Abstract

Systems and methods are presented for analyzing a credit card or other financial transaction and, based on whether a score for the transaction meets or exceeds a user-selected threshold, sending a transaction notification message to a consumer's electronic device such as a cell phone.
LOG ON TO AN ENROLLMENT WEB SITE

VIEW A DISPLAY SHOWING A RANGE OF POSSIBLE THRESHOLDS

INPUT A THRESHOLD VALUE INTO THE WEBSITE

SUBMIT THE THRESHOLD VALUE TO THE WEB SITE SUCH THAT THE THRESHOLD VALUE IS STORED IN A DATABASE

FIG. 5
FRAUD AND REPUTATION PROTECTION USING ADVANCED AUTHORIZATION AND RULES ENGINE

CROSS-REFERENCES TO RELATED APPLICATIONS

[0001] This application claims the benefit of U.S. Provisional Application No. 61/173,371, filed Apr. 28, 2009 titled “Alerts Based System and Method” (Attorney Docket 01622-048000US), hereby incorporated by reference in its entirety for all purposes.

BACKGROUND

[0002] 1. Field of the Invention

[0003] Generally, systems and methods are disclosed for financial data processing of transactions through a payment processing network. More specifically, methods and systems are disclosed for alerting a user, based on a score, of a possible fraudulent transaction by sending a transaction notification message to a consumer device such as a cellular phone.

[0004] 2. Discussion of the Related Art

[0005] Fraud and identity theft have become more of a problem as more consumers use credit and other payment cards to complete financial transactions. The number of transactions completed through payment cards and their respective accounts, as opposed to through cash and checks, has grown to cover a substantial portion of the financial transactions people make.

[0006] Because of fraud, sending various types of alerts to users over various communication channels has become increasingly popular with users who want warnings regarding their personal information and associated assets or accounts. Alerts also benefit issuers, the banks or financial institutions that issue a card to a consumer, and acquirers, the banks or financial institutions that process data for merchants.

[0007] Originally, information, messages, and alerts were delivered by traditional communication channels such as by postal mail. Postal mail messages were frequently delivered within a periodic statement or a monthly bill on a regular basis and often included recent activity as well as any miscellaneous announcements or updates. Although they were delivered on a regular basis, messages that were delivered by traditional post inherently required entities, such as credit card issuers, to collect batches of information before they send it out to a user business. For example, credit card issuers traditionally sent paper statements through postal mail to users at the end of a financial period, usually on a monthly basis. The credit card account activity included in the monthly statements are usually days, if not weeks, old due to the delay caused by generation and delivery of the paper statements. While the information in the monthly statements may be useful, delays in the dissemination of information for some period of time while the information is collected into a batch can be undesirable in trying to deliver critical information to users.

[0008] For example, if an identity thief obtained a user’s credit card or credit card number to make unauthorized purchases, the user would not be alerted to this fact until the user received and reviewed the monthly statement. Due to the delay in generating and delivering paper-based statements, the identity thief would have the opportunity and ability to make multiple unauthorized purchases before the user was alerted by the information in the paper-based statement. In addition, there was essentially no way for the alerting entity to cost-effectively or practically confirm delivery of the paper statement to the user.

[0009] To increase the speed and reliability with which users are alerted to suspicious or potentially fraudulent use of user account or identity information, some entities, such as credit card issuers, offer telephone notification services to contact the user whenever suspicious activity is detected. In such systems, a human or an automated system calls the user to alert him or her whenever suspicious activity is discovered in a near to real-time manner. Although such telephone alert systems are sometimes effective at quickly delivering alerts to users, they are relatively resource intensive, requiring either many telephone operators or complex automated telephone dialers with access to many relatively expensive telephone lines. As such, telephone alert systems are effectively not scalable or practical for entities that need to service and send alerts to large numbers of users or businesses.

[0010] As described above, there is a need for timely, cost-effective, reliable and scalable solution for delivering alerts to large numbers of users.

BRIEF SUMMARY

[0011] Embodiments in accordance with the present disclosure generally relate to automatically sending a transaction notification message to a user’s cellular phone or other consumer device based on a transaction score, the score being determined from transaction data corresponding to an authorization request.

[0012] Whether the score is sent can be based on a user-selectable threshold, such that a score equal to or higher than the threshold causes a message to be sent, and a score lower than the threshold results in no message being sent. The threshold can be entered, chosen, or selected by the user in an enrollment process. Enrollment can be through the consumer device, through a user’s personal computer, or by an unrelated electronic device.

[0013] The score itself can be calculated using user-selected weightings or other parameters. For example, one user can build a potential fraud score by weighting transaction location concerns (e.g. a purchase in a foreign country) at 30%, type of merchant (e.g. adult bookstore, a merchant category code (MCC)) at 30%, and purchase amount (e.g. $500) at 40%, for his or her score. Another user can choose different weightings.

[0014] The score itself can be included in the message content, the message content can be based upon the score (e.g. thumbs up, a yellow caution sign, a red X), or the message can be simply sent or not depending on whether the score meets or exceeds a threshold value.

[0015] Based on a score, a coupon for another transaction can be sent which can later be used to calculate a future score. For example, a credit card transaction may be suspicious because it is for a plane ticket to an overseas destination for a cardholder that does not normally travel. Partly or wholly based upon the elevated fraud score, a coupon for a tourist attraction in the destination city can be sent with an alert message to the cardholder’s cell phone. If the coupon is used at the tourist attraction along with the card that bought the plane ticket, then the score for the transaction at the tourist attraction is lowered.

[0016] One embodiment in accordance with the present disclosure relates to receiving an authorization request message comprising transaction data at a server computer.
authorization request message requests approval to conduct a transaction. It further relates to generating a score based on the transaction data, comparing the score to a user selected threshold, and sending a transaction notification message to a consumer device used by a consumer if the score meets or exceeds the threshold.

[0017] An embodiment can include a selection of a communication channel based on the score. For example, a user can select to be notified by an interactive voice response (IVR) phone call if the score is extremely high, by a short message service (SMS) message on a cell phone if the score is high but not extremely high, and by email if the score is a lower score.

[0018] Other embodiments relate to machine-readable tangible storage media and computer systems which employ or store instructions for the methods described above.

[0019] A further understanding of the nature and the advantages of the embodiments disclosed and suggested herein may be realized by reference to the remaining portions of the specification and the attached drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0020] FIG. 1A illustrates a cellular phone with a short message system (SMS) cardholder alert message in accordance with an embodiment.

[0021] FIG. 1B illustrates a cellular phone with an alternate cardholder alert message with a coupon in accordance with an embodiment.

[0022] FIG. 2 is a network-level diagram illustrating messages between entities in accordance with an embodiment.

[0023] FIG. 3 is a system-level diagram illustrating a coupon used for authentication in accordance with an embodiment.

[0024] FIG. 4 is a flowchart illustrating a process in accordance with an embodiment.

[0025] FIG. 5 is a flowchart illustrating a process in accordance with an embodiment.

[0026] FIG. 6A shows a block diagram of a portable consumer device in accordance with an embodiment.

[0027] FIG. 6B shows a block diagram of a portable consumer device in accordance with an embodiment.

[0028] FIG. 7 shows a block diagram of an exemplary computer apparatus that can be used in some embodiments.

[0029] The figures will now be used to illustrate different embodiments in accordance with the invention. The figures are specific examples of embodiments and should not be interpreted as limiting embodiments, but rather exemplary forms and procedures.

DETAILED DESCRIPTION

[0030] Embodiments in accordance with the present disclosure generally relate to automatically sending a transaction notification message to a cell phone, personal digital assistant (PDA), or other consumer device based on a transaction score. The score is determined from transaction data from an authorization request/response within a payment processing network. In certain embodiments, the score determines whether a message is sent or not. In some embodiments, the score itself is part of the message or at least affects the content of the message.

[0031] The transaction score can be any number, character, or other representation that represents ordinal values. For example, a score can be “100,” an “A+,” or a “two-thumbs up.” Number scores can be within pre-established ranges, such as 0 to 100, or can include the range of all real numbers and associated mathematical constructs (e.g. positive infinity is the highest score, empty set represents no valid score). Likewise, character scores can be within predefined ranges, such as “A” to “F”, or can be unbounded (e.g. “AAAA” is better than “AAA”). Other representations are also envisioned, such as “straight flush” being better than “four-of-a-kind,” which is better than a “full house.” Another example is “platinum,” “gold,” “silver,” “bronze,” and “lump of coal.” Scores can include alphanumeric characters and symbols that can be ordered with respect to other scores. For example, “A+” can be better than “100.”

[0032] A score can represent an intangible risk that a transaction is fraudulent or a real-world probability that the transaction is fraudulent (e.g. the probability that an attempted transaction was initiated by a stolen credit card is 0.79). Scores can also represent directly measurable quantities represented in the real world, such as the number of times that a card has been used thus far.

[0033] Embodiments can be used by credit, debit, or other payment card companies and their customers to combat identity theft in which a thief fraudulently makes purchases using another person’s payment card or account number. Embodiments can also be used in non-theft related areas, such as to identify a change in spending behavior in a cardholder himself/herself.

[0034] A threshold for a score can be any number, character, or other representation that represents ordinal values and can be compared with a score. For example, a threshold value of “50” can be compared with a score of “79.” The score of “79” exceeds (numerically) the threshold of “50.” Embodiments also include scores in which a smaller number score “exceeds” a larger threshold value (e.g. a score of “3” “exceeds” a score of “5” if a lower number indicates a higher probability of fraud).

[0035] A consumer device can be an electronic device that networks continuously or intermittently to a wide area network, local network, or other network.

[0036] I. Exemplary Messages

[0037] FIG. 1A illustrates a cellular phone with a short message system (SMS) cardholder alert message in accordance with an embodiment. Cell phone 100 includes display 102 upon which message 104 is displayed to a user. In the exemplary embodiment, and SMS cardholder alert message informs the user that a large purchase (e.g. $500) was made recently (e.g. within a few minutes) at a store. The message, which was sent because a score for the transaction exceeded a threshold preselected by the user, relates this fact to the user.

[0038] A user can reply or otherwise respond to the SMS message to indicate whether he or she believes that the purchase was fraudulent. A user’s response is sent back to the originator of the message, which can then alert the processing network, joint cardholders, police, or other authorities as to possible fraud.

[0039] Cell phone 100 can also, naturally, be used for audio communication of the cardholder alert message, such that a voice message can be relayed through the device’s speaker. For example, the message can be sent in a voicemail as opposed to or in conjunction with a text message.

[0040] FIG. 1B illustrates a cellular phone with an alternate cardholder alert message with a coupon offer. Alternate message 106 includes a dynamic display in which the minutes and
seconds that have elapsed since the transaction was made are updated in real- or near-real-time.

[0041] Displayed button 108 can be depressed by the user to download and display a coupon offer. The offer can simply give details of a merchant selling a particular item, or the offer can include codeword, alphanumeric sequence, displayed bar code, or other coupon code which can be redeemed at a merchant. Using the coupon or otherwise responding to the coupon offer at the merchant can affect the generation of future scores. For example, a standalone purchase of gasoline at an out-of-the-way gas station may generate an elevated score by a fraud detection system. However, if a coupon was offered for gasoline at the out-of-the-way gas station, and the coupon is then used at the gas station, then the generated score may be lower than it was in the case of the standalone purchase.

[0042] II. Exemplary Processes

[0043] FIG. 2 is a network-level diagram illustrating messages between entities in accordance with an embodiment. Other systems according to embodiments may include fewer or more components than are specifically shown in the figure.

[0044] The figure shows an identity thief 202, payment card 204, seller's reader/terminal 206, acquirer 208, payment processing system 210, advanced authorization module 211, issuer 212, Internet protocol (IP) gateway 214, cardholder 216, portable electronic device 218, joint cardholder 220, personal computer 222, online banking web service 224, client computer 226, and enrollee 228. Many of the above entities are operatively connected with each other. Acquirer 208 and issuer 212 can communicate through payment processing system 210. An “issuer” is typically a business entity (e.g., a bank) which maintains a financial account for the buyer and issues a credit card payment card or other portable consumer device to the buyer. A “seller” is typically an entity that engages in transactions, such as a store, supplier, merchant, person, or service provider. The seller's reader/terminal 206 is used by legitimate buyers and, in the exemplary case, thief 202, to attempt a purchase. The seller's reader/terminal 206 can comprise a computer, telephone, or other communications means.

[0045] In a typical, non-fraudulent payment transaction, a buyer (i.e. the “payor”) may order goods or services from a seller. The buyer can then send a payment instruction for the purchase using seller's reader/terminal 206. Reader/terminal 206 can transmit the payment instruction, or authorization request, to acquirer 208. Acquirer 208 then sends an authorization request, which may be the same request as it received from reader/terminal 206, to payment processing system 210. Payment processing system 210 can parse the authorization request to determine the identity of the proper cardholder and send an authorization request to the cardholder's bank, issuer 212. Issuer 212 sends either an authorization or a denial for the transaction in an authorization response, which flows back to payment processing system 210. An authorization response is sent from payment processing system 210 to acquirer 208, and then to the seller's reader/terminal 206. If the transaction is approved, funds are transferred between the proper parties.

[0046] As used herein, an “acquirer” is typically a business entity, e.g., a commercial bank that has a business relationship with a particular merchant or other entity. Some entities can perform both issuer and acquirer functions. Embodiments encompass such single-entity issuer-acquirers.

[0047] The buyer can be an individual or an organization such as a business that is capable of purchasing goods or services.

[0048] Payment processing system 210 can have a server computer as well as a database. The server computer can be a powerful computer or a cluster of computers. For example, the server computer can be a large mainframe, a minicomputer cluster, or a group of servers functioning as a unit. In one example, the server computer may be a database server coupled to a web server. The server computer may comprise a computer readable medium comprising code for processing transactions as detailed below, including code for receiving messages from merchants, acquirers, and issuers, code for generating a score based on transaction data, code for comparing the score to a user selected or other threshold, and code for sending a transaction notification message to a consumer device used by a consumer if the score meets, exceeds, or falls below, the threshold.

[0049] Payment processing system 210 may comprise or use a payment processing network such as VisaNet™ or Banknet™. Payment processing system 210 and any communication network that communicates with payment processing system 210 may use any other suitable wired or wireless network, including the Internet. Payment processing system 210 can be adapted to process ordinary debit or credit card transactions along with push payment transactions.

[0050] A buyer can use an access device to communicate with issuer 212 or payment processing system 210. The access devices according to embodiments of the invention can be in any suitable form. Examples of access devices include point of sale (POS) devices, cellular phones, personal data assistants (PDAs), personal computers (PCs), tablet PCs, handheld specialized readers, set-top boxes, electronic cash registers (ECRs), automated teller machines (ATMs), virtual cash registers, kiosks, security systems, access systems, and the like. The access device may comprise a convenient interface such as a web browser on a computer that communicates over the Internet. In certain embodiments, the buyer may have a portable consumer device, such as a payment card, associated with accounts hosted by issuer 212. In one aspect, the payment card can interact with reader/terminal 206 to create a payment instruction message to send. In other aspects, the payment card can include the relevant payment account information. The buyer can provide the relevant payment account information that is included on the payment card to reader/terminal 206 or directly to either issuer 212 or payment processing system 210.

[0051] Reader/terminal 206 may comprise a processor and a computer readable medium, wherein the computer readable medium comprises code for obtaining an account number associated with a consumer; code for sending an authorization request message comprising the account number and an amount for a transaction to a payment processing network; and code for receiving an authorization response message comprising a unique transaction identifier for the transaction.

[0052] For simplicity of illustration, one buyer, one seller, one reader/terminal 206, one acquirer 208, and one issuer 212 are shown. However, it is understood that in embodiments of the invention, there can be multiple consumers, portable consumer devices, merchants, reader/terminals or other access devices, acquirers, issuers, as well as server computers, databases, accounts, etc.

[0053] In an exemplary fraudulent transaction, thief 202 attempts to purchase something (e.g. goods or services) from
a seller through seller's reader/terminal 206. As in the nominal case, an authorization request is sent from reader/terminal 206 to acquirer 208. The authorization request flows to payment processing system 210. In payment processing system 210, advanced authorization module 211 analyzes the transaction and generates a score.

The score relates to the real-life probability of the attempted purchase being conducted by a thief, by fraud, etc. The score can take into account data about the transaction, including the time of day, the amount, the merchant, the merchant's history, the geographic location of the transaction, the subject matter of the transaction, the number of attempts, and other variables. For example, advanced authorization module 211 can generate a score of 0.82 on a scale of 0 to 1.00.

Advanced authorization module 211 compares the score to a threshold. If the threshold is met, surpassed, breached, or otherwise exceeded, then payment processing system 210 sends a transaction notification message through IP gateway 214 to portable electronic device 218 to be read by cardholder 216 and/or personal computer 222 to be read by joint cardholder 220. A transaction notification message can be of many forms, some of which are examined in FIGS. 1A-1B.

Upon receipt of a transaction notification message, cardholder 216 and/or joint cardholder 220 may or may not have the option of responding to the transaction notification message. A response can include an indicator, which is sent back through IP gateway 214 to payment processing system 210, in order so that the transaction is halted, delayed, or flagged for further analysis.

While the transaction notification message is en route to the legitimate cardholder's consumer device, or while advanced authorization module 211 is processing, the authorization request is transmitted to issuer 212. This authorization request may include the score generated by advanced authorization module 211. As with the nominal case, issuer 212 sends an authorization response back to payment processing system 210. The authorization response may approve or deny the authorization request. The authorization response proceeds back through the chain to acquirer 208 and seller's reader/terminal 206.

One embodiment allows a user to select or enter a threshold. Enrollee 228, which may be the same person as cardholder 216 or joint cardholder 220, uses client computer 226 to connect with online banking service 224. Enrollee 228 subscribes to the cardholder alert service and selects a threshold above which an alert will be sent. For example, enrollee 228 can specify that any score over 0.75 will result in a transaction notification message being sent to his or her cellular phone. As another example, enrollee can specify that any score that is not a C+ or higher should be sent to the enrollee.

During enrollment, enrollee 228 specifies the personal electronic device(s) to which messages will be sent. For example, enrollee can enter the phone number of his or her cell phone or the email address of his or her personal email account.

In some embodiments, the enrollee can also specify multiple thresholds and multiple consumer devices. For example, enrollee 228 can specify that any score rated less than five stars be emailed to his or her email account, any score rated two-to-three stars be sent as an SMS text message to a cell phone, and any score rated one star or less be verified through an interactive voice response (IVR) telephone call to the cell phone. Thus, faster communication channels are selected when there is a higher probability of fraud. Table 1 illustrates an entry form showing user selections for one embodiment.

<table>
<thead>
<tr>
<th>Score Threshold</th>
<th>Device Type</th>
<th>Address or Phone number</th>
<th>Message Type</th>
<th>Require Approval</th>
</tr>
</thead>
<tbody>
<tr>
<td>≤ 5 Email account</td>
<td><a href="mailto:my_email@domain.com">my_email@domain.com</a></td>
<td>Rich Text</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>2-3 Phone</td>
<td>571-555-1212</td>
<td>SMS</td>
<td>no</td>
<td></td>
</tr>
<tr>
<td>≤ 1 Phone</td>
<td>571-555-1212</td>
<td>IVR</td>
<td>yes</td>
<td></td>
</tr>
</tbody>
</table>

An enrollee can also specify different communication methods for different scores on different cards used for an account. For example, the enrollee may want his or her own card to generate messages according to Table 1, while the use of debit cards of his or her children drawing money from the same account could have a different table. For example, in the different table any score less than 5 might require approval through IVR from the enrollee's cell phone. Other methods for helping to lower fraud are available as well.

Many inputs can go into advanced authorization module 211 for determining a score for a particular transaction. For example, an enrollee can submit data during a web session with his or her issuer's web site or through in-person enrollment at his or her bank's branch. The enrollee can set triggers and other preferences that should be of note to advanced authorization module 211. Transactional activities, such as activities at a physical point of sale system, e-commerce/MOTO, ATM, etc. can also be considered. The intelligent notification engine, which works in conjunction with advanced authorization module 211, uses the infrastructure, trigger rules/preferences, and notification message reporting in order to assemble, compute, or otherwise generate outputs, such as a score. These outputs can be included in one or more delivery mechanisms and channels, such as in email, web site postings, or text messages. Advanced authorization module 211 can encompass the user input and message generation aspects of the system as well.

FIG. 3 is a system-level diagram illustrating a coupon used for authentication and score adjustment. Enrollee 328 enrolls in an alert system using a Web connected client device 326. Default selections, entered by enrollee's bank (an issuer) or payment processing system 210, are used for thresholds that enrollee 328 does not enter or select. Those thresholds which enrollee does not explicitly select, but are defaulted, are considered adopted by the enrollee and therefore used. The enrollee's enrollment data is stored in database 332, which can be one or multiple databases. When a transaction occurs, payment processing system 210 uses advanced authorization module 211 to generate a score. The generated score is compared to the user entered thresholds, and because the score exceeds one or more thresholds, a transaction notification message is sent to consumer device 318 of accountholder 316. As illustrated in FIG. 1B, a button or link to a coupon can be sent with the transaction notification message.

In some embodiments, whether the coupon is sent or not can be based on the generated score. For example, if the score is a 5 (out of 5), then no coupon is sent. However, if the score is 3, then a coupon is sent. The type, amount off the
retail price, merchant, location of use, and other factors of the coupon can be modified based on the score as well. For example, if there is great need for determining whether a card was stolen, then a coupon with a sizable discount can be sent.

[0065] Coupon 334 can entice user 316 to perform a different transaction at a different venue or the same venue as the first transaction. In one example, the generated score may be low because the first transaction was in a different state than that in which the cardholder resides. A couple is then sent to offer a great deal at a restaurant in the other state. If the coupon, which is sent to the consumer device, is used at the prescribed restaurant, then its use is fed back into database 332. A future score for another transaction outside the state may then be increased (or decreased) based on the coupon’s use. The use of the coupon helps verify the identity of the user and thus lowers the probability that the second transaction in the same geographic location was fraudulent.

[0066] FIG. 4 is a flowchart illustrating a process in accordance with an embodiment. This process, process 400, can be automated in a computer or other machine. The process can be coded in software, firmware, or hard coded as machine-readable instructions and run through a processor that can implement the instructions. In operation 402, an authorization request message comprising transaction data is generated from a reader/terminal. In operation 404, the authorization request message is sent to a server computer in a payment processing network. In operation 406, an authorization request message comprising transaction data is received at the server computer. The authorization request message requests approval to conduct a transaction in the exemplary embodiment. In operation 408, a score based on the transaction data is generated using the server computer in the payment processing network. In operation 410, the authorization request message is sent with the score to an issuer, such as a bank.

[0067] In operation 412, the score, generated in operation 408, is compared to a user selected threshold. The user selected threshold could have been input in free form by the user, chosen from a list of selections, or otherwise selected by a user. In operation 414, it is determined whether an alert has already been sent out. In operation 416, an alert is generated and sent to a consumer device used by a consumer if, and only if, the score meets or exceeds the threshold. The alert includes a transaction notification message which may include how much the threshold is exceeded (if at all) by the score or other pertinent data. In operation 418, an authorization response message is sent to the reader/terminal in response to the authorization request message. These operations may be performed in the sequence given above or in different orders as applicable.

[0068] FIG. 5 is a flowchart illustrating a process in accordance with an embodiment. Process 500 includes several operations which can be performed by a user who is also a cardholder or account holder. In operation 502, a user logs on to an enrollment web site for a payment card. In operation 504, the user views a display showing a range of possible thresholds, between which the user can input or otherwise select a threshold value. In operation 506, the user inputs a threshold value into the web site. In operation 508, the threshold value is submitted to the web site such that the threshold value is stored in a database. These operations may be performed in the sequence given above or in different orders as applicable. For example, the user may view the range of possible thresholds after inputting an out-of-bounds threshold value.

[0069] III. Portable Devices and Computer Apparatuses

[0070] FIGS. 6A-6B show block diagrams of portable consumer devices and subsystems that may be present in computer apparatuses in systems according to embodiments of the invention.

[0071] The portable consumer device that is used in embodiments of the invention may be in any suitable form. For example, the portable consumer device can be hand-held and compact so that they can fit into a consumer's wallet and/or pocket (e.g., pocket-sized). They may include smart cards, ordinary credit or debit cards (with a magnetic strip and without a microprocessor) such as payment cards, keychain devices (such as the SpeedPass™ commercially available from ExxonMobil Corp.), etc. Other examples of portable consumer devices include cellular phones, personal digital assistants (PDAs), pagers, payment cards, security cards, access cards, smart media, transponders, and the like. The portable consumer devices can also be credit devices (e.g., a debit card), credit devices (e.g., a credit card), or stored value devices (e.g., a stored value card).

[0072] An exemplary portable consumer device 640 in the form of a phone may comprise a computer readable medium and a body as shown in FIG. 6A. FIG. 6A shows a number of components, and the portable consumer devices according to embodiments of the invention may comprise any suitable combination or subset of such components.) The computer readable medium 644 may be present within the body 658, or may be detachable from it. The body 658 may be in the form of a plastic substrate, housing, or other structure. The computer readable medium 644 may be a memory that stores data and may be in any suitable form including a magnetic stripe, a memory chip, encryption algorithms, private or private keys, etc. The memory also preferably stores information such as financial information, transit information (e.g., as in a subway or train pass), access information (e.g., as in access badges), etc. Financial information may include information such as bank account information, bank identification number (BIN), credit or debit card number information, account balance information, expiration date, consumer information such as name, date of birth, etc.

[0073] Information in the memory may also be in the form of data tracks that are traditionally associated with credit cards. Such tracks include Track 1 and Track 2. Track 1 (“International Air Transport Association”) stores more information than Track 2 and contains the cardholder's name as well as account number and other discretionary data. This track is sometimes used by the airlines when securing reservations with a credit card. Track 2 (“American Banking Association”) is currently most commonly used. This is the track that is read by ATMs and credit card checkers. The ABA (American Banking Association) designed the specifications of this track and all world banks must generally abide by it. It contains the cardholder's account, encrypted PIN, plus other discretionary data.

[0074] The portable consumer device 640 may further include a contactless element 656, which is typically implemented in the form of a semiconductor chip (or other data storage element) with an associated wireless transfer (e.g., data transmission) element, such as an antenna. Contactless element 656 is associated with (e.g., embedded within) portable consumer device 640, and data or control instructions transmitted via a cellular network may be applied to contactless element 656 by means of a contactless element interface (not shown). The contactless element interface functions to
permit the exchange of data and/or control instructions between the mobile device circuitry (and hence the cellular network) and an optional contactless element 656.

[0075] Contactless element 656 is capable of transferring and receiving data using a near field communications ("NFC") capability (or near field communications medium) typically in accordance with a standardized protocol or data transfer mechanism (e.g., ISO 14443/NFC). Near field communications capability is a short range communications capability, such as RFID, Bluetooth®, infra-red, or other data transfer capability that can be used to exchange data between the portable consumer device 640 and an interrogation device. Thus, the portable consumer device 640 is capable of communicating and transferring data and/or control instructions via both cellular network and near field communications capability.

[0076] The portable consumer device 640 may also include a processor 646 (e.g., a microprocessor) for processing the functions of the portable consumer device 640 and a display 650 to allow a consumer to see phone numbers and other information and messages. The portable consumer device 640 may further include input elements 652 to allow a consumer to input information into the device, a speaker 654 to allow the consumer to hear voice communication, music, etc., and a microphone 648 to allow the consumer to transmit her voice through the portable consumer device 640. The portable consumer device 640 may also include an antenna 642 for wireless data transfer (e.g., data transmission).

[0077] Portable consumer device 640 may be used by a buyer to initiate push payments. In some implementations, portable consumer device 640 can include an interface to allow the buyer to create a payment request message. The portable consumer device 640 can then send the payment request message to a payment processing network using contactless element 656 or over a wireless or wired communications channel.

[0078] An example of a portable consumer device 660 in the form of a card is shown in FIG. 6B. FIG. 6B shows a plastic substrate 662. A contactless element 666 for interfacing with an access device 660 may be present on or embedded within the plastic substrate 662. Consumer information 668 such as an account number, expiration date, and consumer name may be printed or embossed on the card. Also, a magnetic stripe 664 may also be on the plastic substrate 662.

[0079] As shown in FIG. 6B, the portable consumer device 660 may include both a magnetic stripe 664 and a contactless element 666. In other embodiments, both the magnetic stripe 664 and the contactless element 666 may be in the portable consumer device 660. In other embodiments, either the magnetic stripe 664 or the contactless element 666 may be present in the portable consumer device 660. In some implementations, portable consumer device 660 can comprise a purchase card. Purchase card 660 can include a buyer identifier associated with the buyer, an account number associated with an account controlled by the buyer and used for payments, or other identifying information. This identifying information can be used by the buyer when creating payment instruction messages, as described above.

[0080] FIG. 7 shows a block diagram of an exemplary computer apparatus that can be used in some embodiments, such as that shown in FIG. 2. Any of the elements in FIG. 2 (e.g., the reader/terminal 206, the acquirer 208, etc.) may use any suitable number of subsystems to facilitate the functions described herein.

[0081] The subsystems shown in FIG. 7 are interconnected via a system bus 710. Additional subsystems such as a printer 708, keyboard 718, fixed disk 720 (or other memory comprising computer readable media), monitor 714, which is coupled to display adapter 712, and others are shown. Peripherals and input/output (I/O) devices, which couple to I/O controller 702, can be connected to the computer system by any number of means known in the art, such as through serial port 716. For example, serial port 716 or external interface 722 can be used to connect the computer apparatus to a wide area network such as the Internet, a mouse input device, or a scanner. The interconnection via system bus 710 allows the central processor 706 to communicate with each subsystem and to control the execution of instructions from system memory 704 or the fixed disk 720, as well as the exchange of information between subsystems. The system memory 704 and/or the fixed disk 720 may embody a computer readable medium.

[0082] Embodiments of the invention are not limited to the above-described embodiments. For example, although separate functional blocks are shown for an issuer, payment processing system, and acquirer, some entities perform all of these functions and may be included in embodiments of the invention.

[0083] It should be understood that the present invention as described above can be implemented in the form of control logic using computer software in a modular or integrated manner. Based on the disclosure and teachings provided herein, a person of ordinary skill in the art can know and appreciate other ways and/or methods to implement the present invention using hardware and a combination of hardware and software.

[0084] Any of the software components or functions described in this application, may be implemented as software code to be executed by a processor using any suitable computer language such as, for example, Java, C++ or Perl using, for example, conventional or object-oriented techniques. The software code may be stored as a series of instructions, or commands on a computer readable medium, such as a random access memory (RAM), a read only memory (ROM), a magnetic medium such as a hard-drive or a floppy disk, or an optical medium such as a CDROM. Any such computer readable medium may reside on or within a single computational apparatus, and may be present on or within different computational apparatuses within a system or network.

[0085] Embodiments of the invention contain a number of advantages. In certain implementations, the consumer can select her or her own threshold for receiving alerts. The threshold effectively insulates the consumer from the complexities of how a score is created. The user can set different thresholds for different card accounts, depending on his or her risk tolerance for the respective card. For example, a threshold for a business credit card may be high and a threshold for his or her personal debit card may be low. As another example, a threshold for his or her away-at-college child’s card may be high, while a stay-at-home teenager’s card threshold may be low. As another example, a newly married couple can set a very low threshold for a credit card which neither one uses except in cases of emergency. The threshold could be set low enough for any expenditure to trigger an alert to the spouses’ cell phones to indicate, covertly to the other spouse, an emergency.

[0086] Other advantages of some embodiments include lessening nuisance alerts which would otherwise be caused
by a threshold set by a card processing network company. A 'one size fits all' threshold set by such a company is abandoned in favor of users being able to set their own thresholds. All parties in the transaction may have access to increased fraud and risk detection as well as rewards and other benefits programs.

The above description is illustrative and is not restrictive. Many variations of the invention will become apparent to those skilled in the art upon review of the disclosure. The scope of the invention should, therefore, be determined not with reference to the above description, but instead should be determined with reference to the pending claims along with their full scope or equivalents.

One or more features from any embodiment may be combined with one or more features of any other embodiment without departing from the scope of the invention.

A recitation of "a", "an" or "the" is intended to mean "one or more" unless specifically indicated to the contrary. A recitation of "she" is meant to be gender neutral, and may be read as "he" or "she", unless specifically indicated to the contrary.

All patents, patent applications, publications, and descriptions mentioned above are herein incorporated by reference in their entirety for all purposes. None is admitted to be prior art.

1.-18. (canceled)

19. A method comprising:
receiving transaction data at a server computer, wherein the transaction data requests approval to conduct a transaction;
generating a score based on the transaction data;
if the score is in a first score range, then providing a notification to a person using a first communication mode; and
if the score is in a second score range, then providing the notification to the person using a second communication mode.

20. The method of claim 19 wherein the transaction data is in an authorization request message.

21. The method of claim 19 wherein the first communication mode comprises an e-mail, and the second communication mode comprises a text message.

22. The method of claim 19 wherein the first communication mode provides the notification in a first message type and the second communication mode provides the notification in a second message type.

23. The method of claim 19 wherein the first communication mode comprises a first type of notification delivery channel and the second communication mode comprises a second type of delivery channel.

24. The method of claim 19 wherein the transaction data is associated with a transaction conducted using a payment device, which is issued by an issuer.

25. The method of claim 24 wherein the method is performed by a computer in a payment processing network, and wherein the transaction data is present in an authorization request message, and wherein the method further comprises:

sending the authorization request message to the issuer and receiving an authorization response message from the issuer.

26. A computer comprising a processor, and a computer readable medium coupled to the processor, the computer readable medium comprising code for implementing a method comprising:

receiving transaction data at a server computer, wherein the transaction data requests approval to conduct a transaction;
generating a score based on the transaction data;
if the score is in a first score range, then providing a notification to a person using a first communication mode; and
if the score is in a second score range, then providing the notification to the person using a second communication mode.

27. The computer of claim 26 wherein the transaction data is in an authorization request message.

28. The computer of claim 26 wherein the first communication mode comprises an e-mail, and the second communication mode comprises a text message.

29. The computer of claim 26 wherein the first communication mode provides the notification in a first message type and the second communication mode provides the notification in a second message type.

30. The computer of claim 26 wherein the first communication mode comprises a first type of notification delivery channel and the second communication mode comprises a second type of delivery channel.

31. The computer of claim 26 wherein the transaction data is associated with a transaction conducted using a payment device, which is issued by an issuer.

32. The computer of claim 26 wherein the transaction data is present in an authorization request message, and wherein the method further comprises:

sending the authorization request message to the issuer and receiving an authorization response message from the issuer.

* * * * *