US 20070073617A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2007/0073617 A1**

Tolbert et al. (43) **Pub. Date: Mar. 29, 2007**

(54) **SYSTEM AND METHOD FOR EVALUATION OF MONEY TRANSFER PATTERNS**

(75) Inventors: **Seth Tolbert**, Highlands Ranch, CO (US); **Noel Brandt**, Highlands Ranch, CO (US); **Robert A. Bulkley**, Castle Rock, CO (US); **Robert Degen**, Parker, CO (US)

Correspondence Address:
TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834 (US)

(73) Assignee: **First Data Corporation**, Greenwood Village, CO

(21) Appl. No.: **11/535,362**

(22) Filed: **Sep. 26, 2006**

Related U.S. Application Data

(63) Continuation-in-part of application No. 10/091,000, filed on Mar. 4, 2002.

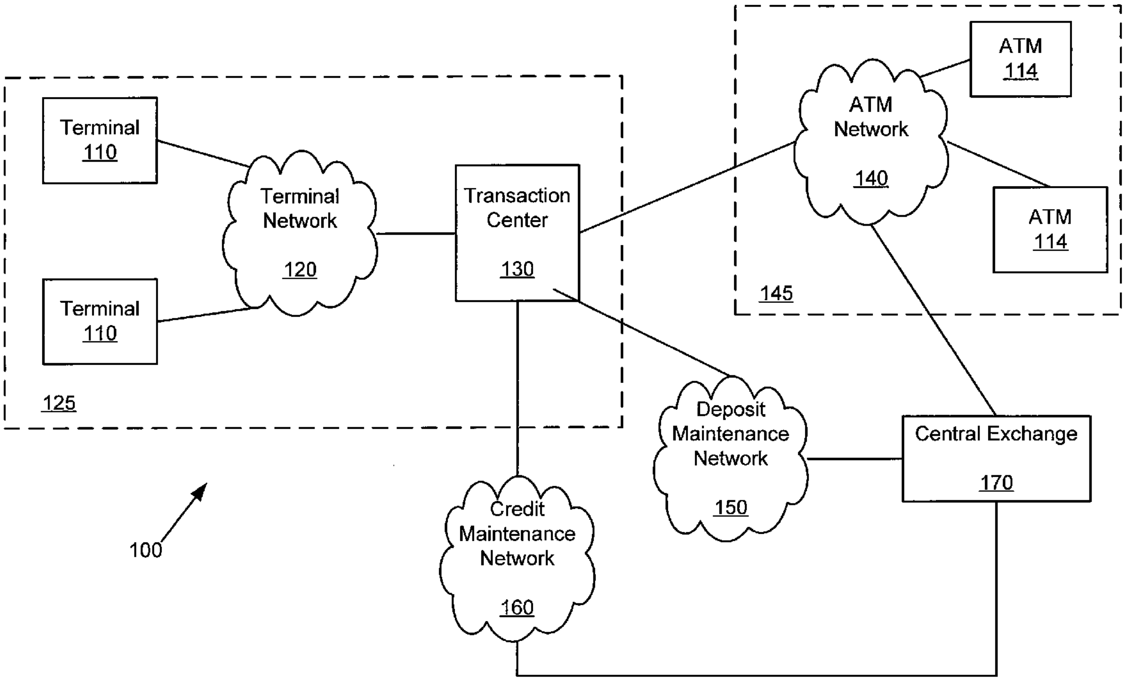
Publication Classification

(51) **Int. Cl.**
G06Q 40/00 (2006.01)

(52) **U.S. Cl.** **705/39**

(57) **ABSTRACT**

A system and method for evaluating records of money transfers for suspicious or irregular transaction patterns. A fraud processing server evaluates money transfer records by blocks, each block consisting of records having the same characteristic relating to location, such as the country where the transfer originates. A second characteristic of the records, such as value, sending agent, or time-of-day, is aggregated and compared to a threshold value. If the threshold value is met, the block of records is analyzed to identify individual records that are suspicious or irregular.



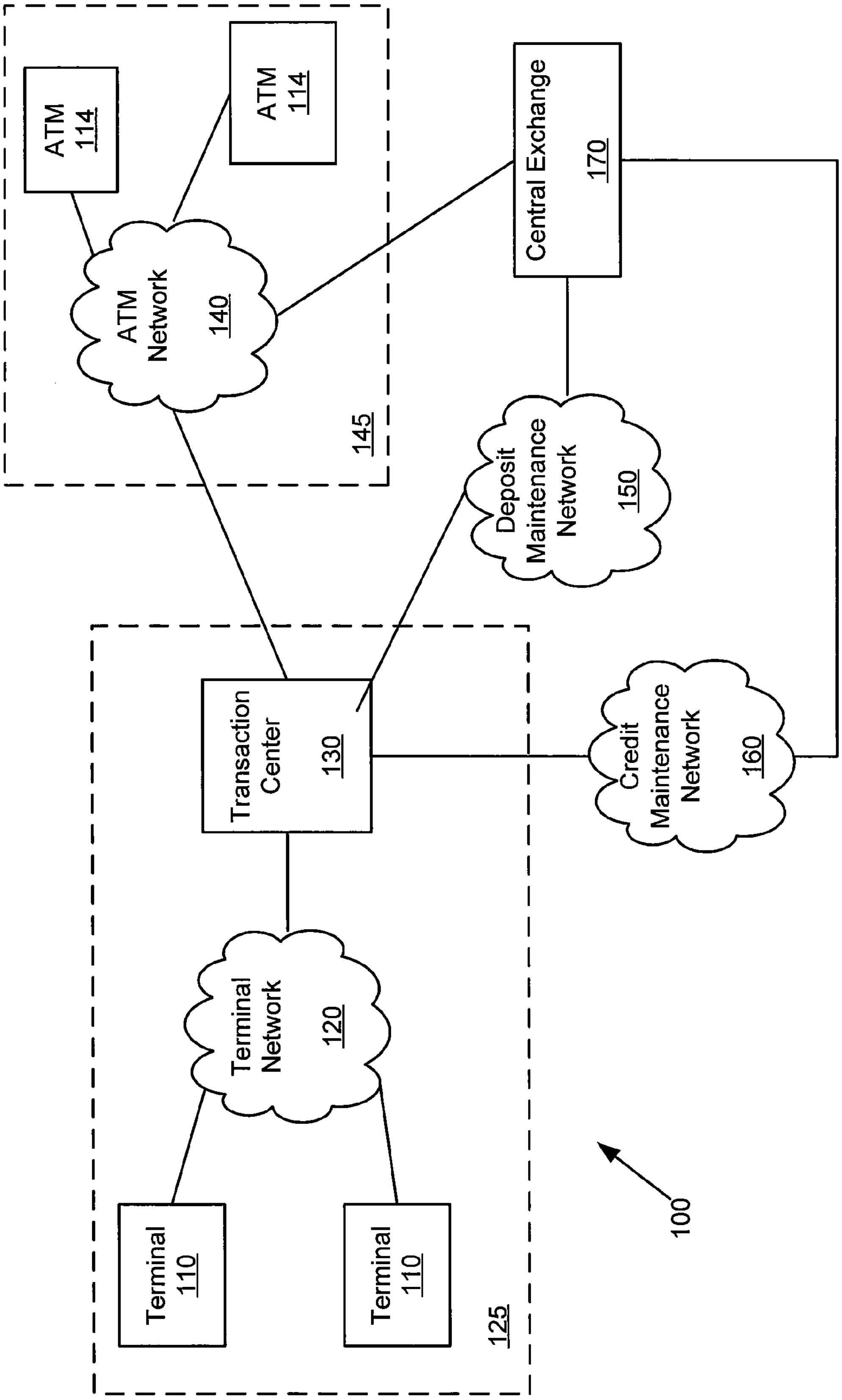

ATM
114
ATM
114
Central Exchange
170
ATM
Network
140
145
Deposit
Maintenance
Network
150
Transaction
Center
130
Credit
Maintenance
Network
160
Terminal
Network
120
Terminal
110
Terminal
110
125
100

FIGURE 1

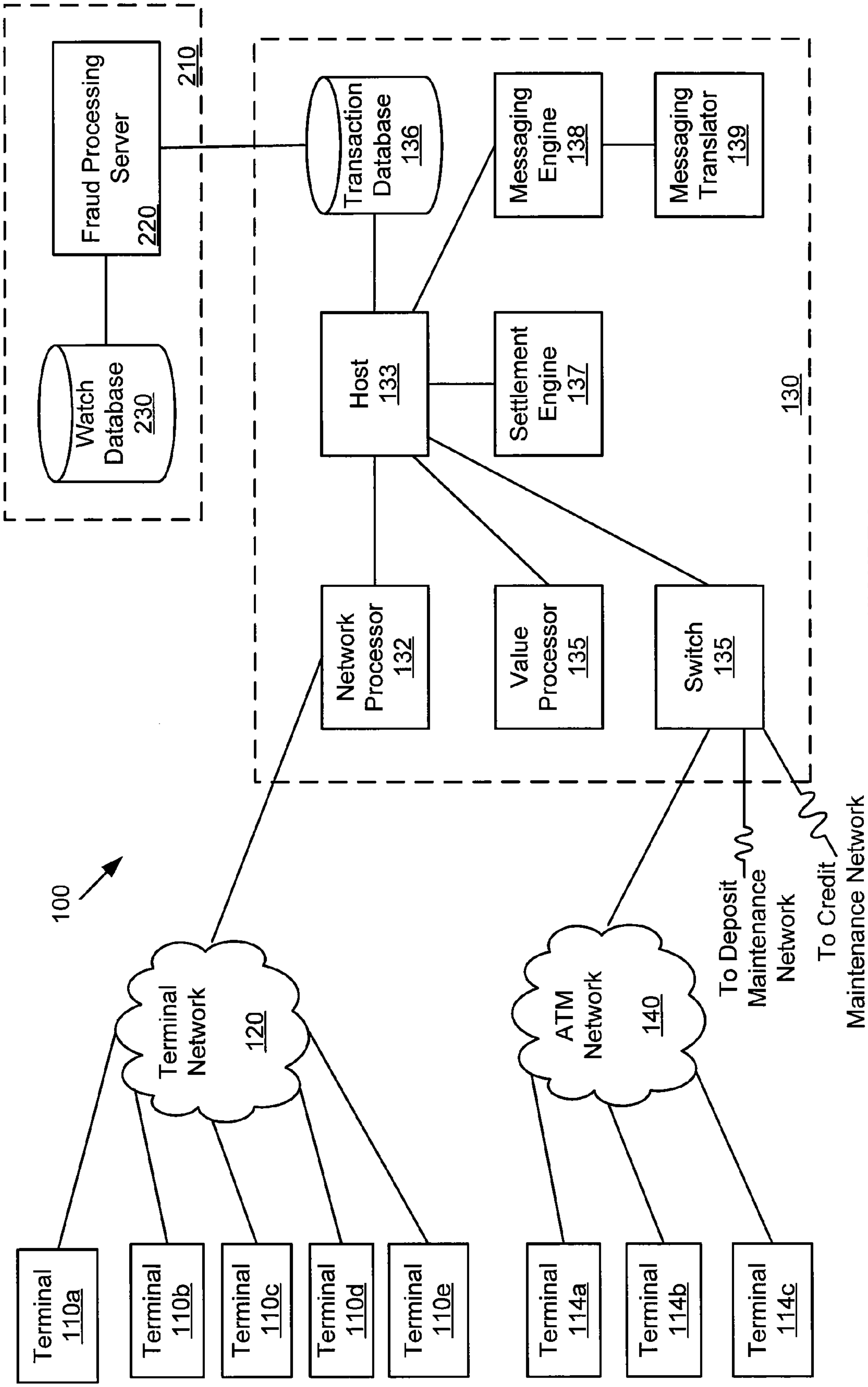

100
Watch Database 230
Fraud Processing Server 220
210
Transaction Database 136
Messaging Engine 138
Messaging Translator 139
Host 133
Settlement Engine 137
130
Network Processor 132
Value Processor 135
Switch 135
To Deposit Maintenance Network
To Credit Maintenance Network
Terminal Network 120
ATM Network 140
Terminal 110a
Terminal 110b
Terminal 110c
Terminal 110d
Terminal 110e
Terminal 114a
Terminal 114b
Terminal 114c

FIGURE 2

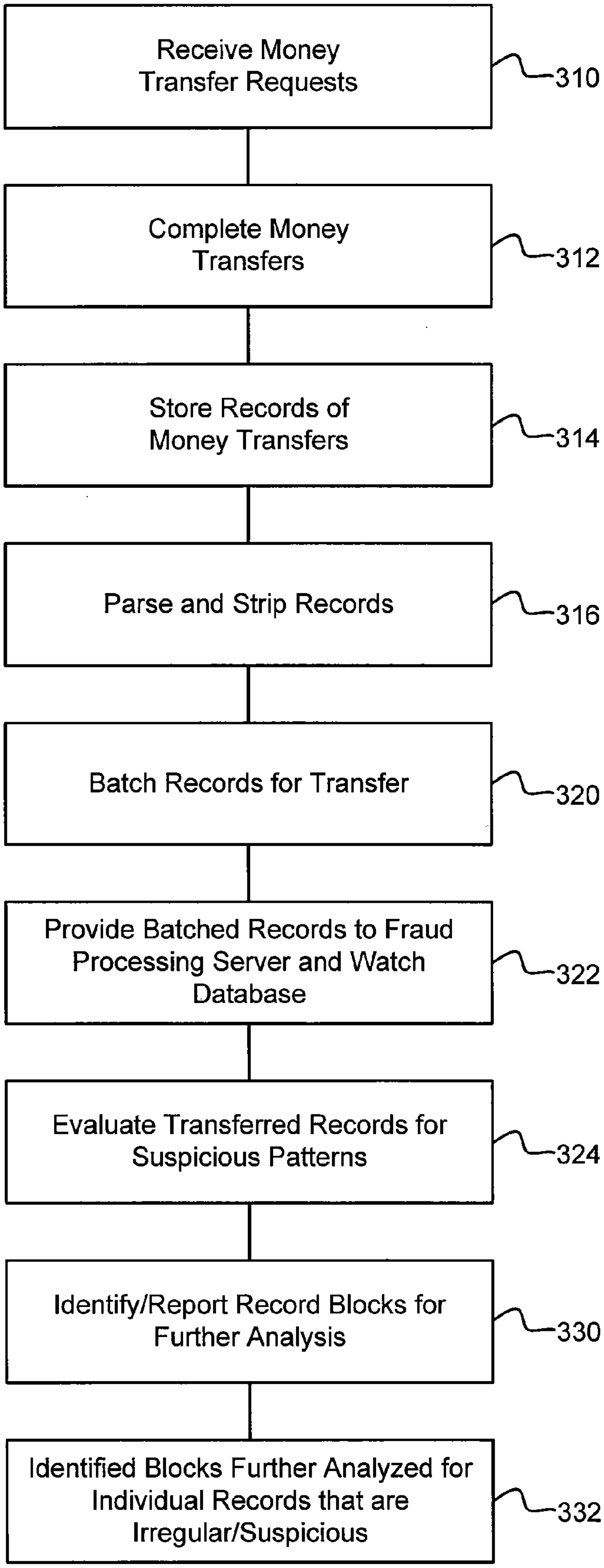

Receive Money Transfer Requests
310
Complete Money Transfers
312
Store Records of Money Transfers
314
Parse and Strip Records
316
Batch Records for Transfer
320
Provide Batched Records to Fraud Processing Server and Watch Database
322
Evaluate Transferred Records for Suspicious Patterns
324
Identify/Report Record Blocks for Further Analysis
330
Identified Blocks Further Analyzed for Individual Records that are Irregular/Suspicious
332

FIGURE 3

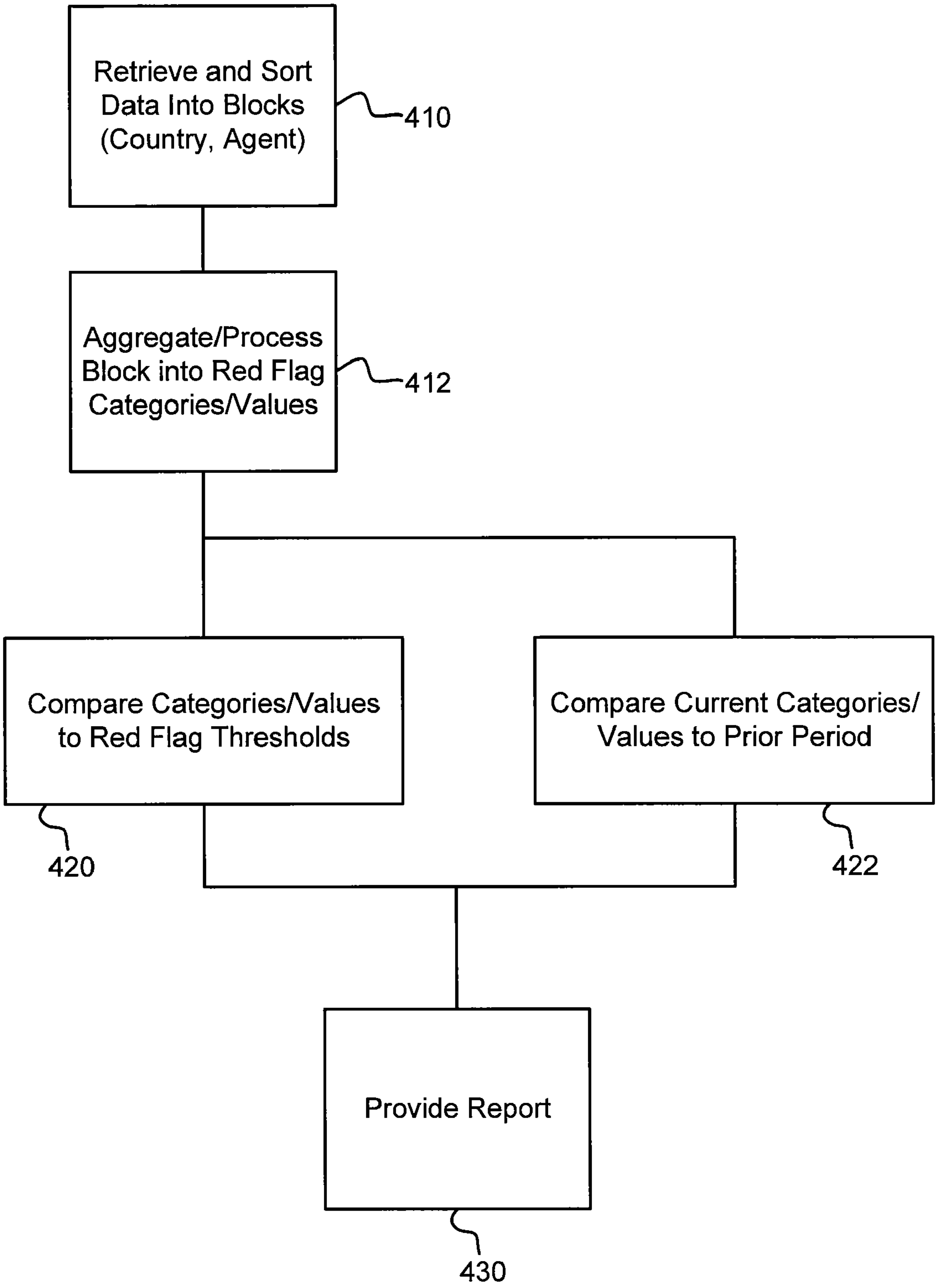

Retrieve and Sort Data Into Blocks (Country, Agent)
410
Aggregate/Process Block into Red Flag Categories/Values
412
Compare Categories/Values to Red Flag Thresholds
420
Compare Current Categories/ Values to Prior Period
422
Provide Report
430

FIGURE 4

Agent Banding – Mexico (September 1, 2006)

Send Agent	Transactions	Band $0 – 899	Band $900 - 999	Band $1000 - 2799	Band $2800 - 2999	Band $9000 - 9999	Band Over $10000
Agent 1	152	21	4	41	75	1	10
Agent 2	281	119	9	112	15	0	0
Agent 3	271	63	5	115	10	0	0
Agent 4	219	44	5	112	8	0	50

FIGURE 5A

Time of Day – Mexico (September 1, 2006)

Send Agent	Transactions	Within Business Hours	Outside Business Hours
Agent 1	152	143	9
Agent 2	281	190	91
Agent 3	271	250	21
Agent 4	219	207	12

FIGURE 5B

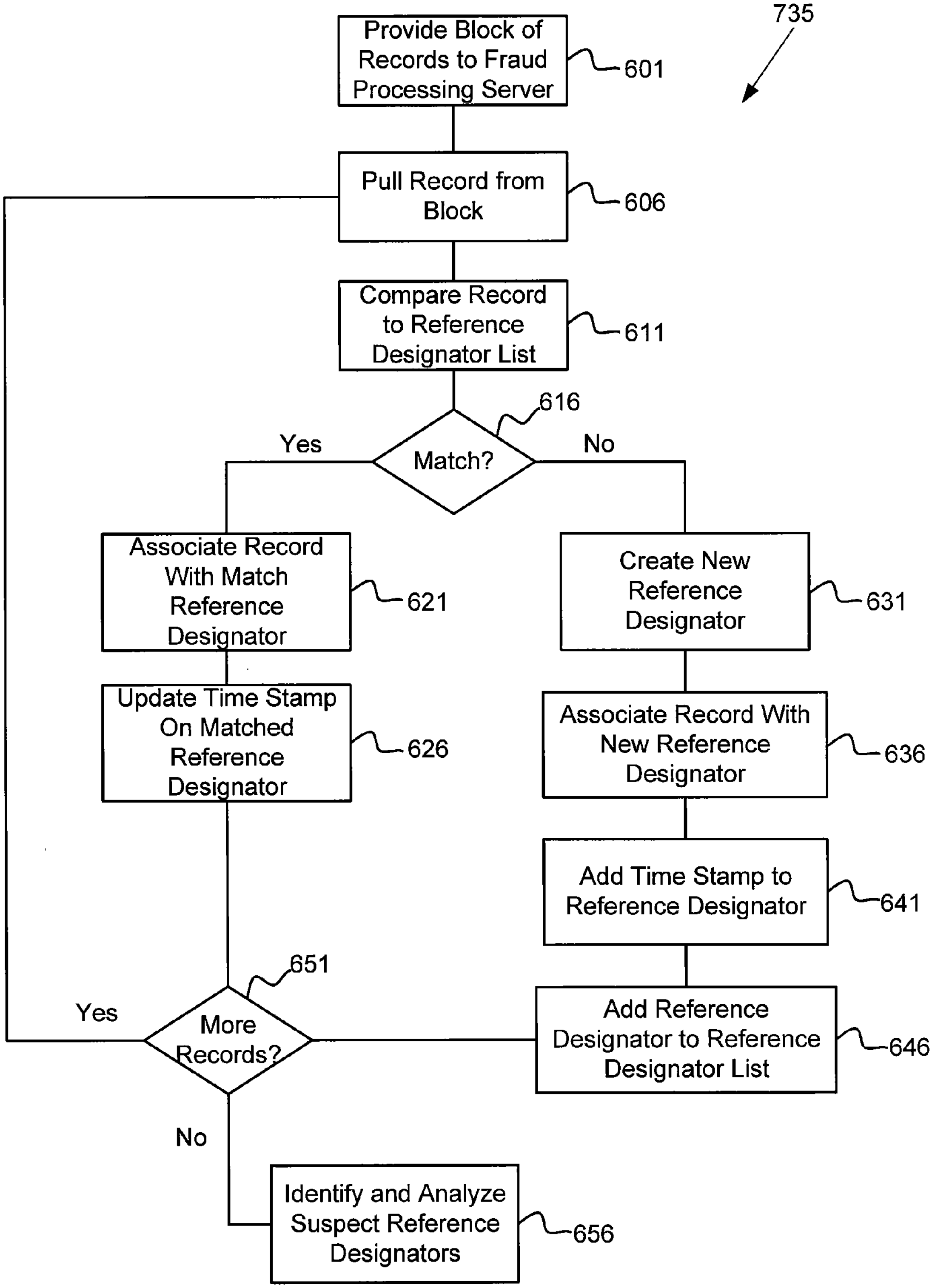

735
Provide Block of Records to Fraud Processing Server
601
Pull Record from Block
606
Compare Record to Reference Designator List
611
616
Match?
Yes
No
Associate Record With Match Reference Designator
621
Create New Reference Designator
631
Update Time Stamp On Matched Reference Designator
626
Associate Record With New Reference Designator
636
Add Time Stamp to Reference Designator
641
651
Yes
More Records?
Add Reference Designator to Reference Designator List
646
No
Identify and Analyze Suspect Reference Designators
656

FIGURE 6

SYSTEM AND METHOD FOR EVALUATION OF MONEY TRANSFER PATTERNS

CROSS-REFERENCES TO RELATED APPLICATIONS

[0001] This application is a continuation-in-part of U.S. patent application Ser. No. 10/091,000, filed Mar. 4, 2002, entitled "Money Transfer Evaluation Systems And Methods," the entire disclosure of which is hereby incorporated by reference.

BACKGROUND OF THE INVENTION

[0002] Electronic transactions, such as electronic money transfers, play an important role in today's economy. Money transfers may be performed in a variety of ways, including, for example, by using the Internet, by using a phone to contact a service representative or an IVR system, by an in-person visit to a financial institution or money transfer location, and the like. For example, to perform a money transfer transaction a sender may visit a money transfer location and fill out a money transfer application. This application may request, among other things, the name of the sender, the name of the recipient, a pick-up location, the amount of money to be transferred, and depending on the amount, certain kinds of identifying data (such as sender's driver license number, social security number, and so forth). This information is transmitted to a central database, and the money to be transferred is collected from the sender. When ready to receive the money, the recipient may proceed to the pick-up location and provide the proper identification. The database is accessed to confirm the recipient and to determine the amount of money to be paid to the recipient. After payment, the date and time of payment may also be transmitted to the database.

[0003] It has been reported that some have attempted to abuse money transfer systems, such as persons associated with organized crime, drug dealers, terrorist organizations and the like. Various procedures exist to curb such abuses. For example, the United States government has implemented laws and regulations with reporting and other requirements that aim to reduce the improper use of monetary transfer transactions. For example, in the United States current money transfer regulations require a sender provide a photo ID if a transaction is $**1000** or more, and two IDs and a social security number if a transfer is $3000 or above. However, reporting requirements are well known to criminal elements, and are thus easily avoided by manipulating money transfer activities to avoid detection. In addition, regulatory reporting requirements may be useful in detecting suspicious individual transactions after they have been conducted, but are not useful to detect groups of transactions that individually are not suspicious, but taken as a whole may indicate patterns of transactions or activity that are suspicious or irregular.

BRIEF SUMMARY OF THE INVENTION

[0004] There is provided, in accordance with embodiments of the present invention, a network/system and method for detecting and evaluating suspicious or irregular patterns of money transfer transactions.

[0005] In one embodiment, a method for evaluating electronic money transfers includes electronically storing records of money transfer requests, each record having a first data field representing a first characteristic of the money transfer request and a second data field representing a second characteristic of the money transfer request, sorting the money transfer records to create at least one data block where the records all have the same first characteristic (such as location), calculating a collective value for the second characteristic, comparing the collective value against a predetermined threshold value, indicating a potentially suspicious/irregular money transfer pattern if the collective value meets the threshold value, and analyzing individual records within the block for irregular money transfers if an irregular money transfer pattern has been indicated.

[0006] A more complete understanding of the present invention may be derived by referring to the detailed description of the invention and to the claims, when considered in connection with the Figures.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] In the Figures, similar components and/or features may have the same reference label. Further, various components of the same type may be distinguished by following the reference label with a second label that distinguishes among the similar components. If only the first reference label is used in the specification, the description is applicable to any one of the similar components having the same first reference label irrespective of the second reference label.

[0008] FIG. **1** is a block diagram illustrating a money transfer system according to one embodiment of the invention.

[0009] FIG. **2** illustrates in greater detail the money transfer system of FIG. **1**.

[0010] FIG. **3** is a flow diagram illustrating a process for evaluating money transfer records in the system of FIGS. **1** and **2**.

[0011] FIG. **4** is a flow diagram illustrating steps within the process of FIG. **3** for evaluating blocks of records for suspicious patterns of money transfers.

[0012] FIG. **5***a* illustrates an example of evaluating a block of money transfer records, using transaction value bands.

[0013] FIG. **5***b* illustrates a second example of evaluating a block of money transfer records, using time-of-day data.

[0014] FIG. **6** is an example of one method for analyzing a block of records that has been identified as having a suspicious pattern of money transfers.

DETAILED DESCRIPTION OF THE INVENTION

[0015] There are various embodiments and configurations for implementing the present invention. Generally, the embodiments provide systems and methods for using blocks of money transfer records in order to identify or indicate potentially suspicious or irregular money transfer patterns. If a block of money transfer records has a potentially irregular pattern, that block is then subjected to a more detailed analysis to determine if specific transfers within the block are likely to be criminal, fraudulent or otherwise improper.

[0016] The evaluation of money transfer patterns provides many useful features and advantages. For example, suspicious money transfer patterns not only alert a system operator of the need to investigate further for fraudulent or criminal activity, but also provide a basis for monitoring money transfer agents and their compliance with standards and policies for accepting money transfer requests.

[0017] The evaluation of money transfers may include several major sub processes. In some embodiments, the evaluation involves three sub processes: sorting the money records into predefined blocks of data, evaluating the blocks for suspicious patterns, and then analyzing any block having a suspicious pattern.

[0018] In the first sub process (sorting all money transfer records into one or more blocks), the blocks are sorted according to a first characteristic, which in disclosed embodiments relates to location. In specific examples, the location may be associated with the country where the money transfer request was made, or the agent network that processed the money transfer request.

[0019] In the second sub process, the blocks are then evaluated for patterns that indicate suspicious activity. For example, a money transfer system operator may periodically evaluate all money transfers being requested within a specific country, and those transfers have been sorted into a block of records in the first sub process (the sort may be done in a batch form, say at the end of each business day). Then, in the second sub process that block of records is evaluated for indicators of suspicious activities by collectively looking at one or more second characteristics of the records (different than the first characteristic). As examples, the second characteristic may relate to something other than location, such as the volume of activity, the average transferred amount, the number of transfers that fall within a monetary range or band that might be suspicious (e.g., very large amounts, or very large numbers of smaller amounts), or the time of day that money transfers are made.

[0020] In one specific example to be described below, the number of transactions falling within certain ranges are counted. The ranges may be selected to reflect regulatory requirements. For example, money transfers involving large amounts are required by authorities in some jurisdictions to be accompanied by additional sender identification (e.g., in the United States, two IDs plus a social security number or tax ID are required for transfers of $3000 or more, as opposed to only a single photo ID if the money transfer is below $3000). A large count for transactions in a selected range, e.g., just below $3000 (i.e., $2800-2999), may indicate attempts by senders to avoid compliance with such regulatory requirements. There are, of course, many possible characteristics/patterns that may be evaluated in each block (as will be described below).

[0021] Finally, a third sub process is used to analyze any block that has been indicated as having suspicious patterns. This analysis could be manual (especially if the block is not large), but more likely would be computerized. In one embodiment, the analysis is done using the process described in the aforementioned application Ser. No. 10/091,000, by taking the block of records (having the suspicious pattern) and assigning reference designators for records that share certain similar or identical data fields. This analysis is particularly useful in the present invention, since the records are available electronically and have already been sorted into a block of interest (i.e., country, agent network, or other location).

[0022] Turning now to the drawings, FIG. **1** illustrates a money transfer system **100** comprised of an interface system **125**, an automated teller machine (ATM) system **145**, a deposit maintenance network **150**, a credit maintenance network **160** and a central exchange **170**. Interface system **125** is communicably coupled to ATM system **145** via an ATM network **140**, deposit maintenance network **150** and credit maintenance network **160**. In general, interface system **125** unifies a variety of transfer systems while supporting a variety of mechanisms for introducing and receiving information to and/or from money transfer system **100**.

[0023] Interface system **125** comprises a transaction center **130** and one or more terminals **110** in communication via a terminal network **120**. Terminal network **120** can be any communication network capable of transmitting and receiving information in relation to a transfer of value from one entity to another. For example, terminal network **120** can comprise a TCP/IP compliant virtual private network (VPN), the Internet, a local area network (LAN), a wide area network (WAN), a telephone network, a cellular telephone network, an optical network, a wireless network, or any other similar communication network. In particular embodiments, terminal network **120** provides message based communications between terminals **110** and transaction center **130**.

[0024] Terminals **110** can be any terminal or location where value is accepted and/or provided in relation to money transfers across money transfer system **100**. Thus, in some instances, terminal **110** is at a money transfer agent location, such as a convenience store where a clerk can receive value from a sender and initiate transfer of the value to a receiver via money transfer system **100**. In such cases, the clerk can typically also provide transferred value to a receiver.

[0025] In other instances, terminal **110** is an automated system for receiving value from a sender for transfer via money transfer system **100** and/or for providing value to a receiver that was transferred via money transfer system **100**. To accommodate various different payment instruments and types, terminal **110** can include a variety of interfaces. For example, terminal **110** can include a mechanism for receiving cash, credit cards, checks, debit cards, stored value cards and smart cards. Such terminals may also be used at the payout end to print a check or money order, or to credit a cash card or stored value card. Examples of such terminals are described in U.S. Pat. No. 6,547,132 (U.S. application Ser. No. 09/634,901, entitled "POINT OF SALE PAYMENT SYSTEM," filed Aug. 9, 2000 by Randy J. Templeton et al.), which is hereby incorporated by reference.

[0026] In yet other instances, terminal **110** is a personal computer operated by a sender of value. Such a terminal can be communicably coupled to transaction center **130** via the Internet. The terminal can further include a web browser capable of receiving commands for effectuating transfer of value via money transfer system **100**.

[0027] Terminal identification information can be associated with each terminal **110**. Such identification information includes, but is not limited to, a physical location, a telephone number, an agent identification number, a terminal identification number, a security alert status, an indication of the type of terminal, a serial number of a CPU, an IP address, the name of a clerk, and the like.

[0028] Terminals **110** may also be operated in agent networks, i.e. a plurality of terminals at different locations may operated by the same agent entity. There could many such agent networks within system **100** at locations around the world.

[0029] Using money transfer system **100**, value can be transferred from any of a number of points. For example, value can be transferred from terminal **110** to itself or any other terminal **110**, from any terminal **110** to a deposit account via deposit maintenance network **150** or credit maintenance network **160**, from any terminal **110** to any ATM **114** via ATM network **140**. Many other transfers to/from ATMs **114**, deposit accounts, terminals, and/or credit accounts can be accomplished using money transfer system **100**. The ATM system **145** is only illustrative, it being understood that such a system is merely one of many possible optional means for money to be conveniently transferred/received without the use of conventional, agent-operated money transfer terminals, and the transfer of money within system **100** may or may not involve the use of ATMs **114**.

[0030] Referring to FIG. **2**, a fraud watch system **210** is provided in communication with transaction center **130** of money transfer system **100**. As illustrated, transaction center **130** includes a network processor **132** to process data received and transmitted via terminal network **120**. Data to/from network processor **132** is available to a host **133** that may communicate with one or more of a value translator **135**, a transaction database **136**, a settlement engine **137** and a messaging engine **138** to perform functions associated with transferring value via money transfer system **100**. In turn, messaging engine may communicate with a message translator **139**. The data received and/or provided by transaction center **130** may include information on the sender, information on the recipient, identification information associated with the sender (e.g., type of ID presented, driver's license number, etc.) or with the terminal **110** (terminal ID number), the type and amount of value transferred, a desired location to transfer the value, and the like. In some cases, a value translator **135** may be used to change the type of value. For example, value translator **135** may do a foreign currency conversion, or may transfer from one type of value to another, e.g. frequent flyer miles to United States Dollars. All information that is processed may conveniently be stored in transaction database **136**.

[0031] Settlement engine **137** may be used to facilitate the crediting and debiting of various accounts during a transfer. For example, if a sender requests that funds from a credit card account be used in the transfer, settlement engine **137** is used to contact credit maintenance network **160** to charge the card and to manage the fees involved in the transaction. Such fees may be those charged by the credit organization as well as internal fees that are a part of the money transfer transaction. Settlement engine **137** may be used in a similar manner when crediting or debiting checking accounts, stored value accounts, customer loyalty (e.g., frequent flyer) accounts and the like.

[0032] In some cases, the sender may also wish to send a message with the value. Such a message may be a simple greeting, business or legal terms, and the like. Messaging engine **138** is employed to convert the message to the proper format depending on the type of output device that is to be used with receiving the money. For example, the output device may be a printer that physically prints the message onto some type of media. Alternatively, the message may be temporarily displayed on a display screen, such as on a kiosk, ATM machine, point of sale device, an e-mail, a web page or the like. The sender or recipient may also indicate that the message needs to be translated to a different language. In such cases, message translator **139** may be used to translate the message into the other language. This may be accomplished by simply doing a word look up for each corresponding word in the other language. More complex language translation capabilities may also be used.

[0033] Once a value transfer is properly processed, data indicating the transfer is sent by a switch **134** to the appropriate network as shown. This may be to ATM network **140**, deposit maintenance network **150** and/or credit maintenance network **160** to complete the transaction.

[0034] A monitoring or fraud watch system **210** includes a fraud processing server **220** and a watch database **230**. Fraud watch system **210** is associated with transaction center **130** in a manner that allows for access to transaction database **136**. Such association can be provided by direct wired communication between transaction database **136** and fraud processing server **220**, by direct or network communication between transaction center **130** and fraud processing server **220**, or by any other mechanism that provides fraud watch system **210** with access to transaction database **136**. In one particular embodiment, fraud processing server **220** is communicably coupled to terminal network **120** and accesses transaction database **136** via network processor **132** and host **133**. In another embodiment, fraud processing server **220** is directly coupled to host **133** and accesses transaction database **136** via host **133**. It will be recognized by one of ordinary skill in the art that a number of other mechanisms exist within the scope of the present invention for providing access by fraud processing server **220** to transaction database **136**.

[0035] Fraud processing server **220** can be a microprocessor based device capable of retrieving data from transaction database **136**, searching and manipulating the data, maintaining a form of the data on watch database **230**, and providing access to data at database **230**. Such access to the data can include formatting the data and providing the data in an easily accessible form. In some embodiments, fraud processing computer is a single computer, such as a personal computer or a database server. In other embodiments, fraud processing server is a group of two or more computers. In such embodiments, fraud processing computer can include a central computer associated with one or more peripheral computers. Such peripheral computers can be personal computers or portable devices, such as lap top computers and/or personal digital assistants. In a particular embodiment, fraud processing server **220** includes a SQL server, while in other embodiments, it includes an ORACLE server.

[0036] Fraud processing server **220** includes a computer readable medium capable of maintaining instructions executable to perform the functions associated with fraud processing server **220**. The computer readable medium can be any device or system capable of maintaining data in a form accessible to fraud processing server **220**. For example, the computer readable medium can be a hard disk drive either integral to fraud processing server **220** or external to the server. Alternatively, the computer readable medium can be a floppy disk or a CD-ROM apart from fraud processing server **220** and accessible by inserting into a drive (not shown) of fraud processing server **220**. In yet other alternatives, the computer readable medium can be a RAM integral to fraud processing server **220** and/or a microprocessor (not shown) within the server. One of ordinary skill in the art will recognize many other possibilities for implementing the computer readable medium. For example, the computer readable medium can be a combination of the aforementioned alternatives, such as, a combination of a CD-ROM, a hard disk drive and RAM.

[0037] Referring to FIG. **3**, an overall process is illustrated for completing money transfers and then evaluating money transfer records for suspicious money transfer patterns. Many of the steps in the process are controlled by fraud processing server **220**. In addition, the storage of records for the evaluation may be at watch database **230**. This permits money transfer records to be evaluated separately from the money transfer operations performed at the transaction center **130**, thus improving performance and minimizing operational impact on the host **133** and transaction database **136**.

[0038] As illustrated in FIG. **3**, the operator of the money transfer system **100** receives a request at a terminal **110** (e.g., agent operated terminal) from a sender to make a money transfer (step **310**). The money transfer is completed (step **312**), so that money may be picked up by the recipient (e.g., at a money transfer agent location as described earlier), and a record of the transfer stored at transaction database **136** (step **314**). At predetermined intervals (e.g., at the end of each business day so as to minimize impact on actual money transfer operations), the records are readied for evaluation by parsing and stripping the records of data that is deemed not useful in the evaluation (step **316**). In one embodiment, transactions of $500 or less are removed from the records since smaller transactions may be deemed not likely involved in fraudulent or criminal activity. However it should be appreciated that the amount of data stripped from the records can be large, little or none, depending on the preferences of the system operator.

[0039] At step **320**, the parsed and stripped records are batched by host **133** and transaction database **136**, and then are transferred for storage and processing at the server **220** and database **230** (step **322**). While parsing and stripping are illustrated as performed at host **133** (this could reduce the amount of data needing to be stored at watch database **230**), it should be appreciated the entire money records from transaction database **136** could be transferred to server **220** and database **230**, with parsing and stripping steps then performed at server **220** after the transfer.

[0040] The records are then evaluated for indications of suspicious or irregular patterns (step **324**), as will be described below in conjunction with FIG. **4**. If a suspicious pattern is indicated, those blocks of records having the suspicious patterns are identified or reported to the system operator (step **330**) and subjected (step **332**) to further analysis, e.g., at server **220**, to identify individual records that may be fraudulent, criminal, or otherwise improper (as will be described in conjunction with FIG. **6**).

[0041] Referring to FIG. **4**, one embodiment is illustrated for carrying out the identification of suspicious money transfer patterns (collectively referred to above as step **324** in FIG. **3**). As seen, at step **410** specific blocks of records stored at watch database **230** are retrieved and sorted by fraud processing server **220** for evaluation. The blocks are formed so that all records within the block have a common characteristic useful for evaluation. In the embodiment of FIG. **4**, the characteristic is location related, i.e., the system operator chooses records for a specific country or for a specific agent network. In some cases, the money transfer records from a selected country may be large, so the block may be made smaller and more manageable by choosing all records for a country corridor (i.e., transfers from one selected country to a second selected country). Other possible characteristics (location related or otherwise) could be used to create each block for evaluation.

[0042] Next, the system takes all records within each block and aggregates the data in selected fields of the records (to create collective value for each field), according to selected secondary categories or characteristics (step **412**). As one example (to be described later in conjunction with FIG. **5***a*), the system may look at each record in the selected block of records (Mexico) and check the field of each record for the transaction amount. A count is provided for the number of transactions falling into each of several transaction value bands for each agent within Mexico.

[0043] At step **420**, the server **220** compares the aggregated category/secondary characteristic data to predetermined red flag or threshold values, and provides a report (step **430**) of any patterns that are potentially suspicious. The report can also include a simultaneous comparison of the same data to previous periods (step **422**). Comparisons to previous periods (e.g., previous week, previous month) are useful when the system **210** is being used to monitor agent networks for compliance with policies and procedures (increasingly irregular data patterns may indicate a need for compliance training, and improving data patterns may indicate the success of a recent compliance program).

[0044] Referring to FIG. **5***a*, the money transfers made at various agent locations for one data block (Mexico) are shown. The agent identifiers (Agent **1**, Agent **2**, etc.) may each represent a single agent or represent a group of agents operating in a single agent network. As can be seen, Agent **1** has a disproportionately large number (75) of transactions falling within the range of $2800-2900, and Agent **4** has a disproportionate number (30) of very large transactions in excess of $10000. At step **420**, the server **220** may be programmed to identify and report any agent having more than 50% of transactions in the $2800-2999 band (such as Agent **1**), and any agent having more than 25% of transactions in the Over $10000 band (such as Agent **4**). In view of the suspicious patterns, the transactions of those agents (or the entire block) can then be further evaluated for determining whether individual transactions within the block are likely to have resulted from improper activity (step **332**, FIG. **3**).

[0045] Another example of evaluating a block of records is seen in FIG. **5***b*, in this instance using time-of-day data collected at the time a money transfer is requested. As seen, for all agents in Mexico on a given date, those money transfer requests made both within normal agent business hours (e.g., 7 AM to 11 PM) and outside normal business hours (11 PM to 7 AM) are reported. As can be seen, Agent **2** has an irregularly high number of outside normal business hour transfers (91), which may indicate, for example, use of the system by criminals to transfer money at times to avoid day time scrutiny, or failure of individual agents to record the proper, actual time of transfers. The block of transfers can be further analyzed (e.g., using the process to be described with reference to FIG. **6**), and either suspicious individual transactions identified, or the agent required to undergo compliance training as to the proper process for time stamping transactions.

[0046] As mentioned earlier, there are many possible characteristics that can be considered in aggregating data for suspicious patterns and comparison to red flags/thresholds. The following describes examples of such characteristics, it being understood that such description is not intended to be limiting:

[0047] Country Corridor Characteristics

[0048] For a given country, various characteristics of transactions to other countries can be evaluated, such as total number of transactions, total monetary amount of all transactions, the smallest and largest transactions, and the ratio of payees to senders. Past experience can lead to developing threshold values that represent an unusual level of activity. An aggregated value for any characteristic that exceeds the threshold represents a suspicious pattern.

[0049] As an example, these characteristics may be evaluated for all daily money transfers from the U.S. to each of several dozen other countries, including Nigeria. A high ratio of payees to senders for transfers from the U.S. to Nigeria (as compared to transfers from the U.S. to other countries) may indicate that large amounts of money are being distributed to Nigeria using many money transfers in smaller amounts, in an attempt to launder money.

[0050] Agent Characteristics

[0051] For each agent within one sending country, the total number of transactions, total monetary amount of all transactions, or the total number of payees/recipients that exceed predetermined thresholds may represent an unexpectedly high level of activity by one agent, and hence a suspicious pattern.

[0052] Agent to Agent Characteristics

[0053] The number of transactions (within one sending country) from each sending agent to each receiving agent might represent (if exceeding a predetermined threshold) a suspicious pattern, due to an attempt by a sending agent to steer transactions to a pick-up location or agent chosen or preferred by the sending agent, rather than chosen by the sender. Compliance training for the sending agent may be warranted.

[0054] Consumer Characteristics

[0055] For a given country, and for each sender, the total number of transactions, the total monetary amount of all transactions, and the total number of payees may indicate a pattern of senders attempting to launder money by transferring large amounts of money to multiple payees/recipients.

[0056] Biographical Characteristics

[0057] These characteristics include the nature of the sender's ID (photo or no photo), social security number, phone number, and so forth. Any aggregation that exceeds a threshold may represent an irregular or suspicious pattern. As an example, a large number of transactions using one social security number may indicate a suspicious pattern. As another example, a high percentage of transactions (e.g., 80%) completed by one sending agent without photo IDs being presented by the sender may be a suspicious pattern and indicate compliance training for that agent is warranted.

[0058] Once a block of data had been identified as having potentially suspicious patterns, that block (or, if desired, a selected subset of the block) is then subject to further analysis at step **324** (FIG. **3**), to either identify individual transactions that are suspicious, or to determine that the patterns are harmless. Many methods can be used to perform this further analysis. For example, the analysis could be manual, with a trained analyst reviewing records individually to find those that appear to be part of fraudulent or criminal activity. However, in most cases, the records in a suspicious block may be many thousand or more (since it may represent, for example, all transaction on a given day across an entire country), and so a process involving more automated steps can be used.

[0059] One such process for analyzing individual records in shown in FIG. **6**, and is described also in aforementioned application Ser. No. 10/091,000. Basically, the process groups transfer records together that have identical (or nearly identical) data fields. For example, if a number of transfers have the same sender name, same recipient name, same recipient phone number, or other sender or recipient identifying data, they are collected and given a single reference designator. In some embodiments, depending on the number of the records under a single designator, the records can be further analyzed manually or further sorted or grouped by fraud processing server **220** to provide an analyst with specific transactions (e.g., under a single reference designator) that could be fraudulent.

[0060] This is illustrated in FIG. **6**, where a block of records (i.e., a block having a suspicious pattern, such as the pattern in FIG. **5***a*or FIG. **5***b*) is provided to the fraud processing server **220** (step **601**). Each record is pulled from the block (step **606**) and compared to records grouped in any existing reference designator (step **611**). In other words, if records have already been analyzed and assigned a reference designator because of identical fields, the record in question is compared to the records in those existing designators for matches. If there is a match (step **616**) then the record in question is associated (step **621**) with the matched record designator (i.e., the record is grouped or clustered with the other records already grouped together under a single reference designator), and a time stamp (indicating the time/date of the most recent transaction within the reference designator) is updated (step **626**). If there is no match, then the record is given its own reference designator and a time stamp (steps **631**, **636**, **641**, **646**), and is added to the list or set of reference designators for comparison to additional records, if any remain to be checked (step **651**).

[0061] Each reference designator (cluster of money transfer records) can then be searched or analyzed (step **656**) to identify specific sender names, specific recipient names or other identifying data associated with likely fraudulent or criminal activity. This final analysis can be done manually or may involved automated checking (using fraud processing server **220**) of the common data fields in reference designator lists against known suspect user names or other identifiers.

[**0062**] As should be apparent, methods other than that described above are available for analyzing blocks of records having suspicious patterns, as represented by step **324** in FIG. **3**. For example, an analysis method could be used as described in U.S. application Ser. No. 10/434,409, entitled "SYSTEMS AND METHODS FOR GRADUATED SUSPICIOUS ACTIVITY DETECTION," filed May 7, 2003 by Robert G. Degen et al., which is hereby incorporated by reference. Under such analysis method, transactions are grouped according to affinities between transactions (e.g., common data points, such as sender names), and with increasing levels of scrutiny in order isolate suspect money transfers.

[**0063**] While a detailed description of presently preferred embodiments of the invention has been given above, various alternatives, modifications, and equivalents will be apparent to those skilled in the art without varying from the spirit of the invention.

[**0064**] Therefore, the above description should not be taken as limiting the scope of the invention, which is defined by the appended claims.

What is claimed is:

1. A method for evaluating electronic money transfers, comprising:

electronically storing records of money transfer requests, wherein each record is associated with a money transfer request and has at least two data fields, a first data field representing a first characteristic of the money transfer request and a second data field representing a second characteristic of the money transfer request;

sorting the money transfer records to create at least one data block, wherein all records in the data block have the same first characteristic;

calculating a collective value of the second characteristic of all the records in the data block;

comparing the collective value against a predetermined threshold value, threshold value chosen to represent potentially irregular money transfer transactions;

indicating a potentially irregular money transfer pattern if the collective value meets the threshold value; and

analyzing individual records within the block for irregular money transfers if an irregular money transfer pattern has been indicated.

2. The method of claim 1, wherein the first characteristic is related to the location of the money transfer request.

3. The method of claim 2, wherein the first characteristic is the country where the money transfer request in made.

4. The method of claim 2, wherein the first characteristic is the agent network receiving the money transfer request.

5. The method of claim 2, wherein the second characteristic is related to the value of the money transfer request.

6. The method of claim 5, wherein the value of each money transfer request is assigned to one of a plurality of value bands, each band representing a predetermined range of transferred monetary amounts, and wherein the collective value represents the number of money transfer requests having transferred monetary amounts falling within one of the value bands.

7. The method of claim 6, wherein predetermined range has an upper limit below $3000.

8. The method of claim 7, wherein predetermined range has a lower limit above $2800.

9. The method of claim 2, wherein the second characteristic is related to the time-of-day of each transaction.

10. The method of claim 9, wherein the second characteristic is related to whether the transaction is during normal business hours or outside normal business hours, wherein the collective value is the total number of transactions outside normal business hours, and wherein the threshold value is a percentage of the transactions outside normal business hours in relation to the total number of transactions.

11. The method of claim 10, wherein the comparing step compares, for each of a plurality of agents, the collective value of the total number of transactions outside normal business hours to the threshold value.

12. The method of claim 2, wherein the second characteristic is chosen from a group consisting of:

transaction value band characteristics;

country corridor characteristics;

agent characteristics;

agent to agent characteristics;

consumer characteristics; and

biographical characteristics.

13. The method of claim 1, wherein the electronic records are stored at a money transfer system, wherein the stored records are transferred to a monitoring system programmed for carrying out the steps of sorting the money transfer records, calculating a collective value for the second characteristic of all the records in the data block, comparing the collective value of the second characteristic against a predetermined threshold value, indicating a potentially irregular money transfer pattern if the collective value of the second characteristic of all records in the data block meets the threshold value, and analyzing individual records within the data bock for irregular money transfers, and wherein the threshold value is a red flag threshold selected by the operator of the money transfer system based on experience.

14. The method of claim 1, wherein the money transfer records include a first sender identification associated with a first money transfer request and at least a second sender identification associated with a second money transfer request, and wherein the step of analyzing individual records comprises:

performing an analysis of the records, wherein the analysis indicates the first sender identification and the second sender identification are related;

creating a reference designator, wherein the reference designator is associated with records having the related first and second sender identifications; and

searching the records associated with the reference designator to determine if any of records are suspicious money transfer requests.

15. The method of claim 14, wherein the step of searching includes searching the records to determine if any of the money transfer requests are by a known suspicious user.

16. A method for evaluating electronic money transfers, comprising:

receiving a plurality of money transfer requests;

electronically storing records of the money transfer requests, wherein each record is associated with one money transfer request and has data that defines characteristics of that money transfer request, including at least an location characteristic relating to the location where the money transfer request was made and a transaction characteristic relating to a characteristic other than location;

sorting the money transfer records into at least one block, wherein all records in the block have the same location characteristic;

aggregating the transaction characteristic of all the records in the block to arrive at a collective value for the transaction characteristic;

defining a red flag threshold level for the collective value, the threshold level chosen to represent, if met, a suspicious money transfer pattern;

comparing the collective value for the transactional characteristics with the threshold level;

indicating a suspicious money transfer pattern if the collective value for the transaction characteristic meets the threshold level; and

analyzing individual records within the block if a suspicious money transfer pattern has been indicated.

17. A system for evaluating money transfer records, comprising:

a database for storing a plurality money transfer records, each record having a plurality of data fields relating to the money transfer, including a first field relating to a characteristic of the location where the money transfer was requested and a second field relating to a transaction characteristic not related to location;

a fraud processing server for evaluating the money transfer records, the fraud processing server programmed to:

sort the money records into one or more blocks of records, each block having the same characteristic in the first field;

aggregate the data in the second field of the records in the block to obtain a collective value of the characteristics in the second field;

compare the collective value to a threshold value, wherein the threshold level is chosen to represent, if met, a suspicious money transfer pattern; and

indicating a suspicious money transfer pattern if the collective value meets the threshold value, so that the block of records can be further analyzed to identify suspicious individual money transfers.

18. The system of claim 17, wherein the characteristic in the first field identifies the country where the money transfer request in made.

19. The system of claim 17, wherein the characteristic in the first field identifies the agent network processing the money transfer request.

20. The system of claim 17, wherein the characteristic in the second field identifies the value of the money transfer request.

21. The system of claim 17, wherein the characteristic in the second field identifies the time-of-day of each transaction.

22. The system of claim 17, wherein the characteristic in the second field is chosen from a group consisting of:

transaction value band characteristics;

country corridor characteristics;

agent characteristics;

agent to agent characteristics;

consumer characteristics; and

biographical characteristics.

23. The system of claim 17, wherein the database is a fraud watch database, wherein records are collected and stored by a host computer and an associated transaction database within an money transfer system in response to money transfer requests by senders of money transfers, and wherein the fraud watch database and fraud processing server are separate from the host computer and transaction database, in order to minimize operational impact on the host computer and transaction database.

* * * * *