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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
25 August 2011 (25.08.2011)

PCT

(10) International Publication Number
WO 2011/103432 A2

(51) **International Patent Classification**:
G06Q 40/00 (2006.01) ***G06Q 20/00*** (2006.01)

(21) **International Application Number**:
PCT/US2011/025443

(22) **International Filing Date**:
18 February 2011 (18.02.2011)

(25) **Filing Language**: English

(26) **Publication Language**: English

(30) **Priority Data**:
61/306,369 19 February 2010 (19.02.2010) US

(71) **Applicant** *(for all designated States except US)*: **FINSHPHERE CORPORATION** [US/US]; 505 106th Avenue NE, Suite 200, Bellevue, Washington 98004 (US).

(72) **Inventors; and**
(75) **Inventors/Applicants** *(for US only)*: **FERGUSON, William M.** [US/US]; 12116 Mannix Road, San Diego, California 92129 (US). **WICKERT, Steven A.** [US/US]; 4437 Mission Avenue, Apt. B204, Oceanside, California 92057 (US). **REEDER, Mary A.** [US/US]; 6839 38th Avenue NE, Seattle, Washington 98115 (US). **PATHRIA, Anu K.** [US/US]; 4945 Via Papel, San Diego, California 92122 (US).

(74) **Agent**: **DOUGLAS, Christopher TL**; Black Lowe & Graham, 701 Fifth Avenue, Suite 4800, Seattle, Washington 98104 (US).

(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.

[Continued on next page]

(54) **Title**: SYSTEM AND METHOD FOR FINANCIAL TRANSACTION AUTHENTICATION USING TRAVEL INFORMATION

(57) **Abstract**: Systems and methods for verifying a distant-from-home financial transaction related to a customer account based on travel indicators in earlier purchase transactions made by that customer.

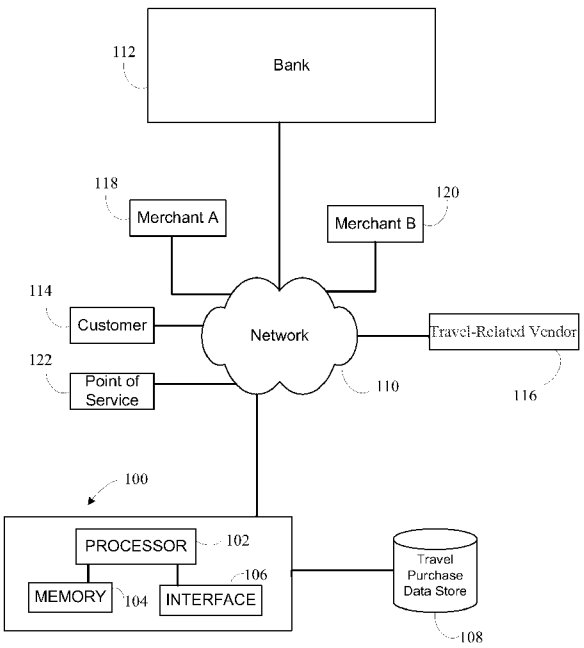

FIG. 1

WO 2011/103432 A2

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

Published:

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

SYSTEM AND METHOD FOR FINANCIAL TRANSACTION AUTHENTICATION USING TRAVEL INFORMATION

INVENTORS
William M. Ferguson
Steve A. Wickert
Mary A. Reeder
Anu K. Pathria

CROSS REFERENCES TO RELATED APPLICATIONS

[0001] This application claims priority to and the benefit of the filing date of U.S. Provisional Patent Application No. 61/306,369 filed February 19, 2010, which is hereby incorporated by reference in its entirety.

FIELD OF THE INVENTION

[0002] This invention relates generally to authentication of financial account transactions (including non-monetary transactions or activities such as online banking logins) and, more specifically, to computerized authentication of transactions.

BACKGROUND OF THE INVENTION

[0003] Financial fraud detection systems often presume that there is increased risk when a transaction on a customer's account occurs far from home. Thus, when customers of financial institutions travel, it is common for their attempted financial transactions while on the road to be declined. The frequency of these declined transactions has been a chronic problem for the financial industry. A common characteristic of compromised financial instruments is having a transaction far from home take place on the account. However, more often than not, distant transactions are legitimate. When organizations frequently decline

these transactions, they lose not only their reputation as a dependable financial institution, but also lose significant revenue from lost fees related to the declined transactions. New authentication solutions have been introduced such as out-of-wallet questions, Chip and PIN, and Secure Code. However, easy and convenient authentication of customers continues to be elusive. Furthermore, these solutions can be enormously expensive. Additionally, some potential users have considered them to be too expensive to implement. For example, banks in the United States have elected to forego Chip and PIN as an anti-fraud solution for credit and debit cards. Additionally, many solutions such as out-of-wallet questions are cumbersome and intrusive to the customer.

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] Preferred and alternative examples of the present invention are described in detail below with reference to the following drawings:

[0005] FIGURE 1 is a diagram of a computerized system in a financial network environment used to provide transaction authentication based on previous travel purchase information;

[0006] FIGURE 2 is a flowchart of a method of authenticating financial transactions based on posting and authorization information; and

[0007] FIGURE 3 is a flowchart of a method of providing transaction authentication based on bank card authorization transactions.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

[0008] Systems and methods for financial transaction authentication using travel-related information are disclosed herein. Systems and methods in accordance with an embodiment of

the invention enhance existing financial transaction authentication solutions by analyzing travel-related purchase transactions for indications of future travel. When a bank normally would have flagged a distant-from-home transaction as risky, travel-related information can dramatically enhance the true understanding of the transaction risk, thereby ensuring better customer quality of service, increased authorizations and decreased false positive fraud indications.

[0009] Authentication using travel-related information provides financial institutions, processors and associations a new tool to increase approved transactions. From the resulting decreased fraud review workload in fraud operations centers, related organizations can transfer the new review capacity to finding additional fraudulent activities. To accomplish this, travel-related information is used that pertains to previously purchased travel-related transactions to identify the likelihood of future distant-from-home locations and timeframes of the bank customer. When a transaction occurs near locations that could be anticipated by an earlier transportation purchase by the bank customer, the transaction can be deemed less risky than if it were not known that the customer was going to be traveling to that location. The precise level of risk is determined by offline statistical modeling of variables generated from historic transaction data along with fraud results data. A statistical regression analysis or neural network modeling technique may be used, for example.

[0010] Financial institutions such as JPMorgan Chase & Co. (New York, NY USA) and Citibank (New York, NY USA), card associations such as Visa Inc. (San Francisco, CA USA) and MasterCard Worldwide (Harrison, NY USA), processors such as Fiserv, Inc.

(Brookfield, WI USA) and Total System Services, Inc. (TSYS) (Columbus, GA USA), and payment networks such as Automated Clearing House (ACH) and PayPal (San Jose, CA USA), rely on a combination of tools to attempt to authenticate financial transactions. Authentication using travel-related information strengthens current investments in authentication technology. For example, a currently installed fraud detection system may indicate that a Moscow-located transaction for a Houston-based customer looks highly risky. Using travel-related information, the Moscow transaction may be further analyzed by looking for a previous transaction for that customer for an airline-purchase transaction to or near Moscow. That planned-travel knowledge enables authentication solutions to better distinguish legitimate from truly risky distant transactions.

[0011] FIGURE 1 is a diagram of a computerized system 100 in a financial network environment used to provide transaction authentication using previous travel purchase information. The system 100 is referred to as a travel analysis platform in some embodiments of the invention. The system 100 includes a processor 102 in data communication with a memory 104 and an interface 106. The system 100 also includes a travel-related purchase data store 108 in data communication with the processor 102. The system 100 is also in data communication with a network 110, such as the Internet. A bank 112, a customer 114, a travel-related vendor 116, a first merchant 118 designated as Merchant A, a second merchant 120 designated as Merchant B, and a point of service 122 are also shown in data communication with the network 110.

[0012] In the example shown, the network 110 facilitates communication between the customer 114 and the travel-related vendor 116, between the point of service 122 and the bank 112, between the merchants 118 and 120 and the bank 112, and between the system 100 and the bank 112. However, in other embodiments, other forms of communication may be used between some or all of these entities. For example, a separate payment processing network may be used for communications between the bank 112 and the point of service 122 and/or between the bank 112 and the merchants 118 and 120. Although a processor, memory, and interface is shown only for the system 100, it should be understood that the bank 112, the customer 114, the travel-related vendor 116, the first merchant 118, the second merchant 120, and the point of service 122 operate and communicate with computerized systems. Additionally, the computerized systems may include a display that allows transaction approval and decline messages to be viewed by a user. For example, a screen may be present at the point of service 122 that shows an approval or decline message or a display on a computerized device such as a mobile phone operated by the customer 114 may show an approval or decline message for transactions performed with the mobile phone.

[0013] In an example embodiment, the bank 112 serves as a credit card issuer to the customer 114. The customer 114 uses the credit card to make purchases from the travel-related vendor 116, such as an airline or a travel agent and/or purchases from the first merchant 118 and the second merchant 120. Later, the customer 114 uses the credit card at the point of service 122 which is located in a location that is at least a predetermined distance from the home of the customer 114.

[0014] Generally, the system 100 is designed to authenticate transactions where banks are concerned with various types of fraud characterized by (among other things) remote-from-home activity. In an example embodiment, the system has the ability to provide financial transaction authentication for at least the following non-limiting use cases: purchase transactions with a debit or credit card at a physical merchant terminal location; purchase transactions with a debit or credit card at an online merchant; purchase transactions with an alternative payment network such as Paypal at an online merchant; ATM activity with a debit or credit card; online banking related to an account with a debit card or credit card; and mobile banking related to an account with a debit card or credit card.

[0015] FIGURE 2 is a flowchart of a method 200 of authenticating financial transactions based on posting and authorization information. First, at a block 202, the bank customer 114 purchases a plane ticket for future distant travel from an airline or agent such as the travel vendor 116 with a bank card. Next, at a block 204, the airline or agent requests authorization from the card issuer such as the bank 112 for the ticket purchase. Next, at a block 206, the issuer bank 112 returns an authorization response message approving the transaction that is received by the airline or agent. Then, at a block 208, the airline or agent sends a posting transaction to the bank 112 including the itinerary for the ticket. A posting transaction generally triggers a money transfer from the issuer bank to the merchant bank. Generally the posting transaction message format provides for travel specific information such as detailed flight information. Next, at a block 210, the bank 112 sends the authorization and posting data for the ticket purchase to a travel analysis platform such as the system 100. Then, at a

block 212, the travel analysis platform stores the transaction information (including the travel itinerary) in a database or other memory device such as the travel-related purchase data store 108.

[0016] Later, at a block 214, during the travel-related to the earlier plane ticket purchase, the customer performs a financial transaction at a point-of-service such as the point of service 122 (e.g., merchant POS, ATM, PC, Mobile Phone) far from home. Then, at a block 216, the point-of-service device sends an authorization request to the financial institution such as the bank 112 for approval. Next, at a block 218, the bank's legacy fraud system indicates that the remote transaction is high risk and the account is flagged to be blocked. Then, at a block 220, the same authorization request is sent to the travel analysis platform from the bank 112. In some embodiments, the authorization request sent to the travel analysis platform from the bank 112 may differ in some manner from the initial authorization request from the point of service 122 to the bank 112. In some embodiments a merchant can send additional information to the travel analysis program, such as IP address information, purchase information and/or information related to the purchaser like an IP address used. Next, at a block 222, the travel analysis platform analyzes historic transaction detail for the account including the airline ticket purchase relating to planned travel that matches the geographic area and date of the new transaction. In an example embodiment, the processor 102 analyzes information previously stored in the travel-related purchase data store 108 based on programming instructions stored in the memory 104. Then, at a decision block 224, the transaction analysis platform determines whether there is low risk from the new transaction.

[0017] If the risk level is determined to be low, a message is sent from the travel analysis platform to the bank 112 to unblock the account at a block 226. In some embodiments, an indicator that corresponds to a level of the risk determined by the system 100 is sent rather than an unblock message. Then, at a block 228, a transaction approval is sent from the bank 112 to the point of service 122 based on the information received at the bank 112 from the system 100.

[0018] If the service performs in real time, an authorization response is sent with "Approve." If the service performs in "one-behind" mode, the current transaction may still be blocked, but subsequent transactions could be approved. If it was determined at the decision block 224 that the risk level is not low, an indication is sent from the system 100 to the bank 112 that the risk level is high at a block 230. Then, at a block 232, a transaction decline is sent from the bank 112 to the point of service 122.

[0019] FIGURE 3 is a flowchart of a method 400 of providing transaction authentication based on bank card authorization transactions. First, at a block 402, the bank customer 114 makes various purchases with a bank card before traveling at vendors such as the first merchant 118 and the second merchant 120, for example. Then, at a block 404 for each purchase, the merchants 118 and 120 request authorization from the card issuer such as the bank 112. Next, at a block 406, the issuer bank 112 returns an authorization response message for each transaction that is received by the merchants 118 and 120. Then, at a block 408, the bank 112 sends the authorization data for the pre-travel purchase to a travel analysis platform such as the system 100. Next, at a block 410, the travel analysis platform stores the

transaction information in a database or other memory device such as the travel-related purchase data store 108.

[0020] Later, at a block 412, the customer 114 performs a financial transaction at a predetermined distance from their home location. Next, at a block 414, the point-of-service device 122 (e.g., merchant terminal, ATM, PC, Mobile Phone) sends an authorization request to a financial institution such as the bank 112 for approval. Then, at a block 416, a bank's legacy fraud system, which is complemented by the systems and methods disclosed herein, indicates that the remote transaction is high risk and the account is flagged to be blocked. Next, at a block 418, the same authorization request is sent from the bank 112 to the travel analysis platform. In some embodiments, the authorization request sent to the travel analysis platform from the bank 112 may differ in some manner from the initial authorization request from the point of service 122 to the bank 112. Then, at a block 420, the travel analysis platform analyzes historic transaction detail for the account including the travel-related purchase information that matches the geographic area and date of the new transaction. Next, at a decision block 422, the transaction analysis platform determines whether there is low risk from the new transaction.

[0021] If risk level is determined to be low, a message is sent from the travel analysis platform to the bank 112 to unblock the account at a block 424. In some embodiments, an indicator that corresponds to a level of the risk determined by the system 100 is sent rather than an unblock message. Then, at a block 426, a transaction approval is sent from the bank 112 to the point of service 122 based on the information received at the bank 112 from the

system 100. If the service performs in real time, an authorization response is sent with "Approve." If the service performs in "one-behind" mode, the current transaction may still be blocked, but subsequent transactions could be approved. If it was determined at the decision block 422 that the risk level is not low, an indication is sent from the system 100 to the bank 112 that the risk level is high at a block 428. Then, at a block 430, a transaction decline is sent from the bank 112 to the point of service 122.

[0022] With regard to the methods 200 and 400 described in FIGURES 2 and 3 respectively, a number of variables may be derived for a modeling and scoring process performed by the system 100 for any given moment in a financial account in determining the risk level at the blocks 222 and 420. In an embodiment, the derived variables include geographic distance between the home address of the customer 114 and a location of the current transaction point of service 122, geographic distance between an airport on the travel itinerary (as identified in card posting data, for example) and the point of service location of the current transaction, and/or time difference between the current transaction and the expected on-the-ground period of the nearest airport on the travel itinerary (as identified in posting data, for example).

[0023] Still with respect to the methods 200 and 400, additional factors may also be used in deriving variables. For example, when traveling in the past, whether the customer has visited this particular merchant before, or this particular chain. If so, this may be indicative of current legitimate travel. An additional factor is whether the customer has recently made purchases at merchant types that are highly indicative of pending legitimate travel such as travel services, dry cleaning, pre-paid airport parking, pre-paid car rental, or hotel

reservations, for example. This might be determined from analyzing whether the merchant identifiers from purchases are within numeric blocks of merchant identifiers reserved for hotels and car rentals, for example. In other embodiments the system may analyze factors such as seasonality of travel; property ownership, reward card points, and/or previous travel habits.

[0024] Additional factors related to airline ticket purchases may also be used. The magnitude of the price for airline ticket purchases may be used, for example. Pricing information may be indicative of distance and also indicative of the time window between when the travel was purchased and when the travel occurs. Other variables related to likely destination location and distance from home may also be used based on what air carrier the travel will be on. For example, Hawaiian Air flies between the contiguous United States to Hawaii and only a few other places. Airlines such as British Air, Aer Lingus, Aeroflot, Air Nippon, and Quantas do not fly domestic U.S. routes. Knowing the air carrier to be used by a legitimate customer can help predict the reasonableness of the locations of purchases made far from the customer's home location.

[0025] While the preferred embodiment of the invention has been illustrated and described, as noted above, many changes can be made without departing from the spirit and scope of the invention. For example, additional or fewer steps may be performed in the methods 200 and 400 and/or some of the steps may be performed in a different order or concurrently. Additionally, although the system 100 is shown as being separate from the bank 112, the system 100 may be integrated within the systems of the bank 112 rather than existing as a

separate system accessed over a network. Although the method 200 uses card posting information including a travel itinerary and method 400 uses travel-related purchase information without posting information or an itinerary, some embodiments may incorporate aspects of both methods such that both travel itinerary information from card posting data and travel-related purchase information such as purchases from a car rental company could be used. Different or additional travel-related purchase data elements may also be used than those described. Accordingly, the scope of the invention is not limited by the disclosure of the preferred embodiment. Instead, the invention should be determined entirely by reference to the claims that follow.

[0026] The embodiments of the invention in which an exclusive property or privilege is claimed are defined as follows:

1. A method in a computing system, comprising:

storing an indication of a pending travel event in a travel analysis platform, the indication of the travel event generated based on a travel-related financial transaction;

generating a current location of a user based on the stored indication of the travel event in the travel analysis platform;

receiving a current transaction authorization request from a point of service;

generating a transaction approval indication when a location of the current transaction authorization request and the generated current location of the user, based on the indication of the travel event in the travel analysis program, are within a predetermined distance; and

transmitting to a bank, a request to communicate a transaction approval indication to the point of service that transmitted the current transaction authorization request.

2. The method of claim 1 comprising:

storing a plurality of travel transactions relating to a travel event;

determining travel characteristics for a user based on the stored transactions;

generating an indication of the pending travel event based on determined travel characteristics; and

populating the travel analysis platform based on the determined travel characteristics.

3. The method of claim 2 wherein the indication of a travel event is itinerary information.

4. The method of claim 3 comprising:

determining a carrier for the travel transaction;

comparing the location of the current transaction authorization request with a known destination of the determined carrier;

generating a transaction approval indication when a known destination of the determined air carrier is within a predetermined distance from the location of the current transaction authorization request.

5. The method of claim 4 comprising:

comparing the location of the current transaction authorization request with historic transaction information; and

transmitting an indication of transaction approval when the location of the current transaction authorization request matches historic transaction information.

6. The method of claim 5 comprising:

generating an indication of pending travel, based on one or more transactions that are suggestive of pending travel; and

populating the travel analysis platform with the generated indication of pending travel.

7. The method of claim 6 comprising:

calculating a time period a user is in a location based on at least one of distance from an airport and time between flights.

8. The method of claim 1 wherein the monitored transactions are financial transactions using at least one of a bank card, online payment and mobile bill payment.

9. The method of claim 8 wherein travel characteristics are at least one of flight date, flight time, arrival location, and hotel location.

10. The method of claim 9 comprising:

estimating at least one of a distance and time of travel based on a price of an airline ticket; and

transmitting an indication of transaction approval when the estimated distance of travel is within a predetermined threshold of the actual distance from a residence of the user.

11. The method of claim 1 comprising:

using a computerized verification system, sending the transaction approval indication from the computerized verification system to a computerized payment network, wherein the computerized verification further comprises at least one of of a risk score indicator and a binary risk indicator,; and

determining whether the transaction should be authorized.

12. A computing system configured to facilitate a transaction approval system, comprising:

a memory;

a module stored on the memory that is configured, when executed, to:

generate a travel itinerary in a travel analysis platform based on one or more travel-related financial transactions;

receive a current transaction authorization request;

predict a current location of a user based on the generated travel itinerary; and

transmit a transaction approval recommendation when a location of the received transaction authorization request and the predicted current location of the user are within a predetermined distance.

13. The computing system of Claim 12 wherein the module is further configured, when executed, to:

receive a current transaction authorization request when a computerized verification system flags a current transaction.

14. The computing system of Claim 13 wherein the module is further configured, when executed, to:

determine a carrier for the travel transaction;

compare the location of the current transaction authorization request with a known destination of the determined carrier; and

generate a transaction approval indication when a known destination of the determined air carrier is within a predetermined distance from the location of the current transaction authorization request.

15. The computing system of Claim 12 wherein the module is further configured, when executed, to:

generate an indication of pending travel, based on one or more transactions that are suggestive of pending travel; and

populate the travel analysis platform with the generated indication of pending travel.

16. The computing system of Claim 12 wherein the module is further configured, when executed, to:

estimate at least one of a distance and a date of travel based on a price of an airline ticket; and

transmit an indication of transaction approval when the estimated distance of travel is within a predetermined threshold of the actual distance from a residence of the user.

17. A computer-readable medium whose contents, when executed, cause a computing system to facilitate a transaction approval system, by performing a method comprising:

storing a received travel itinerary in a travel analysis platform;

determining a current location of a user based on the travel itinerary;

receiving a current transaction authorization request from a bank;

generating a transaction approval indication when a location of the current transaction authorization request and the generated current location of the user are within a predetermined distance; and

providing the transaction approval indication to the bank that transmitted the current transaction authorization request.

18. The computer-readable medium of claim 17 comprising:

estimating a distance of travel based on a price of an airline ticket; and

providing an indication of transaction approval when the estimated distance of travel is within a predetermined threshold of the actual distance from a residence of the user.

19. The computer-readable medium of claim 17 comprising:

using a computerized verification system, sending the transaction approval indication from the computerized verification system to a computerized payment network; and

determining whether the transaction should be authorized based on the transaction approval indication at the computerized payment network.

20. The computer-readable medium of claim 17 wherein the computer-readable medium is at least one of a memory in a computing device or a data transmission medium transmitting a generated signal containing the contents.

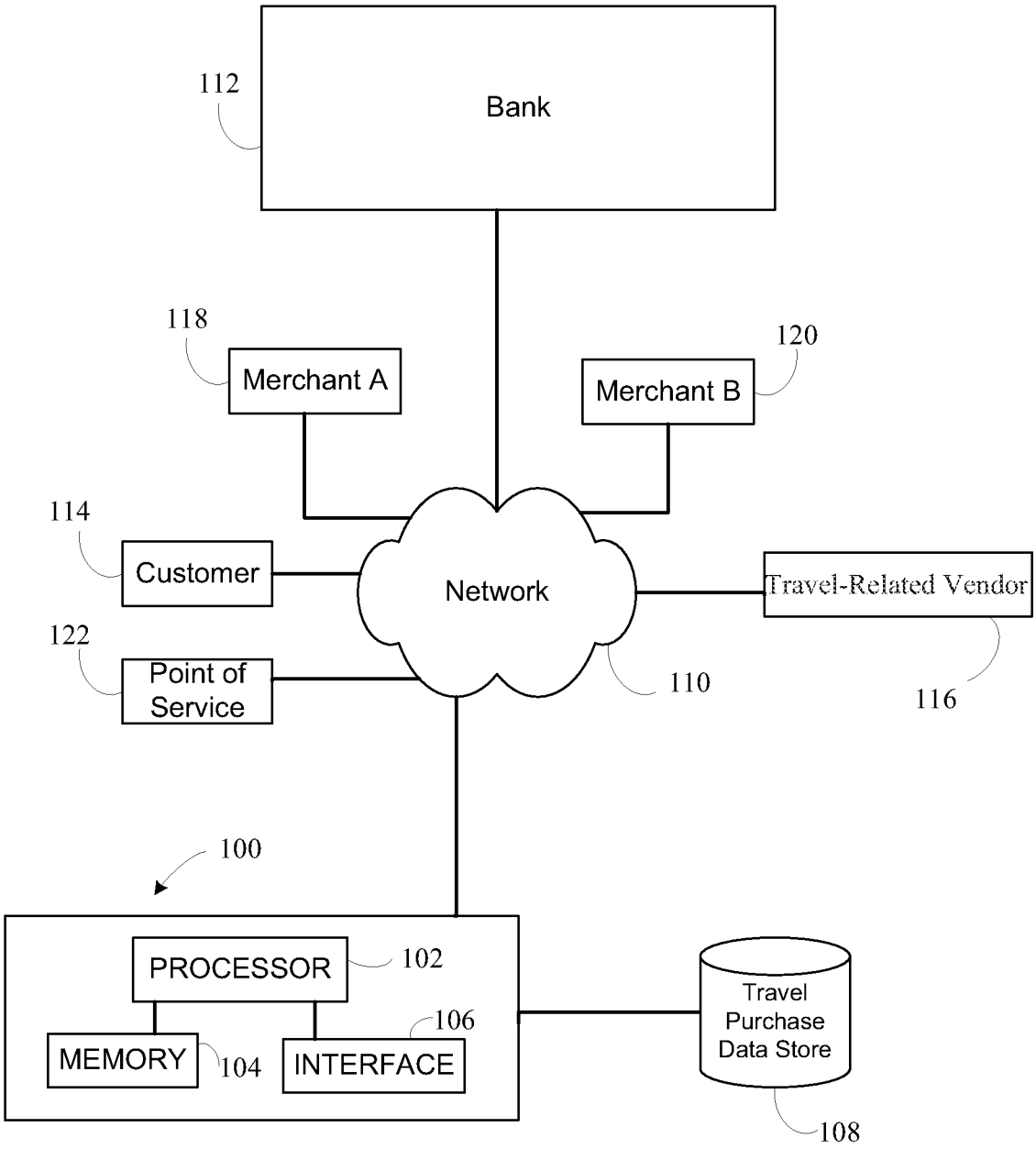
112
Bank
118
Merchant A
120
Merchant B
114
Customer
Network
Travel-Related Vendor
122
Point of Service
110
116
100
PROCESSOR
102
MEMORY
104
106
INTERFACE
Travel Purchase Data Store
108

FIG. 1

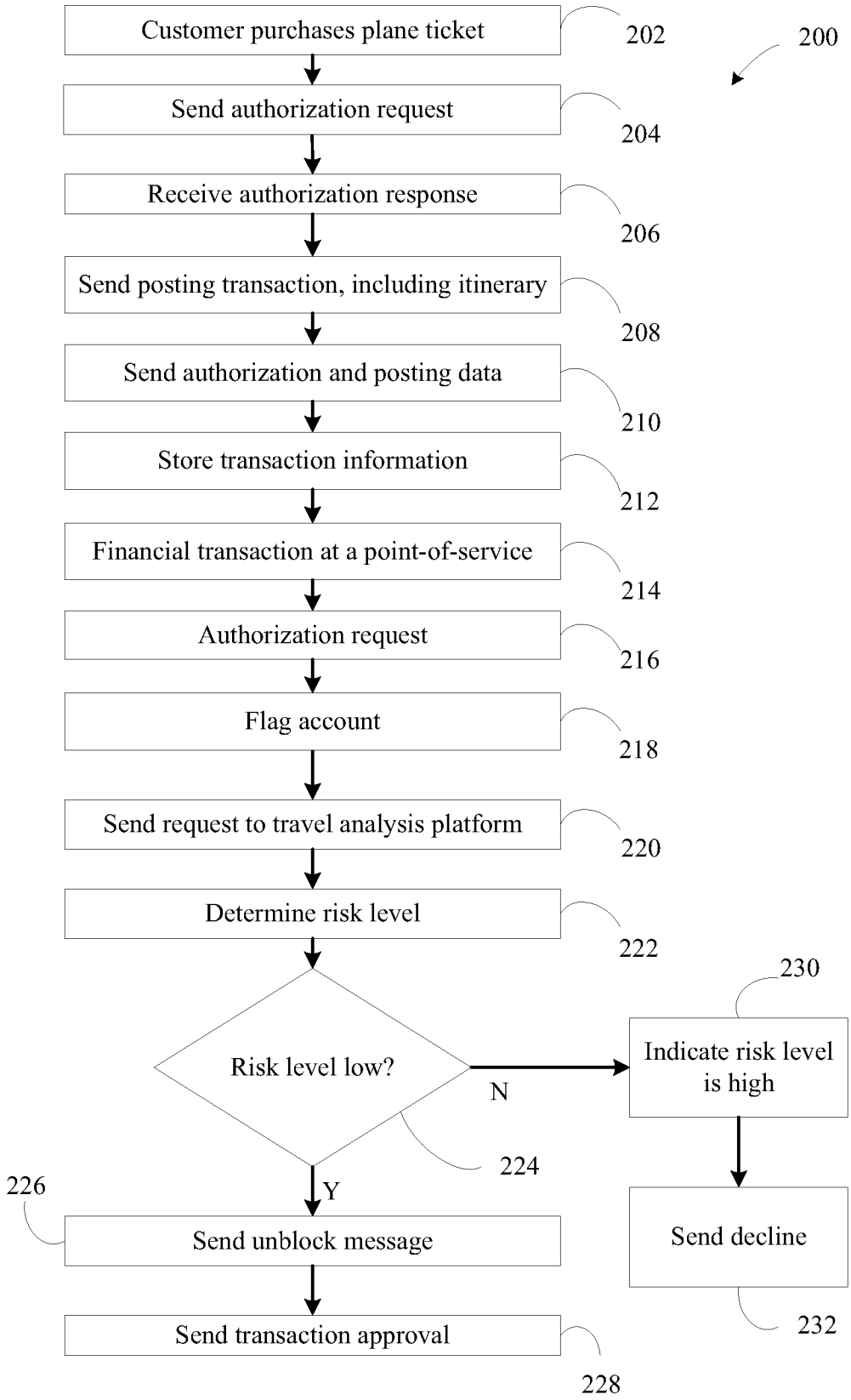
Customer purchases plane ticket
202
200
Send authorization request
204
Receive authorization response
206
Send posting transaction, including itinerary
208
Send authorization and posting data
210
Store transaction information
212
Financial transaction at a point-of-service
214
Authorization request
216
Flag account
218
Send request to travel analysis platform
220
Determine risk level
222
Risk level low?
N
Y
224
230
Indicate risk level is high
Send decline
232
226
Send unblock message
Send transaction approval
228

FIG. 2

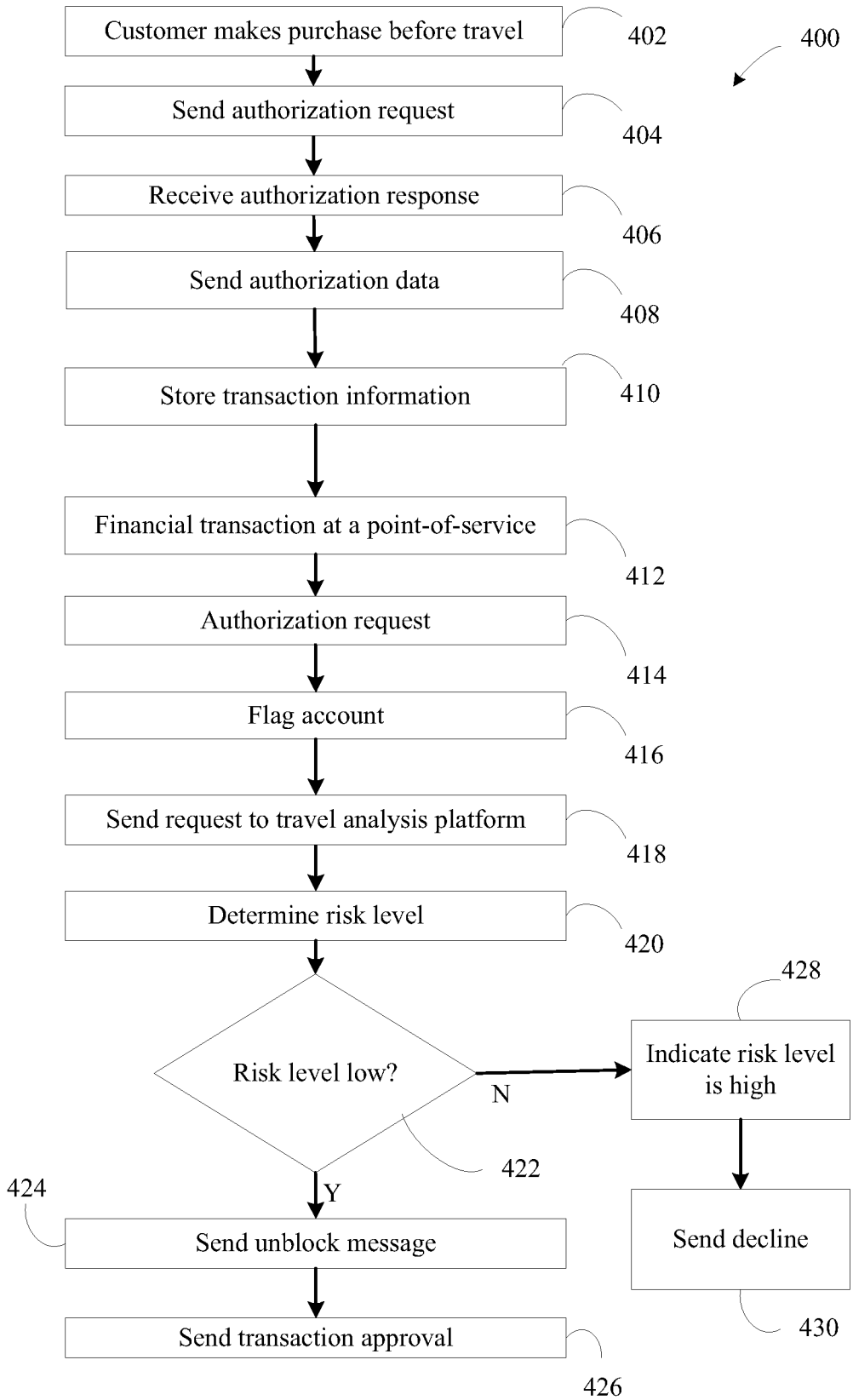
Customer makes purchase before travel
402
400
Send authorization request
404
Receive authorization response
406
Send authorization data
408
Store transaction information
410
Financial transaction at a point-of-service
412
Authorization request
414
Flag account
416
Send request to travel analysis platform
418
Determine risk level
420
Risk level low?
N
Y
422
428
Indicate risk level is high
Send decline
430
424
Send unblock message
Send transaction approval
426

FIG. 3