly, the above examples provide a method for authorising a transaction, for example, over a network in which payment details are automatically captured and can be tested for potentially fraudulent activity by matching the location of the transaction terminal on which the transaction was made using a cardholder or user's payment vehicle, with the location of the mobile device (e.g. smart phone) of the user or cardholder at the time the transaction was made.

[00122] Throughout this specification and claims which follow, unless the context requires otherwise, the word “comprise”, and variations such as “comprises” or “comprising”, will be understood to imply the inclusion of a stated integer or group of integers or steps but not the exclusion of any other integer or group of integers.

[00123] Persons skilled in the art will appreciate that numerous variations and modifications will become apparent. All such variations and modifications which become apparent to persons skilled in the art, should be considered to fall within the spirit and scope that the invention broadly appearing before described. Thus, for example, it will be appreciated that features from different examples above may be used interchangeably where appropriate.

CLAIMS

1. A host server for authorising a transaction, comprising:

a processor; and

a memory device in communication with the processor and storing program instructions thereon, the processor operative with the program instructions:

to receive, from one or more transaction terminals, transaction information comprising one or more transactions and, for each said transaction:

to receive:

payment vehicle credentials of a payment vehicle used to make the transaction;

a time at which the transaction was made; and

a transaction terminal location of the transaction terminal at which the transaction was made;

to fetch from a database, the database comprising one or more stored payment vehicle credentials associated with a respective mobile device identifier, a mobile device identifier associated with the payment vehicle credentials;

to receive, from a mobile device management server, location data for a mobile device associated with the mobile device identifier and identifying a location of the mobile device at the time at which the transaction was made; and

to determine whether the transaction terminal location matches the location of the mobile device ("**location matching**") and:

decline authorisation of the transaction if the transaction terminal location does not match the location of the mobile device; and

authorise the transaction if the transaction terminal location matches the location of the mobile device.

2. The host server of claim 1, wherein the processor is operative with the program instructions to determine whether the transaction terminal location matches the location of the mobile device by determining if the transaction terminal location is the same as the location of the mobile device.

3. The host server of claim 1, wherein the processor is operative with the program instructions to determine whether the transaction terminal location matches the

location of the mobile device by determining if the transaction terminal location is within a predetermined distance of the location of the mobile device.

4. The host server of any preceding claim, wherein the payment vehicle has an available balance for use in processing the transaction, and the processor is operative with the program instructions to authorise the transaction by determining if a value of the transaction is at most equal to the available balance.

5. The host server of any preceding claim, wherein the mobile device identifier and payment vehicle credentials are associated with an account, and location matching only occurs for accounts for which location matching is activated, wherein the processor is operative with the program instructions to:
    - o determine whether location matching is activated for the account; and
    - o authorise the transaction if location matching is not activated for the account.

6. The host server of claim 5, wherein the processor is operative with the program instructions to:
    - o receive a deactivation request from the transaction terminal; and
    - o deactivate location matching for the account in response to the deactivation request.

7. The host server of claim 5, wherein the processor is operative with the program instructions to:
    - o receive a deactivation request from the mobile device; and
    - o deactivate location matching for the account in response to the deactivation request.

8. The host server of any preceding claim, wherein the processor is operative with the program instructions to receive location data for the mobile device by:
    - o send a location capture request to mobile device management server; and
    - o receive the location data for the mobile device from the mobile device management server, in response to the location capture request.

9. The host server of any preceding claim, wherein each transaction further comprises a transaction identifier and the processor operative with the program instructions:

to store the transaction information in a first memory;

to store the location data in a second memory,

to receive a request for review of a candidate fraudulent transaction, the request comprising a candidate fraudulent transaction identifier;

to match the candidate fraudulent transaction identifier to the transaction identifier of a suspect transaction, the suspect transaction being one of the one or more transactions,

to fetch, from the database, the mobile device identifier associated with the payment vehicle credentials by identifying the mobile device identifier of the suspect transaction; and

to determine, at the host server, whether the transaction terminal location matches the location of the mobile device by determining whether the transaction terminal location matches the location of the mobile device at the time the suspect transaction was made and:

decline authorisation by confirming the suspect transaction is potentially fraudulent; and

authorise the transaction by confirming the suspect transaction is potentially valid.

10. A transaction authorisation computer process comprising:

receiving, at a host server and from one or more transaction terminals, transaction information comprising one or more transactions and, for each said transaction:

receiving:

payment vehicle credentials of a payment vehicle used to make the transaction;

a time at which the transaction was made; and

a transaction terminal location of the transaction terminal at which the transaction was made,

and, for each transaction:

fetching, from a database comprising one or more stored payment vehicle credentials associated with a respective mobile device identifier, a mobile device identifier associated with the payment vehicle credentials;

receiving, at the host server, location data from a mobile device management server, the location data being for a mobile device associated with the mobile device identifier and identifying a location of the mobile device at the time at which the transaction was made; and

determining, at the host server, whether the transaction terminal location matches the location of the mobile device ("**location matching**") and:

declining authorisation of the transaction if the transaction terminal location does not match the location of the mobile device; and

authorising the transaction if the transaction terminal location matches the location of the mobile device.

11. The computer process of claim 10, wherein determining whether the transaction terminal location matches the location of the mobile device comprises determining if the transaction terminal location is the same as the location of the mobile device.

12. The computer process of claim 10, wherein determining whether the transaction terminal location matches the location of the mobile device comprises determining if the transaction terminal location is within a predetermined distance of the location of the mobile device.

13. The computer process of any one of claims 10 to 12, wherein the payment vehicle has an available balance for use in processing the transaction, and authorising the transaction comprises determining if a value of the transaction is at most equal to the available balance.

14. The computer process of any one of claims 10 to 13, wherein the mobile device identifier and payment vehicle credentials are associated with an account, and location matching only occurs for accounts for which location matching is activated, the computer process further comprising:

- determining, at the host server, whether location matching is activated for the account; and
- authorises the transaction if location matching is not activated for the account.

15. The computer process of claim 14, further comprising:
    - receiving, at the host server, a deactivation request from the transaction terminal; and
    - deactivating location matching for the account in response to the deactivation request.

16. The computer process of claim 14, further comprising:
    - receiving, at the host server, a deactivation request from the mobile device; and
    - deactivating location matching for the account in response to the deactivation request.

17. The computer process of any one of claims 10 to 16, wherein receiving location data for the mobile device comprises:
    - sending a location capture request to mobile device management server; and
    - receiving, at the host server, the location data for the mobile device from the mobile device management server, in response to the location capture request.

18. The computer process of any one of claims 10 to 17, wherein each transaction further comprises a transaction identifier and the method further comprises:

    storing the transaction information in a first memory;

    storing the location data in a second memory,

    receiving, at the host server, a request for review of a candidate fraudulent transaction, the request comprising a candidate fraudulent transaction identifier;

    matching, at the host server, the candidate fraudulent transaction identifier to the transaction identifier of a suspect transaction, the suspect transaction being one of the one or more transactions,

wherein:

from, from the database, the mobile device identifier associated with the payment vehicle credentials comprises identifying the mobile device identifier of the suspect transaction; and

determining, at the host server, whether the transaction terminal location matches the location of the mobile device comprises determining whether the transaction terminal location matches the location of the mobile device at the time the suspect transaction was made and:

declining authorisation comprises confirming the suspect transaction is potentially fraudulent; and

authorising the transaction comprises confirming the suspect transaction is potentially valid.

19. A network for authorising a transaction, comprising:

a host server;

one or more transaction terminals;

a database; and

a mobile device manager server,

wherein the host server comprises:

a processor; and

a memory device in communication with the processor and storing program instructions thereon, the processor operative with the program instructions:

to receive, from the one or more transaction terminals, transaction information comprising one or more transactions and, for each said transaction:

payment vehicle credentials of a payment vehicle used to make the transaction;

a time at which the transaction was made; and

a transaction terminal location of the transaction terminal at which the transaction was made,

and, for each transaction:

to fetch from the database, the database comprising one or more stored payment vehicle credentials associated with a

respective mobile device identifier, a mobile device identifier associated with the payment vehicle credentials;

to receive, from the mobile device management server, location data for a mobile device associated with the mobile device identifier and identifying a location of the mobile device at the time at which the transaction was made; and

to determine whether the transaction terminal location matches the location of the mobile device ("**location matching**") and:

decline authorisation of the transaction if the transaction terminal location does not match the location of the mobile device; and

authorise the transaction if the transaction terminal location matches the location of the mobile device.