A system and method for distributing coupons to consumers at the point-of-sale, where the benefit offered in the coupon can be determined according to a risk analysis. The coupon can then be applied to a transaction taking place at the point-of-sale or stored for future use.
Consumer Requests Coupons

Conduct Risk Assessment(s)

Search for Coupons

Select Appropriate Coupon Discounts Based on Risk Assessment

Offer Coupon(s) to Consumer
PORTABLE CONSUMER DEVICE
INCLUDING DATA BEARING MEDIUM
INCLUDING RISK BASED BENEFITS

CROSS-REFERENCES TO RELATED
APPLICATIONS

[0001] This patent application claims priority to U.S. Pro-
visional Application No. 60/982,682 filed Oct. 25, 2007,
etitled “Mobile Phone Payment System and Method,” which
is hereby incorporated by reference in its entirety for all
purposes.

BACKGROUND

[0002] Many entities offer coupons for a variety of reasons.
For example, manufacturers and merchants may issue cou-
pons to reduce their inventories. Manufacturers and mer-
chants may also issue coupons to promote new products.
Financial entities, such as issuers, may also offer coupons
to promote their financial services. Entities will also of-
collaborate with each other to cross-promote products for
a variety of reasons. Despite all these efforts, coupons often go
unused because consumers are either unaware that coupons
collaborate with each other to cross-promote products for
exist or are unable to obtain relevant coupons.

[0003] One problem faced by coupon offering entities is
that they often do not have all of the information that they
need to determine what discounts they would like to offer to
a consumer. For example, coupon offering entities do not
know the fraud or credit risk that a consumer presents at the
time and place of sale because coupons are issued and dis-
tributed before a purchasing transaction takes place. As a
result, coupon offering entities are not able to factor the fraud
or credit risk of a consumer into any offered discount.

[0004] Coupon offering entities would not only like a better
means to distribute coupons to consumers, but they would
also like a better means to tailor specific coupons for specific
consumers.

[0005] Further, in the context of credit and debit trans-
actions, consumers that are inclined to conduct fraudulent trans-
actions may not have the ability to eventually pay for the
transactions, can create potential losses for manufacturers,
and issuers. It would be desirable to encourage consumers who do not present a high
risk of fraud and/or a high-risk of non-payment to conduct
transactions.

[0006] Embodiments of this disclosure address these and
other problems.

SUMMARY

[0007] Embodiments of the invention are, without limitation,
directed to methods, systems, computer readable media,
and devices.

[0008] One embodiment of the invention is directed to a
method comprising receiving a coupon, wherein a benefit
offered by the coupon is based on a risk assessment. The risk
assessment may be associated with an intended recipient’s
ability to eventually pay for goods or services in a transaction.
The coupon is provided to a merchant by the recipient of the
coupon (e.g., a consumer).

[0009] Another embodiment of the invention is directed to
a method comprising performing a risk analysis, and select-
ing a coupon using the risk analysis. A benefit provided by
the coupon varies with a result of the risk analysis. The coupon is
then sent to a consumer.

[0100] Another embodiment of the invention is directed to
a method comprising conducting a risk analysis and request-
ing one or more coupons from one or more coupon-issuing
entities. The request includes a risk assessment. The method
also includes receiving a coupon from the one or more
coupon-issuing entities, where the value of the coupon is based
on the risk analysis. The coupon is sent to a consumer.

[0101] Other embodiments of the invention are directed to
systems, computer readable media, and devices that are as-
correlated with such methods.

[0102] These and other embodiments of the invention are
addressed in further detail below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0103] FIG. 1 is a block diagram of an exemplary system
for conducting a payment transaction.

[0104] FIG. 2 is a block diagram of an exemplary portable
consumer device that can be used to conduct a payment
transaction.

[0105] FIG. 3 is a block diagram of an exemplary payment
processing network.

[0106] FIG. 4 is a block diagram of an exemplary system
for conducting a payment transaction.

[0107] FIG. 5 flow chart showing the steps taken according
to one embodiment.

[0108] FIG. 6 shows a block diagram of subsystems that
may be present in computer apparatuses that are used in
system, according to embodiments of the invention.

DETAILED DESCRIPTION

[0109] Embodiments of the invention are directed to meth-
ods and systems for providing coupons to consumers where
the benefits offered in the coupons are linked to risk analyses.
For instance, one embodiment of the invention is directed to
a method comprising receiving a coupon, where a benefit
offered by the coupon is based on a risk assessment. The risk
assessment may assess the risk of whether or not the intended
recipient of the coupon will pay for a particular good or
service in a transaction. The coupon can be provided to a
merchant and redeemed by the recipient in a transaction.

[0120] The transaction being conducted can be a credit or
debit transaction. With credit transactions, there is always a
risk that the person that conducts the transaction will not pay his or her credit bill. In embodiments of the invention, the
benefit that is offered by the coupon can be high if there is a
low risk that the intended recipient (e.g., a consumer) will
follow through and eventually pay for the transaction in full.
Conversely, the coupon can give a discount that can be less if
there is a higher risk that the consumer will follow through
and pay for the transaction in full. In this way, various parties
such as issuers, manufacturers, and payment processing orga-
nizations can encourage increases in transactions conducted
by consumers that have a lower risk of defaulting on their
credit obligations.

[0121] With debit and credit transactions, there is always a
risk that the debit or credit account is being used fraudulently.
For example, identity theft can compromise either credit or
debit accounts. If a credit or debit account that has typically
been used by a consumer for small-ticket purchases, such as
groceries, suddenly starts to be used in transactions for expen-
sive home theater equipment, the chances that the credit or
debit account is being used fraudulently increases. The risk
may increase further if, for example, the unusual and expen-
sive purchases are made in locations far from the consumer’s residence. On the other hand, a credit or debit account that is frequently used to make expensive purchases may pose a lower fraud risk. In some embodiments of the invention, the benefit offered by a coupon can increase as the fraud risk for a transaction decreases. As a result, coupon issuing entities can encourage increases in transactions that have a lower risk of being fraudulent.

[0022] Illustratively, bank A may issue a credit card A to consumer A. Consumer A may have a high credit score, because he has a history of paying off his monthly credit card bills on time. He may also live in an area where fraud rarely occurs. Consumer A may then request a coupon from bank A using a phone or computer, or bank A may push the coupon to Consumer A’s phone or computer. The coupon may provide a discount of 2% on any purchase made by Consumer A with credit card A. Conversely, bank A may issue a credit card B to consumer B. Consumer B may have a lower credit score, since she generally pays off her monthly balance, missed making payments once in the last year. She also lives in an area where fraud rarely occurs. Consumer B may then request a coupon from bank A or bank B may push the coupon to Consumer B. The coupon may provide a discount of 1% on any purchase made by Consumer B with credit card B.

[0023] As illustrated by this specific example, a greater discount can be provided to Consumer A than consumer B, since Consumer A is more likely to pay for purchases made with credit card A than Consumer B will pay for purchases made with credit card B.

[0024] In embodiments of the invention, such risk based coupons may be generated before consumers actually approach merchants to conduct face-to-face transactions. In other embodiments of the invention, such risk based coupons can be generated during a transaction and after a consumer has selected good or services for purchase.

[0025] More specific descriptions of embodiments of the invention are provided below.

I. Exemplary Systems and Payment Transactions

[0026] FIG. 1 shows a system 20 that can be used to conduct a payment transaction according to an embodiment. The system 20 includes a merchant 22 and an acquirer 24 associated with the merchant 22. In a typical payment transaction, a consumer 30 may purchase goods or services at the merchant 22 using a portable consumer device 32. In some embodiments, the portable consumer device 32 is a wireless portable consumer device, such as a mobile phone. In some embodiments, the portable consumer device 32 communicates with an access device 34 associated with the merchant. The acquirer 24 can communicate with an issuer 28 via a payment processing network 26.

[0027] The consumer 30 may be an individual, or an organization such as a business that is capable of purchasing goods or services.

[0028] The portable consumer device 32 may be in any suitable form. For example, some portable consumer devices can be hand-held and compact so that they can fit into a consumer’s wallet and/or pocket (e.g., pocket-sized). The portable consumer device 32 typically comprises a processor, and a memory, input devices, and output devices, operatively coupled to the processor. Specific examples of portable consumer devices include cellular or wireless phones, personal digital assistants (PDAs), pagers, desktop computers, laptop computers, smart cards, and the like. The portable consumer devices can also be debit devices (e.g., a debit card), credit devices (e.g., a credit card), or stored value devices (e.g., a stored value card).

[0029] The merchant 22 may also have, or may receive communications from, an access device 34 that can interact with the portable consumer device 32. 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, PDAs, personal computers (PCs), tablet PCs, handheld specialized readers, set-top boxes, electronic cash registers (ECRs), automated teller machines (ATMs), virtual cash registers (VCRs), kiosks, security systems, access systems, and the like.

[0030] If the access device 34 is at a point of sale terminal, any suitable point of sale terminal may be used including card or phone readers. The card or phone readers may include any suitable contact or contactless mode of operation. For example, exemplary readers can include RF (radio frequency) antennas, magnetic stripe readers, etc. to interact with the portable consumer devices 32.

[0031] The acquirer 24 refers to any suitable entity that has an account with merchant 22. For example, acquirer may be a bank that operates a bank account for merchant.

[0032] The payment processing network 26 may include data processing subsystems, networks, and operations used to support and deliver authorization services, exception file services, and clearing and settlement services. An exemplary payment processing network may include VisaNet™, payment processing networks such as VisaNet™ are able to process credit card transactions, debit card transactions, and other types of commercial transactions. VisaNet™, in particular, includes a VIP system (Visa Integrated Payments system) which processes authorization requests and a Base II system which performs clearing and settlement services.

[0033] The payment processing network 26 may include a server computer. A server computer is typically a powerful computer or 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 payment processing network 26 may use any suitable wired or wireless network, including the Internet.

[0034] The payment processing network 26 in system 20 is also connected to various manufactures 29 and merchants 22, in addition to issuers 28 and acquirers 24. This interconnectivity between all of these parties allows for many new applications and services to be provided to all connected parties.

[0035] Issuer 28 refers to any suitable entity that may open and maintain an account associated with consumer 30. Some examples of issuers may be a bank, a business entity such as a retail store, or a governmental entity. In many cases, issuer may also issue a payment card to consumer. In some embodiments, issuer may also be the acquirer 24.

[0036] In a typical purchase transaction, the consumer 30 purchases goods or services at the merchant 22 using the portable consumer device 32 such as a mobile phone. The consumer’s portable consumer device 32 can interact with an access device 34 such as a POS point of sale terminal at the merchant 22. A request to authorize the purchase can then be made by the access device to an acquirer 24, which can then be forwarded to an issuer 28 via a payment processing network 26. A response to this request can then be forwarded back to the access device and the merchant back up through this communication chain.
In another method for conducting a purchase transaction, the portable consumer device 32 is capable of communicating directly with the payment processing network 26 without using an access device 34. Information may be sent from the portable consumer device directly to the payment processing network. The information may include the amount of a transaction, the merchant ID, information about the portable consumer device itself (e.g., phone number, SIM card number, etc.), or any other relevant data. The information may be sent using SMS through a short code, MMS (multimedia message), etc. Once the information is received at the payment processing network, the payment processing network can retrieve additional information such as any account numbers associated with the portable consumer device. This additional information may be stored at the payment processing network in a database that links portable consumer device data to account numbers. Once this information is gathered, an authorization request message may be reformatted and then forwarded to an issuer.

When a portable consumer device 32 can communicate with an access device 34, such as a point of sale, the level of sophistication increases. For example, SKUs can be transferred from the POS terminal to the mobile phone. SKU information can be transferred to the payment processing network. This SKU information may be used by the payment processing network to select coupons for the consumer. The coupons may come from the manufacturer, the issuer, the payment processing network, and/or the merchant.

Additionally, authentication processes, security measures, and other new forms of connectivity can all be used as a part of a risk analysis. This risk analysis can be used to determine, at least in part, the discount offered to a consumer in a coupon. Some examples of new authentication processes and security measures are described below.

In some embodiments, a portable consumer device 32 sends a PIN to the payment processing network 26 before other messages are sent to the payment processing network. In another embodiment, the portable consumer device may have a camera that captures a picture of the access device 34 display. A message including a picture of the access device display can then be sent to the payment processing network. The picture may include a bar code or other type of code. The payment processing network may have image recognition software that can recognize the information on the access device that has been captured as an image. If image capture is not used, the access device can transmit the transaction data to the portable consumer device using a wireless communication mechanism including an NFC (near field communication) mechanism such as Bluetooth, IR, etc.

Another way to authenticate the transaction, is to match the GPS location of the portable consumer device 32 (or operator information) with location information derived from the merchant ID. If a payment processing network 26 is able to match the two pieces of location information, then the transaction can be considered by the payment processing network to be authentic. GPS information taken from the portable consumer device can also be compared to other information for security purposes, such as the owner’s home address, previous purchase locations, etc.

In embodiments of the invention, the portable consumer device 32 may have specialized software that allows the device to interact directly with a payment processing network 26. This specialized software may have access to information such as account information, encrypted account information, or a secure element or other chip information associated with the portable consumer device. The specialized software may also be able to use a secure protocol or secure channel to communicate information to the payment processing network. A consumer 30 may use the portable consumer device to confirm the merchandise being purchased. For example, the consumer may authenticate himself/herself to the phone using a password, PIN, fingerprint (biometric), facial recognition, voice recognition, or other challenge response mechanisms. Once a consumer is authenticated to the portable consumer device, the user can authorize the device to conduct the transaction.

In another embodiment, the portable consumer device 32 may communicate with an access device 34 and gather information from the merchant 22 (or vice versa) before sending information directly to a payment processing network 26. For example, the merchant may sign the transaction and may send an electronic signature to the phone, and the phone may take this electronic signature and other transaction information and may forward this information to the payment processing network. In another embodiment, an access device may receive an identifier, such as a verification value, phone number, or SIM card number, from the phone. The POS terminal may then return this information to the phone along with a merchant ID or POS terminal ID, and this information may be sent to the payment processing network (e.g., directly via the phone or through the merchant and acquirer) as evidence that the phone and the POS terminal were interacting during the transaction.

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 network, and acquirer, some entities perform all of these functions and may be included in embodiments of invention.

An exemplary portable consumer device 32 in the form of a phone may comprise a computer readable medium and a body as shown in FIG. 2. (FIG. 2 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 32(b) may be present within the body 32(h), or may be detachable from it. The body 32(b) may be in the form a plastic substrate, housing, or other structure. The computer readable medium 32(b) may be a memory that stores data and may be in any suitable form including a magnetic stripe, a memory chip, etc. The memory 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. Any of this information may be transmitted by the portable consumer device 32.

In some embodiments, and regardless of the type of portable consumer device that is used, information in the memory may also be in the form of data tracks that are traditionally associated with credits 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 abide by it. It contains the cardholder’s account, encrypted PIN, plus other discretionary data.

[0047] The portable consumer device 32 may further include a contactless element 32(g), 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 32(g) is associated with (e.g., embedded within) portable consumer device 32 and data or control instructions transmitted via a cellular network may be applied to contactless element 32(g) 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 32(g).

[0048] Contactless element 32(g) 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 32 and an interrogation device. Therefore, the portable consumer device 32 is capable of communicating and transferring data and/or control instructions via both cellular network and near field communications capability.

[0049] The portable consumer device 32 may also include a processor 32(c) (e.g., a microprocessor) for processing the functions of the portable consumer device 32 and a display 32(d) to allow a consumer to see phone numbers and other information and messages. The portable consumer device 32 may further include input elements 32(e) to allow a consumer to input information into the device, a speaker 32(f) to allow the consumer to hear voice communication, music, etc., and a microphone 32(i) to allow the consumer to transmit her voice through the portable consumer device 32. The portable consumer device 32 may also include an antenna 32(a) for wireless data transfer (e.g., data transmission).

[0050] FIG. 3 shows a block diagram of one embodiment of a payment processing network 26. The payment processing network in FIG. 3 has connections with a portable consumer device 32, a manufacturer 29, a merchant 22, and an issuer 28. The embodiment shown in FIG. 3 illustrates an embodiment where a value-added services engine (VASE) 26(a) links various connections for the payment processing network to facilitate value-added services between the connected parties. For example, the VASE can provide for coupons, healthcare processing, travel processing, government processing, emergency cards, prepaid cards, gift cards, private label cards, etc., by integrating services from payment processing networks, manufacturers, merchants, and issuers. In one embodiment, the VASE is connected to a fraud risk module 26(b) and a credit risk module 26(c). These risk modules can help the VASE provide risk assessments of consumers and of transactions. Risk assessments can then be incorporated into the various services the VASE can provide. One of these services, a couponing value-added service, is described in more detail below.

II. Value-Added Service

Linking Coupon Benefit to Risk

[0051] One service that a VASE 26(a) can provide is a couponing service.

[0052] The VASE 26(a) can push risk-based coupons to a consumer without the need for a consumer’s request. For example, a bank, manufacturer, or payment processing organization may generate coupons based on risk scores of consumers. The benefits associated with those coupons can vary depending upon the risk associated with each individual consumer. Such coupons can then be sent to the consumers (e.g., via mail, e-mail, SMS message, etc.).

[0053] In other embodiments, a consumer can request the risk-based coupons. For example, a consumer 30 with a portable consumer device 32 can contact a payment processing network 26 (or a payment processing organization that operates the payment processing network 26) to request coupons related to a payment transaction that the consumer is conducting at an access device 34. In some embodiments, a consumer requesting coupons while conducting a transaction at a POS terminal can automatically redeem the coupons at the POS terminal for the instant transaction.

[0054] More specifically, the VASE 26(a) receives a coupon request from a consumer on behalf of the payment processing network. The VASE can generate a risk assessment related to the coupon request. This risk assessment can then be used by a payment processing network 26, manufacturer 29, merchant 22, and/or issuer 28 to select coupons that are appropriate for the consumer or the transaction using the risk assessment. Any coupons offered to the consumer can then be transmitted to either the consumer or a merchant. Coupons can be stored by consumers, merchants, or other parties for later use.

[0055] As shown in FIG. 3, various embodiments of payment processing network 26 may have a fraud risk module 26(b). A fraud risk module is able to collect and analyze data relating to a consumer 30 in order to determine the risk that a consumer request received by the payment processing network is fraudulent. For example, one embodiment of a fraud risk module may analyze the location from where the consumer request originated. The fraud risk module can compare the location to other data, such as the home or business address of the consumer. The fraud risk module may then assign or adjust a fraud risk score based on the comparison of this location information. Other factors may also be used by a fraud risk module. For example, a fraud risk module might analyze the value of the transaction, the types of items being purchased (e.g., there are more fraudulent transactions involving the purchase of consumer electronics than transactions involving perishable food), the order history of the consumer, the communication medium or protocol used to transmit the transaction request (e.g., a face-to-face transaction may be less risky than an Internet-based transaction, since merchant can individually authenticate the consumer), any security features in the portable consumer device, the shipping parameters in the request, the time of day the request was made, the location from which the request was made, whether the request was authenticated using a PIN, other security mechanisms used, etc. The fraud risk assess-
ment can then be shared with coupon-issuing entities, such as issuers 28 and manufacturers 29, via a VASE 26(a), so that those entities may use the fraud risk assessment when forming responses to a consumer’s request for coupons.


[0057] In various embodiments a credit risk module 26(c) may be present in the payment processing network 26. A credit risk module can analyze a consumer’s 30 credit history to determine the potential risk that a consumer will not be able to fulfill any payment obligations for a given transaction. For example, if a consumer has frequently made late payments on a credit account that is being used in a purchasing transaction, then the credit risk module can assign a higher credit risk score to for that transaction. Other credit risk factors may include the percent of the credit limit current used by a consumer, the number of credit accounts opened by the consumer, the length of the consumer’s credit history, etc. The credit risk assessment can then be shared with coupon-issuing entities, such as issuers 29 and manufacturers 30, via a VASE 26(a), so that those entities may use the credit risk assessment when forming responses to a consumer’s request for coupons.

[0059] FIG. 4 illustrates a payment processing system according to an embodiment of the invention. The entities illustrated in FIG. 4 are the same entities as illustrated in FIG. 1. Not all of the connections illustrated in FIG. 1 are shown in FIG. 4 for clarity of illustration. FIG. 5 illustrates the steps taken according to an embodiment of the invention. The steps outlined in FIG. 5 have a corresponding reference in FIG. 4. FIGS. 3, 4 and 5 will be discussed together for the purpose of illustrating embodiments of the invention.

[0060] At step 610, a consumer 30 requests one or more coupons. In one embodiment, the consumer 30 uses a portable consumer device 32 to request coupons from a payment processing network 26. Note that the consumer 30 can, in one embodiment, use a wireless portable consumer device 32, such as a phone, to communicate directly with the payment processing network 26 to send a coupon request message to it.

[0061] The information included in a coupon request message can include a variety of pieces of information. For example, if the consumer 30 is requesting the coupon while in the process of conducting a purchase transaction at an access device 34 located at a merchant, then the coupon request message might include a device ID, POS ID, merchant ID, transaction ID, item ID, etc. Additionally, a coupon request message might include information about the consumer or about any credit or debit accounts owned by the consumer. In some embodiments, a PIN, location information, or other security data may also be transmitted as a part of the coupon request.

[0066] There are a variety of ways that a benefit provided by a coupon can be determined. For example, a coupon-issuing entity may have a set of similar coupons available. Each device 34 via a wireless (e.g., contactless mode) communication channel, or a contact-based communication channel (e.g., placing the portable consumer device 32 in contact with the access device 34). This transaction information may be sent from the portable consumer device 32 directly to the payment processing network 26 without passing through the acquirer.
coupon in the set offers a different discount on a product. For example, a set of coupons may contain coupons giving 3%, 5%, and 7% off a given item. Alternatively, a coupon may be offered with a variable discount that may be calculated as a function of the risk. For example, a coupon may have an open-ended discount ranging between 3%-7%. The precise discount offered to a consumer will fall somewhere in this range depending on the risk assessment. Of course, discounts may also be offered in absolute terms (e.g. $3.00 off), in free items (e.g. buy two, get one free), in response to accumulated transactions, or using any other well-known promotional scheme. Coupons may also be offered for a combination of items as well. For example, buying item A results in a coupon offering a discount on item B. Benefits may also be in a variety of forms. For example, a benefit may offer a discounted price, free items related to the transaction, free gifts such as show tickets, extra rewards points, lower interest rates, free or upgraded shipping, etc. One skilled in the art will recognize that there are many different types of benefits that can be offered to a consumer.

[0067] At step 650, any coupons that are selected for the consumer 30 are offered to the consumer. In one embodiment, the payment processing network 26 sends a coupon response message to a consumer’s wireless portable communication device 32. This is shown in FIG. 4 at 650(a). Once a consumer’s wireless portable consumer device 32 receives this coupon response message, a consumer can redeem the coupon, store it for later use, or even delete the coupon. In another embodiment, the coupon is sent to a merchant 22, shown at 650(b), or the acquirer 34, shown at 650(c)(1), in a coupon response message. If the coupon is shared with the acquirer 34, the acquirer 34 may forward the coupon to the merchant 22 shown as 650(c)(2). In one embodiment, the discount may be reflected on a display on the access device 34 (e.g., a POS terminal), while the consumer 30 conducts a payment transaction at the access device 34. In this embodiment, the coupon may be immediately used in the instant payment transaction. A merchant may also store the coupon on behalf of the consumer for later use.

[0068] In other embodiments, a number may be provided to the consumer 30 (e.g., via the merchant’s access device 34, through a phone call, through e-mail, or through the Internet) by the payment processing network 26. This code may be then used for a purchase made by the consumer over the Internet, using a phone or mail order system, or any other appropriate purchasing means.

[0069] It should also be noted that in alternative embodiments, a consumer may not request coupons. Instead, coupons may be pushed to the consumer during the normal course of conducting a payment transaction. In one embodiment, the payment processing network receives a request for a request to authorize the use of a credit or debit account for a transaction. In addition to handling this request, the payment process network may conduct a risk assessment, search for coupons, and forward coupons to the consumer or merchant as described above even if there has not been an explicit coupon request made.

[0070] For illustrative purposes, a “DVD example” will be used to demonstrate an embodiment distributing coupons to a consumer at the point-of-sale where the discounts offered in the coupons are linked to the risk of the consumer and transaction.

[0071] A consumer 30 at a store of a merchant 22 is about to purchase a number of DVDs. The consumer goes to an access device 34, such as a POS terminal, of the merchant to begin a typical payment transaction for the DVDs. After the DVDs have been scanned into the POS device, the consumer swipes a wireless portable consumer device 32, such as a mobile phone, at the POS device. The wireless portable consumer device has been configured to provide account information for a credit account that is to be used to pay for the DVDs. In addition, the POS device can provide additional information to the wireless portable consumer device. For example, the POS device may communicate information concerning the POS device, such as a POS ID and merchant ID, to the wireless portable consumer device. Additionally, the POS device may send to the wireless portable consumer device information concerning the transaction, such as a transaction ID and SKUs for the DVDs. The wireless consumer device can then send a coupon request message to a payment processing network 26 to request coupons that might be available for the ongoing payment transaction.

[0072] The payment processing network receives the consumer’s request for coupons and proceeds to conduct a risk assessment of the consumer 30 and of the transaction. The consumer 30 might have no credit problems and frequently purchases relatively small ticket items from the current merchant 22. As a result, the chance that the underlying purchase transaction is fraudulent or poses a high default risk to any parties is very low. As a result, the payment processing network 26 may deem this payment transaction as a very low risk transaction. However, a less trustworthy consumer conducting an unusual transaction may end up generating a risk assessment that indicates that there is a higher credit, fraud, or other risk.

[0073] The payment processing network 26 may then search its own coupon repository for any coupons that might apply to the underlying payment transaction. In addition, the payment processing network may request available coupons in a coupon request message sent to the movie studios that produced the DVDs (i.e. manufacturers 29), the retailer selling the DVDs (i.e. merchant 22), and the issuer 28 behind the credit account being used to purchase the DVDs. This coupon request message may contain any risk assessment conducted by the payment processing network. The risk assessment may be embodied by a risk score. The risk score could reflect the risk of fraud, the credit risk, or a combination of fraud risk and credit risk. For example, the risk score may indicate whether or not the consumer will eventually pay for transaction being conducted. In this Example, the risk score for the consumer 30 may be “9” on a scale of 1-10 with 1 being the riskiest and 10 being the least risky. The risk score in this example may embody both fraud risk and credit risk.

[0074] In this DVD example, the payment processing network 26, the merchant 22, and the issuer 28 all have no coupons that are relevant to the DVD payment transaction. However, the movie studio 29 is willing to offer a coupon on one of the purchased DVDs because a sequel to the DVD is going to appear in theaters soon. The coupons available for the DVD are $1, $2, and $3 off. Since the risk assessment given to the consumer 30 by the payment processing network is low, the movie studio offers the $3 coupon to the consumer. The movie studio sends a coupon response message to the payment processing network 26 that contains the coupon. If the risk assessment made by the payment processing network 26 had determined that the risk for the transaction was moderate, then the movie studio might have offered the $2 cou-
pon. If the risk was severe, then the S1 coupon might have been offered by the movie studio.

[0075] Finally, the coupon from the movie studio 29 is sent to the consumer's 30 wireless portable consumer device 32. The wireless portable consumer device 32 then sends a message to the access device 34 regarding the coupon, and a $3 discount is given to the consumer while at the access device 34. As previously discussed, alternative embodiments may send the coupon to other destinations, such as the access device 32 via the acquirer 24, without passing through the portable consumer device 32.

[0076] One advantage for consumers is that consumers will be able to get greater discounts offered to them in coupons. The discount in coupons can be based on the risk of the consumer and the risk of a transaction. Also, consumers may benefit because coupons may become easier to redeem at the point-of-sale. Consumers may also benefit because it will be easier for consumers to find coupons that might apply to a purchasing transaction they are conducting.

[0077] An advantage to coupon-issuing entities, such as merchants, manufacturers, issuers and payment processing network, is that coupon-issuing entities are able to get reliable information on consumers and their purchasing transactions in real-time. As a result, coupon-issuing entities may be able to target promotions and coupons more precisely. Additionally, the ability to ink risk to discount can enable coupon-issuing entities to maintain better relationships with more valued consumers.

[0078] Certain embodiments of the invention may include none, some, or all of the above technical advantages. One or more other technical advantages may be readily apparent to one skilled in the art from the figures, descriptions, and claims included herein.

III. Computer Apparatuses

[0079] FIG. 6 shows a block diagram of subsystems that may be present in computer apparatuses that can be used according to various embodiments.

[0080] The various participants and elements in the previously described Figures may operate using one or more computer apparatuses to facilitate the functions described herein. Any of the elements in the Figures may use any suitable number of subsystems to facilitate the functions described herein. Examples of such subsystems or components are shown in FIG. 6. The sub-systems shown in FIG. 6 are interconnected via a system bus 775. Additional sub-systems such as a printer 774, keyboard 778, fixed disk 779 (or other memory comprising computer readable media), monitor 776, which is coupled to display adapter 782, and others are shown. Peripherals and input/output (I/O) devices, which couple to I/O controller 771, can be connected to the computer system by any number of means known in the art, such as serial port 777. For example, serial port 777 or external interface 781 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 allows the central processor 773 to communicate with each sub-system and to control the execution of instructions from system memory 772 or the fixed disk 779, as well as the exchange of information between sub-systems. The system memory 772 and/or the fixed disk 779 may embody a computer readable medium. Any of these elements may be present in the previously described features. For example, the previously described directory server and access control server may have one or more of these components shown in FIG. 6.

[0081] A computer readable medium according to an embodiment may comprise code for performing any of the functions described above. For example, the previously described payment processing network may comprise server with a computer readable medium comprising: a) code for receiving a coupon request message over a network; and b) code for sending a coupon response message. The server may also have a processor coupled to the computer readable medium, where the processor executes instructions embodied by computer code on the computer readable medium.

[0082] 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 will know and appreciate other ways and/or methods to implement the present invention using hardware and a combination of hardware and software.

[0083] 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 CD-ROM. 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.

[0084] A recitation of "a", "an" or "the" is intended to mean "one or more" unless specifically indicated to the contrary.

[0085] The above description is illustrative and is not restrictive. Many variations of the disclosure will become apparent to those skilled in the art upon review of the disclosure. The scope of the disclosure 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.

[0086] 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 disclosure.

[0087] 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.

What is claimed is:

1. A method comprising:
   receiving a coupon, wherein a benefit offered by the coupon is based on a risk assessment; and
   providing the coupon to a merchant.

2. The method of claim 1 wherein the risk assessment comprises a fraud risk analysis.

3. The method of claim 1 wherein the risk assessment comprises a credit risk analysis.

4. The method of claim 1 wherein the receiving the coupon comprises receiving the coupon at a portable consumer device.
5. The method of claim 4 wherein providing the coupon to the merchant comprises providing the coupon to an access device located at the merchant.
6. The method of claim 4 further comprising: storing the received coupon in the portable consumer device.
7. The method of claim 1 wherein the benefit is a discount that is greater when the risk assessment indicates that it is likely that an intended recipient of the coupon will eventually pay for a good or service.
8. The method of claim 7 wherein receiving the coupon comprises receiving the coupon at a phone.
9. The method of claim 7 further comprising: sending a request for one or more coupons, prior to receiving the coupon.
10. The method of claim 1 wherein the coupon originates from a manufacturer, an issuer, or a payment processing network.
11. A computer-readable medium comprising code for performing the method of claim 1.
12. A portable consumer device with a processor and the computer-readable medium of claim 11.
13. A method comprising: performing a risk analysis; selecting a coupon using the risk analysis, wherein a benefit offered by the coupon varies with a result of the risk analysis; and sending the coupon to a consumer.

15. A method comprising:
   conducting a risk analysis;
   requesting one or more coupons from one or more coupon-issuing entities, wherein the request includes a risk assessment;
   receiving a coupon from the one or more coupon-issuing entities, wherein the value of the coupon is based on the risk assessment; and
   sending the coupon.
16. The method of claim 15 wherein the risk assessment was generated using a fraud risk analysis.
17. The method of claim 15 wherein the risk assessment was generated using a credit risk analysis.
18. The method of claim 15 wherein the coupon-issuing entities include manufacturers, issuers, merchants and a payment processing network.
19. A computer-readable medium comprising code for performing the method of claim 15.
20. A server computer with a processor and the computer-readable medium of claim 19.