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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 August 2010 (05.08.2010)

PCT

(10) International Publication Number
WO 2010/086608 A2

(51) International Patent Classification: Not classified

(21) International Application Number:
PCT/GB2010/000139

(22) International Filing Date:
28 January 2010 (28.01.2010)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0901407.7 28 January 2009 (28.01.2009) GB

(71) Applicant *(for all designated States except US)*: **VALIDSOFT (UK) LIMITED** [GB/GB]; 9 Devonshire Square, London EC2M 4YF (GB).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **CARROLL, Pat** [IE/GB]; 403 Altmore House, Tara Street, Tullamore, Co. Offlay (IE). **PETERSEN, John** [AU/GB]; 97 Engadine Street, London SW18 5DU (GB). **ALFORD, Jonathan** [GB/GB]; 1 Hill End, Orpington, Kent BR6 0SJ (GB).

(74) Agent: **REDDIE & GROSE**; 16 Theobalds Road, London WC1X 8PL (GB).

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

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

Published:

— *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

WO 2010/086608 A2

(54) Title: CARD FALSE-POSITIVE PREVENTION

(57) Abstract: A method for authenticating a transaction is disclosed. The method comprises the steps of: receiving data identifying a region where a transaction is being requested; receiving data identifying a mobile communication device associated with a person requesting the transaction; determining from Location Register (LR) data for the mobile communication device data identifying a region where the mobile communication device is located; comparing the data identifying the region where the transaction is being requested with the data identifying the region where the mobile communication device is located; and authenticating the transaction in dependence on the result of the comparison.

Card False-Positive Prevention

Field of the Invention

This invention relates to determining the validity of a requested transaction and to false-positive prevention such as card present false-positive prevention. More particularly, this invention relates to financial transactions and to card-present false-positive prevention as well as to cross-border card present false-positive prevention.

Background of the Invention

A false-positive event occurs when a user attempts to carry out a legitimate financial transaction which is declined because the financial provider (for example an issuing bank providing customers with a debit card or credit card) has incorrectly identified that transaction as being potentially fraudulent. The transaction may be a cross-border card-present transaction. A cross-border transaction may be on in which the transaction occurs in a different region to the region where the user is registered with the financial provider. That is to say, a cross-border card-present transaction could be one where a user withdraws cash from an ATM (automated teller machine) using his credit or debit card abroad or one where a user purchases goods at a Point-of-Sale (PoS) using his credit or debit card abroad. In both cases, the card must be physically present at the point of the transaction e.g. at the ATM or PoS. This is in contrast to a card-not-present transaction where the details of the card are present, for example the name of the card holder, the card number, expiry date, as well as security information. The card itself is not present at the location where the transaction is carried out. A card-not-present transaction may occur as a result of an internet or mail order transaction. Furthermore, the transaction may be a cross-border transaction, i.e. one where the transaction occurs in a country other than the country where the cardholder's issuing bank issued the card.

Cross-border card-present fraud is on the increase and now accounts for 40% of all card crime on UK issued cards. Technology such as Chip and PIN (personal identification number) is ineffective at preventing cross-border card-present fraud as skimmed (counterfeit) cards are simply used at ATMs and PoS devices in countries that don't support Chip and PIN, such as the US, when verification reverts to the card's magnetic stripe. Chip and PIN technology allows payment using debit or credit cards. Instead of using a signature to verify payments, the card user must enter a PIN number known only to the card holder.

Banks and other financial service providers generally attempt to prevent card-present fraud through the use of 3rd party software risk engines or in-house logic within the real-time authorisation process in an attempt to determine whether a transaction is likely to be fraudulent. Others will decline all cross-border transactions unless the cardholder has previously supplied the financial service provider with an accurate travel itinerary (which may still prove insufficient).

The main problem with the risk-engine approach is that risk engines are highly inaccurate in determining potentially fraudulent transactions. False-positive rates arising from such risk engines are extremely high, typically between 80% and 90%, resulting in substantial inconvenience and cost for the cardholders and banks alike. By false-positive rate, we mean the percentage of incorrectly declined transactions within the total number of declined transactions. Due to the high volumes and costs currently associated with determining false-positives, financial service providers cannot typically decline all of the transactions they would like to, resulting in fraudulent transactions being authorised. This arises when the cost of prevention exceeds the cost of fraud. The main costs to the financial service provider and the customer are incurred in the resolution process of a false-positive transaction.

Therefore, there is a problem that financial service providers often incorrectly identify and decline genuine transactions as potentially fraudulent, particularly when the transactions are carried out in an overseas country, which is not the card's country of issue, by the legitimate cardholder.

As a result, because the financial service provider has declined the transaction, it usually contacts the cardholder to confirm whether the transaction was actually fraudulent. This is done either manually by fraud centre operators, which is very expensive, or electronically by outbound dialling services, some of which can be inefficient and expensive. In many cases, however, because of the time taken for the financial service provider to instigate this process, the cardholder contacts the financial service provider directly (from abroad) to attempt to resolve the issue.

This is far from satisfactory because the cost of telephoning the financial service provider from abroad may be prohibitively high. Furthermore, the difference in time zone between countries may mean that the card holder is unable to contact the

financial service provider if it is out of working hours in the country where the card was issued.

Summary of the Invention

The invention is defined in its various aspects in the appended claims to which reference should now be made.

According to one aspect of the present invention, a method for deriving probability data relating to the validity of a requested financial transaction comprises the steps of: receiving location data relating to a requested transaction; receiving data identifying a mobile communication device associated with a person requesting the transaction; determining from Home Location Register (HLR) data for the mobile communication device location data for the mobile communication device; comparing the location data relating to the transaction with the location data from the mobile communication device; and determining probability data relating to the validity of the requested transaction in dependence on the result of the comparison.

According to another aspect of the present invention, apparatus for deriving probability data relating to the validity of requested financial transaction comprises: means for receiving location data relating to a requested transaction; means for receiving data identifying a mobile communication device associated with a person requesting the transaction; means for determining from Home Location Register (HLR) data for the mobile communication device location data for the mobile communication device; means for comparing the location data relating to the transaction with the location data from the mobile communication device; and means for determining probability data relating to the validity of the requested transaction in dependence on the result of the comparison.

Preferred embodiments of the invention derive probability data relating to the validity of a requested financial transaction by receiving location data relating to a requested transaction; receiving data identifying a mobile communication device associated with a person requesting the transaction; determine from Home Location Register (HLR) data for the mobile communication device location data for the mobile communication device; compare the location data relating to the transaction with the location data from the mobile communication device; and determine probability data relating to the validity of the requested transaction in dependence on the result of the comparison.

This allows the probability of legitimacy of a transaction to be determined to enable the issuing bank to better determine whether to allow or deny the transaction. This means that fewer false positive transactions occur, providing an improved service to the card holder and a reduction in cost to the issuing bank.

Detailed Description of Preferred Embodiments

An embodiment of the invention will now be described, by way of example only, with reference to the accompanying drawings in which:

Figure 1 shows a schematic diagram of the system architecture of an embodiment of the invention; and

Figure 2 shows a flow diagram showing the main steps performed by an embodiment of the invention.

Referring to figure 1, a false positive prevention system comprises a server or computer 101. The server or computer 101 determines whether a transaction is likely to be fraudulent or not, as described in further detail below. The system can further comprise a mobile network data aggregator 103; mobile networks, 105, 106, a mobile communication device (not shown), a bank 107, and a customer 109. Furthermore, the system may also comprise a resolution system 111, although this feature is not essential, and so it is shown in dashed lines in figure 1. The main steps carried out by an embodiment of the invention will now be described.

Referring to figure 2, a user first starts a transaction at a means for performing or carrying out a transaction, at step 201. The means for carrying out the transaction may be an ATM or PoS. If the transaction is being requested at an ATM, the user inserts a card into the ATM and enters his PIN number. Alternatively, if the transaction is being carried out at a PoS, then the user may physically pass the card to the retailer who inserts the card into a card reader for processing. The user may optionally enter a PIN, if the card is a chip and PIN card. Other verification schemes such as signature may also be used, alternatively or in addition to a PIN. In all cases, the card comprises data associated with an individual or user which allows the user's account to be identified. Usually this information is in the form of a sequence of decimal numbers.

The ATM or PoS then contacts the financial service provider (card issuer) 107 at step 203, and the Issuing bank or financial service provider 107 authorisation process starts. In this, the financial service provider receives a transaction request, at step 205. The ATM or PoS sends information enabling the identity of the card holder to be deduced. This information may comprise the card number and may be sent by conventional means or using wireless means known to the skilled person. The information also may be sent in any suitably encrypted form known to the skilled person.

Once the bank or financial service provider 107 has received the transaction request, it may optionally perform additional processing to determine (using software risk engines or in-house logic) whether the transaction is likely to be fraudulent, for example if the transaction is for a large amount. However, if the financial service provider 107 determines that the transaction is likely to be genuine, then it can proceed directly to the authorisation process, at step 217, allowing the transaction at step 219. If the financial service provider determines that the transaction is likely to be fraudulent, then it passes the request to the server, 101.

However, if the financial service provider does not perform this additional processing, then it passes the transaction information directly to the server 101.

In one embodiment, the server 101 may be located within the financial service provider's organisation. However preferred embodiments have a server 101 which is physically separate from the financial service provider, and the transaction information (for example card number or/and name or/and transaction amount) is sent using wireless or conventional wire technology to the server, 101.

In one embodiment, the server 101 then extracts country code information contained within the transaction information, at step 207.

In an alternative embodiment, the financial service provider extracts the country code information from the transaction information. The financial service provider may also assign a reference number to the transaction. This has the advantage that potentially sensitive financial information such as the card number does not have to be sent to the server 101.

The financial service provider then searches a customer data base or look up table for information identifying a mobile communication device, as shown in table 1.

Card Holder Name	Card number	Telephone number
Mr A Smith	5432 1234 5678 9998	00 44 7981 123 789
Mr A Smith	5432 1234 5678 9999	00 44 7981 123 789
Mr N Jones	5432 1234 0123 4567	00 44 7981 567 831

Table 1: Part of a look up table in an issuing bank.

It does this by using the card holder identifying information (for example the card number) to search a look up table. The look up table has card holder identifying information for each card holder and also information enabling the card holder's mobile communication device to be determined. The card holder identifying information for each user is associated with at least one piece of information enabling the card holder's communication device to be determined. If the mobile communication device is a portable telephone, then this information may be the (unique) telephone number of the portable telephone associated with the user carrying out the transaction. Further, each card holder may have more than one entry in the look up table because they may have more than one card with the financial service provider.

The financial service provider then sends the information identifying the mobile communication device as well as the extracted country code (i.e. location) relating to the transaction to the server 101. Preferably, a transaction reference number is also sent. This could be an arbitrary number assigned to the transaction by the financial service provider. This information may be sent in an encrypted form.

The server 101 receives the information identifying the mobile communication device (mobile telephone number) of the customer 109 from the issuing bank it then performs a HLR lookup from a commercially available database. An HLR database, is held by every mobile network provider and comprises information on that provider's permanent subscribers. Included in the information is the Network Country Code to which a subscriber is currently assigned, for use with customers who are roaming. The HLR database is frequently updated to take account of changes in the user's position.

The server 101 performs the HLR lookup by opening one or more communication channel(s) to a mobile network data aggregator 103, at step 209. The network data aggregator holds HLR information for mobile communication devices registered with a mobile network provider. The network data aggregator may have HLR data of more than one mobile network service provider 105, 106. This has the advantage that it is not necessary to interrogate each service provider separately in order to obtain the HLR data of a mobile communication devices registered with different service providers.

The network data aggregator 103 is able to extract the Mobile Country Code (MCC) indicator held for every permanent subscriber within the Home Location Register (HLR) database of the subscriber's mobile network, at step 211 using the information enabling the card holder's communication device to be determined (i.e. mobile telephone number). The MCC code associated with the information identifying the mobile communication device (telephone number)is then passed to the server 101.

The server 101 then compares the received country indicator contained within the (cross-border) ATM or PoS transaction with the received Mobile Country Code (MCC) indicator.

At step 213, the probability of a transaction being legitimate is calculated. There are a number of ways in which this may be performed. The simplest way in which a legitimate transaction is detected is if the extracted country code of where the transaction is taking place matches the determined MCC indicator. For example, a transaction with an extracted country code relating to Australia will have a high probability of legitimacy if the determined MCC indicator also relates to Australia. In this case, the transaction is likely to be legitimate, because it is most likely that the legitimate card holder is in the same or a similar location to their mobile communication device. For a legitimate transaction the legitimate card holder carrying out the transaction is likely to have the mobile communication device on their person. In this case, the location of the transaction will be the substantially the same as the location of the user's mobile communication device.

The HLR data of a mobile communication device can be determined using techniques known to the skilled person, for example using the mobile GSM (Global System for Mobile) network or using 3rd generation mobile networks. This allows the

position of the mobile communication device to be determined to an accuracy of at least 50m.

In one embodiment the system can be configured so that a transaction is determined to be genuine only if the thus determined location of the mobile communication device is within a predetermined distance of the location where the transaction is occurring, for example 50 or 100m.

In an alternative embodiment, the system is configured such that a transaction is determined to be genuine only if the mobile communication device is determined to be in the same city or state or country as the place where the transaction is taking place. This embodiment is useful because card users frequently leave mobile devices at home or in hotels when performing a transaction.

In some cases, the transaction country code will not match the MCC indicator, even though the transaction is being carried out by a legitimate user. This could occur if the transaction is taking place close to the border of a country, for example the border or France and Germany. In this case, if the MCC indicator is determined to be close to a border, the transaction may be allowed even though the transaction country code and the MCC indicator do not match, provided the transaction is occurring in a country which neighbours (i.e. within a predetermined distance) of the country code determined using the MCC.

The system may also determine the probability of a transaction being fraudulent, at step 213, rather than just determining whether the transaction is genuine (1) or fraudulent (0). In this case a number between 0 and 1 may be assigned to the transaction.

In one embodiment, the probability of the transaction being fraudulent is larger when the distance between the location of the transaction and the user's mobile communication device is larger.

At step 215, the transaction request is updated with the determined probability value, for example 0.9 (meaning that there is a 90% probability that the transaction is genuine) or whole number for example 1 or 0 (meaning that the transaction has determined with 100% probability of it being genuine or fraudulent). The probability is

then passed to the bank or financial service provider 101 as part of the transaction information, and at step 217, the bank or financial service provider allows or denies the transaction in dependence upon the determined probability. If the transaction is allowed it is completed at step 219.

In this way, embodiments of the invention reduce the incidence of false-positive transactions.

A consequence of reducing the incidence of false-positives is a potential increase in the detection of true positives (fraudulent transactions) by allowing more suspect transactions to be declined. By true positive we mean a fraudulent transaction declined for being identified as potentially fraudulent. Embodiments of the invention therefore, to achieve maximum effectiveness, require cardholders to take and activate their mobile communication devices (mobile phones) abroad (though not necessarily to carry them on their person) and also require issuing banks to record accurate mobile phone information on their cardholder databases. This is an increasing trend due to the increasing incidence of cross-border false-positives and is actively encouraged by banks. The Association for Payment Clearing Services (APACS) advises card holders to make sure their card company has up-to-date contact details for them, including a mobile number, especially if travelling overseas.

In a further embodiment, an automated resolution process, at step 221, is provided, however this is optional. This allows for the immediate and automatic resolution of any transaction declined through having a low probability of legitimacy (potentially fraudulent transaction). The automated resolution process predicts if the decline is a true-positive (fraudulent transaction) or false-positive (legitimate transaction). Depending on which outcome, the automated resolution process connects the cardholder directly with the bank or financial service provider (i.e. fraud department) to resolve the issue of the fraudulent card and any previous fraudulent transactions. Alternatively it can update the cardholder's information and request the cardholder to resubmit the declined transaction. Because the resolution process can occur immediately the transaction is declined, it streamlines the process, provides a better customer experience and provides the opportunity for the cardholder to retry the transaction, in the case of false-positive, whilst still in the vicinity of the original declined transaction.

Embodiments of the invention use HLR information in conjunction with card-present financial transaction data to predict the probability of legitimacy. Using HLR databases to determine the country location of a subscriber has advantages over techniques such as Latitude/Longitude tracking in terms of cost, timeliness and privacy. Embodiments of the invention allow more true positive cross-border card present financial transactions to be identified, while also reducing the number of false positive transactions.

Embodiments of the invention also allow invalid mobile telephone numbers to be identified (ones that are no longer in use) using the HLR information thereby avoiding processing errors. This also allows these numbers to be identified and for the financial service provider to request new telephone numbers from the card holder. Embodiments of the invention can run as a hosted service or in-house.Although embodiments of the invention have been described with reference to financial cards, it is not in fact necessary for any card to actually be present when the transaction is taking place. For example, a user may use biometric information such as finger print(s) or retina scan(s) as a unique identifier of their account whilst also giving authorisation information. The authorisation information can be an additional PIN or can be the biometric information itself.

In other embodiments, a user can be provided with a unique combination of code or/and pin number to enter at an ATM. This allows their financial service provider to provide the user with cash from the ATM without the need for a physical card. The withdrawn cash is then debited from the user's account which is identified using the unique code.

It will be appreciated that the present invention finds applicability in determining the validity or authenticity of any transaction being attempted at an ATM or PoS or any other means for carrying out a transaction. The transaction may be a financial transaction. Further, embodiments of the invention may be implemented in hardware or software. Embodiments may be implemented in the ATM or PoS or other means for carrying out a transaction, although, it is preferable to implement the system at a centralised computer or server 101. In addition to using Home Location Register database information, the system 101 may use Visitor Location register database information. These databases may be referred to as Location Register (LR) databases.

In one embodiment, the location data relating to where a financial transaction is being requested may comprise data identifying a region where a transaction is being requested. For example, embodiments of the invention may use an ATM

country code indicator or a PoS country code indicator. These financial transaction country indicators may be labels such as "UK" or "44" and serve to identify a particular region, but do not contain sufficient information to determine where the region is located or even where within the region the ATM or PoS is located or positioned.

Further, the location data of the mobile communication device may comprise data identifying a region where a mobile communication device is located.

For example, embodiments of the invention may use a Mobile Country Code (MCC) indicator, such as "UK" or "44". The server 101 may extract the Mobile Country Code indicator from the Home Location Register Data. The server 101 may extract the Mobile Country Code indicator from the LR data of a number of mobile devices using the data identifying a mobile communication device which is associated with a person requesting the transaction. The LR data corresponding to the mobile device of the user requesting the transaction may then be searched to extract the country code indicator. For example, a search for the field "MCC" in the LR database, will reveal a match, and the data value associated with that match is the MCC value or indicator. The data identifying a mobile communication device may be a mobile telephone number or other subscriber information such as an International Mobile Subscriber Identity (IMSI).

The data identifying a region where a mobile communication device is located may be a label such as "UK" or "44" and serve to identify a particular region where the device is located, but do not contain sufficient information to determine where the region is located or even where within the region the device is located or positioned.

Using data identifying a region rather than location data itself has advantages in that the server 101 does not know the position of the mobile communication device, so that a user's privacy is maintained. The server 101 just knows what the value is of the identifier which represents a particular region. For example, if the user's mobile communication device is located within the UK, the data identifying the region where the mobile device is located may be a number such as "44". This information does not allow the position of the mobile communication to be determined.

Further, using data identifying a region rather than the location data itself also has the advantage in that the server 101 or computer does not know the position or location of the ATM or PoS where the user is attempting a transaction. This also has benefits to the user in terms of privacy.

Further, the indicator or data identifying a region where the financial transaction is requested are not unique. That is to say, all ATMs or PoSs within a particular geographic region are assigned a particular country indicator, such as "44".

Further, the indicator or data identifying a region where a mobile communication device associated with a user requesting a transaction is located is also not unique. That is to say, the mobile phone country indicator assigned to a particular phone is not unique and that a number of mobile phones within a particular region or country share the same code.

Having indicators which are not unique has the advantage that the step of comparing the data identifying a region where a financial transaction is requested with the data identifying a region where a mobile communication device is located is simplified.

This is because it is not necessary to determine the distance of the ATM or PoS from the mobile communication device, for example using the position (x1, y1, z1) of the mobile device and the position (x2, y2, z2) of the ATM or PoS. All that is required is to compare the data or identifier of the region where the ATM or Pos is located with the data identifier of the region where the mobile communication device is located. This simplifies, and hence, improves the response time of the system. It also advantageous in terms of increased privacy for the user.

A transaction may be validated or determined as authentic if the region identifier where the ATM or POS is located matches the region identifier where the mobile communication device is located.

In some countries additional identifiers of the region in which the mobile device is located may also be provided. For example, for transactions within the United States, the data identifying the regions where a mobile device is located also may comprise a city or state identifier. This identifier is also located in the HLR data. However, these city or state identifiers are also not unique in that a number of mobile devices may be assigned the same city or state identifier. Further, the city or state identifiers may not contain sufficient information to enable the location of the region covered by the city or state to be determined or indeed to determine where within the city or state region the mobile device is located.

As previously described, embodiments of the invention may receive the HLR data from a mobile network aggregator. Further, the transaction may be a card-present transaction or a card-not-present transaction or a cross-border transaction. The location data of the mobile communication device may be receivable from more than one network aggregator. The LR data may comprise data from more than one

mobile network service provider. Further, a probability of legitimacy of the requested transaction may be determined in real time or post authorisation.

Further, embodiments of the invention may decline a transaction if a determined probability of legitimacy is below a predetermined value. The probability data may also be used to identify a false positive transaction. The transaction data and the data identifying a mobile communication device may be received from a financial service provider. The method may also comprise the step of automatically contacting the person requesting the transaction, for example via telephone.

Embodiments of the invention may also comprise the step of controlling a means for carrying out a transaction in dependence upon the result of the comparison. This step may be an alternative to the step of authenticating the transaction in dependence on the result of the comparison.

For example, if the data identifying the region where the transaction is being requested matches the data identifying the region where the mobile communication device is located an ATM or PoS or other means for carrying out a transaction may be controlled such that cash is dispensed or such that the PoS performs the transaction.

Claims

1. A method for authenticating a transaction comprising the steps of:

receiving data identifying a region where a transaction is being requested;

determining from Location Register (LR) data for a mobile communication device associated with a person requesting the transaction data identifying a region where the mobile communication device is located;

comparing the data identifying the region where the transaction is being requested with the data identifying the region where the mobile communication device is located; and

authenticating the transaction in dependence on the result of the comparison.

2. A method according to claim 1 further comprising the step of receiving data identifying a mobile communication device associated with a person requesting the transaction.

3. A method according to any preceding claim further comprising the step of receiving the Location Register data for the mobile device associated with the person requesting the transaction.

4. A method according to claims 2 or 3 in which the data identifying the mobile communication device associated with the person requesting the transaction is used to determine the region where the mobile communication device is located from the LR data.

5. A method according to any preceding claim further comprising the step of extracting the data identifying a region where a transaction is being requested from transaction data received from a means for carrying out a transaction by searching transaction data.

6. A method according to any preceding claim wherein the data identifying the region where the mobile communication device is located is determined from Home Location Register data or Visitor Location Register data.

7. A method according to any preceding claim wherein the LR data is received from a mobile network aggregator storing LR data of a plurality of mobile devices registered with different mobile service providers.

8. A method according to any preceding claim wherein the transaction occurs between two regions.

9. A method according to any preceding claim in which the transaction occurs within a single region.

10. A method according to any preceding claim in which the data identifying a region where a mobile communication device is located comprises Mobile Country Code (MCC) data or data identifying a state or a city.

11. A method according to any preceding claim in which the data identifying a region where a transaction is being requested comprises transaction country data or data identifying a state or a city.

12. A method according to any preceding claim further comprising the step of allowing the transaction if the transaction is determined to be authentic.

13. A method according to any preceding claim in which the transaction is determined to be authentic if the data identifying the region where the transaction is being requested matches the data identifying the region where the mobile communication device is located.

14. A method according to any preceding claim further comprising the step of declining the transaction if the transaction is determined not to be authentic.

15. A method according to any preceding claim in which the transaction is not determined to be authentic if the data identifying a region where a transaction is being requested does not match the data identifying a region where a mobile communication device is located.

16. A method according to claim 14 further comprising the step of establishing a connection between the mobile communication device of the user requesting the transaction and the service provider of the transaction and preferably where the connection is via real-time voice telephony or via short message service (SMS).

17. A method according to any preceding claim in which the data identifying the region where the transaction is being requested and in particular the data identifying the region where the mobile communication device is located are received from a financial service provider or from a means for carrying out the transaction.

18. A method according to any preceding claim further comprising the step of controlling a means for carrying out a transaction in dependence upon the result of the comparison.

19. A method for deriving probability data relating to the validity of a requested financial transaction comprising the steps of:

receiving data identifying a region where a transaction is being requested;

determining from Location Register (LR) data for a mobile communication device associated with a person requesting the transaction data identifying a region where the mobile communication device is located;

comparing the data identifying the region where the transaction is being requested with the data identifying the region where the mobile communication device is located; and

determining probability data relating to the validity of the requested transaction in dependence on the result of the comparison.

20. A method according to claim 19 further comprising the step of receiving data identifying a mobile communication device associated with a person requesting the transaction.

21. Apparatus for authenticating a transaction comprising:

means for receiving data identifying a region where a transaction is being requested;

means for determining from Location Register (LR) data for a mobile communication device associated with a person requesting the transaction data identifying a region where the mobile communication device is located;

means for comparing the data identifying the region where the transaction is being requested with the data identifying the region where the mobile communication device is located; and

means for authenticating the transaction in dependence on the result of the comparison.

22. Apparatus according to any preceding claim further comprising means for receiving data identifying a mobile communication device associated with a person requesting the transaction.

23. Apparatus according to any preceding claim in which the Location Register data for the mobile device associated with the person requesting the transaction is received from a mobile network service provider.

24. Apparatus according to claims 22 or 23 in which the data identifying the mobile communication device associated with the person requesting the transaction is used to determine the region where the mobile communication device is located from the LR data.

25. Apparatus according to any preceding claim further comprising means for extracting the data identifying a region where a transaction is being requested from transaction data received from a means for carrying out a transaction by searching transaction data.

26. Apparatus according to any preceding claim wherein the data identifying the region where the mobile communication device is located is determined from Home Location Register data or Visitor Location Register data.

27. Apparatus according to any preceding claim further comprising a mobile network aggregator storing LR details of a plurality of mobile devices registered with different mobile service providers.

28. Apparatus according to any preceding claim in which the data identifying a region where a mobile communication device is located comprises Mobile Country Code (MCC) data or data identifying a state or a city.

29. Apparatus according to any preceding claim further comprising a means for allowing the transaction if the transaction is determined to be authentic.

30. Apparatus according to any preceding claim in which the transaction is determined to be authentic if the data identifying the region where the transaction is being requested matches the data identifying the region where the mobile communication device is located.

31. Apparatus according to any preceding claim in which the transaction is not determined to be authentic if the data identifying a region where a transaction is being requested does not match the data identifying a region where a mobile communication device is located.

32. Apparatus according to claim 30 further comprising means for establishing a connection between the mobile communication device of the user requesting the transaction and a service provider of the transaction.

33. Apparatus according to any preceding claim in which the data identifying the region where the transaction is being requested and in particular the data identifying the region where the mobile communication device is located are received from a financial service provider or from a means for carrying out the transaction.

34. Apparatus according to any preceding claim further comprising means for connecting in particular via real-time voice telephony or via short message service (SMS) the mobile device of the person requesting the transaction to a transaction service provider.

35. Apparatus according to any preceding claim further comprising a controller for controlling a means for carrying out a transaction in dependence upon the result of the comparison.

36. Apparatus for deriving probability data relating to the validity of requested financial transaction comprising:

means for receiving data identifying a region where a transaction is being requested;

means for determining from Location Register (LR) data for a mobile communication device associated with a person requesting the transaction data identifying a region where the mobile communication device is located;

means for comparing the data identifying the region where the transaction is being requested with the data identifying the region where from the mobile communication device is located; and

means for determining probability data relating to the validity of the requested transaction in dependence on the result of the comparison.

37. Apparatus according to claim 36 further comprising means for receiving data identifying a mobile communication device associated with a person requesting the transaction.

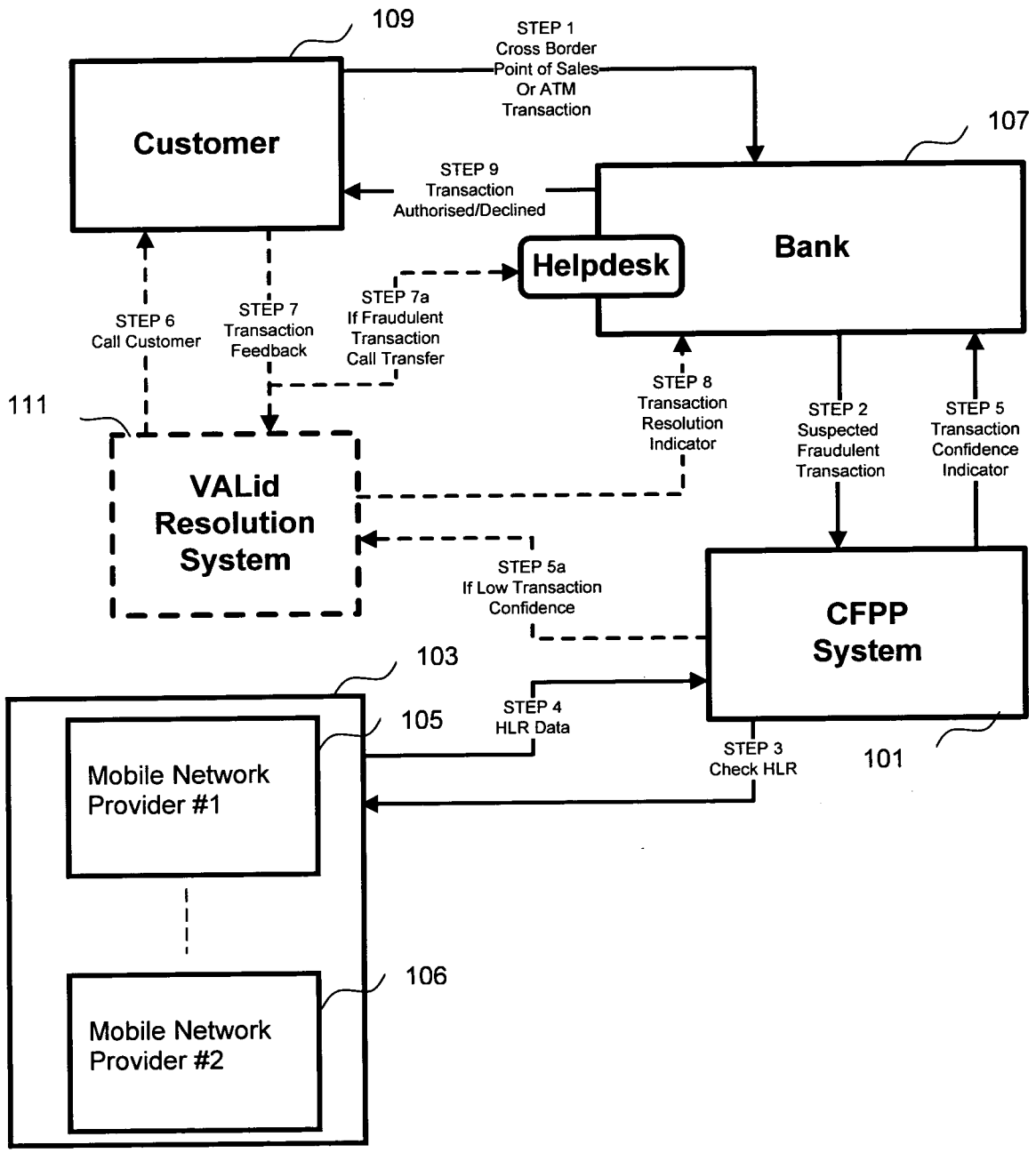
109
STEP 1
Cross Border
Point of Sales
Or ATM
Transaction
Customer
107
STEP 9
Transaction
Authorised/Declined
Bank
Helpdesk
STEP 6
Call Customer
STEP 7
Transaction
Feedback
STEP 7a
If Fraudulent
Transaction
Call Transfer
111
STEP 8
Transaction
Resolution
Indicator
STEP 2
Suspected
Fraudulent
Transaction
STEP 5
Transaction
Confidence
Indicator
VALid
Resolution
System
STEP 5a
If Low Transaction
Confidence
CFPP
System
103
105
STEP 4
HLR Data
STEP 3
Check HLR
101
Mobile Network
Provider #1
106
Mobile Network
Provider #2

Figure 1

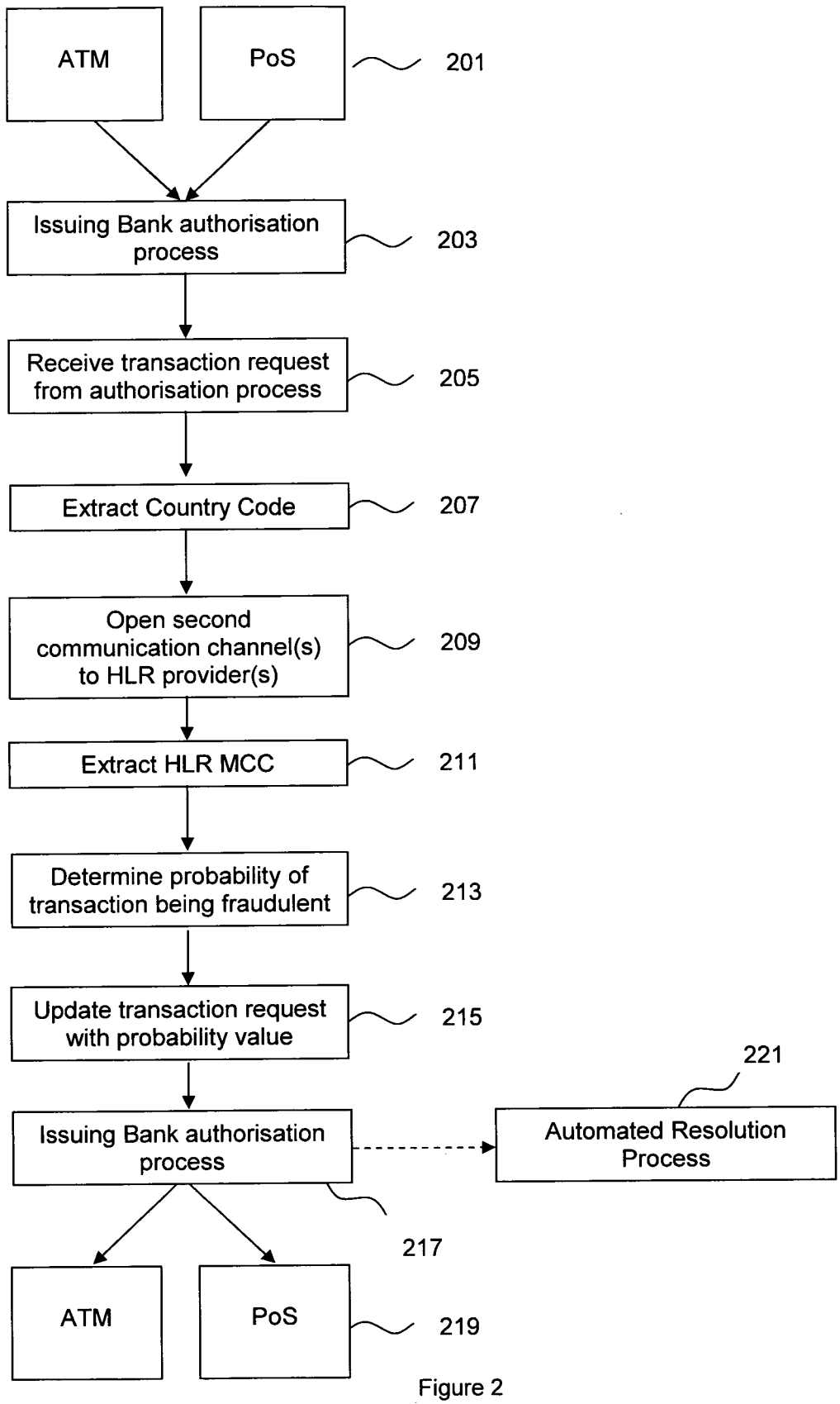
ATM
PoS
201
Issuing Bank authorisation process
203
Receive transaction request from authorisation process
205
Extract Country Code
207
Open second communication channel(s) to HLR provider(s)
209
Extract HLR MCC
211
Determine probability of transaction being fraudulent
213
Update transaction request with probability value
215
221
Issuing Bank authorisation process
Automated Resolution Process
217
ATM
PoS
219

Figure 2