SYSTEM, METHOD AND COMPUTER PROGRAM PRODUCT FOR AUTHORIZING TRANSACTIONS USING ENHANCED AUTHORIZATION DATA

Inventors: Janet L. Biffle, Scottsdale, AZ (US); Danielle Domenica, Phoenix, AZ (US); Chanderpreet Duggal, Phoenix, AZ (US); Kristin Hoyne Gomes, State College, PA (US); Stuart Goulden, Wharton, NJ (US); Chinv H. Khor, Glendale, AZ (US); Vernon Marshall, Montclair, NJ (US); Sabyasachi Mohanty, Jersey City, NJ (US); Ian R. Webb, Darien, CT (US)

Correspondence Address:
STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.
1100 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005 (US)

Assignee: American Express Travel Related Services Company, Inc., a New York Corporation

Applied No.: 11/303,018
Filed: Dec. 16, 2005

ABSTRACT

The present invention provides systems, methods and computer program products for authorizing transactions based on, at least in part on, enhanced authorization data. In one embodiment, enhanced authorization data is received in a request for authorization to accept a transaction instrument as payment. Examples of enhanced authorization data include an automatic number identifier, an information identifier, an email address, a contact telephone number, a ship-to-name, a ship-to-address, an Internet Protocol address, and a seller identification. A risk analysis is performed based, at least in part, on the enhanced authorization data to determine the risk of the request being associated with a fraudulent purchase. The risk may be calculated by comparing the enhanced authorization data with information stored about the transaction instrument or with historical transaction information. Furthermore, the velocity of transactions associated with the enhanced authorization data may be measured in calculating the risk.
RECEIVE ENHANCED AUTHORIZATION DATA IN A REQUEST FOR AUTHORIZATION TO ACCEPT A PAYMENT ASSOCIATED WITH A TRANSACTION INSTRUMENT

MAKE AN AUTHORIZATION DECISION FOR THE REQUEST BASED, AT LEAST IN PART, UPON THE ENHANCED AUTHORIZATION DATA

RESPOND WITH THE AUTHORIZATION DECISION

FIG. 2
FIG. 3

300

Purchaser

302

Merchant 1

304

Merchant 2

306

Merchant N

308

 Authorization System

314

9/7/2004 5:32 PM
Stan Rogers
555 Bermuda Ave
funstuff@abc.com

316

9/7/2004 5:05 PM
Joe White
2213 E. Main St
funstuff@abc.com
IP: 123.22.15.18

318

9/7/2004 6:01 PM
Jennifer Saks
3133 S Central Ave
funstuff@abc.com

320
FIG. 4
ACCOUNT HOLDER INITIATES TRANSACTION WITH AIRLINE CARRIER FOR PURCHASE OF AN AIRLINE TICKET

AIRLINE CAPTURES ENHANCED TRANSACTION VARIABLES FOR THE TRANSACTION

AIRLINE TRANSMITS ENHANCED TRANSACTION VARIABLES TO FINANCIAL INSTITUTION IN STANDARD FORMAT WITH REQUEST FOR AUTHORIZATION OF THE TRANSACTION

FINANCIAL INSTITUTION PROCESSES RECEIVED TRANSACTION VARIABLES AGAINST A FRAUD RISK MATRIX

FINANCIAL INSTITUTION REPLIES TO THE AUTHORIZATION REQUEST WITH AN APPROVAL, DECLINE OR CALL REFERRAL MESSAGE TO AIRLINE BASED ON OUTCOME OF FRAUD RISK MATRIX AND STANDARD DECISIONING CRITERIA

AIRLINE PROCESSES TRANSACTION IN ACCORDANCE WITH REPLY

FIG. 5
FIG. 6
ACCOUNT HOLDER INITIATES TRANSACTION WITH TRAVEL AGENCY FOR PURCHASE OF AN AIRLINE TICKET

TRAVEL AGENT CAPTURES ENHANCED TRANSACTION VARIABLES FOR THE TRANSACTION

TRAVEL AGENCY PROVIDES ENHANCED TRANSACTION VARIABLES FINANCIAL INSTITUTION VIA GLOBAL DISTRIBUTION SERVICE PROVIDER IN STANDARD FORMAT WITH REQUEST FOR AUTHORIZATION OF THE TRANSACTION

FINANCIAL INSTITUTION PROCESSES RECEIVED TRANSACTION VARIABLES AGAINST A FRAUD RISK MATRIX

FINANCIAL INSTITUTION REPLIES TO THE AUTHORIZATION REQUEST WITH AN APPROVAL, DECLINE OR CALL REFERRAL MESSAGE TO TRAVEL AGENCY BASED ON OUTCOME OF FRAUD RISK MATRIX AND STANDARD DECISIONING CRITERIA

TRAVEL AGENCY PROCESSES TRANSACTION IN ACCORDANCE WITH REPLY

FIG. 7
SYSTEM, METHOD AND COMPUTER PROGRAM PRODUCT FOR AUTHORIZING TRANSACTIONS USING ENHANCED AUTHORIZATION DATA

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention generally relates to fraud detection and more particularly to reducing fraudulent transactions.

2. Related Art

Credit cards, charge cards, and other transaction instruments are commonly accepted today as a form of payment under a variety of circumstances. A transaction instrument may be used to make a purchase in person, for example, at a retail store, a restaurant, or a hotel by physically presenting a merchant with the transaction instrument. A transaction instrument may also be used to make a purchase without physically presenting the transaction instrument by relaying information associated with the transaction instrument, such as account number, account name, expiration date, and billing address, to a merchant. Examples of merchants that accept transaction instruments as payment without physically receiving the transaction instrument include Internet, telephone and mail order merchants.

Although transaction instruments provide a convenient means for making payments, they are vulnerable to fraud. A transaction instrument may be copied, or information about a transaction instrument necessary to make purchases may be stolen. While the card member and card issuer are unsuspecting of any fraudulent activity, numerous fraudulent purchases may be charged to the card member's transaction instrument.

To counteract fraudulent purchases, a card issuer may employ a risk analysis when a merchant requests authorization to receive a transaction instrument as payment. Risk analysis is utilized to evaluate the risks of a purchase being fraudulent. If the risks are determined to be unacceptable, the card issuer may deny the merchant's request to receive the transaction instrument as payment. For example, if a transaction instrument is reported as being lost, risk analysis may indicate an unacceptable level of risk for any further purchases involving the transaction instrument. The card issuer may then deny any requests made by merchants for authorization to accept the transaction instrument as payment.

Although conventional risk analysis reduces incidences of fraud, its ability to distinguish genuine and fraudulent purchases is limited because only a limited amount of information about a purchase is provided to a card issuer from the merchant. Conventional risk analysis is based on transaction account information and payment information. Transaction account information may include, for example, account number, account name, expiration date, billing address, and credit card verification (CCV) number. Payment information may include, for example, payment amount and payment recipient. Conventional risk analysis does not utilize other information associated with a purchase such as, for example, a ship-to-address, an email address of the purchaser, an IP address of the machine from which the purchase was initiated, etc.

Given the foregoing, what is needed is a system, method and computer program product that accepts a greater amount of purchase-related information than that used by conventional risk analysis to further reduce incidences of fraud.

BRIEF DESCRIPTION OF THE INVENTION

Systems, methods and computer program products for authorizing transactions based at least in part on enhanced authorization data are provided. Enhanced authorization data includes information associated with a purchase other than transaction account information and payment information. The enhanced authorization data may be received from a merchant in a request for authorization to accept a transaction instrument as payment. A decision to approve, deny, or refer the request is made based, at least in part, on the enhanced authorization data. The authorization decision is then provided to the merchant.

Examples of enhanced authorization data include an automatic number identification (ANI), an information identifier (II), an email address, a contact telephone number, a ship-to-name, a ship-to-address, an Internet Protocol (IP) address, and a seller identification. Enhanced authorization data may be specific to a particular industry or category of merchants. For example, merchants dealing in airline tickets may provide information such as a passenger name, a travel date and/or a destination city as enhanced authorization data.

Enhanced authorization data is collected, for example, by a merchant in the course of fulfilling a purchase desired by a purchaser. When enhanced authorization data is provided with a request for authorization to accept a transaction instrument as payment, risk analysis is performed using the enhanced authorization data to calculate the risks of the purchase being fraudulent.

In performing risk analysis, enhanced authorization data may be compared with historical transaction information as well as with information stored for a card member associated with the request. Historical transaction information includes information about previous transactions. Historical transaction data may be compared to determine, for example, if the enhanced authorization data was provided previously in fraudulent purchases. Historical transactions may also be examined to determine the rate, also referred to as velocity, at which transactions associated with an enhanced authorization data are initiated to evaluate the risks of the request being fraudulent.

Once a risk is calculated for a request, it is compared with a range of acceptable risks to make an authori-
The authorization decision is provided to the merchant in response to the merchant’s request for authorization. If the request is approved, the merchant may complete the purchase by accepting the transaction instrument as payment. If the request is denied, the merchant may ask for another form of payment from the purchaser to complete the purchase. If the request is referred, the merchant or the purchaser may be asked to contact the card issuer to provide additional information so that the request may be approved.

If a request is approved and it is later determined to be associated with a fraudulent purchase, the merchant may be contacted to reverse the authorization. If the purchase has not yet been fulfilled, for example, because the purchased item has not yet been shipped, the merchant may cancel the purchase. A request may be determined as being fraudulent, for example, by contacting a card member of the transaction instrument associated with the request to confirm the validity of the transaction or purchase.

An advantage of the present invention is that a more sophisticated risk analysis may be performed since enhanced authorization data provides additional information that can be used to distinguish between requests for genuine transactions and fraudulent transactions. Furthermore, since enhanced authorization data is typically captured by a merchant during the ordinary course of processing a purchase, the purchaser is not burdened with providing information other than that the purchaser is ordinarily asked to provide. Another advantage of the present invention is that since enhanced authorization data is independent of transaction account information, it may be used to correlate fraudulent activity patterns experienced across multiple card members and merchants.

Further features and advantages of the present invention as well as the structure and operation of various embodiments of the present invention are described in detail below with reference to the accompanying drawings.

The features and advantages of the present invention will become more apparent from the detailed description set forth below when taken in conjunction with the drawings in which like reference numbers indicate identical or functionally similar elements. Additionally, the left-most digit of a reference number identifies the drawing in which the reference number first appears.

FIG. 1 is a system diagram of an exemplary environment in which the present invention can be implemented.

FIG. 2 is a flowchart illustrating an example authorization process.

FIG. 3 is a diagram illustrating an example of risk analysis based on the velocity of transactions.

FIG. 4 is a block diagram of a first exemplary financial transaction network for processing financial transactions involving the purchase of airline tickets.

FIG. 5 is a flowchart illustrating a first exemplary method for processing a financial transaction involving the purchase of airline tickets using enhanced transaction variables.

FIG. 6 is a block diagram of a second exemplary financial transaction network for processing financial transactions involving the purchase of airline tickets.

FIG. 7 is a flowchart illustrating a second exemplary method for processing a financial transaction involving the purchase of airline tickets using enhanced transaction variables.

FIG. 8 is a block diagram of an exemplary computer system useful for implementing the present invention.

DETAILED DESCRIPTION

I. OVERVIEW AND TERMINOLOGY

Systems, methods and computer program products for authorizing transactions based at least in part on enhanced authorization data are provided. In the detailed description of the invention that follows, references to “one embodiment”, “an embodiment”, “an example embodiment”, etc., indicate that the embodiment described may include a particular feature, structure, or characteristic, but every embodiment may not necessarily include the particular feature, structure, or characteristic. Moreover, such phrases are not necessarily referring to the same embodiment. Further, when a particular feature, structure, or characteristic is described in connection with an embodiment, it is submitted that it is within the knowledge of one skilled in the art to effect such feature, structure, or characteristic in connection with other embodiments whether or not explicitly described. After reading the following description, it will be apparent to one skilled in the relevant art(s) how to implement the following invention in alternative embodiments.

The terms “business” or “merchant” may be used interchangeably with each other and shall mean any person, entity, distributor system, software and/or hardware that is a provider, broker and/or any other entity in the distribution chain of goods or services. For example, a merchant may be a grocery store, a retail store, a travel agency, a service provider, an on-line merchant or the like.

A “transaction account” as used herein refers to an account associated with an open account or a closed account system (as described below). The transaction account may exist in a physical or non-physical embodiment. For example, a transaction account may be distributed in non-physical embodiments such as an account number, frequent-flyer account, telephone calling account or the like. Furthermore, a physical embodiment of a transaction account may be distributed as a financial instrument.

A financial transaction instrument may be traditional plastic transaction cards, titanium-containing, or other metal-containing, transaction cards, clear and/or translucent transaction cards, foldable or otherwise unconventionally-sized transaction cards, radio-frequency enabled transaction cards, or other types of transaction cards, such as credit, charge, debit, pre-paid or stored-value cards, or any other like financial transaction instrument. A financial transaction instrument may also have electronic functionality provided by a network of electronic circuitry that is printed or otherwise incorporated onto or within the transaction instrument (and typically referred to as a “smart card”), or be a fob having a transponder and an RFID reader.
“Open cards” are financial transaction cards that are generally accepted at different merchants. Examples of open cards include the American Express®, Visa®, MasterCard®, and Discover® cards, which may be used at many different retailers and other businesses. In contrast, “closed cards” are financial transaction cards that may be restricted to use in a particular store, a particular chain of stores or a collection of affiliated stores. One example of a closed card is a pre-paid gift card that may only be purchased at, and only be accepted at, a clothing retailer, such as The Gap® store.

Stored value cards are forms of transaction instruments associated with transaction accounts, wherein the stored value cards provide cash equivalent value that may be used within an existing payment/transaction infrastructure. Stored value cards are frequently referred to as gift, pre-paid or cash cards, in that money is deposited in the account associated with the card before use of the card is allowed. For example, if a customer deposits ten dollars of value into the account associated with the stored value card, the card may only be used for payments up to ten dollars.

An “account,” “account number” or “account code,” as used herein, may include any device, code, number, letter, symbol, digital certificate, smart chip, digital signal, analog signal, biometric or other identifier/indicia suitably configured to allow a consumer to access, interact with or communicate with a financial transaction system. The account number may optionally be located on or associated with any financial transaction instrument (e.g., rewards, charge, credit, debit, prepaid, telephone, embossed, smart, magnetic stripe, bar code, transponder or radio frequency card).

The terms “card member,” “card holder,” and/or the plural form of these terms are used interchangeably throughout herein to refer to those persons or entities that own or are authorized to use a transaction account.

The terms “user,” “consumer,” “purchaser,” and/or the plural form of these terms are used interchangeably throughout herein to refer to those persons or entities that are alleged to be authorized to use a transaction account.

The terms “payment vehicle,” “financial transaction instrument,” “transaction instrument” and/or the plural form of these terms are used interchangeably throughout to refer to a financial instrument.

II. SYSTEM

Referring to FIG. 1, a system diagram of an exemplary system 100 in which the present invention can be implemented is shown.

System 100 includes a purchaser 102, a merchant 104, an authorization system 106, a card member database 108, and a transaction database 110. Purchaser 102 interacts with merchant 104 to make a purchase with a transaction instrument. Merchant 104 asks for authorization to accept the transaction instrument as payment by sending a request to authorization system 106. Authorization system 106 performs risk analysis on the request using information, for example, from card member database 108 and transaction database 110. Based on the risk analysis, authorization system 106 makes an authorization decision to approve, deny or refer the request. The authorization decision is provided to merchant 104. Merchant 104 completes the purchase if the request is approved or asks for an alternative form of payment from the purchaser if the request is denied. If the request is referred, merchant 104 may contact the card issuer or ask the purchaser to contact the card issuer to provide additional information to have the request approved.

Purchaser 102 may interact with merchant 104 in person (e.g., at the box office), telephonically, or electronically (e.g., from a user computer via the Internet) to make a purchase. When interacting in person, purchaser 102 may physically present a transaction instrument to merchant 104 as a form of payment. When communicating with merchant 104 through a telephone or a computer (e.g., using a web enabled computer, kiosk, terminal or the like), purchaser 102 may provide information associated with a transaction instrument, such as account number, expiration date, account name, and billing address, to merchant 104 to make a payment using the transaction instrument.

Along with providing a transaction instrument as payment, purchaser 102 may provide additional information to merchant 104 while making a purchase. For example, purchaser 102 may provide a ship-to-address or a ship-to-name that is different than a name or billing address associated with the transaction instrument. Purchaser 102 may provide an email address or a contact telephone number to merchant 104 so that purchaser 102 may be updated with the status of a purchase.

Furthermore, merchant 104 may obtain additional information about purchaser 102 from other sources while interacting with purchaser 102. For example, if purchaser 102 is communicating with merchant 104 over a telephone, merchant 104 may receive an automatic number identification (ANI) and a corresponding information identifier (II) for purchaser 102 from a telephone company. ANI provides the telephone number of the telephone used by purchaser 102 to communicate with merchant 104. II identifies the type of telephone used by purchaser 102 such as, for example, a cellular telephone, coin-operated telephone, prison telephone, or a standard land-line telephone. In another example, if purchaser 102 is communicating with merchant 104 over the Internet, the Internet Protocol (IP) address of the machine that purchaser 102 used to initiate the purchase may be captured by whatever Internet-based commerce system utilized by merchant 104.

Merchant 104 is any entity or system capable of receiving a payment from purchaser 102 using a transaction instrument. Merchant 104 may offer goods and services in exchange for payment from purchaser 102. Merchant 104 may be, for example, an Internet commerce, telephone order or mail order company. Merchant 104 may also be, for example, an aggregator or a third-party biller that facilitates transactions between purchaser 102 and a seller (not shown). Examples of aggregators or third-party billers include eBay® and PayPal®. If merchant 104 is an aggregator or a third-party biller, merchant 104 may capture information such as a seller identification and/or description of the type of goods or services sought to be purchased by purchaser 102 from the seller. Goods and services purchased through merchant 104 may be delivered physically (e.g., through the mail) or electronically (e.g., such as by downloading software over the Internet) to purchaser 102.

When purchaser 102 wishes to make a payment using a transaction instrument, merchant 104 makes a
request to authorization system 106 for authorization to accept the transaction instrument as payment. Merchant 104 formats the request using a computer device to include information about the transaction instrument, payment information, and enhanced authorization data. Examples of enhanced authorization data include, for example, an ANI, an II, an email address, a contact telephone number, a ship-to-name, a ship-to-address, an IP address, and a seller identification. The request is transmitted to authorization system 106. The request may be sent to authorization system 106 over, for example, a telephone network, intranet, the Internet, wireless communications, and/or the like.

[0045] Authorization system 106 receives the request for authorization to accept a transaction instrument as payment and performs a risk analysis to assess the risks of the request being associated with a fraudulent purchase. In assessing the risks, authorization system 106 may compare the information in the request with information in card member database 108 and transaction database 110. Card member database 108 includes information about card members and transaction instruments. For example, card member database 108 may include the billing address, email address, and contact telephone number of each card member. Transaction database 110 includes information about previous transactions (e.g., purchases). For example, transaction database 110 may include information about previous requests for authorization, decisions made for the previous requests, and any subsequent information obtained for those requests, such as whether a purchase associated with a request was later reported as being fraudulent. Although databases 108 and 110 are shown separately, as would be appreciated by one skilled in the relevant arts, the two databases may be implemented as a single or multiple databases. The risk analysis will be described in more detail below.

[0046] After risk analysis is performed for the request, authorization system 106 makes an authorization decision to approve, deny, or refer the request and provides the decision to merchant 104. If the request is approved, merchant 104 may accept the transaction instrument as payment. If the request is denied, merchant 104 may inform purchaser 102 that the request was denied and ask purchaser 102 for another form of payment to complete the purchase. If the request is referred, merchant 104 and/or purchaser 102 may be asked to contact a card issuer to provide additional information to have the request approved.

[0047] If at a later time a purchase that was approved by authorization system 106 is determined to be fraudulent, authorization system 106 or a card issuer may contact merchant 104 to reverse the approval. If merchant 104 has not yet completed the purchase, for example, by not shipping goods to purchaser 102, merchant 104 may cancel the purchase.

III. PROCESS

[0048] FIG. 2 illustrates an example process 200 for authorizing a request to receive a transaction instrument as payment. Process 200 begins at step 202.

[0049] In step 202, a request for authorization to accept a payment associated with a transaction instrument is received from a merchant such as merchant 104. The merchant makes a request when a purchaser provides the merchant with a transaction instrument or information about the transaction instrument to make a payment for a purchase. The request may include enhanced authorization data such as, for example, an ANI, an II, an email address, a contact telephone number, a ship-to-name, a ship-to-address, an IP address, or a seller identification that was obtained by the merchant during the course of fulfilling the purchase. Enhanced authorization data may be specific to a particular industry or category of merchants. For example, merchants dealing in airline tickets may provide as enhanced authorization data information such as passenger name, travel date, or destination city.

[0050] In step 204, an authorization decision is made based, at least in part, upon the enhanced authorization data included in the request received in step 202. The authorization decision is based on a risk analysis performed using the information in the request. If the risks are within a range of acceptable risks, a decision to approve the request is made. If the risks are outside the range of acceptable risks, a decision to deny or refer the request is made.

[0051] Various risk analysis may be performed using the enhanced authorization data provided in a request. For example, enhanced authorization data may be compared with information stored about the transaction instrument or with information stored about a card member associated with the transaction instrument to assess risks. If the enhanced authorization data includes an email address, contact telephone number, or a ship-to-name, each can be compared with stored values of the card member’s email address, telephone numbers, and name, respectively. If the comparisons match, less risk is assigned to the request. In another example, if the enhanced authorization data includes an IP address, it can be compared with the IP address, for example, of the machine the card member uses to access the card issuer’s bank website. If the IP addresses match, less risk is assigned to the request.

[0052] Historical transaction information may also be compared with enhanced authorization data to calculate risks. Historical transaction information includes information about previous transactions. For example, if enhanced authorization data includes a ship-to-address, it may be compared with prior ship-to-addresses used in historical transactions. If the ship-to-address is associated with numerous historical transactions that were reported as being fraudulent, more risk is assigned to the request.

[0053] In evaluating enhanced authorization data with historical transaction information, transaction information associated with other card members and other merchants may be used to calculate risks. For example, if the enhanced authorization data includes a seller identification, an ANI, or an II information, this information may be compared with historical transactions across multiple card members and merchants. If the seller identification, ANI, or II information provided in the request is associated with fraudulent activity across multiple card members and merchants, a greater level of risk may be assigned to the request.

[0054] Furthermore, historical transactions may be examined to determine the velocity of transactions associated with an enhanced authorization data to calculate risks. The velocity of transactions is the rate at which transactions are initiated in a designated period of time. For example, if an IP address is included as part of an enhanced authorization data, the velocity of prior transactions which are also asso-
associated with the IP address can be measured. If the velocity is atypically high for the IP address, a greater level of risk may be associated with the request. Assessing risks based on the velocity of transactions is explained in greater detail herein with respect to FIG. 3.

[0055] As would be appreciated by persons skilled in the relevant arts, enhanced authorization data such as an ANI, II, an email address, a contact telephone number, a ship-to-name, a ship-to-address, an IP address, or a seller identification may be used in different ways to assess the risks of an authorization request being associated with a fraudulent purchase.

[0056] In step 206, the authorization decision made in step 204 is sent to the merchant that provided the request in step 202. The merchant proceeds according to the authorization decision. If the request is approved, the merchant completes the purchase. If the request is denied, the merchant may inform the purchaser that the transaction instrument was denied and/or ask the purchaser for another form of payment to complete the purchase. If the request is referred, the merchant may contact the card issuer or ask the purchaser to contact the card issuer to provide additional information to have the request approved.

[0057] FIG. 3 illustrates a diagram 300 that shows an example of risk analysis based on the velocity of transactions. Diagram 300 includes a purchaser 302, merchants 304, 306 and 308, authorization system 106, and request data 314, 316, and 318. Diagram 300 depicts examples of three requests for authorization to accept transaction instruments as payment from three different merchants 304, 306, and 308.

[0058] As shown by request data 314, a first request for authorization to accept a transaction instrument as payment was made by merchant 304 on Sep. 7, 2004 at 5:05 PM. Along with the date and time, transaction account information associated with the transaction instrument such as the name of the account holder (e.g., Joe White) and billing address (e.g., 2213 E. Main St) was provided by merchant 304 in the request. Furthermore enhanced authorization data such as the email address of the purchaser (e.g., funstuff@abc.com) and IP address of the machine with which the purchaser initiated the purchase (e.g., 123.22.15.18) was also provided by merchant 304 to authorization system 106 in the request.

[0059] A second request for authorization to accept a transaction instrument as payment, as shown by request data 316, was made by merchant 306 just 27 minutes after the first request (e.g., Sep. 7, 2004 at 5:32 PM). In addition to the date and time information, request data 316 includes transaction account information such as the name of the account holder (e.g., Stan Rogers) and billing address (e.g., 555 Bermuda Ave). Request data 316 further includes an email address of the purchaser (e.g., funstuff@abc.com) as enhanced authorization data.

[0060] When a third request for authorization, as shown by request data 318, is received by authorization system 106, the velocity of historical transactions may be examined to assess the risk of the third request being associated with a fraudulent purchase. Request data 318 includes a date and time (e.g., Sep. 7, 2004 at 6:01 PM), name of the account holder (e.g., Jennifer Saks) and billing address (e.g., 3133 S Central Ave.). Request data 318 further includes, as enhanced authorization data 320, an email address of the purchaser (e.g., funstuff@abc.com). To determine the velocity of transactions, authorization system 106 examines historical transactions that are associated with enhanced authorization data received in the request such as, for example, enhanced authorization data 320. Request data 314 and request data 316 are examined since they both contain enhanced authorization data 320 (e.g., funstuff@abc.com). The velocity of these requests is considered by authorization system 106 in assessing the risks of the third request being associated with a fraudulent purchase. In the example depicted in diagram 300, considering that all three requests occurred within one hour of each other, each request is associated with a different transaction instrument, and all requests point to a single purchaser 302 as identified by the enhanced authorization data 320, authorization system 106 may assign a greater level of risk for the third request. If the transaction accounts associated with the three requests do not have a history of being associated with enhanced authorization data 320, the velocity of transactions as depicted in FIG. 3 may suggest that purchaser 302 is making fraudulent purchases using transaction instruments belonging to several people (e.g., Joe White, Stan Rogers, and Jennifer Saks).

[0061] Based on the risk analysis performed by authorization system 106 for the third request, authorization system 106 provides an authorization decision to merchant 308. Card members associated with transaction instruments provided in the first, second, and third requests may be contacted to determine the validity of the requests. If a request is determined to be associated with a fraudulent purchase, the appropriate merchant may be contacted to cancel a purchase associated with the request.

IV. EXAMPLE EMBODIMENT

[0062] An example embodiment, according to the present invention, is provided below with reference to enhanced authorization data as it relates to merchants dealing with airline travel tickets.

[0063] Financial institutions currently have existing transaction networks over which financial transactions between its account holders and various merchants may be completed. Financial institutions are therefore uniquely positioned to offer advanced risk identification and prevention measures to its customers, merchants and partners by leveraging these existing networks, or by establishing new networks where these capabilities are provided.

[0064] The processes introduced herein enable financial institutions to make improved fraud risk management decisions for transactions, particularly those involving travel tickets such as airline tickets. By capturing and analyzing certain additional information at the point of authorization of a charge, the risk that the transaction is fraudulent may be more accurately evaluated before the ticket purchase is authorized. In an embodiment, real-time fraud risk decisions are based on an evaluation of the data traditionally provided in an authorization request plus ten additional transaction variables that have routinely been captured by the merchant and are now transmitted to the financial institution with a real-time authorization request.

[0065] The processes will be described throughout with reference to airline tickets. However, it should be readily
apparent that the processes may be used regarding any transaction in which similar data may be captured and evaluated. In an embodiment, the additional transaction variables provided with respect to the purchase of airline tickets may include: an airline reservation code for the ticket; the passenger name listed on the ticket; an origin airport for the ticket; a destination airport for the ticket; a travel date for the ticket; a description of routing airports or city codes of the airline ticket (e.g., New York to Miami returning to New York: JFK-MIA-MIA-JFK); a class of service (e.g., first class, business class, or coach class; including fare basis information and ticket designator information); an indicator of whether the airline ticket is an electronic ticket; a number of passengers for which tickets are purchased; and a code corresponding to an airline carrier for which the ticket is booked. Advantageously, these ten variables are typically captured in various transactions by airlines and other airline ticket merchants, such as travel agencies and online travel web sites. However, these transaction variables have not previously been provided as part of real-time authorization requests to financial institutions that maintain account holder accounts, and such transaction variables have not been used for fraud risk screening by financial institutions prior to or during the real-time authorization of a transaction.

[0066] According to the present disclosure, then, one or more of the additional transaction variables are now transmitted from the merchant to a financial institution in an automated manner and in a standardized format over the financial transaction network during a transaction initiation and authorization process so that standard authorization times (based on all types of financial transactions using similar payment vehicles) are not affected. The received transaction variables (traditional plus additional) are immediately presented to one or more software-implemented fraud-risk models maintained by the financial institution, which are well-known in the relevant art(s), but must now account for additional variables as described below with respect to FIG. 5. Such software-implemented fraud-risk models would then evaluate the received transaction variables, and from this, an immediate risk decision (e.g., to accept or refer the transaction for further identification, or a request to contact the financial institution) based on a determined risk factor can be made.

[0067] In various embodiments, the transaction variables may be used in combination with standard information utilized by financial institutions to authorize transactions (e.g., amount of transaction, status of account holder account, purchases and transaction history of the particular account holder, available credit for the financial account, and a transaction history of the particular merchant). The combination of the processes introduced herein with standard authorization decision-making criteria will provide enhanced fraud risk assessment before the ticket or service is authorized for payment on a payment vehicle. This, in turn, will reduce the incidence of fraudulent transactions and reduce processing costs for charge backs and the like.

[0068] Turning now to FIG. 4, there is depicted a conceptual block diagram of a first exemplary transaction network 400, over which the processes of the present disclosure may be performed. In the network 400, an account holder 402 may initiate a transaction with an airline carrier server 404 for the purchase of airline tickets in any standard manner. When the account holder wishes to pay for the tickets using a payment vehicle, the airline carrier server 404, in turn, may communicate with a financial institution server 406 of the financial institution that maintains the account corresponding to the payment vehicle.

[0069] In various embodiments, the account holder 402 may communicate with the airline carrier over the Internet using a computer terminal or the like, via telephone, or in person. The account holder 402 may use a credit card, charge card, stored value card, debit card or other type of payment vehicle for the transaction.

[0070] The airline carrier server 404 may be any type of computer server, or group of distributed servers, that include appropriate processors, memory and network communication devices, as well as application and operating systems software that includes processing instructions and programming for performing the processes disclosed herein. The airline carrier server 404 may communicate with the financial server 406 using any existing transaction processing network, with little need for changes to existing network hardware. Merchants and financial institutions may require certain software changes to capture and transmit the ten transaction variables with authorization requests for ticket purchases in an acceptable format. When the transaction involves an AMERICAN EXPRESS card, for example, the transaction variables can be sent in the AMERICAN EXPRESS Authorization ISO 8583 Version 1 Specification format.

[0071] Turning now to FIG. 5, there is depicted a flowchart of an exemplary method 500 for processing a financial transaction involving the purchase of airline tickets using enhanced transaction variables. The method 500 commences when an account holder initiates a transaction with an airline carrier for a purchase of an airline ticket (step 502). During the course of the transaction, the airline receives certain of the transaction variable information from the account holder, including the account holder name; a passenger name; an origin airport for the ticket; a destination airport for the ticket; a travel date for the ticket; a description of routing airports or city codes of the airline ticket (e.g., New York to Miami returning to New York: JFK-MIA-MIA-JFK); a class of service (e.g., first class, business class, or coach class; including fare basis information and ticket designator information); an indicator of whether the airline ticket is an electronic ticket. During the course of the transaction, the airline may also determine a reservation code for the ticket and supply its airline carrier code (step 504).

[0072] Upon agreement of the terms of the ticket, the airline receives a method of payment from the account holder, and then contacts the financial institution maintaining the account holder’s account. The airline then transmits the enhanced transaction variables, in addition to the variables traditionally provided, to the financial institution in a standard format with a request to authorize the transaction for payment (step 506).

[0073] Next, at step 508, the financial institution processes the received transaction variables through at least one fraud-risk model in order to determine the risk of fraud presented by the transaction variables using historical transaction data. Any transactions identified as high risk may be referred for further identification or in case of extreme risk declined. Such a result may occur where the risk models determine
that the probability of fraud is within a range of unacceptable values. This range may be established based on historical data so that legitimate transactions are not unduly prevented by the fraud-risk models. The range may be adjusted over time as more historical data is collected and analyzed.

[0074] Alternatively, or in addition thereto, where the fraud-risk models indicate a risk factor within a certain range of unacceptable values for the transaction, the financial institution may instead transmit a request to be contacted by the account holder by telephone or the like (referred to herein as a call referral message) before the transaction can be authorized. Alternatively, when the fraud-risk models indicate that the risk is within a range of acceptable values, the transaction may then continue to be processed in a standard manner.

[0075] The financial institution replies to the authorization request with an approval, declination or call referral message based on the outcome of the fraud-risk model along with standard authorization decision-making criteria (step 510). The airline then processes the transaction in accordance with the reply received from the financial institution (step 512), after which process 500 ends.

[0076] The fraud-risk model or models may be generated from collected data regarding fraudulent and/or legitimate transactions over a large group of account holders on a national or international scale. A risk value may be determined for each collected transaction variable or for inter-comparisons between the received transaction variables, using such historical transaction data. These empirically-determined, risk values may be applied within the risk models in any of a variety of useful manners to determine an overall risk for a given transaction.

[0077] The received transaction variable data can be applied to historical data in any of a wide variety of useful ways using a wide number of formulas and other forms of risk models. Since historical financial transaction data is used to determine the risk, these values and formulas will be largely dependant on the empirical data used. The formulas may further be refined over time by examining changes in the historical data patterns as time progresses, as will be readily apparent to one of ordinary skill in the art.

[0078] In one example, transactions in which a reservation code is provided may have less risk of fraud than transactions in which no reservation code is provided. The fraud-risk model may then apply a risk value to a received transaction based on whether a reservation code has been provided and the historical data on prior transactions in which a reservation code has not been received.

[0079] In another example, historical data may reveal that fraudulent transactions are more likely for tickets of a certain type of routing (e.g., one-way ticket purchases may have a greater risk of being fraudulent than round-trip purchases, a certain class of service, or for certain airline carriers. Appropriate risk values will then be applied to these individual transaction variables for each transaction received.

[0080] In a further example, a transaction is received in which the transaction variable “Passenger Name” is not the same as the transaction variable “Account Holder Name.” The risk value based on such inter-comparison of received transaction variables may be determined based on data of prior fraudulent transactions. For example, it may be that the historical data shows that 5% of transactions in which the Passenger Name does not match the account holder name are fraudulent. A risk value of 0.05 for this transaction variable may accordingly be applied within the fraud-risk models for any transaction in which this is the case, and this value may be added, multiplied or combined with similar determinations for other risk values regarding the remaining transaction variables to determine an overall risk factor for the transaction.

[0081] It is important that the introduction of this fraud risk decision-making process to financial transaction authorization processes not substantially impact the standard time it currently takes to authorize a credit transaction with airlines or travel agencies, and does not unduly impact the identification and processing of legitimate transactions. That is, legitimate transactions should never be misidentified as fraudulent. Appropriate values and formulas for the risk values and the fraud-risk models, as well as range of acceptable and unacceptable values for transaction risk, may be designed with this goal in mind and refined over time by continuously analyzing historical transaction data to ensure that this goal is achieved.

[0082] Another embodiment of the present disclosure, shown in FIG. 6, involves the case where the merchant selling the ticket is a travel agent or other third-party, and not the travel carrier engaging in a direct sale. Accordingly, a second exemplary transaction network 600 may include the account holder 402, in communication with a travel agency server 602 or other third-party merchant. The travel agency server 602, in turn, may communicate with the financial institution via a third-party processing system 604, such as may be provided by existing Global Distribution Service (GDS) providers.

[0083] In such existing systems, only minor hardware and software changes may be needed to accommodate the processes disclosed herein, so that the third-party processors can capture and transmit additional variables for fraud risk screening. In examples where the payment vehicle is maintained by AMERICAN EXPRESS, the travel agencies and Global Distribution System providers must be able to send this information to AMERICAN EXPRESS in the authorization request using the ISO 8583 Version 1 Specification format. Other third-party processors who assist in transferring authorization requests to American Express or other financial institutions (i.e., issuers of payment vehicles used for such transactions) on behalf of airlines or GDS’s must also be able to accept and transfer this information in the authorization stream as specified herein.

[0084] Turning now to FIG. 7, there is depicted a flowchart of an exemplary method 700 for processing a financial transaction involving the purchase of airline tickets from a travel agency or other third-party merchant. The method 700 is similar to the method 500 described above.

[0085] The method 700 commences when an account holder initiates a transaction with the merchant for the purchase of an airline ticket (step 702). The travel agency captures the transaction variables (the variables in a traditional authorization request and the ten listed above) for the transaction as received from the airline and the account holder (step 704) and transmits them to the financial insti-
tion - in almost all cases via the airline or a GDS - in a standard format with the request for authorization of the transaction (step 706).

[0086] The financial institution processes the received transaction variables against at least one fraud-risk model (step 708) and, in various embodiments, applies standard authorization decision-making criteria as well. The financial institution replies to the authorization request real-time with an approval, declination or call referral message based on outcome of the fraud-risk model and standard decisioning criteria (step 710). The travel agency then processes the transaction in accordance with the received reply (step 712), after which the process 700 ends.

[0087] The enhanced processes disclosed herein are an important tool that can be consistently implemented for all airline transactions in which the enhanced data (i.e., the additional transaction variables) is transmitted to a card issuer in the real-time authorizations request. Such data is already collected by airlines, travel agencies and GDS's for other purposes, and can be transmitted onwards to issuers with only minor adjustments to current software and without requiring the replacement of network hardware currently used in many systems.

[0088] Airlines that participate in providing this enhanced data will realize fewer fraudulent airline tickets charged back to them since the fraud models used have a higher probability of detecting and preventing fraudulent transactions than in existing systems. Airline ticket merchants will also spend less time serving fraudulent customers or investigating charge backs, resulting in reduced operational expenses. Additionally, the system makes it harder for a card holder that legitimately enters into a transaction from later claiming that the transaction was fraudulent. In this manner, the card issuer, card holder and airline vendors each benefit from the security provided by the disclosed processes.

[0089] The card issuer may secure the collected enhanced transaction data in a variety of known and effective manners so that card member information cannot be obtained or used by unauthorized third parties.

[0090] The disclosed enhancements to financial transaction processing have applicability to various types of transactions involving travel tickets (e.g., train tickets, cruise tickets, car rentals and the like) other than the specific examples involving airlines as described herein, as will be apparent to one of ordinary skill in the art. The risk values and overall ranges of acceptable risk values may be the same or different for different transaction types. The type of ticket purchased can be readily identified based on the merchant or the carrier code received with the transaction variables.

[0091] Although the best methodologies for the invention have been particularly described in the foregoing disclosure, it is to be understood that such descriptions have been provided for purposes of illustration only, and that other variations both in form and in detail can be made thereupon by those skilled in the art without departing from the spirit and scope thereof, which is defined first and foremost by the appended claims.

V. EXAMPLE IMPLEMENTATIONS

[0092] The present invention may be implemented using hardware, software or a combination thereof and may be implemented in one or more computer systems or other processing systems. However, the manipulations performed by the present invention were often referred to in terms, such as adding or comparing, which are commonly associated with mental operations performed by a human operator. No such capability of a human operator is necessary, or desirable in most cases, in any of the operations described herein which form part of the present invention. Rather, the operations are machine operations. Useful machines for performing the operation of the present invention include general purpose digital computers or similar devices.

[0093] In fact, in one embodiment, the invention is directed toward one or more computer systems capable of carrying out the functionality described herein. An example of a computer system 800 is shown in FIG. 8.

[0094] Computer system 800 includes one or more processors, such as processor 804. Processor 804 is connected to a communication infrastructure 806 (e.g., a communications bus, cross-over bar, or network). Various software embodiments are described in terms of this exemplary computer system. After reading this description, it will become apparent to a person skilled in the relevant art(s) how to implement the invention using other computer systems and/or architectures.

[0095] Computer system 800 can include a display interface 802 that forwards graphics, text, and other data from communication infrastructure 806 (or from a frame buffer not shown) for display on display unit 816.

[0096] Computer system 800 also includes a main memory 808, preferably random access memory (RAM), and may also include a secondary memory 810. Secondary memory 810 may include, for example, a hard disk drive 812 and/or a removable storage drive 814, representing a floppy disk drive, a magnetic tape drive, an optical disk drive, etc. Removable storage drive 814 reads from and/or writes to a removable storage unit 818 in a well known manner. Removable storage unit 818 represents a floppy disk, magnetic tape, optical disk, etc. which is read by and written to by removable storage drive 814. As will be appreciated, removable storage unit 818 includes a computer usable storage medium having stored therein computer software and/or data.

[0097] In alternative embodiments, secondary memory 810 may include other similar devices for allowing computer programs or other instructions to be loaded into computer system 800. Such devices may include, for example, a removable storage unit 822 and an interface 820. Examples of such may include a program cartridge and cartridge interface (such as that found in video game devices), a removable memory chip (such as an erasable programmable read only memory (EPROM), or programmable readonly memory (PROM)) and associated socket, and other removable storage units 822 and interfaces 820, which allow software and data to be transferred from removable storage unit 822 to computer system 800.

[0098] Computer system 800 may also include a communications interface 824. Communications interface 824 allows software and data to be transferred between computer system 800 and external devices. Examples of communications interface 824 may include a modem, a network interface (such as an Ethernet card), a communications port, a
Personal Computer Memory Card International Association (PCMCIA) slot and card, etc. Software and data transferred via communications interface 824 are in the form of signals 828 which may be electronic, electromagnetic, optical or other signals capable of being received by communications interface 824. These signals 828 are provided to communications interface 824 via a communications path (e.g., channel) 826. This channel 826 carries signals 828 and may be implemented using wire or cable, fiber optics, a telephone line, a cellular link, an radio frequency (RF) link and other communications channels.

[0099] In this document, the terms “computer program medium” and “computer usable medium” are used to generally refer to media such as removable storage drive 814, a hard disk installed in hard disk drive 812, and signals 828. These computer program products provide software to computer system 800. The invention is directed to such computer program products.

[0100] Computer programs (also referred to as computer control logic) are stored in main memory 808 and/or secondary memory 810. Computer programs may also be received via communications interface 824. Such computer programs, when executed, enable computer system 800 to perform the features of the present invention, as discussed herein. In particular, the computer programs, when executed, enable processor 804 to perform the features of the present invention. Accordingly, such computer programs represent controllers of computer system 800.

[0101] In an embodiment where the invention is implemented using software, the software may be stored in a computer program product and loaded into computer system 800 using removable storage drive 814, hard drive 812 or communications interface 824. The control logic (software), when executed by processor 804, causes processor 804 to perform the functions of the invention as described herein.

[0102] In another embodiment, the invention is implemented primarily in hardware using, for example, hardware components such as application specific integrated circuits (ASICs). Implementation of the hardware state machine so as to perform the functions described herein will be apparent to persons skilled in the relevant art(s).

[0103] In yet another embodiment, the invention is implemented using a combination of both hardware and software.

VI. CONCLUSION

[0104] While various embodiments of the present invention have been described above, it should be understood that they have been presented by way of example, and not limitation. It will be apparent to persons skilled in the relevant art(s) that various changes in form and detail can be made therein without departing from the spirit and scope of the present invention. Thus, the present invention should not be limited by any of the above described exemplary embodiments, but should be defined only in accordance with the following claims and their equivalents.

[0105] In addition, it should be understood that the figures illustrated in the attachments, which highlight the functionality and advantages of the present invention, are presented for example purposes only. The architecture of the present invention is sufficiently flexible and configurable, such that it may be utilized (and navigated) in ways other than that shown in the accompanying figures.

[0106] Further, the purpose of the foregoing Abstract is to enable the U.S. Patent and Trademark Office and the public generally, and especially the scientists, engineers and practitioners in the art who are not familiar with patent or legal terms or phraseology, to determine quickly from a cursory inspection the nature and essence of the technical disclosure of the application. The Abstract is not intended to be limiting as to the scope of the present invention in any way.

What is claimed is:

1. A method for authorizing a financial transaction, comprising:
   - receiving, from a device associated with a merchant, a request for authorization to accept a transaction instrument as payment for a purchase, the request including enhanced authorization data;
   - making an authorization decision for the request based, at least in part, upon the enhanced authorization data; and
   - sending the authorization decision to the device.
2. The method of claim 1, wherein the enhanced authorization data includes at least one of: an automatic number identification or an information identifier.
3. The method of claim 1, wherein the enhanced authorization data includes at least one of: an email address; a contact telephone number; a ship-to-name; a ship-to-address; an Internet Protocol (IP) address; or a seller identification.
4. The method of claim 1, wherein the enhanced authorization data includes at least one of: a passenger name; a travel date; a routing description; an electronic ticket indicator; an origin city; a destination city; a class of service; a number of passengers; a reservation code; or carrier code.
5. The method of claim 1, wherein the making step comprises:
   - calculating a risk based, at least in part, on the enhanced authorization data; and
   - comparing the risk with a range of acceptable risks.
6. The method of claim 5, wherein the calculating step comprises:
   - calculating the risk based, at least in part, on a historical transaction associated with the enhanced authorization data.
7. The method of claim 6, wherein the historical transaction is associated with another transaction instrument.
8. The method of claim 5, wherein the historical transaction is associated with another transaction instrument.
9. The method of claim 5, wherein the calculating step comprises:
   - calculating the risk based, at least in part, on the velocity of transactions associated with the enhanced authorization data.
10. The method of claim 1, further comprising:
   - receiving an indication from a card member that the purchase is fraudulent; and
   - reversing the authorization decision.
11. A system for authorizing a financial transaction comprising:

a processor; and

a memory in communication with the processor, wherein the memory stores a plurality of processing instructions for directing the processor to:

receive, from a device associated with a merchant, a request for authorization to accept a transaction instrument as payment for a purchase, the request including enhanced authorization data;

make an authorization decision for the request based, at least in part, upon the enhanced authorization data; and

send the authorization decision to the device.

12. The system of claim 11, wherein the enhanced authorization data includes at least one of: an automatic number identification or an information identifier.

13. The system of claim 11, wherein the enhanced authorization data includes at least one of: an email address; a contact telephone number; a ship-to-name; a ship-to-address; an Internet Protocol (IP) address; or a seller identification.

14. The system of claim 11, wherein the enhanced authorization data includes at least one of: a passenger name; a travel date; a routing description; an electronic ticket indicator; an origin city; a destination city; a class of service; a number of passengers; a reservation code; or a carrier code.

15. The system of claim 11, wherein the processing instructions for directing the processor to make an authorization decision include instructions for directing the processor to:

calculate a risk based, at least in part, on the enhanced authorization data; and

compare the risk with a range of acceptable risks.

16. The system of claim 15, wherein the processing instructions for directing the processor to calculate a risk include instructions for directing the processor to:

calculate the risk based, at least in part, on a historical transaction associated with the enhanced authorization data.

17. The system of claim 16, wherein the historical transaction is associated with another transaction instrument.

18. The system of claim 15, wherein the processing instructions for directing the processor to calculate a risk include instructions for directing the processor to:

calculate the risk based, at least in part, on the velocity of transactions associated with the enhanced authorization data.

19. The system of claim 15, wherein the processing instructions for directing the processor to calculate a risk include instructions for directing the processor to:

calculate the risk based, at least in part, on a comparison between the enhanced authorization data and information stored by a card issuer about a card member associated with the transaction instrument.

20. The system of claim 11, wherein the plurality of processing instructions includes instructions for directing the processor to:

receive an indication from a card member that the purchase is fraudulent; and

reverse the authorization decision.

21. A computer program product comprising a computer usable medium having control logic stored therein for causing a computer to associate a reference magnetic signature with a transaction instrument, said control logic comprising:

first computer readable program code means for causing the computer to receive, from a device associated with a merchant, a request for authorization to accept a transaction instrument as payment for a purchase, the request including enhanced authorization data;

second computer readable program code means for causing the computer to make an authorization decision for the request based, at least in part, upon the enhanced authorization data; and

third computer readable program code means for causing the computer to send the authorization decision to the device.

22. The computer program product of claim 21, wherein the enhanced authorization data includes at least one of: an automatic number identification or an information identifier.

23. The computer program product of claim 21, wherein the enhanced authorization data includes at least one of: an email address; a contact telephone number; a ship-to-name; a ship-to-address; an Internet Protocol (IP) address; or a seller identification.

24. The computer program product of claim 21, wherein the enhanced authorization data includes at least one of: a passenger name; a travel date; a routing description; an electronic ticket indicator; an origin city; a destination city; a class of service; a number of passengers; a reservation code; or a carrier code.

25. The computer program product of claim 21, wherein the second computer readable program code means comprises:

fourth computer readable program code means for causing the computer to calculate a risk based, at least in part, on the enhanced authorization data; and

fifth computer readable program code means for causing the computer to compare the risk with a range of acceptable risks.

26. The computer program product of claim 25, wherein the fourth computer readable program code means comprises:

sixth computer readable program code means for causing the computer to calculate the risk based, at least in part, on a historical transaction associated with the enhanced authorization data.

27. The computer program product of claim 26, wherein the historical transaction is associated with another transaction instrument.

28. The computer program product of claim 25, wherein the fourth computer readable program code means comprises:

sixth computer readable program code means for causing the computer to calculate the risk based, at least in part,
on the velocity of transactions associated with the enhanced authorization data.

29. The computer program product of claim 25, wherein the fourth computer readable program code means comprises:

sixth computer readable program code means for causing the computer to calculate the risk based, at least in part, on a comparison between the enhanced authorization data and information stored by a card issuer about a card member associated with the transaction instrument.

30. The system of claim 21, further comprising:

fourth computer readable program code means for causing the computer to receive an indication from a card member that the purchase is fraudulent; and

fifth computer readable program code means for causing the computer to reverse the authorization decision.