

**TRANSACTION VERIFICATION SYSTEMS AND
METHODS FOR VERIFYING A TRANSACTION**

TECHNICAL FIELD

[0001] Various embodiments relate to transaction verification systems and methods for verifying a transaction.

BACKGROUND

[0002] Cashless modes of payments have become popular among consumers for the convenience that they offer. They enable quicker transactions free from the need to count cash and to find change. However, cashless modes of payments also tend to come with the risk of fraud, by for example, identity theft. Consumers' digital payment accounts may be compromised when their credentials are stolen. Unauthorized purchases may be made using the compromised payment accounts to the detriment of the account holders.

SUMMARY

[0003] According to various embodiments, there may be provided a method for verifying a transaction. The method may include: receiving in a verification server, an identifier of a consumer and a transaction request, from a merchant terminal; wherein the transaction request includes at least one of merchant location, time and date, and monetary value of an ongoing transaction; retrieving from a consumer database, an expenditure profile and a safe zone profile based on the identifier of the consumer; wherein the expenditure profile includes a spending pattern of the consumer in relation to at least one of merchant location, type of purchase, frequency of purchase, time and day of purchase, and monetary value of transaction; wherein the safe zone profile includes a list of safe locations; and comparing the transaction request against at least one of the expenditure profile and the safe zone profile to detect deviations from at least one of the spending pattern and the list of safe locations.

[0004] According to various embodiments, there may be provided a transaction verification system including: a network receiver configured to receive from a merchant terminal, an identifier of a consumer and a transaction request for each transaction, wherein the transaction request includes at least one of merchant location, time and date, and monetary

value of an ongoing transaction; a consumer database storing a plurality of expenditure profiles and a plurality of safe zone profiles for a corresponding plurality of consumers, wherein each expenditure profile includes a spending pattern of the corresponding consumer in relation to at least one of merchant location, type of purchase, frequency of purchase, time and day of purchase, and monetary value of transaction, wherein each safe zone profile includes a list of safe locations; a verification server configured to retrieve the expenditure and the safe zone profile of the consumer from the consumer database, based on the received identifier of the consumer; and a comparison engine configured to compare the transaction request against at least one of the expenditure profile and the safe zone profile of the consumer to detect deviations from at least one of the spending pattern and the list of safe locations of the consumer.

[0005] According to various embodiments, there may be provided a non-transitory computer-readable medium including instructions which, when executed by a computer, makes the computer perform a method for verifying a transaction, the method including: receiving in a verification server, an identifier of a consumer and a transaction request, from a merchant terminal; wherein the transaction request includes at least one of merchant location, time and date, and monetary value of an ongoing transaction; retrieving from a consumer database, an expenditure profile and a safe zone profile based on the identifier of the consumer; wherein the expenditure profile includes a spending pattern of the consumer in relation to at least one of merchant location, type of purchase, frequency of purchase, time and day of purchase, and monetary value of transaction; wherein the safe zone profile includes a list of safe locations; and comparing the transaction request against at least one of the expenditure profile and the safe zone profile to detect deviations from at least one of the spending pattern and the list of safe locations.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] In the drawings, like reference characters generally refer to the same parts throughout the different views. The drawings are not necessarily to scale, emphasis instead generally being placed upon illustrating the principles of the invention. In the following description, various embodiments are described with reference to the following drawings, in which:

[0007] FIG. 1 shows a flow diagram that illustrates data flow in a fraud detection method according to various embodiments.

[0008] FIG. 2 shows a schematic diagram of a commerce system.

[0009] FIG. 3 shows a flow diagram of a method for verifying transactions according to various embodiments.

[0010] FIG. 4 shows a diagram that illustrates a rule of the fraud rule engine according to various embodiments.

[0011] FIG. 5 shows a diagram that illustrates a rule of the fraud rule engine according to various embodiments.

[0012] FIG. 6 shows a diagram that illustrates a rule of the fraud rule engine according to various embodiments.

[0013] FIG. 7 shows a diagram that illustrates a rule of the fraud rule engine according to various embodiments.

[0014] FIG. 8 shows a diagram that illustrates a rule of the fraud rule engine according to various embodiments.

[0015] FIG. 9 shows an example of a table that stores information on a consumer's trajectory, according to various embodiments.

[0016] FIG. 10 shows an example of a graphical user interface (GUI) of a notification message sent by a fraud rule engine according to various embodiments.

[0017] FIG. 11 shows a flow diagram of a method for verifying a transaction according to various embodiments.

[0018] FIG. 12 shows a conceptual diagram of a transaction verification system according to various embodiments.

[0019] FIG. 13 shows a conceptual diagram of a transaction verification system according to various embodiments.

[0020] FIG. 14 shows a block diagram of a computing device according to various embodiments.

DESCRIPTION

[0021] Embodiments described below in context of the systems are analogously valid for the respective methods, and vice versa. Furthermore, it will be understood that the embodiments described below may be combined, for example, a part of one embodiment may be combined with a part of another embodiment.

[0022] It will be understood that any property described herein for a specific system may also hold for any system described herein. It will be understood that any property described herein for a specific method may also hold for any method described herein. Furthermore, it will be

understood that for any system or method described herein, not necessarily all the components or steps described must be enclosed in the device or method, but only some (but not all) components or steps may be enclosed.

[0023] In this context, the transaction verification system as described in this description may include a memory which is for example used in the processing carried out in the system. A memory used in the embodiments may be a volatile memory, for example a DRAM (Dynamic Random Access Memory) or a non-volatile memory, for example a PROM (Programmable Read Only Memory), an EPROM (Erasable PROM), EEPROM (Electrically Erasable PROM), or a flash memory, e.g., a floating gate memory, a charge trapping memory, an MRAM (Magnetoresistive Random Access Memory) or a PCRAM (Phase Change Random Access Memory).

[0024] In the specification the term “comprising” shall be understood to have a broad meaning similar to the term “including” and will be understood to imply the inclusion of a stated integer or step or group of integers or steps but not the exclusion of any other integer or step or group of integers or steps. This definition also applies to variations on the term “comprising” such as “comprise” and “comprises”.

[0025] The term “coupled” (or “connected”) herein may be understood as electrically coupled or as mechanically coupled, for example attached or fixed, or just in contact without any fixation, and it will be understood that both direct coupling or indirect coupling (in other words: coupling without direct contact) may be provided.

[0026] In order that the invention may be readily understood and put into practical effect, various embodiments will now be described by way of examples and not limitations, and with reference to the figures.

[0027] In the context of various embodiments, a “consumer” may be but is not limited to being interchangeably referred to as a “customer”. A consumer or a customer may be a person who purchases an item from a merchant, in other words, makes a transaction with the merchant.

[0028] In the context of various embodiments, a transaction verification method may include, or may be part of, the process of fraud detection.

[0029] In the context of various embodiments, a fraud rule engine may include, or may be part of, a transaction verification system.

[0030] Conventional fraud detection systems typically use only the merchant location and a set of fraud rules to detect suspicious transactions. Conventional fraud detection systems do not take into consideration user behavior in conjunction with merchant data. For example, the

conventional fraud detection systems do not utilize information on consumers' location or trajectory and consumers' spending habits, and therefore only analyzes transactions in silo without a holistic view. In this digital era where almost every consumer is on a mobile network, consumers generate a lot of traceable data based on their activities. This generated data may be harnessed to detect unauthorized activities with improved accuracy.

[0031] According to various embodiments, a fraud detection method may include acquiring information on a consumer's past journeys. The fraud detection method may include analyzing the consumer's past journeys to recognize a pattern of the consumer's typical journey, for example, from home to office and vice versa. The fraud detection method may include demarcating safe zones that are at least substantially located along the consumer's typical journey. The fraud detection method may include alerting the consumer when a transaction occurs outside of the safe zones.

[0032] The fraud detection method may also include acquiring data on a consumer's past transactions. The data on the transactions may include information on the merchants where the transactions take place. The fraud detection method may include analyzing the consumer's past transactions to recognize a pattern of the consumer's expenditure. For example, the consumer may typically patronize a particular shop at a certain time of the day, or on certain days of the week, or on a regular basis. For example, the consumer may typically spend no more than a certain amount of money in one transaction at a particular shop. For example, the consumer may always purchase items belonging to a certain category from a particular merchant. The fraud detection method may include identifying atypical transactions that deviate from the pattern of the consumer's expenditure, and alerting the consumer when an atypical transaction is identified.

[0033] The fraud detection method may also include acquiring data on past transactions of a sizeable group of consumers. The fraud detection method may include analyzing the past transactions of the group, to determine expenditure trends of different demographics. The data acquired may include information on the consumers that may be used to categorize the consumers into different demographics, for example, age, gender, occupation, ethnicity, nationality etc. The data acquired may also include the geographic locations, the transaction amounts, the category of merchants etc, of the transactions. The fraud detection method may include classifying a consumer into one of the demographics, and identifying atypical transactions that deviate from the expenditure trends of the demographic that the consumer belongs to. The consumer may be alerted when an atypical transaction is identified.

[0034] The systems and methods as described herein may be used in the context of payment transactions using payment processing systems, which are configured to process credit and debit card or e-wallet transactions

[0035] FIG. 1 shows a flow diagram 100 that illustrates data flow in a fraud detection method according to various embodiments. A customer 102 may purchase goods or services from merchants 104, for example Merchants A, B and C. The customer 102 may make payments to the merchants 104 in exchange for goods or services. When the customer 102 purchases the goods or services from the merchants 104, location and transactional data 106 may be transmitted to a fraud rule engine 108. The location and transactional data 106 may include information on the locations of the merchants 104 which sold the goods or services to the customer 102. The location and transactional data 106 may also include information on the purchase, such as the purchase price, the description of the goods or services that are purchased, the time of purchase, the transaction reference number and the mode of payment. Information about the customer 102 may also be collected and transmitted to the fraud rule engine 108. The information about the customer 102 may be location trajectory and activity data 110. The location trajectory and activity data 110 may include at least one of the customer 102's geographical location at the time of purchase, the trajectory of the customer 102's journeys for the day, the trajectories of the customer 102's past journeys, the customer 102's past purchases and the customer 102's personal profile. The fraud rule engine 108 may process the location and transactional data 106, and the location trajectory and activity data 110, to detect any suspicious purchase. The fraud rule engine 108 may identify anomalies in the location and transactional data 106 based on the location trajectory and activity data 110. The fraud rule engine 108 may be trained on the location trajectory and activity data 110. Upon detecting any suspicious purchase, the fraud rule engine 108 may transmit a customer notification 112 to the customer 102. The customer notification 112 may be transmitted via a wireless network, such as a mobile network or internet, to a computer terminal associated with the consumer. The computer terminal may be a mobile terminal such as a mobile phone. A communication code registered to the consumer may be retrieved from a consumer database, based on an identity of the consumer. The communication code may be a phone number of the mobile terminal. The customer notification 112 may include a request for verification message. The fraud rule engine 108 may reject the transaction or notify a payment network to halt the transaction, if a verification message from the consumer is not received within a verification time window, i.e. time out duration.

[0036] FIG. 2 shows a schematic diagram 200 of a commerce system. The commerce system may include an acquirer 208, a payment network 206, and an issuer 204, each of these being communicatively coupled to a network 202. The network 202 may be a wired and/or a wireless network, such as a local area network (LAN), a wide area network (WAN), the Internet, a mobile communications network, and/or any other public and/or private network. The network 202 may be capable of supporting communication among two or more of the illustrated parts of the system. In a non-limiting example, the network 202 may include a plurality of networks, where some networks may be accessible to only part of the transaction system. In a non-limiting example, the transaction system may include different groups of components, each group being communicatively coupled to a respective network of the plurality of networks. For example, the acquirer 208, the payment network 206, and the issuer 204 may each be connected via a private payment transaction network (not illustrated) that is part of the network 202 for processing payment account transactions; while the merchants 104 a-d may each be connected with consumers 102 for effecting payment account transactions, for example, through a public network, such as the Internet, that is also part of the network 202.

[0037] The issuer 204 may be configured to issue payment accounts to consumers 102. Each consumer 102 may be associated with at least one payment account. The consumers 102 may fund their transactions with the merchants through the payment accounts. The payment account, then, may be represented by one or more payment devices such as credit cards, debit cards, electronic devices that can access electronic wallets, etc., that may be used by the consumer 102 at the merchants 104 a-d for the purchase of the products.

[0038] The commerce system may include multiple merchants, for example Merchant A 104a to Merchant D 104d. It should be appreciated that the commerce system may include any number of merchants. The merchants 104a-104d may offer products for sale to consumers 102. Each of the merchants 104a-104d may have a respective physical location, for example, of its brick-and-mortar retail outlet. The consumer 102 may regularly travel from region Y 220b to region Z 220a, for example, as part of his daily commute from home to work.

[0039] The commerce system may include a fraud rule engine 108. The fraud rule engine 108 may be a standalone device, or as indicated by the dotted lines, may be incorporated into any one of the payment network 206, the issuer 208, the consumer device 212 and the acquirer 208. The fraud rule engine 108 may be a processor, or a computer, or a set of computer executable instructions. The fraud rule engine 108 may be configured to detect fraud or to

verify transactions when a consumer 102 makes a payment at a merchant. The fraud rule engine 108 may analyze the transactions. If the fraud rule engine 108 detects potentially fraudulent transactions, the fraud rule engine 108 may send a notification to the consumer 102 regarding the transaction and the consumer can approve or decline the transaction. The fraud rule engine 108 may transmit the notification to a consumer device 212, and the consumer 102 may respond to the notification using the consumer device 212. The consumer device 212 may be a mobile phone, or a mobile computer, or a dedicated security device such as a security token. The fraud rule engine 108 may determine the probability of fraud of the transactions based on a set of rules, which may be predefined or may be determined by the fraud rule engine based on analyzing a set of data. The fraud rule engine 108 may refine or update the set of rules when it receives new data.

[0040] By tracking the consumer's daily movements, the fraud rule engine 108 may be able to learn or predict the consumer's location. The fraud rule engine 108 may define a safe zone 222 where the consumer has a high probability of being present. The information of the safe zone 222 may be stored in a safe zone profile of the consumer. The safe zone may differ depending on the time and date, thus the safe zone profile may include a list of safe locations with respect to a plurality of times and days. The safe zone 222 may be defined as a region within a predefined distance away from the consumer 102's expected trajectory. The fraud rule engine 108 may compute a probability of the consumer 102 being present at various locations away from the expected trajectory further based on more information such as the consumer 102's past transaction history, to select locations associated with probabilities higher than a probability threshold, as being part of the safe zone 222 or being markers or boundaries of the safe zone 222. In the illustrated example, Merchant A 104a, Merchant B 104b and Merchant C 104c may be within the safe zone 222; while Merchant D 104d in Region X 220c, may be outside of the safe zone 222. The fraud rule engine 222 may also define the safe zone 222 based on geographical information. The geographical information may include postal codes, territories, states, cities, counties, or countries. For example, the consumer 102 may live and work near the border of his country, such that part of the neighboring country may be within a threshold distance away from the consumer 102's daily trajectory. However, the consumer 102 may be unlikely to cross the border to make a purchase as that may be inconvenient due to border checks. Given these information, the fraud rule engine 108 may exclude the neighboring country from the safe zone 222. When the consumer 102 makes a transaction at Merchant D 104d, the fraud rule engine 108 may

determine that the Merchant D 104d is physically located outside of the safe zone 222, and may thereby transmit a notification to the consumer 102, through the network 202.

[0041] The fraud rule engine 108 may be coupled to a machine learning engine 210. The machine learning engine 210 may include at least one of supervised and unsupervised algorithms for analyzing the transactions. The unsupervised algorithms may carry out anomaly detection using clustering algorithms. The supervised algorithms may be trained on previously tagged declined transactions. The output of the machine learning engine 210 may be provided to the fraud rule engine 108 to improve the accuracy of the fraud rule engine 108.

[0042] The fraud rule engine 108 may also update its set of rules based on new information provided by the consumer, or acquired through other means. For example, if the consumer is travelling overseas, or continuously detected as being located outside of his usual geographical area, the fraud rule engine may determine that the safe zone may require updating or an additional temporary safe zone may be defined. The fraud rule engine 108 may update the safe zone in real-time based on the location of the consumer device during the transaction.

[0043] In a non-limiting example of a payment account transaction, the consumer 102 may seek to purchase food from a merchant, using his payment account to fund the purchase. The consumer 102 may present a payment device to the merchant. In connection therewith, the merchant may receive and/or retrieve credentials for the consumer's payment account from the payment device, for example, via a point-of-sale (POS) terminal. The merchant may transmit an authorization request through the network 202 to the acquirer 208. The acquirer 208 may be associated with processing transactions at the merchant 104a. In turn, the acquirer 208 may communicate with the issuer 204 through the payment network 206, via the network 202, for authorization of the transaction. The issuer 204 may determine if the consumer's payment account is in good standing and if there is/are sufficient credit/funds to complete the transaction. Before the issuer 204 accepts the transaction, the issuer 204 may request or receive a verification message from the fraud rule engine 108. If the fraud rule engine 108 determines that the transaction is not suspicious, for example, because the merchant is Merchant A 104a which is within the safe zone 222, the fraud rule engine 108 may issue a positive verification message to the issuer 204. If the issuer 204 accepts the transaction, an authorization reply may be provided back to the merchant approving the transaction, and the merchant may then be able to proceed in the transaction. The transaction may be later cleared and settled between the merchant and the acquirer 208 and between the acquirer 208, the payment network 206, and the issuer 204 (in accordance with settlement

arrangements, etc.). Conversely, the issuer 204 may decline the transaction, due to insufficient funds or credit in the payment account, or if the issuer 204 receives a negative verification message from the fraud rule engine 108. The fraud rule engine 108 may transmit a negative verification message, for example, if the merchant is Merchant D 104d outside of the safe zone 222 and upon querying the consumer 102, receives a denial message from the consumer 102. The issuer 204 may transmit an authorization reply back to the merchant declining the transaction, and the merchant may be able to terminate the transaction with the consumer, or request an alternate form of funding. The fraud rule engine 108 may collect the transaction data generated, collected, and stored as part of the above interactions among the merchant, the acquirer 208, the payment network 206, the issuer 204, and the consumer 102. The fraud rule engine 108 may improve its accuracy in detecting suspicious activity, using the collected transaction data.

[0044] The machine learning engine 210, the fraud rule engine 108, the payment network 206, the acquirer 208, the consumer device 212, merchants 104a-d may each include, house, or be part of a computing device 230 which will be described in further details with respect to FIG. 14.

[0045] FIG. 3 shows a flow diagram 300 of a method for verifying transactions according to various embodiments. In 302, a transaction may occur at a merchant. A consumer may have initiated payment using a payment system. In 304, a fraud rule engine may acquire location trajectory and activity details of the consumer. The consumer location trajectory may be determined by a consumer device carried by the consumer, for example a mobile phone or a portable computer that includes a global positioning system (GPS) device. The consumer activity details may include information on an expenditure profile of the consumer. The expenditure profile may include past transactions carried out by the consumer. The expenditure profile may include a spending pattern of the consumer in relation to at least one of merchant location, type of purchase, frequency of purchase, time and day of purchase, and monetary value of transaction. In 304, the fraud rule engine may also acquire personal information or a general profile of the consumer. The personal information of the consumer may include his or her hobbies, occupation, often frequented shops, age etc. The general profile of the consumer may be a classification of the consumer into an age range such as “teenager” or “working adult”, or gender. In 306, the fraud rule engine may acquire information about the merchant and the transaction. Information on the merchant may include the merchant location, or details such as the nature of the goods and services that the merchant offers. The information on the transaction may include the monetary value of the

transaction, the time of the transaction, and the mode of payment. The fraud rule engine may acquire this information from a payment network. In 308, the fraud rule engine may analyze the data obtained in 304 and 306, and determine whether the transaction is anomalous. The fraud rule engine may determine that a transaction is anomalous if the transaction breaches a set of predefined rules. The fraud rule engine may also define the rules based on analyzing the data received in 304. The predefined rules may include a definition of a safe zone of the consumer. The fraud rule engine may determine transactions that take place within the safe zone, in other words, when the merchant is located within the safe zone, to be verified or to be unsuspecting. Conversely, if the transaction is taking place outside of the safe zone, the fraud rule engine may determine the transaction to be potentially fraudulent. If the fraud rule engine determines that the transaction is not suspicious, the fraud rule engine may instruct a payment network to process the payment for the transaction in 310. If the fraud rule engine determines that the transaction is potentially fraudulent, the fraud rule engine may proceed to 312. In 312, the fraud rule engine may send a notification message to a consumer device, such as a laptop or a mobile phone, through a wireless network. The notification message may include at least one of the payment amount, the merchant name, the merchant address, the items purchased. The notification message may include a request for the consumer's manual authentication of the transaction. In 314, the consumer may reply to the notification through the consumer device, to either approve or deny the transaction. The consumer device may transmit the consumer's reply to the fraud rule engine. If the consumer approves the transaction, the fraud rule engine may transmit a message to a payment network. Consequently, in 310, the payment for the transaction may be processed, in other words, deducted from a payment account of the consumer. When the consumer approves the transaction, the fraud rule engine may also update its rules in 316, for example to re-define the safe zone to include the location of the merchant where the transaction is taking place. Optionally, the notification message sent in 312 may also query the consumer on whether the rules of the fraud rule engine should be updated, for example whether the merchant is to be added to a safe merchant list or whether the present location is to be added to the safe zone. The reply from the consumer may include an affirmative or negative response as to whether the rules of the fraud rule engine should be updated.

[0046] According to various embodiments, the method for verifying transactions may be applicable to transactions carried out in brick and mortar stores, where the consumer purchases goods or services in person at the merchant's location.

[0047] According to various embodiments, the method for verifying transactions may be applicable to web transactions, where the consumer purchases goods or services online. For web transactions, the merchant location may be defined as the web URL or the web address of the online store, for example, “http://www.amazon.com”. The safe zone profile of the consumer may include a list of safe web URLs. The fraud rule engine may compile the list of safe web URLs based on the consumer’s online transaction history. The consumer may also manually input the websites of his preferred online merchants into the list of safe web URLs. When the consumer makes an online purchase, the fraud rule engine may compare the web address of the online merchant against the list of safe web URLs. If the web address of the online merchant is not part of the list of safe web URLs, the fraud rule engine may determine the online purchase to be suspicious and may send an alert to a computer terminal that the consumer is using to access the Internet.

[0048] FIG. 4 shows a diagram 400 that illustrates a rule of the fraud rule engine according to various embodiments. In a non-limiting example, a consumer may reside in Singapore. The consumer’s home 406 may be in central-southern Singapore. The consumer may work in an office 408 that is located in eastern Singapore. The consumer may commute from home 406 to the office 408 on every weekday morning, and may be commute from the office 408 to home 406 on every weekday evening. The consumer may pass by merchants 404b, 404c, 404d and 404f during his weekday commutes. The fraud rule engine may receive data on the consumer’s weekday commutes directly or indirectly through a wireless network, from the consumer’s device that includes a location tracker such as a GPS. The consumer device may upload the consumer’s trajectory data onto a server, and the fraud rule engine may retrieve the trajectory data from the server. The consumer device may also send the consumer’s trajectory data directly to the fraud rule engine, for example, if the fraud rule engine resides in the consumer device. The consumer device may be configured to run a mobile application that includes at least part of the fraud rule engine.

[0049] The fraud rule engine may determine a safe zone 402 based on the consumer’s trajectory of travel to and fro between home 406 and the office 408. The safe zone 402 may be a predefined distance away from the trajectory path. The consumer may be able to input the predefined distance, for example, into the mobile application. Alternatively, the consumer may be able to manually input his trajectory path, or his safe zone 402, if he prefers not to have his movements tracked by the fraud rule engine. When a payment network receives a request for payment from the consumer’s payment account (for example, digital wallet, credit card, debit card, electronic vouchers etc.), the payment network may transmit details of the

transaction and the merchant to the fraud rule engine. For example, a merchant 404g located at western Singapore may request for a payment from the consumer's payment account. The merchant 404g may be located beyond the safe zone 402. The fraud rule engine may compare the location of the merchant 404g with the safe zone 402 and determines that the location of the merchant 404g breaches the safe zone rule. As a result, the fraud rule engine may send a request for verification message to the consumer device, to seek the consumer's confirmation on the authenticity of the transaction.

[0050] The fraud rule engine may recognize that the safe zone 402 may be valid only for weekdays, as the consumer may have a different commuting pattern on weekends. The fraud rule engine may determine a different safe zone for weekends. The consumer may also be associated with different safe zones depending on other factors such as the time of the day, the month of the year and the season of the year.

[0051] FIG. 5 shows a diagram 500 that illustrates a rule of the fraud rule engine according to various embodiments. The fraud rule engine may obtain information about the consumer, for example, gender, age or age group, hobbies etc. The fraud rule engine may also receive statistical information of the expenditure patterns of different demographics. The statistical information may be provided by governmental organizations, private companies or academic institutions. The fraud rule engine may also obtain the statistical information from an information engine. The information engine may be a standalone engine, or may part of the fraud rule engine. The information engine may be able to crowd source information to compute the statistical information. For example, the information engine may include, or may be integrated into, an application that can be installed on mobile phones. The application may pose survey questions to the consumers from time to time, to collect information on the consumers' expenditure patterns. The application may reward the consumers with promo codes, vouchers or reward points, for participating in the surveys. The statistical information may indicate preferences of different demographics, for example, a first town 502 may be popular among male consumers, a second town 504 may be popular among female consumers, while a third town 506 may be popular among teenagers. The statistical information may also be predicted based on census conducted in the various towns. For example, the first town 502 may include a large heavy industry park where most of the employees are male, such that the gender ratio in the first town 502 is skewed towards men. For example, the second town 504 may include a disproportionate number of merchants that target female consumers, such as nail salons, beauty salons, ladies' spa and ladies' gyms. For example, the third town 506 may be a university town, or may include several schools, such

that many students frequent the third town 506. Based on information on at least one of the population, the types of shops, the industries and the facilities in the towns, the information engine may generate a profile of the typical consumer in the respective towns. The fraud rule engine may receive the profile of the typical consumer in the towns. When a transaction query is sent to the fraud rule engine, the fraud rule engine may compare the consumer's profile against the profile of the typical consumer in the locale where the transaction is being made. If the consumer's profile does not match the profile of the typical consumer in the locale, the fraud rule engine may send the consumer a notification seeking the consumer's verification of the transaction. Alternatively, the fraud rule engine may use the profile of the consumer as only part of the criteria, or only one rule of the set of rules in determining a suspicious transaction. The fraud rule engine may combine the information from the information engine with the safe zone information, to improve the accuracy of detecting fraudulent transactions. The fraud rule engine may modify the safe zone of the consumer, based on the information of the typical consumer in the different regions. For example, if the consumer's safe zone includes part of the second town 504, but the consumer is a man, the fraud rule engine may reduce the size of the safe zone to exclude the second town 504.

[0052] FIG. 6 shows a diagram 600 that illustrates a rule of the fraud rule engine according to various embodiments. The fraud rule engine, or the information engine, may generate data on the average recency of transactions for each merchant, based on consumer activity. In other words, a typical time between purchases at each merchant may be determined. For example, a consumer 102 may shop once every two days at the merchant 604b, in other words, the recency is low for the merchant 604b. In other words, the consumer 102 may be a frequent shopper at the merchant 604b. When a transaction is made at merchant 604a, the fraud rule engine may retrieve the consumer 102's past transaction history and may find that the consumer last shopped at the merchant 604a two days ago. However, the average recency of the consumer 102's transactions at the merchant 604a may be 45 days. Thus, it may be unusual for the consumer 102 to be back at the merchant 604a so soon. The fraud rule engine may determine the transaction at the merchant 604a to be suspicious. The fraud rule engine may also raise an alarm bell, i.e. send a notification to the consumer, if the transaction is taking place at a merchant where the consumer has no transaction history.

[0053] FIG. 7 shows a diagram 700 that illustrates a rule of the fraud rule engine according to various embodiments. The fraud rule engine, or the information engine, may generate data on the average frequency of transactions for each merchant, based on consumer activity. The set of rules of the fraud rule engine may include a safe frequency threshold for a consumer 102 at

each merchant. For example, the consumer 102 may typically patronize merchant 604a up to three times a day. The merchant 604a may be for example, a café where the consumer 102 purchases drinks. For example, the consumer 102 may typically patronize merchant 604b only once in a month. The merchant 604b may be for example, a warehouse club which sells goods in large quantities. The consumer 102 may manually set, or the fraud rule engine may determine the safe frequency threshold for merchant 604a as three times a day and the safe frequency threshold for merchant 604b as once a month. When a second transaction of the week is being made at the merchant 604b, the fraud rule engine may determine that the transaction is suspicious as the frequency of transaction at the merchant 604b has exceed the safe frequency threshold.

[0054] FIG. 8 shows a diagram 800 that illustrates a rule of the fraud rule engine according to various embodiments. The fraud rule engine may have a rule against multiple same-value transactions occurring at the same merchant 804 or within an area 806. Such repeated identical transactions may be typical of automated scripts distributed to trick payment networks. For example, if transactions of \$100 occurs repeatedly for more than a threshold of three times within a time threshold of for example, 1 day, at the merchant 804 or within the area 806, the fraud rule engine may notify the consumer and seek his verification of the latest transaction.

[0055] FIG. 9 shows an example of a table 900 that stores information on a consumer's trajectory, according to various embodiments. The fraud rule engine may use the information stored in the table 900 to define the safe zone of the consumer. The table 900 may include a plurality of columns. Each row of the table 900 may correspond to one position in the consumer's trajectory. Column 902 may list a serial number of each entry. Column 904 and column 906 may list the location of the consumer, in any one format of GPS coordinates, latitude and longitude, or map reference or other suitable formats. Column 908 may state the date. Column 910 may state the time when the consumer is present at the location indicated in columns 904 and 906. Column 912 may indicate an identifier of the consumer device that provided the consumer's location. Column 914 may indicate an identifier of the consumer. Column 916 may indicate whether a transaction involving the consumer occurred at the time and location. In the example table 900, row 990 shows that a consumer (UserID: A001) made a purchase at a first location (corresponding to a first merchant) in the morning at 8.45am. Row 992 shows that the same consumer made a purchase at a second location (corresponding to a second merchant) fifteen minutes later at 9am. Row 994 shows that the same consumer made a purchase at the second merchant later in the day at 6pm. Row 996 shows that the

same consumer made a purchase at the first merchant later in the day at 6.15pm. From the data in the table 900, the fraud rule engine may determine a commuting pattern and expenditure pattern. The consumer appears to travel in a direction from the first merchant to the second merchant in the morning, stopping by both merchants to make purchases. The consumer appears to travel in the reverse direction from the second merchant to the first merchant in the evening, also stopping by both merchants to make purchases. The fraud rule engine may compare transactions against the established commuting and expenditure pattern and may classify deviations from the established patterns as suspicious transactions. If the consumer verifies that the deviations are valid transactions, the fraud rule engine may update the established patterns to take into account the deviations.

[0056] FIG. 10 shows an example of a graphical user interface (GUI) 1000 of a notification message 1002 sent by a fraud rule engine according to various embodiments. The notification message 1002 may be received and displayed on a consumer device 212. The notification message 1002 may include options for the consumer to provide his response to approve or reject the suspicious transaction.

[0057] FIG. 11 shows a flow diagram 1100 of a method for verifying a transaction according to various embodiments. The method for verifying a transaction may include, or may be part of, the fraud detection method described throughout the specification. Element 1102 may include receiving in a verification server, an identifier of a consumer and a transaction request, from a merchant terminal. The verification server may include, or may be part of, the fraud rule engine 108 and/or the payment network 206. The identifier of the consumer may include the user identifier in column 914 of table 900. The identifier of the consumer may include the name of the consumer, or the identifier of the payment account of the consumer. The merchant terminal may reside with the merchant, and may be configured to facilitate payment, for example, may be a POS terminal. The transaction request may include at least one of the merchant location, time and date, and monetary value of an ongoing transaction. Element 1104 may include retrieving from a consumer database, an expenditure profile and a safe zone profile based on the identifier of the consumer. The consumer database may be stored on a server, or may be stored in a memory of the fraud rule engine 108. The expenditure profile may include a spending pattern of the consumer in relation to at least one of merchant location, type of purchase, frequency of purchase, time and day of purchase, and monetary value of transaction. The safe zone profile may include a list of safe locations with respect to a plurality of times and days. Element 1106 may include comparing the transaction request against at least one of the expenditure profile and the safe zone profile to detect

deviations from at least one of the spending pattern and the list of safe locations. A deviation may hint at a suspicious transaction.

[0058] According to various embodiments, a non-transitory computer-readable medium may be provided. The non-transitory computer-readable medium may include instructions which, when executed by a computer, makes the computer perform the method described with respect to FIG. 11.

[0059] FIG. 12 shows a conceptual diagram of a transaction verification system 1200 according to various embodiments. The transaction verification system 1200 may include, or may be part of, the fraud rule engine 108. The transaction verification system 1200 may include a network receiver 1202, a consumer database 1204, a verification server 1206, and a comparison engine 1208. The network receiver 1202 may be configured to receive from a merchant terminal, an identifier of a consumer and a transaction request for each transaction. The transaction request may include at least one of merchant location, time and date, and monetary value of an ongoing transaction. The consumer database 1204 may store a plurality of expenditure profiles and a plurality of safe zone profiles for a corresponding plurality of consumers. Each expenditure profile may include a spending pattern of the corresponding consumer in relation to at least one of merchant location, type of purchase, frequency of purchase, time and day of purchase, and monetary value of transaction. Each safe zone profile may include a list of safe locations with respect to a plurality of times and days of the corresponding consumer. The verification server 1206 may be configured to retrieve the expenditure and the safe zone profile of the consumer from the consumer database, based on the received identifier of the consumer. The comparison engine 1208 may be configured to compare the transaction request against at least one of the expenditure profile and the safe zone profile of the consumer to detect deviations from at least one of the spending pattern and the list of safe locations of the consumer. The verification server 1206 may be further configured to retrieve from the consumer database, a communication code (for example: telephone number, or user ID) registered to the consumer based on the identity of the consumer, upon the comparison engine detecting deviations from at least one of the spending pattern and the plurality of safe locations of the consumer. The network receiver 1202, the consumer database 1204, the verification server 1206 and the comparison engine 1208 may be coupled with each other, like indicated by lines 1220, for example communicatively coupled, for example electrically coupled.

[0060] FIG. 13 shows a conceptual diagram of a transaction verification system 1300 according to various embodiments. Like the transaction verification system 1200, the

transaction verification system 1300 may include, or may be part of, the fraud rule engine 108. In addition to the transaction verification system 1200, the transaction verification system 1300 may include a safe zone generator 1310. The safe zone generator 1310 may be configured to generate the safe zone profile based on at least one of past transactions requests of the consumer and past journeys taken by the consumer. The safe zone generator 1310 may be further configured to update the safe zone profile in real-time, based on a location of a mobile terminal associated with the consumer during the ongoing transaction. The transaction verification system 1300 may also include an expenditure profile generator 1312. The expenditure profile generator 1312 may be configured to generate the expenditure profile based on past transaction requests of the consumer. The expenditure profile generator 1312 may further be configured to generate the expenditure profile based on statistical information in relation to at least one of the consumer's age, gender and hobbies. The transaction verification system 1300 may further include a network transmitter configured to transmit a request for verification message to a mobile terminal or a consumer device using the communication code. The network transmitter may be configured to connect to the network 202. The transaction verification system 1300 may further include a verification processor configured to reject the ongoing transaction if a verification message is not received from the mobile terminal or consumer device within a verification time window. The network receiver 1202, the consumer database 1204, the verification server 1206, the comparison engine 1208, the safe zone generator 1310 and the expenditure profile generator 1312 may be coupled with each other, like indicated by lines 1330, for example communicatively coupled, for example electrically coupled.

[0061] FIG. 14 shows a block diagram of a computing device 230 according to various embodiments. The computing device 230 may include, for example, one or more servers, workstations, personal computers, laptops, tablets, smartphones, POS terminals, other suitable computing devices, etc. In addition, the computing device 230 may be a single computing device, or may be a cluster of computing devices located in close proximity, or multiple computing devices distributed over a geographic region. In the commerce system of FIG. 2, each of the merchants 104 a-d, the acquirer 208, the payment network 206, the issuer 204, and the consumer device 212 may include, or may be implemented in, a computing device 230, coupled to (and in communication with) the network 202. The computing device 230 may include a processor 1402 and a memory 1404 coupled to (and in communication with) the processor 1402. The processor 1402 may include one or more processing units (e.g., in a multi-core configuration, etc.) including, without limitation, a

central processing unit (CPU), a microcontroller, a reduced instruction set computer (RISC) processor, an application specific integrated circuit (ASIC), a programmable logic device (PLD), a gate array, and/or any other circuit or processor capable of the functions described herein. The above examples are exemplary only, and are not intended to limit in any way the definition and/or meaning of the processor. The memory 1404, as described herein, may permit data, instructions, etc., to be stored therein and retrieved therefrom. The memory 1404 may include one or more computer-readable storage media, such as, without limitation, dynamic random access memory (DRAM), static random access memory (SRAM), read only memory (ROM), erasable programmable read only memory (EPROM), solid state devices, flash drives, CD-ROMs, thumb drives, floppy disks, tapes, hard disks, and/or any other type of volatile or nonvolatile physical or tangible computer-readable media. The memory 1404, and/or data structures included therein, may be configured to store, without limitation, transaction data, other data relating to the merchants (e.g., including relational geographic data between the merchants etc.) and the consumers, and/or other types of data and/or information suitable for use as described herein. Furthermore, in various embodiments, computer-executable instructions may be stored in the memory 1404 for execution by the processor 1402 to cause the processor 1402 to perform one or more of the functions described herein. The memory 1404 may be a physical, tangible, and non-transitory computer readable storage media. It should be appreciated that the memory 1404 may include a variety of different memories, each implemented in one or more of the functions or processes described herein.

[0062] The computing device 230 may also include a presentation unit 1406 (or output device or display device) that may be coupled to (and is in communication with) the processor 1402. It should be appreciated that the computing device 230 may include output devices other than the presentation unit 1406. The presentation unit 1406 may output information, either visually or audibly to a user 1420 of the computing device 230, for example, a consumer, a user associated with any one of the payment network 206, the issuer 204 or the consumer 102. It should be further appreciated that various interfaces may be displayed at the computing device 230, and in particular at presentation unit 1406, to display information, such as, for example, transaction data, etc. The presentation unit 1406 may include, without limitation, a liquid crystal display (LCD), a light-emitting diode (LED) display, an organic LED (OLED) display, an “electronic ink” display, etc. In some embodiments, presentation unit 1406 may include multiple devices.

[0063] The computing device 230 may further include an input device 1408 that may receive inputs from the user 1420 of the computing device 230 (i.e., user inputs). The input device 1408 may be coupled to (and may be in communication with) the processor 1402 and may include, for example, a keyboard, a pointing device, a mouse, a stylus, a touch sensitive panel (e.g., a touch pad or a touch screen, etc.), another computing device, and/or an audio input device. A touch screen, such as that included in a tablet, a smartphone, or similar device, may behave as both a presentation unit 1406 and an input device 1408. In addition, the computing device 230 may also include a network interface 1410 coupled to (and in communication with) the processor 1402 and the memory 1404. The network interface 1410 may include, without limitation, a wired network adapter, a wireless network adapter, a mobile network adapter, or other device capable of communicating to one or more different networks 1412, including the network 202. The computing device 230 may include the processor 1402 and one or more network interfaces incorporated into or with the processor 1402.

[0064] The following examples pertain to further embodiments.

[0065] Example 1 is a method for verifying a transaction, the method including: receiving in a verification server, an identifier of a consumer and a transaction request, from a merchant terminal; wherein the transaction request includes at least one of merchant location, time and date, and monetary value of an ongoing transaction; retrieving from a consumer database, an expenditure profile and a safe zone profile based on the identifier of the consumer; wherein the expenditure profile includes a spending pattern of the consumer in relation to at least one of merchant location, type of purchase, frequency of purchase, time and day of purchase, and monetary value of transaction; wherein the safe zone profile includes a list of safe locations; and comparing the transaction request against at least one of the expenditure profile and the safe zone profile to detect deviations from at least one of the spending pattern and the list of safe locations.

[0066] In example 2, the subject-matter of example 1 can optionally include upon detecting deviations from at least one of the spending pattern and the list of safe locations, retrieving from the consumer database, a communication code registered to the consumer based on the identity of the consumer; transmitting a request for verification message to a mobile terminal associated with the consumer using the communication code; and rejecting the ongoing transaction if a verification message is not received from the mobile terminal within a verification time window.

[0067] In example 3, the subject-matter of example 1 or example 2 can optionally include generating the safe zone profile based on past transaction requests of the consumer.

[0068] In example 4, the subject-matter of any one of examples 1 to 3 can optionally include updating the safe zone profile in real-time, based on a location of a mobile terminal associated with the consumer during the ongoing transaction.

[0069] In example 5, the subject-matter of any one of examples 1 to 4 can optionally include generating the safe zone profile based on past journeys taken by the consumer.

[0070] In example 6, the subject-matter of any one of examples 1 to 5 can optionally include generating the expenditure profile based on past transaction requests of the consumer.

[0071] In example 7, the subject-matter of any one of examples 1 to 6 can optionally include generating the expenditure profile based on statistical information in relation to at least one of the consumer's age, gender, and hobbies.

[0072] In example 8, the subject-matter of any one of examples 1 to 7 can optionally include that the list of safe locations vary according to a time of a day or day of a week.

[0073] Example 9 is a transaction verification system including: a network receiver configured to receive from a merchant terminal, an identifier of a consumer and a transaction request for each transaction, wherein the transaction request includes at least one of merchant location, time and date, and monetary value of an ongoing transaction; a consumer database storing a plurality of expenditure profiles and a plurality of safe zone profiles for a corresponding plurality of consumers, wherein each expenditure profile includes a spending pattern of the corresponding consumer in relation to at least one of merchant location, type of purchase, frequency of purchase, time and day of purchase, and monetary value of transaction, wherein each safe zone profile includes a list of safe locations; a verification server configured to retrieve the expenditure and the safe zone profile of the consumer from the consumer database, based on the received identifier of the consumer; and a comparison engine configured to compare the transaction request against at least one of the expenditure profile and the safe zone profile of the consumer to detect deviations from at least one of the spending pattern and the list of safe locations of the consumer.

[0074] In example 10, the subject-matter of example 9 can optionally include that the verification server is further configured to retrieve from the consumer database, a communication code registered to the consumer based on the identity of the consumer, upon the comparison engine detecting deviations from at least one of the spending pattern and the list of safe locations of the consumer.

[0075] In example 11, the subject-matter of example 10 can optionally include: a network transmitter configured to transmit a request for verification message to a mobile terminal associated with the consumer using the communication code; and a verification processor configured to reject the ongoing transaction if a verification message is not received from the mobile terminal within a verification time window.

[0076] In example 12, the subject-matter of any one of examples 9 to 11 can optionally include: a safe zone generator configured to generate the safe zone profile based on at least one of past transaction requests of the consumer and past journeys taken by the consumer.

[0077] In example 13, the subject-matter of example 12 can optionally include that the safe zone generator is further configured to update the safe zone profile in real-time, based on a location of a mobile terminal associated with the consumer during the ongoing transaction.

[0078] In example 14, the subject-matter of any one of examples 9 to 13 can optionally include: an expenditure profile generator configured to generate the expenditure profile based on past transaction requests of the consumer.

[0079] In example 15, the subject-matter of example 14 can optionally include that the expenditure profile generator is further configured to generate the expenditure profile based on statistical information in relation to at least one of the consumer's age, gender, and hobbies.

[0080] In example 16, the subject-matter of any one of examples 9 to 15 can optionally include that the list of safe locations vary according to a time of a day or day of a week.

[0081] Example 17 is a non-transitory computer-readable medium including instructions which, when executed by a computer, makes the computer perform a method for verifying a transaction, the method including: receiving in a verification server, an identifier of a consumer and a transaction request, from a merchant terminal; wherein the transaction request includes at least one of merchant location, time and date, and monetary value of an ongoing transaction; retrieving from a consumer database, an expenditure profile and a safe zone profile based on the identifier of the consumer; wherein the expenditure profile includes a spending pattern of the consumer in relation to at least one of merchant location, type of purchase, frequency of purchase, time and day of purchase, and monetary value of transaction; wherein the safe zone profile includes a list of safe locations; and comparing the transaction request against at least one of the expenditure profile and the safe zone profile to detect deviations from at least one of the spending pattern and the list of safe locations.

[0082] While embodiments of the invention have been particularly shown and described with reference to specific embodiments, it should be understood by those skilled in the art that

various changes in form and detail may be made therein without departing from the spirit and scope of the invention as defined by the appended claims. The scope of the invention is thus indicated by the appended claims and all changes which come within the meaning and range of equivalency of the claims are therefore intended to be embraced. It will be appreciated that common numerals, used in the relevant drawings, refer to components that serve a similar or the same purpose.

[0083] It will be appreciated to a person skilled in the art that the terminology used herein is for the purpose of describing various embodiments only and is not intended to be limiting of the present invention. As used herein, the singular forms "a", "an" and "the" are intended to include the plural forms as well, unless the context clearly indicates otherwise. It will be further understood that the terms "comprises" and/or "comprising," when used in this specification, specify the presence of stated features, integers, steps, operations, elements, and/or components, but do not preclude the presence or addition of one or more other features, integers, steps, operations, elements, components, and/or groups thereof.

[0084] It is understood that the specific order or hierarchy of blocks in the processes / flowcharts disclosed is an illustration of exemplary approaches. Based upon design preferences, it is understood that the specific order or hierarchy of blocks in the processes / flowcharts may be rearranged. Further, some blocks may be combined or omitted. The accompanying method claims present elements of the various blocks in a sample order, and are not meant to be limited to the specific order or hierarchy presented.

[0085] The previous description is provided to enable any person skilled in the art to practice the various aspects described herein. Various modifications to these aspects will be readily apparent to those skilled in the art, and the generic principles defined herein may be applied to other aspects. Thus, the claims are not intended to be limited to the aspects shown herein, but is to be accorded the full scope consistent with the language claims, wherein reference to an element in the singular is not intended to mean "one and only one" unless specifically so stated, but rather "one or more." The word "exemplary" is used herein to mean "serving as an example, instance, or illustration." Any aspect described herein as "exemplary" is not necessarily to be construed as preferred or advantageous over other aspects. Unless specifically stated otherwise, the term "some" refers to one or more. Combinations such as "at least one of A, B, or C," "one or more of A, B, or C," "at least one of A, B, and C," "one or more of A, B, and C," and "A, B, C, or any combination thereof" include any combination of A, B, and/or C, and may include multiples of A, multiples of B, or multiples of C. Specifically, combinations such as "at least one of A, B, or C," "one or more of A, B, or C,"

“at least one of A, B, and C,” “one or more of A, B, and C,” and “A, B, C, or any combination thereof” may be A only, B only, C only, A and B, A and C, B and C, or A and B and C, where any such combinations may contain one or more member or members of A, B, or C. All structural and functional equivalents to the elements of the various aspects described throughout this disclosure that are known or later come to be known to those of ordinary skill in the art are expressly incorporated herein by reference and are intended to be encompassed by the claims. Moreover, nothing disclosed herein is intended to be dedicated to the public regardless of whether such disclosure is explicitly recited in the claims. The words “module,” “mechanism,” “element,” “device,” and the like may not be a substitute for the word “means.” As such, no claim element is to be construed as a means plus function unless the element is expressly recited using the phrase “means for.”