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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 September 2012 (13.09.2012)

WIPO | PCT

(10) International Publication Number
WO 2012/121983 A2

(51) International Patent Classification:
G06Q 20/40 (2012.01)

(21) International Application Number:
PCT/US2012/027335

(22) International Filing Date:
1 March 2012 (01.03.2012)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
13/041,178 4 March 2011 (04.03.2011) US

(71) Applicant *(for all designated States except US)*: **BRIGHTERION, INC.** [US/US]; 150 Spear Street, 10th Floor, San Francisco, CA 94105 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **ADJAOUTE, Akli** [US/US]; 3 Community Road, Belvedere, CA 94920 (US).

(74) Agent: **TREYZ, G., Victor**; Treyz Law Group, 870 Market Street, Suite 984, San Francisco, CA 94102 (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, QA, RO, RS, RU, RW, 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, LR, LS, MW, MZ, NA, RW, 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,

[Continued on next page]

(54) Title: SYSTEMS AND METHODS FOR ADAPTIVE IDENTIFICATION OF SOURCES OF FRAUD

(57) Abstract: A fraud detection engine is provided that analyzes transactions for fraudulent transactions. The transactions may include credit card or debit card transactions. The fraud detection engine may identify possible sources of fraud. The fraud detection engine may identify possible phony acceptors that masquerade as genuine merchants. The fraud detection engine may identify compromising points where accounts become compromised and are prone to fraudulent transactions thereafter. The fraud detection engine may receive and analyze transaction data in real-time or in batch mode. The fraud detection engine may use fuzzy logic. The fraud detection engine may use artificial intelligence such as case-based reasoning or business rules.

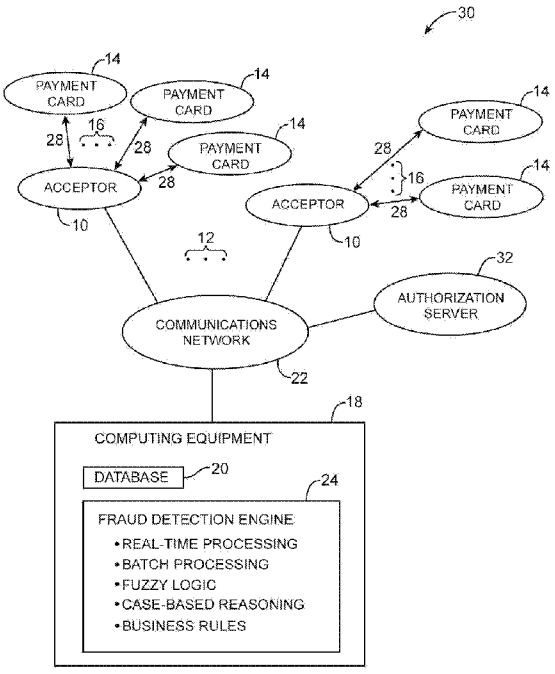

FIG. 1

WO 2012/121983 A2

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))*

SYSTEMS AND METHODS FOR ADAPTIVE IDENTIFICATION OF SOURCES OF FRAUD

This application claims priority to United States patent application No. 13/041,178, filed March 4, 2011, which is hereby incorporated by reference in its entirety.

Background

This invention relates to fraud detection, and more particularly, to analyzing and identifying sources of fraud in real time.

Transactions made with payment cards such as credit cards, prepaid cards, debit cards, and smart phones, can be susceptible to fraud. There are many possible types of fraud. In one type of fraud, a phony merchant may initially (dormant period) masquerade as a genuine merchant and then suddenly begin making many fraudulent transactions using all the previous cards that visited that merchant. In other types of fraud, payment cards or account information may be stolen. Fraudulent transactions may occur on the account after the card has visited a root of compromised accounts (acceptor).

Payment card issuers, such as banks and other financial institutions are often motivated to detect and stop fraudulent transactions. The most costly way is when

the card issuer learns of the fraudulent transactions only when it is reported by a cardholder. However, there may be a delay between the time a fraudulent transaction occurs and when it is noticed and reported by the cardholder. Meanwhile, the source of fraudulent transaction may continue to compromise that account and other cardholders' accounts.

It would be desirable to provide a way to rapidly stop fraudulent transactions and identify in real-time the root/sources of compromised accounts as well as phony merchants.

Summary

A system is provided that analyzes in real-time, inputs from four sources:

1) Scores with high threshold received from various real-time TCP Transaction Servers (TTS).
2) The abnormal activities received from various real-time velocity servers.
3) The patterns from various real-time profiling servers.
4) External sources: flat files, databases, to detect the root of compromising and phony merchants.

The engine will also have access to information from the profiling servers related to:

1) Type of merchant or card or bin or any combination of these fields.
2) Number of transactions for a card in the last 30, 60, 90, 365 days, or other suitable time intervals.
3) Average amount spent by a card on groceries, books, electronic, or other categories in any

previous time interval.

4) Number of cross border travels in the last year.

5) Average purchase amount at that merchant over the last week or other suitable time interval.

6) Number of declined cards at that merchant over the last week or other suitable time interval.

7) Number of high scored transactions at that merchant over the last week or other suitable time interval.

8) Number of cards that visited the merchant and then become fraudulent.

9) Average cash-back amount at that merchant over the 90 days, or other suitable time interval.

A real-time fraud detection engine may be implemented on computing equipment. The fraud detection engine may receive data from transactions over a communications network. The transactions may include genuine and fraudulent transactions.

The real-time fraud detection engine may use smart-agents, Data Mining, Neural network, Business Rules, fuzzy logic, case-based reasoning, optimization, and genetic algorithms. The real-time fraud detection engine may analyze in real-time scores with a high threshold received from various servers such as a TCP Transaction Server, inputs from various velocity servers, as well as patterns received from various profiling servers to identify the possible root of compromised accounts.

The real-time fraud detection engine may also provide a list of possible phony merchants. Phony merchants may masquerade as genuine merchants and conduct fraudulent transactions even if initially (during a dormant period) they act as genuine merchants. The real-time fraud detection engine may provide a list of possible

compromising points. A compromising point may be the point at which a cardholder's account compromised or stolen. A compromising point may be a merchant, terminal, website, etc. A fraud detection engine may analyze transactions data in real-time and provide dynamically updated lists of phony merchants and compromising points. A fraud detection engine may also operate in batch mode.

Further features of the invention, its nature and various advantages will be more apparent from the accompanying drawings and the following detailed description of the preferred embodiments.

Brief Description of the Drawings

FIG. 1 is a diagram of an illustrative transaction system having a fraud detection engine in accordance with an embodiment of the present invention.

FIG. 2 is flow chart showing steps used in real-time fraud detection in accordance with an embodiment of the present invention.

FIG. 3 is an illustrative fuzzy object that may represent information about an acceptor in accordance with an embodiment of the present invention.

FIG. 4 is a diagram of an illustrative fraud detection engine implemented on a distributed architecture in accordance with an embodiment of the present invention.

Detailed Description

This is related to detecting fraudulent transactions and sources of fraud.

Transactions may include transactions made using payment cards such as credit cards, prepaid cards, debit cards, charge cards, stored-value cards, consumer or corporate cards, gift cards, or other types of payment cards. Payment cards may display account information,

such as an account number, expiration date, or security card. Payment cards may also store information. Payment cards may be magnetic stripe cards, smart card, or proximity cards. Payment cards may have associated accounts and users (also known as cardholders). Transactions may also be made on accounts that do not have payment cards. Transactions on an account with a payment card may also be conducted with the physical card, such as in a transaction made over the internet or in a phone call or by mail.

Payment cards and associated accounts may be issued by a financial institution such as a bank or credit card company. The payment card issuer may be known as a card-issuing bank. The card-issuing bank may belong to a credit card association such as Visa or Mastercard.

A transaction may take place between a user (also known as a cardholder) and a merchant (also known as an acceptor). A typical transaction may consist of a payment. A customer may make a payment to a merchant in exchange for goods or services. Other types of transactions may include refunds (also known as credits).

A merchant may have a merchant account at a bank known as an acquiring bank, or acquirer. During a transaction, an acquiring bank may verify the cardholder's account and payment amount with the card-issuing bank. The card-issuing bank may pay the acquiring bank. The acquiring bank may place deposits into a merchant's account at the acquiring bank.

A payment card need not be physically present in order to make a transaction on an account. For example, credit card information may be recited over the phone to make a purchase. Payment card information may also be entered into a website when making an online transaction. Such transactions may be known as card not present (CNP)

transactions.

Payment cards may be vulnerable to many different types of fraud.

In one type of fraud, a phony merchant (also known as a phony acceptor) may masquerade as an authentic merchant. For example, a fraudster may create a website that appears to sell or offer genuine goods and services, but may in fact be a front for fraudulent transactions.

In one type of fraud, a payment card may be stolen, or payment card information may be stolen although the cardholder maintains physical possession of the payment card. For example, a store or restaurant may have a dishonest employee that records credit card information in the course of conducting an authentic transaction. In another example, fraudsters may attach devices known as "skimmers" to ATMs (automatic teller machines) or to gas station fuel pumps that surreptitiously record information from payment cards. Payment card information may also be surreptitiously stolen during online transactions on the internet. Stolen card information may be collected by thieves who then sell the information to others who perpetrate the fraudulent transactions. In this type of fraud, a payment card may be compromised long before any fraudulent transaction has occurred on the account. The point at which a payment card is compromised may be known as a compromising point. The compromising point may be a merchant or may be located at a merchant.

Once a fraudulent transaction has occurred, it might be some time before a cardholder notices that their account has been compromised. For example, a cardholder might not notice a fraudulent transaction on their credit card statement. A fraudulent transaction might deliberately be for a small amount in order to escape notice. As a result, significant time may elapse between

a fraudulent transaction and when a user reports the fraudulent transaction to a bank or payment card issuer. In the meantime, other cardholders' accounts may be compromised by the same phony merchant, or at the same compromising point.

It may therefore be advantageous to detect fraudulent transactions before they are reported by the cardholder. It may also be advantageous to identify possible sources of fraudulent transactions so that other cardholders' accounts may be protected.

FIG. 1 is a diagram of an illustrative transaction system that may be provided with fraud detection.

Transaction system 30 of FIG. 1 may have acceptors 20 that accept transactions 28 with payment cards 14. Transaction system 30 may have any suitable number of acceptors 10, as indicated by dots 12. Acceptors 10 may also be known as merchants. Each acceptor 14 may conduct transactions with any suitable number of payment cards 14, as indicated by dots 16. Payment cards 14 may as credit cards, debit cards, or other payment cards. Payment cards 14 may also be known as payment accounts. Payment accounts need not have an associated card. Transactions 28 involving payment cards 14 need not involve the presence of a physical card, as transactions 28 may be conducted using account information from payment cards 14.

Acceptors 10 may communicate through communications network 22 with an authorization server such as authorization server 32. Authorization server 32 may authorize transactions 28. Authorization server 32 may belong to a card-issuing bank or an acquiring bank. Authorization server 32 may be part of a credit card network such as Visa or Mastercard. Communications

network 22 may be a secure communications network.

Computing equipment 18 may receive data associated with transactions 28 through communications network 22. Computing equipment 18 may receive transaction data from authorization server 32 through communications network 22. Computing equipment 18 may have one or more databases such as database 20. Computing equipment 18 may have a fraud detection engine such as fraud detection engine 24. Computing equipment belong to a financial institution such as a card-issuing bank. Computing equipment may belong to a third-party that analyzes transaction data in order to detect fraud for a card-issuing bank.

Fraud detection engine 24 may process transaction data in order to detect fraudulent transactions and identify sources of fraud. Fraud detection engine 24 may process transaction data in real-time. Fraud detection engine 24 may also be configured to process transaction data in batches. Fraud detection engine 24 may use fuzzy logic to analyze transaction data. Fraud detection engine 24 may use artificial intelligence such as smart agents, case-based reasoning, data mining, neural network, optimization, or expert systems to analyze transaction data.

Fraud detection engine 24 may analyze transaction data in real-time using steps as shown in FIG. 2. In step 34, fraud detection engine 24 may receive data from a transaction. Data from a transaction may include cardholder account information, merchant account information, and payment information such as date, time, and amount. Transaction data from both genuine and fraudulent transactions may be received by fraud detection engine 24. Fraudulent transactions may form a fraction of the total transactions. Data may be received from

approved transactions and unapproved transactions.

In step 36, fraud detection engine 24 may determine whether a transaction has a high risk of being fraudulent. Fraud detection engine 24 may compare each transaction with a cardholder's past history or an acceptor past history to determine which transactions appear abnormal. Qualities about a transaction such as the amount, date, time, and type (e.g., restaurant, online, etc.) may be considered when determining whether a transaction may be a fraudulent transaction.

Fuzzy logic may be used to determine whether a transaction may be fraudulent. For example, each transaction's risk of being fraudulent may be stored as a fuzzy attribute (e.g., a transaction's risk of being fraudulent may fuzzy values such as "low risk", "medium risk", or "high risk." Transactions may also be labeled as "genuine" and "fraud," or "abnormal," "suspicious," and "normal." Artificial intelligence technologies may be used to detect fraudulent transactions. Smart agents, case-based reasoning, data mining, neural network, and optimization may be used to determine whether a transaction may be fraudulent. Expert systems (also known as business rules) may also be used to determine whether a transaction may be fraudulent.

If a transaction has a high risk of being fraudulent, the transaction may be said to be a fraudulent transaction. That transaction may be placed in a pool of high-risk transactions that may undergo further analysis, as shown in step 38.

The steps of receiving transaction data 34, determining a transaction's risk of being fraudulent in step 36 and placing high-risk transactions in a pool to be analyzed in step 38 may be conducted in real-time or in batch mode. When fraud detection engine 24 performs these

steps in real-time, fraud detection engine 24 may continuously receive new transaction data, and dynamically update a list of high-risk (or suspicious) transactions. If fraud detection engine 24 is configured to operate in batch mode, fraud detection engine 24 may, for example, analyze transactions for high-risk transactions at intervals of time, e.g., daily, weekly, bimonthly, etc. Fraud detection engine 24 may also be configured to perform some processes in real-time and other processes in batch mode.

Transaction data may be also be used to determine whether some cards (or accounts) have been compromised. For example, if a large number of fraudulent transactions have occurred on a card, that card might be said to be a compromised or fraudulent card. The risk at which a card might be fraudulent may be stored as a fuzzy value.

Fraudulent transactions may be analyzed by fraud detection engine to determine sources of fraud, as shown in step 42. Fraud detection engine 24 may analyze fraudulent transactions to determine if multiple fraudulent transactions occurred at the same acceptor. Such an acceptor may be a phony merchant. Fraud detection engine 24 may determine whether fraudulent transactions occurred on multiple accounts in which the cardholders had previously visited the same merchant. Such a merchant may be a compromising point.

Fraud detection engine 24 may analyze fraudulent transactions in order to detect patterns of fraud. Fraud detection engine 24 may identify possible sources of fraud, as shown in step 42 of FIG. 2. Fraud detection engine 24 may identify possible phony merchants, as shown in step 44. The risk that a merchant might be a phony merchant may be indicated by a fuzzy value. For example,

a merchant may be labeled as "genuine," "suspicious," "normal," or any suitable fuzzy value. A value that indicated whether a merchant is fraudulent may also be referred to as a score.

Fraud detection engine 24 may identify potential compromising points, as shown in step 45. The likelihood that an acceptor may be a compromising acceptor may be indicated by a fuzzy value such as "genuine," "suspicious," "normal," or any suitable fuzzy value.

If desired, fraud detection engine 24 may also analyze transaction data to identify other types of fraud sources.

Fraud detection engine 24 may perform the analysis of step 42 in real-time. When fraud detection engine 24 is configured to operate in real-time, fraud detection engine 24 may dynamically extract a list of phony acceptors in step 44. Fraud detection engine 24 may dynamically extract a list of compromising points in step 45. Fraud detection engine 24 may assign scores to acceptors that indicate the likelihood that acceptors may be compromising phony.

When fraud detection engine 24 is operated in real-time, results for possible compromising acceptors and phony merchants may be updated very frequently, e.g., every 5 minutes or less, every 2 minutes or less, etc. Fraud detection engine 24 may process a large number of transactions in a short period of time. For example, fraud detection engine 24 may process data from millions of cards or billions of transactions with a response time less than 50 milliseconds.

Fraud detection engine 24 may also operate in batch mode. In batch mode, fraud detection engine 24 may perform analyses in intervals of every week, every two weeks, etc. Fraud detection engine 24 may also perform

some analyses in real-time and some analyses in batch mode.

Fraud detection engine 24 may use fuzzy logic. Fraud detection engine 24 may use fuzzy objects having fuzzy attributes.

FIG. 3A is a diagram of an illustrative fuzzy object that may be used for each acceptor. Acceptor object 46 may be identified by an acceptor key such as Acceptor_Key 48. Acceptor object 46 may have attributes 64. Attribute 50, Num_Comp_Frd_Cards, may represent the number of cards that experienced a first fraudulent transaction after conducting a transaction with this acceptor. A visit to this acceptor may be required to occur within a specified time window before the first fraudulent transaction. The time window may be adjustable depending on the desired depth of analysis.

Attribute 52, Num_Frd_Crds, may represent the number of cards that experienced a fraudulent transaction either before or after a transaction with this acceptor. Num_Frd_Crds_during_w1 53 may represent a number of accounts on which an approved fraudulent transaction takes place within a specific time period known as window of time 1. A visit to this acceptor can take place after the first fraud on an account, as long as a fraudulent transaction occurs within the window of time 1 following the visit. Num_Frd_Crds_during_w2 55 may represent a number of accounts on which an approved fraudulent transaction takes place within another time period known as window of time 2.

Attribute 54, Num_Frds, may represent the number of fraudulent transactions that occurred on cards following a transaction with this acceptor. Num_Frds_during_w1 57 may represent the total number of approved fraudulent transactions that take place within a

specific time period - known as window of time 1 - after a visit to the acceptor. The visit may take place before or after the first fraud on an account. Num_Frds_during_w2 59 may represent the total number of approved fraudulent transactions that take place within another specific time period - known as window of time 2 - after a visit to the acceptor.

Attribute 56, Acceptor_Frds, may represent the number of approved fraudulent transactions that occurred at this acceptor. Any fraudulent transaction at any point in time may be counted.

Num_Cards 58 may represent the total number of cards on which this accepter appears in an approved transaction. Num_Cards may be computed on both genuine and fraudulent cards. Num_Cards may include only approved fraudulent transactions.

Attribute 60, Num_Trx, may represent the number of transactions that have occurred on cards following transactions at this acceptor, including transactions at other acceptors. Num_Trx may be computed on both genuine and fraudulent cards, and may count both fraudulent and genuine transactions. Num_Trx_during_w1 61 may represent the number of transactions that took place within specific time period, known as window of time 1, following a visit to this acceptor. Num_Trx_during_w2 63 may represent the number of transactions that took place within another time period, known as window of time 2, following a visit to this acceptor.

Attribute 62, Acceptor_Trx, may represent the number of transactions that have occurred at this acceptor. Attributes 64 in FIG. 3A may be fuzzy attributes. Acceptor_Trx may count both fraudulent and genuine transactions.

Each acceptor may be given a score, such as

Scores 65 in FIG. 3A. Score 65 may indicate the likelihood of an acceptor being phony, compromising or otherwise fraudulent. Score 65 may be a fuzzy attribute. For example, a card may have a score of "low," "medium," or "high" risk. When fraud detection engine 24 is performing real-time analysis of incoming transaction data, Score 65 may be increased if instances of fraudulent transactions are found to occur at the acceptor, or if fraudulent transactions occur after a visit to the acceptor. The score may be also known as a similarity. There may be one or more scores 65. Each acceptor may have one score indicating its risk of being a phony acceptor and another score indicating its risk of being a compromising point. Acceptors may have any suitable number of scores.

Each card or account 14 may be stored in an associated fuzzy object. An object for a card might have such attributes as account number, name of user, number of fraudulent transaction, geographical data, spending patterns, types of purchases (such as online purchases or purchases made in brick and mortar stores), frequencies of specific merchant categories (in categories such as gas stations, restaurants, etc, as indicated by a merchant category code (MCC). These attributes may be fuzzy attributes. Each card may also have an associated score that indicated the likelihood of the card being compromised. Such a score may be a fuzzy score. For example, a card may have a score of "low," "medium," or "high" risk. A card may also be scored as "normal," "abnormal," "suspicious," or any suitable value.

Each transaction 28 may be stored in an associated fuzzy object. A transaction object may have attributes such as time and date, amount, merchant category code (MCC), location, acceptor identification

information, acquirer identification information (such as an acceptor's bank). These attributes may be fuzzy attributes. For example, time may be a fuzzy attribute that may indicate whether or not a transaction occurred during business hours. A time fuzzy attribute may take into account fuzziness in business hours - for example, sometimes business hours could be considered to end sometimes at 5pm and sometimes at 6pm. Each transaction 28 may have a score that may be stored as a fuzzy attribute of the transaction object. The score may indicate the likelihood of the transaction being fraudulent.

Fuzzy objects for acceptors, cards, and transactions may be stored in a database such as database 20 of FIG. 1. Transaction data may be stored in database 20.

Fraud detection engine 24 may use artificial intelligence such as case-based reasoning and expert systems.

Case-based reasoning is a process of solving new problems based on the solutions of similar past problems. Fraud detection engine 24 may identify sources of fraud based on a history of how sources of fraud were identified in the past.

Expert systems may also be known as business rules. Expert systems may have rules that consist of "IF - THEN" clauses. Fraud detection engine 24 may use such rules to decide whether an acceptor is a compromising acceptor. For example, an acceptor that processes 10,000 transactions, out of which 100 are determined to be fraudulent transactions, might be considered to be a genuine acceptor. On the other hand, an acceptor that processes 250 transactions, out of which 100 are fraudulent transactions, might be considered to be a phony

merchant. Business rule may be fuzzy business rules.

In order to extract a list of phony acceptors, such as in step 44 of FIG. 2, fraud detection engine 24 may compute a fraud risk for each acceptor using fuzzy logic and fuzzy values. The fraud risk may be primarily based on a number or rate of fraudulent transactions that occurred at each acceptor, but may be enhanced based on other attributes. The fraud risk may be a score such as score 65 of FIG. 3A. The computation of fraud risk may be performed by a method known as GetRisk(). After the fraud risk has been computed for the acceptors, the riskiest acceptors may be considered to be on a list of phony acceptors. The fuzzy objects may collaborate to produce this list. Assessing the riskiest acceptors may be performed by a method known as AssessRisk().

In order to extract a list of compromising acceptors, such as in step 45 of FIG. 2, a fraud risk of acceptors may be computed that is primarily based on a rate of fraudulent transactions that occur on a card after a visit to each acceptor. The rate of fraudulent transactions may be a fuzzy attribute. Such a fraud risk may be a score such as one of scores 65 of FIG. 3A. The computation of such a fraud risk may be a performed by a method, which may be called GetRiskCardAfter(). One the risk levels have been computed, the fuzzy objects collaborate so that the compromising acceptors emerge. This step may be performed by another method, which may be called AssessRisk().

Once lists of compromising accepters and phony merchants are produced, actions may be taken against these accepters. Cardholders that have visited those acceptors may be warned, or cards that have visited those acceptors may be refused at future transactions. A suspicious pool

of cards may be provided to a credit card processer such as Visa or Mastercard, or to a bank or financial institution that issues the cards.

Fraud detection engine 24 may perform some analyses in real-time and other analyses in batch mode. For example, fraud detection engine 24 may assess in real time an authorization request submitted by an authorization server of an acquirer. Fraud detection engine 24 may inform the authorization server in real time whether the authorization request of a given transaction should be authorized.

Fraud detection engine 24 may have a portion, also known as a model, that operates in real-time and a portion that operates in batch mode. Fraud detection engine 24 may have a batch mode model that provides, e.g., a black list of acceptors, list of high risk merchants, a list of phony merchants, or other information to a real-time model that assesses transaction authorization requests in real-time.

Fraud detection engine 24 may also receive and analyze transaction data that includes fallback methods, credit transactions such as refunds and merchant authorization reversals, transactions conducted at high-risk merchants, personal account number (PAN) key-entry transactions that exceed typical ratios, abnormal business hours, abnormal seasons, abnormal amounts, inactive merchants, volume of declined transactions and their type (i.e. invalid CVC - card verification code, insufficient funds, etc.), inconsistent authorization and clearing data elements for the same transactions. Fraud detection engine 24 may monitor any desired transaction data for suspicious activity.

Fraud detection engine 24 may monitor merchant authorization requests in real-time and provide real-time

alerts based on suspicious activity. Such activity may include a number of authorization requests that are determined to be riskier than a certain threshold. The threshold may be set by the acquirer for that merchant. Fraud detection engine 24 may monitor a ratio of card present to card not present transactions that are determined to be riskier than a certain threshold set by the acquirer for that merchant. Fraud detection engine 24 may monitor a ratio of PAN key entry transactions to non-PAN transactions that are determined to be riskier than a certain threshold set by the acquirer for that merchant. Fraud detection engine 24 may monitor repeated authorization requests for the same amount or the same account. Fraud detection engine 24 may monitor for an increased number of authorization requests compared to the normal activity for a merchant. Fraud detection engine 24 may monitor for an unusual fallback transaction volume. Such behavior may indicate that a merchant may be a phony merchant.

Fraud detection engine 24 may monitor increases in merchant deposit volume, increases in a merchant's average ticket size and number of transactions per deposit, change in frequency of deposits, frequency of transactions on the same cardholder account, including credit transactions, unusual numbers of credits, or credit dollar volume, exceeding a level of sales dollar volume appropriate to the merchant category, and large credit transaction amounts, significantly greater than the average ticket size for the merchant's sales. Such behavior may indicate that a merchant may be a phony merchant. Fraud detection engine 24 may monitor these behaviors in real-time and provide real-time alerts to an acquirer.

Fraud detection engine 24 may compare daily

deposits from transactions into an acquirer's account at an acquirer's bank and compare against average numbers of transactions and transaction amounts. The average may be taken over a certain period of time, e.g., of 90 days or any suitable period of time. Unusual number of transactions or transaction amounts may indicate suspicious behavior for by the acquirer. For example, suspicious behavior may be considered to be 150% of the average number of transactions or 150% of the usual transactions amounts.

Fraud detection engine 24 may compare average number of transactions and transaction amounts for new merchants with other merchants in the same merchant category code. Unusual number of transactions or transaction amounts may indicate suspicious behavior for by the merchant. For example, suspicious behavior may be considered to be 150% of the average number of transactions or 150% of the usual transactions amounts.

Fraud detection engine 24 may analyze, in real-time, inputs from four sources:

1) Scores with high threshold received from various real-time TCP Transaction Servers (TTS).
2) The abnormal activities received from various real-time velocity servers.
3) The patterns from various real-time profiling servers
4) External sources: flat files, databases, to detect the root of compromising and phony merchants.

The engine will also have access to information from the profiling servers related to:

1) Type of merchant or bin or card ATM or any combination of these fields.
2) Number of transactions for a card in the last

30, 60, 90, 365 days, or other suitable time intervals.

3) Average amount spent by a card on groceries, books, electronic, or other categories in any previous time interval.

4) Number of travels in the last year.

5) Average purchase amount at that merchant over the last week or other suitable time interval.

6) Number of declined cards at that merchant over the last week or other suitable time interval.

7) Number of true fraud at that merchant over the last week or other suitable time interval.

8) Number of cards that visited the merchant and then become fraudulent.

9) Average cash-back amount at that merchant over the 90 days, or other suitable time interval.

The velocity servers and profiling servers will send to the engine all the abnormal activities as described previously.

Transactions that have a risk score that is higher than a certain threshold may be further analyzed. The analysis may be performed at intervals, e.g., every night, every hour, every week, or other suitable interval. The high-risk transactions may be analyzed to determine whether the corresponding cardholder accounts had previously visited a common acceptor. If a number of cardholder accounts had visited a common acceptor, the common acceptor may have been a compromising point for those accounts. The transactions conducted at the common acceptor may or may not have been fraudulent transactions.

Acceptors may be given a score that represents the risk that the acceptor is a compromising acceptor. The high-risk transactions may be further analyzed to

determine what type of fraud occurred at the common acceptor. For example, the fraud may be skimming fraud, where card information is copied. If the fraud that has occurred at a common acceptor is determined to be skimming fraud, that acceptor may be given a higher score than if the fraud is determined to be of another type. Acceptors that have a score that is higher than a certain threshold may be placed on a black list of acceptors.

Cardholder accounts that have previously visited an acceptor on the black list of acceptors may be place on a list of high-risk cardholder accounts. These cardholder accounts may or may not have experienced a fraudulent transaction.

Fraud detection engine 24 may monitor merchant authorization requests in real-time. For each authorization request, fraud detection engine 24 may compare the request with the list of high-risk cardholder accounts and the black list of acceptors. If the authorization request is received from an acceptor on the black list of acceptors, the transaction may be assigned a higher risk score. If the authorization request is on a cardholder account on the list of high-risk cardholder account, the transaction may be assigned a higher risk score. Transactions that have scores above a certain threshold may be denied.

Authorization requests that are received from acceptors on the black list of acceptors may have their associated cardholder accounts placed on the list of high-risk cardholder accounts.

Fraud detection engine 24 may help determine the type of acceptors that are most easily compromised. Such information may be useful to credit card associations such as Visa or MasterCard, or to credit card issuers such as banks.

Fraud detection engine 24 may be implemented using a distributed architecture as shown in the example of FIG. 4. Using a distributed architecture may result in better performances using entry level computing equipment (such as personal desktop computers) rather than costly mainframe computers or other specialized hardware. A fraud detection engine implemented on a distributed architecture may also result in a system that is resilient to disruption. Fraud detection engine 24 may also be known as fraud detection system.

In the example of FIG. 4, fraud detection engine 24 may have a central server such as real time fraud detection server 80. Server 80 may detect the sources (also known as roots) of compromised accounts in real time. Server 80 may receive inputs from other servers 70, 72, 74, and 76.

Transactions server 70 may score live transactions in real time. Transactions server 70 may be a TCP server. Transactions server 70 may identify transactions that have a high score and are likely to be fraudulent and, in real time, send those transactions to server 80.

Velocity server 76 may analyze the behavior of merchants during given time periods such as the previous day, week, month, or other suitable time period. Velocity server 76 may identify any abnormal behavior by merchants. Velocity server 76 may provide analysis results to server 80.

Pattern server 74 may analyze the transactions to identify patterns such as patterns in the average transactions per month for each merchant or the number of transaction of a given transaction type for each merchant.

Server 72 having white lists and black lists may provide such lists to server 80.

The distributed architecture of FIG. 4 is merely an example. Fraud detection system 24 may be implemented on any suitable number of servers. For example, fraud detection system 24 may be implemented on two servers, three servers, four servers, five servers or more, or any suitable number of servers.

According to an embodiment, a method is provided for using a fraud detection engine on a computing system, including at the fraud detection engine on the computing system, receiving transaction data from transactions between cardholder accounts and acceptors, and with the fraud detection engine on the computing system, analyzing transaction data using fuzzy logic, including identifying fraudulent transactions, and identifying sources of fraudulent transactions, wherein the computing system has a distributed architecture.

According to another embodiment, a method is provided wherein identifying the sources of fraudulent transactions includes identifying phony acceptors, wherein phony acceptors include acceptors that have a high rate of fraudulent transactions.

According to another embodiment, a method is provided wherein identifying the sources of fraudulent transactions further includes identifying compromising acceptors, wherein cardholder accounts that have had transactions with compromising acceptors have a higher rate of future fraudulent transactions.

According to another embodiment, a method is provided wherein analyzing the transaction data using fuzzy logic further includes analyzing transaction data in real-time using fuzzy logic.

According to another embodiment, a method is provided wherein analyzing the transaction data using fuzzy logic further includes analyzing transaction data

using case-based reasoning.

According to another embodiment, a method is provided wherein analyzing the transaction data using fuzzy logic further includes analyzing transaction data in batch mode using fuzzy logic.

According to another embodiment, a method is provided wherein identifying the fraudulent transactions includes determining each transaction's risk of being a fraudulent transaction, and assigning a fuzzy value to each transaction that indicates the transaction's risk of being a fraudulent transaction.

According to another embodiment, a method is provided wherein identifying the sources of fraudulent transactions includes determining each acceptor's risk of being a phony acceptor, wherein phony acceptors include acceptors that have a high rate of fraudulent transactions, and assigning a fuzzy value to each acceptor that indicates the acceptor's likelihood of being a phony acceptor.

According to another embodiment, a method is provided, wherein identifying the sources of fraudulent transactions includes determining each acceptor's risk of being a compromising acceptor, wherein cardholder accounts that have had transactions with compromising acceptors have a higher rate of future fraudulent transactions, and assigning a fuzzy value to each acceptor that indicates the acceptor's likelihood of being a compromising acceptor.

According to another embodiment, a method is provided, wherein identifying the fraudulent transactions includes identifying the fraudulent transactions in real-time and wherein identifying the sources of fraudulent transactions includes identifying the sources of fraudulent transactions in batch mode.

According to another embodiment, a method is provided, wherein receiving the transaction data from transactions between cardholder accounts and acceptors includes receiving transaction data from authorized and unauthorized transactions.

According to another embodiment, a method is provided, wherein identifying the sources of fraudulent transactions includes, identifying acceptors having transaction amounts that are unusually high as compared to transactions amounts of other acceptors, wherein the transaction amounts were accumulated following a possible fraudulent transaction.

According to another embodiment, a method is provided, wherein identifying the sources of fraudulent transactions includes identifying acceptors that have transaction amounts that are unusually high in a given time period as compared to transaction amounts for the same acceptors in earlier time periods.

According to another embodiment, a method is provided that also includes assessing transaction authorization requests received from corresponding acceptors in real-time, comparing the corresponding acceptors with a black list of suspicious acceptors, and denying the transaction requests received from corresponding acceptors that appear on the black list of acceptors.

According to another embodiment, a method is provided wherein the authorization requests have corresponding cardholder accounts, the method further including comparing the corresponding cardholder accounts with a list of high-risk cardholder accounts, and denying the authorization requests that correspond to cardholder accounts that appear on the list of high-risk cardholder accounts.

According to another embodiment, a method is provided wherein the authorization requests have corresponding cardholder accounts, the method further including comparing the corresponding cardholder accounts with a list of high-risk cardholder accounts, and adjusting risk scores of the authorization requests that correspond to cardholder accounts that appear on the list of high-risk cardholder accounts.

According to another embodiment, a method is provided wherein the authorization requests have corresponding cardholder accounts, the method further including comparing the corresponding cardholder accounts with a list of high-risk cardholder accounts, and increasing risk scores of the authorization requests that correspond to cardholder accounts that appear on the list of high-risk cardholder accounts.

According to an embodiment, a method is provided that includes, at the fraud detection engine on the computing system, receiving authorization requests between an issuer and an acquirer, and with the fraud detection engine on the computing system, analyzing authorization requests using fuzzy logic, including identifying fraudulent authorization requests, and identifying sources of authorization requests, wherein the computing system has a distributed architecture.

The foregoing is merely illustrative of the principles of this invention and various modifications can be made by those skilled in the art without departing from the scope and spirit of the invention.

What is Claimed is:

1. A method for using a fraud detection engine on a computing system, comprising:

at the fraud detection engine on the computing system, receiving transaction data from transactions between cardholder accounts and acceptors; and

with the fraud detection engine on the computing system, analyzing transaction data using fuzzy logic, comprising:

identifying fraudulent transactions; and

identifying sources of fraudulent transactions, wherein the computing system has a distributed architecture.

2. The method defined in claim 1, wherein identifying the sources of fraudulent transactions comprises:

identifying phony acceptors, wherein phony acceptors comprise acceptors that have a high rate of fraudulent transactions.

3. The method defined in claim 2, wherein identifying the sources of fraudulent transactions further comprises:

identifying compromising acceptors, wherein cardholder accounts that have had transactions with compromising acceptors have a higher rate of future fraudulent transactions.

4. The method defined in claim 1, wherein analyzing the transaction data using fuzzy logic further comprises analyzing transaction data in real-time using

fuzzy logic.

5. The method defined in claim 1, wherein analyzing the transaction data using fuzzy logic further comprises analyzing transaction data using case-based reasoning.

6. The method defined in claim 1, wherein analyzing the transaction data using fuzzy logic further comprises analyzing transaction data in batch mode using fuzzy logic.

7. The method defined in claim 1, wherein identifying the fraudulent transactions comprises:

determining each transaction's risk of being a fraudulent transaction; and

assigning a fuzzy value to each transaction that indicates the transaction's risk of being a fraudulent transaction.

8. The method defined in claim 1, wherein identifying the sources of fraudulent transactions comprises:

determining each acceptor's risk of being a phony acceptor, wherein phony acceptors comprise acceptors that have a high rate of fraudulent transactions; and

assigning a fuzzy value to each acceptor that indicates the acceptor's likelihood of being a phony acceptor.

9. The method defined in claim 1, wherein identifying the sources of fraudulent transactions comprises:

determining each acceptor's risk of being a

compromising acceptor, wherein cardholder accounts that have had transactions with compromising acceptors have a higher rate of future fraudulent transactions; and

assigning a fuzzy value to each acceptor that indicates the acceptor's likelihood of being a compromising acceptor.

10. The method defined in claim 1, wherein identifying the fraudulent transactions comprises identifying the fraudulent transactions in real-time and wherein identifying the sources of fraudulent transactions comprises identifying the sources of fraudulent transactions in batch mode.

11. The method defined in claim 1, wherein receiving the transaction data from transactions between cardholder accounts and acceptors comprises receiving transaction data from authorized and unauthorized transactions.

12. The method defined in claim 1, wherein identifying the sources of fraudulent transactions comprises:

identifying acceptors having transaction amounts that are unusually high as compared to transactions amounts of other acceptors, wherein the transaction amounts were accumulated following a possible fraudulent transaction.

13. The method defined in claim 1, wherein identifying the sources of fraudulent transactions comprises:

identifying acceptors that have transaction amounts that are unusually high in a given time period as

compared to transaction amounts for the same acceptors in earlier time periods.

14. The method defined in claim 1, further comprising:

assessing transaction authorization requests received from corresponding acceptors in real-time;

comparing the corresponding acceptors with a black list of suspicious acceptors; and

denying the transaction requests received from corresponding acceptors that appear on the black list of acceptors.

15. The method defined in claim 14, wherein the authorization requests have corresponding cardholder accounts, the method further comprising:

comparing the corresponding cardholder accounts with a list of high-risk cardholder accounts; and

denying the authorization requests that correspond to cardholder accounts that appear on the list of high-risk cardholder accounts.

16. The method defined in claim 14, wherein the authorization requests have corresponding cardholder accounts, the method further comprising:

comparing the corresponding cardholder accounts with a list of high-risk cardholder accounts; and

adjusting risk scores of the authorization requests that correspond to cardholder accounts that appear on the list of high-risk cardholder accounts.

17. The method defined in claim 14, wherein the authorization requests have corresponding cardholder

accounts, the method further comprising:

comparing the corresponding cardholder accounts with a list of high-risk cardholder accounts; and

increasing risk scores of the authorization requests that correspond to cardholder accounts that appear on the list of high-risk cardholder accounts.

18. A method for using a fraud detection engine on a computing system, comprising:

at the fraud detection engine on the computing system, receiving authorization requests between an issuer and an acquirer; and

with the fraud detection engine on the computing system, analyzing authorization requests using fuzzy logic, comprising:

identifying fraudulent authorization requests; and

identifying sources of authorization requests, wherein the computing system has a distributed architecture.

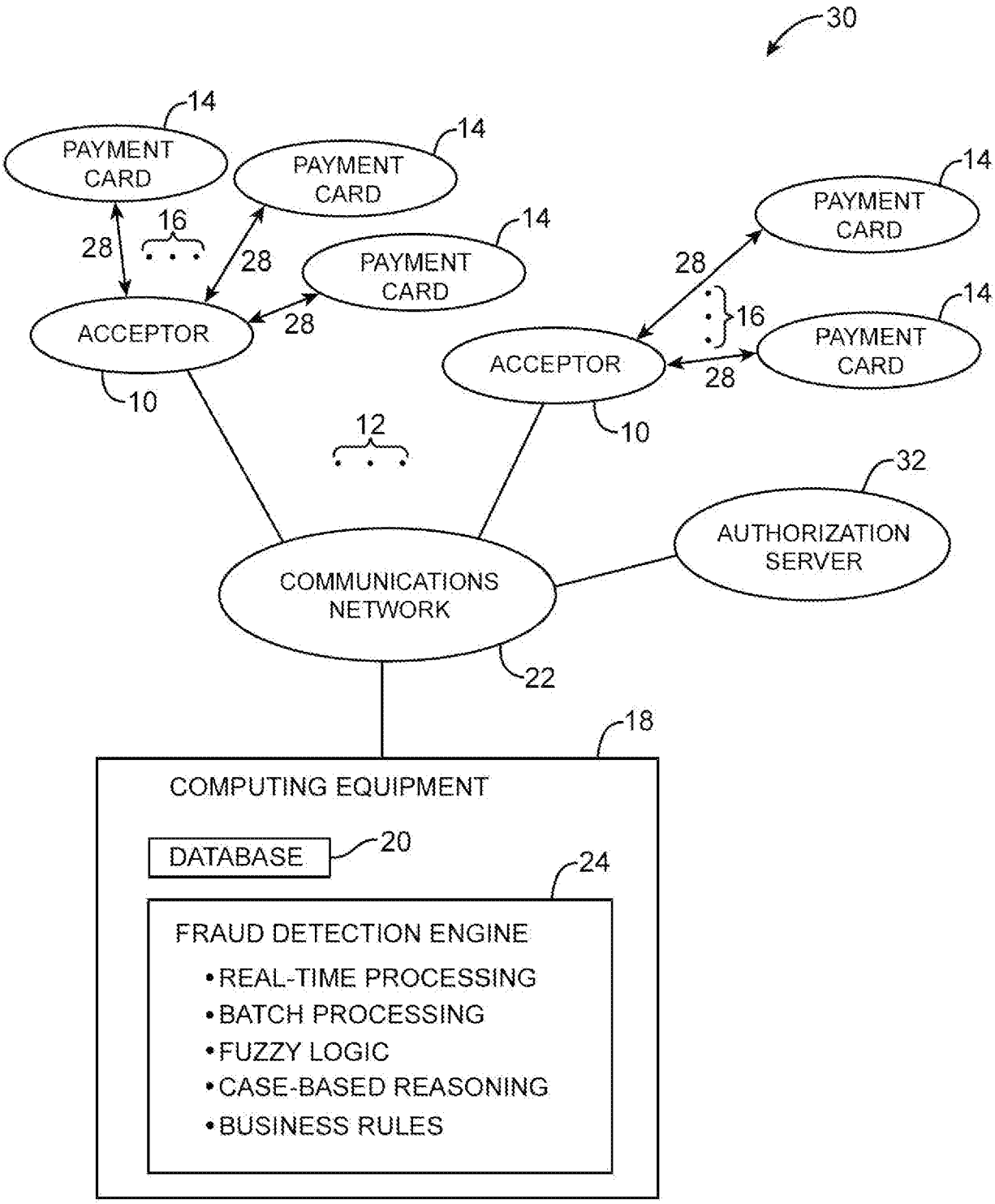
30
14
PAYMENT CARD
14
PAYMENT CARD
14
PAYMENT CARD
14
PAYMENT CARD
14
PAYMENT CARD
16
28
28
28
28
28
16
ACCEPTOR
ACCEPTOR
10
10
12
32
AUTHORIZATION SERVER
COMMUNICATIONS NETWORK
22
18
COMPUTING EQUIPMENT
DATABASE
20
24
FRAUD DETECTION ENGINE
• REAL-TIME PROCESSING
• BATCH PROCESSING
• FUZZY LOGIC
• CASE-BASED REASONING
• BUSINESS RULES

FIG. 1

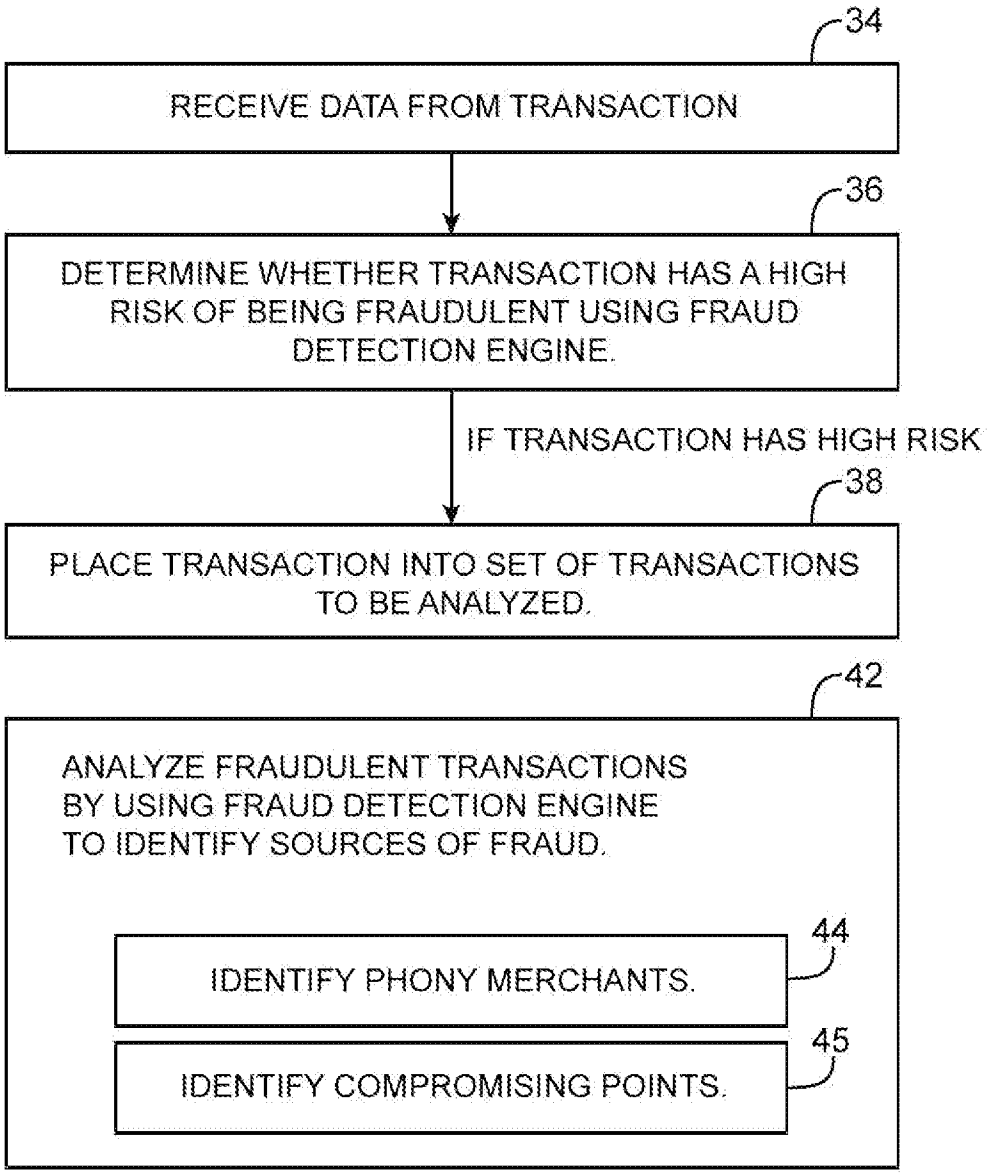
34
RECEIVE DATA FROM TRANSACTION
36
DETERMINE WHETHER TRANSACTION HAS A HIGH RISK OF BEING FRAUDULENT USING FRAUD DETECTION ENGINE.
IF TRANSACTION HAS HIGH RISK
38
PLACE TRANSACTION INTO SET OF TRANSACTIONS TO BE ANALYZED.
42
ANALYZE FRAUDULENT TRANSACTIONS BY USING FRAUD DETECTION ENGINE TO IDENTIFY SOURCES OF FRAUD.
44
IDENTIFY PHONY MERCHANTS.
45
IDENTIFY COMPROMISING POINTS.

FIG. 2

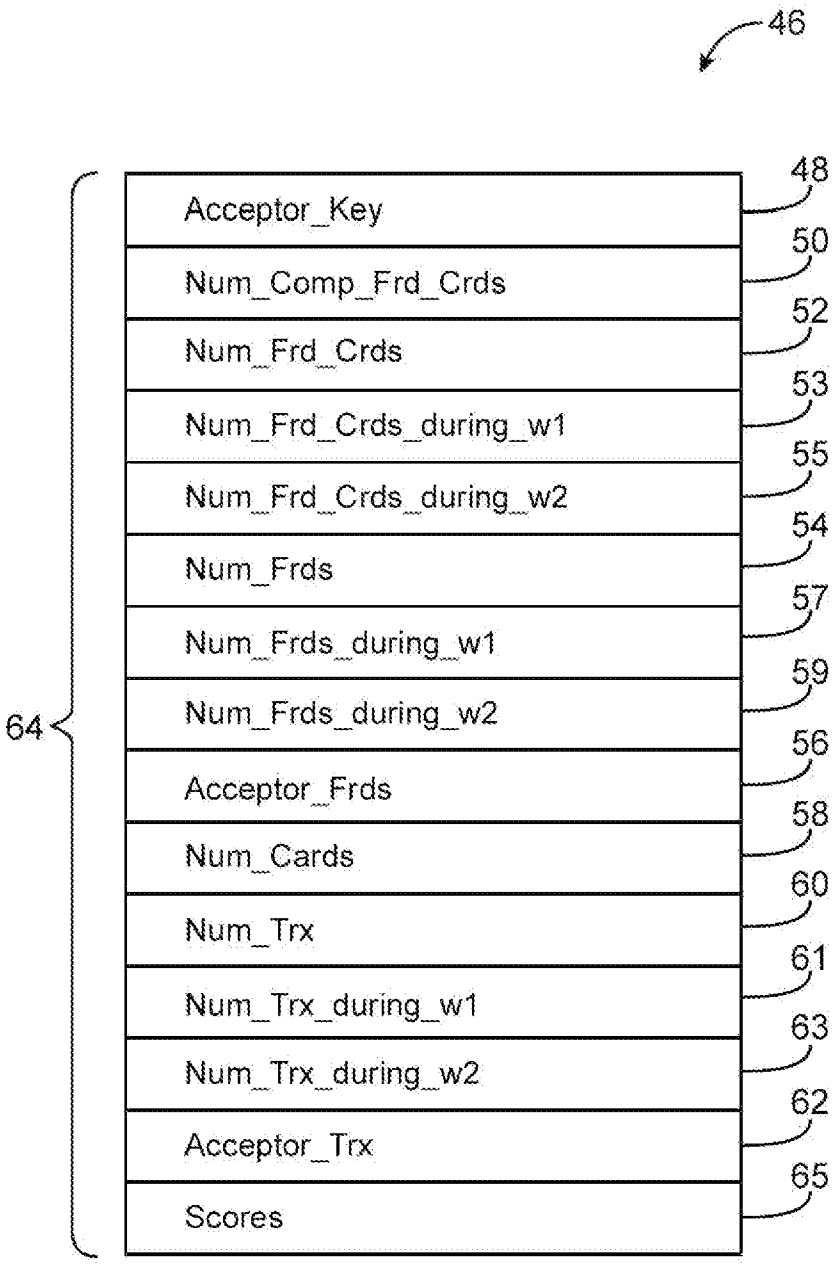
46
48
Acceptor_Key
50
Num_Comp_Frd_Crds
52
Num_Frd_Crds
53
Num_Frd_Crds_during_w1
55
Num_Frd_Crds_during_w2
54
Num_Frds
57
Num_Frds_during_w1
59
Num_Frds_during_w2
56
Acceptor_Frds
58
Num_Cards
60
Num_Trx
61
Num_Trx_during_w1
63
Num_Trx_during_w2
62
Acceptor_Trx
65
Scores
64

FIG. 3

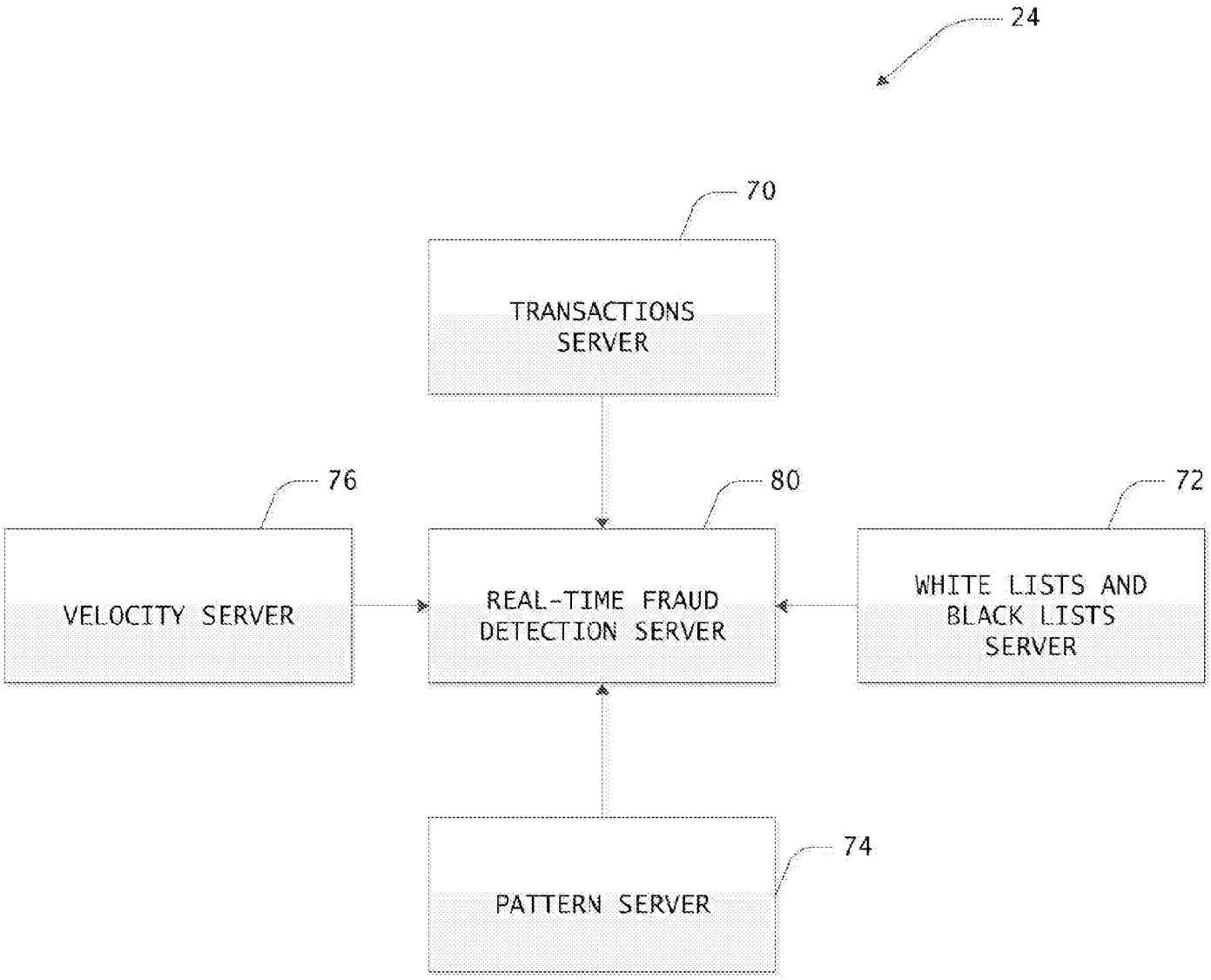
24
70
TRANSACTIONS SERVER
76
VELOCITY SERVER
80
REAL-TIME FRAUD DETECTION SERVER
72
WHITE LISTS AND BLACK LISTS SERVER
74
PATTERN SERVER

FIG. 4