

METHODS AND SYSTEMS FOR PROCESSING A TRANSACTION AUTHORIZATION REQUEST

Technical Field and Background

[0001] The present disclosure relates to processing of transaction authorization requests for payment card transactions. In particular, it provides methods and systems for processing transaction requests in the event that a transaction is declined.

[0002] The processing of transaction authorization requests for payment cards such as credit cards and debit cards typically involves a server associated with an issuer organization such as a bank determining whether to approve or decline the transaction. This decision may be partially based on the status of the payment card holder's account. For example, the decision may be based on a determination on whether there is a sufficient balance or remaining credit limit for the account. The status and history of the merchant involved in the transaction may also be used in the determination. For example, if a merchant has a history of fraudulent transactions or if the issuer organization identifies that a merchant has a high risk of fraudulent transactions, then the transaction may be declined.

[0003] The scenario mentioned above in which a transaction is declined by an issuing organization due to the merchant results in a failure of the transaction. This means that the cardholder has to find another way to purchase the product that they desire or to not make the purchase.

[0004] Additionally, the recent growth in electronic commerce has led to a wide range of online retailers and other merchants. This provides a great choice for customers, however, the quality of service and product offerings can vary between retailers.

Summary

[0005] In general terms, the present disclosure proposes methods and systems for processing a transaction authorization request. The transaction may be declined if either it is determined that a fraud risk associated with the merchant is higher than a threshold, or if reviews or ratings associated with the merchant are below a threshold. In the event that the transaction is declined, an alternative merchant is determined.

[0006] According to a first aspect of the present invention, there is provided a computer implemented method of processing a transaction authorization request. The method comprises: receiving a transaction authorization request at an issuer server, the transaction

authorization request comprising a merchant identifier indicating a merchant associated with the transaction authorization request; looking up merchant validation information associated with the merchant in a merchant validation database using the merchant identifier; analyzing the merchant validation indication to identify if the merchant has a negative validation indication; and if the merchant has a negative validation indication: generating a transaction authorization response indicating that the transaction is declined; and determining an alternative merchant using an alternative merchant database coupled to the issuer server.

[0007] In an embodiment the transaction authorization request relates to an electronic commerce transaction. The method further comprises receiving an indication of a customer order associated with the transaction authorization request, and determining an alternative merchant comprises using the indication of the customer order associated with the transaction authorization request.

[0008] The indication of the customer order may comprise an indication of a parameter of the customer order and determining an alternative merchant may comprise searching an alternative merchant database using the parameter of the customer order. Searching the alternative merchant database using the parameter of the customer order may comprise searching the alternative merchant database for merchants having a product offer having a parameter which matches the parameter of the customer order within an acceptable variation.

[0009] In an embodiment the merchant validation information indicates a risk of fraud at the merchant.

[0010] In an embodiment the merchant validation information indicates a rating of the merchant.

[0011] Analyzing the merchant validation indication to identify if the merchant has a negative validation indication may comprise comparing the rating with a threshold.

[0012] In an embodiment the method further comprises sending an indication of the alternative merchant to a customer associated with the transaction authorization request.

[0013] In an embodiment the method further comprises executing a transaction with the alternative merchant.

[0014] According to a second aspect of the present invention, there is provided system for processing a transaction authorization request. The system comprises: a computer processor and a data storage device, the data storage device having a merchant validation information look up module; a merchant validation information analysis module; a transaction authorization response generation module; and an alternative merchant determination module comprising non-transitory instructions operative by the processor to: receive a transaction authorization request at an issuer server, the transaction authorization request comprising a merchant identifier indicating a merchant associated with the transaction authorization request; look up merchant validation information associated with the merchant in a merchant validation database using the merchant identifier; analyze the merchant validation indication to identify if the merchant has a negative validation indication; and if the merchant has a negative validation indication: generate a transaction authorization response indicating that the transaction is declined; and determine an alternative merchant using an alternative merchant database coupled to the issuer server.

[0015] According to a yet further aspect, there is provided a non-transitory computer-readable medium. The computer-readable medium has stored thereon program instructions for causing at least one processor to perform operations of a method disclosed above.

Brief Description of the Drawings

[0016] Embodiments of the invention will now be described for the sake of non-limiting example only, with reference to the following drawings in which:

Fig. 1 is a block diagram of a data processing system according to an embodiment of the present invention;

Fig. 2 is a block diagram illustrating a technical architecture of the apparatus according to an embodiment of the present invention;

Fig. 3 is a flowchart illustrating a method of processing a transaction authorization request according to an embodiment of the present invention;

Fig. 4 is a block diagram of a data processing system for processing a transaction authorization request according to an embodiment of the present invention; and

Fig. 5 is a flowchart illustrating a method of processing a transaction authorization request according to an embodiment of the present invention.

Detailed Description

[0017] As used herein, the term “payment card” refers to any suitable cashless payment device, such as a credit card, a debit card, a prepaid card, a charge card, a membership card, a promotional card, a frequent flyer card, an identification card, a prepaid card, a gift card, and/or any other device that may hold payment account information, such as mobile phones, Smartphones, personal digital assistants (PDAs), key fobs, transponder devices, NFC-enabled devices, and/or computers. Each type of payment card can be used as a method of payment for performing a transaction. In addition, consumer card account behavior can include but is not limited to purchases, management activities (e.g., balance checking), bill payments, achievement of targets (meeting account balance goals, paying bills on time), and/or product registrations (e.g., mobile application downloads).

[0018] Figure 1 is a block diagram showing a data processing system according to an embodiment of the present invention. The data processing system 100 processes payment card transactions carried out by a cardholder 110 at a merchant 120. The merchant may be a so-called ‘bricks and mortar’ merchant having physical premises or alternatively may be an on-line merchant. A server or point of sale (POS) device associated with the merchant 120 is connected via network to a server associated with an acquiring bank 130.

[0019] A payment network acts as an intermediary during a transaction being made by a cardholder 110 using a payment card at a merchant terminal of a merchant 120. In particular, the cardholder 110 may present the payment card to merchant terminal of merchant 120 as payment for goods or services. The merchant terminal may be a point of sale (POS) device such as a magnetic strip reader, chip reader or contactless payment terminal, or a website having online e-commerce capabilities, for example. A merchant 110 may operate one or a plurality of merchant terminals. The merchant terminal communicates with a system of the acquiring bank 130 or other institution with which the merchant 120 has an established account, in order to request authorisation for the amount of the transaction (sometimes referred to as ticket size) from the system of the acquiring bank 130.

[0020] The system of the acquiring bank 130 routes the transaction authorisation request from the merchant terminal to computer systems of the payment network. The transaction authorisation request is then routed by payment network to computer systems of the appropriate issuer institution, in this case the issuing bank server 140 based on information contained in the transaction authorisation request. The issuer institution associated with the issuing bank server 140 is authorised by the payment network to issue payment devices

such as the payment card of the cardholder 110 to perform transactions over the payment network. The issuer institution associated with the issuing bank server 140 also provides funding of the transaction to the payment network for transactions that are approved.

[0021] The issuing bank server 140 analyses the authorisation request to determine the account number submitted by the cardholder 110, and based on the account number, determine whether the account is in good standing and whether the transaction amount is covered by the cardholder's account balance or available credit. Additionally, the issuing bank server 140 determines using information stored in the merchant validation database whether the merchant 120 has a negative validation indication. This validation indication may be based on whether the merchant 120 has a high risk or fraud. Alternatively, or additionally, this validation indication may be based on reviews or other merchant quality indications stored in the merchant validation database 150. Based on this, the transaction can be approved or declined, and an authorisation response message is transmitted from issuing bank server 140 to via the payment network to the system of the acquiring bank 130. The system of the acquiring bank 130 then sends the authorisation response message to the merchant terminal of the merchant 120. If the authorisation response message indicates that the transaction is approved, then the account of the merchant 120 is credited by the amount of the transaction following subsequent clearing and settlement processes, and the cardholder's account is debited accordingly.

[0022] If the issuing bank server 140 determines that the merchant 120 has a negative validation indication, then an authorization message is sent indicating that the transaction is declined. In addition, the issuing bank server 140 determines an alternative merchant using information stored in an alternative merchant database 160 which is coupled to the issuing bank server 140. It will be appreciated that the merchant validation database 150 and the alternative merchant database 160 may be located on separate physical storage media, or on different logical partitions of a single storage device. In some embodiments, they may be separate logical databases which span multiple storage devices.

[0023] Figure 2 is a block diagram showing a technical architecture of the server of the issuing bank server 200 for performing exemplary methods 300 and 500 which are described below with reference to Figures 3 and 5. Typically, the methods 300 and 500 are implemented by a computer having a data-processing unit. The block diagram as shown Figure 2 illustrates a technical architecture 200 of a computer which is suitable for implementing one or more embodiments herein.

[0024] The technical architecture 200 includes a processor 222 (which may be referred to as a central processor unit or CPU) that is in communication with memory devices including secondary storage 224 (such as disk drives), read only memory (ROM) 226, and random access memory (RAM) 228. The processor 222 may be implemented as one or more CPU chips. The technical architecture 220 may further comprise input/output (I/O) devices 230, and network connectivity devices 232.

[0025] The secondary storage 224 is typically comprised of one or more disk drives or tape drives and is used for non-volatile storage of data and as an over-flow data storage device if RAM 228 is not large enough to hold all working data. Secondary storage 224 may be used to store programs which are loaded into RAM 228 when such programs are selected for execution. In this embodiment, the secondary storage 224 has a merchant validation information look up module 224a, has a merchant validation information analysis module 224b, a transaction authorization response generation module 224c, an alternative merchant determination module 224d; an alternative merchant indication generation module 224e; and a transaction execution module 224f comprising non-transitory instructions operative by the processor 222 to perform various operations of the method of the present disclosure. As depicted in Figure 2, the modules 224a-224f are distinct modules which perform respective functions implemented by the electronic commerce analysis server 200. It will be appreciated that the boundaries between these modules are exemplary only, and that alternative embodiments may merge modules or impose an alternative decomposition of functionality of modules. For example, the modules discussed herein may be decomposed into sub-modules to be executed as multiple computer processes, and, optionally, on multiple computers. Moreover, alternative embodiments may combine multiple instances of a particular module or sub-module. It will also be appreciated that, while a software implementation of the modules 224a-224f is described herein, these may alternatively be implemented as one or more hardware modules (such as field-programmable gate array(s) or application-specific integrated circuit(s)) comprising circuitry which implements equivalent functionality to that implemented in software. The ROM 226 is used to store instructions and perhaps data which are read during program execution. The secondary storage 224, the RAM 228, and/or the ROM 226 may be referred to in some contexts as computer readable storage media and/or non-transitory computer readable media.

[0026] I/O devices 230 may include printers, video monitors, liquid crystal displays (LCDs), plasma displays, touch screen displays, keyboards, keypads, switches, dials, mice, track balls, voice recognizers, card readers, paper tape readers, or other well-known input devices.

[0027] The network connectivity devices 232 may take the form of modems, modem banks, Ethernet cards, universal serial bus (USB) interface cards, serial interfaces, token ring cards, fiber distributed data interface (FDDI) cards, wireless local area network (WLAN) cards, radio transceiver cards that promote radio communications using protocols such as code division multiple access (CDMA), global system for mobile communications (GSM), long-term evolution (LTE), worldwide interoperability for microwave access (WiMAX), near field communications (NFC), radio frequency identity (RFID), and/or other air interface protocol radio transceiver cards, and other known network devices. These network connectivity devices 232 may enable the processor 222 to communicate with the Internet or one or more intranets. With such a network connection, it is contemplated that the processor 222 might receive information from the network, or might output information to the network in the course of performing the above-described method operations. Such information, which is often represented as a sequence of instructions to be executed using processor 222, may be received from and outputted to the network, for example, in the form of a computer data signal embodied in a carrier wave.

[0028] The processor 222 executes instructions, codes, computer programs, scripts which it accesses from hard disk, floppy disk, optical disk (these various disk based systems may all be considered secondary storage 224), flash drive, ROM 226, RAM 228, or the network connectivity devices 232. While only one processor 222 is shown, multiple processors may be present. Thus, while instructions may be discussed as executed by a processor, the instructions may be executed simultaneously, serially, or otherwise executed by one or multiple processors.

[0029] Although the technical architecture 200 is described with reference to a computer, it should be appreciated that the technical architecture may be formed by two or more computers in communication with each other that collaborate to perform a task. For example, but not by way of limitation, an application may be partitioned in such a way as to permit concurrent and/or parallel processing of the instructions of the application. Alternatively, the data processed by the application may be partitioned in such a way as to permit concurrent and/or parallel processing of different portions of a data set by the two or more computers. In an embodiment, virtualization software may be employed by the technical architecture 200 to provide the functionality of a number of servers that is not directly bound to the number of computers in the technical architecture 200. In an embodiment, the functionality disclosed above may be provided by executing the application and/or applications in a cloud computing environment. Cloud computing may

comprise providing computing services via a network connection using dynamically scalable computing resources. A cloud computing environment may be established by an enterprise and/or may be hired on an as-needed basis from a third party provider.

[0030] It is understood that by programming and/or loading executable instructions onto the technical architecture 200, at least one of the CPU 222, the RAM 228, and the ROM 226 are changed, transforming the technical architecture 200 in part into a specific purpose machine or apparatus having the novel functionality taught by the present disclosure. It is fundamental to the electrical engineering and software engineering arts that functionality that can be implemented by loading executable software into a computer can be converted to a hardware implementation by well-known design rules.

[0031] Various operations of an exemplary method 300 will now be described with reference to Figure 3 in respect of processing a transaction authorization request. It should be noted that enumeration of operations is for purposes of clarity and that the operations need not be performed in the order implied by the enumeration.

[0032] In step 302, the issuing bank server 140 receives a transaction authorization request. As described above in relation to Figure 1, the transaction authorization request relates to a transaction between a cardholder 110 and a merchant 120. The merchant 120 may be an online merchant or a physical ‘bricks and mortar’ merchant. The transaction authorization request includes an indication of the merchant 120 and also other details of the transaction.

[0033] In step 304, the merchant validation information look up module 224a of the issuing bank server 140 looks up merchant validation information for the merchant 120. The merchant validation information look up module 224a may use the indication of the merchant included in the transaction authorization request to identify the merchant and look up validation information for the merchant in the merchant validation database 150. The merchant validation database 150 may include a merchant fraud rating and / or review ratings for the merchant 120.

[0034] In step 306, the merchant validation information analysis module 224b of the issuing bank server 140 analyses the merchant validation information. The analysis carried out in step 306 may comprise comparing a fraud risk rating with a threshold or determining if a fraud risk flag is present for the merchant 120. Alternatively, or additionally, the analysis may comprise comparing a review rating with a threshold. The threshold may be set by the issuer.

[0035] In the analysis carried out in step 306, the merchant validation information analysis module 224b of the issuing bank server 140 determines whether the merchant 120 has a positive merchant validation indication or a negative merchant validation indication. As discussed above, a negative merchant validation indication indicates that the merchant 120 has a high risk or fraud and / or that the reviews or ratings of the merchant 120 do not meet the threshold.

[0036] If in step 306 the merchant validation information analysis module 224b of the issuing bank server 140 determines that the merchant 120 has a positive merchant validation indication, the method moves to step 308.

[0037] In step 308, the transaction authorization response generation module 224c of the issuing bank server 140 generates a transaction response indicating that the transaction is approved. As discussed above, in some embodiments the status of the account of the cardholder 110 is checked to ensure that sufficient funds are available or that there is sufficient remaining credit before the response indicating that the transaction is approved is generated.

[0038] If in step 306 the merchant validation information analysis module 224b of the issuing bank server 140 determines that the merchant 120 has a negative merchant validation indication, the method moves to step 310.

[0039] In step 310, the transaction authorization response generation module 224c of the issuing bank server 140 generates a transaction response indicating that the transaction is declined. The method then moves to step 312

[0040] In step 312, the alternative merchant determination module 224d of the issuing bank server 140 determines an alternative merchant. The alternative merchant determination module 224d uses the alternative merchant database 160 to identify an alternative merchant or a selection of alternative merchants.

[0041] In step 314, the alternative merchant indication generation module 224e of the issuing bank server 140 generates an indication of the alternative merchant or alternative merchants and sends this to the cardholder; alternatively, the transaction execution module 224f of the issuing bank server 140 may execute a transaction at the alternative merchant. When the transaction is an on-line or electronic commerce transaction, it is envisaged that in some embodiments the issuing bank sever 140 may store customer preferences indicating whether a transaction is executed by the transaction execution module 224f or whether an

indication of the alternative merchant is sent to the cardholder. In situations where the merchant 120 is a physical or 'bricks and mortar' merchant, the alternative merchant indication generation module 224e will generate an indication that is sent to the cardholder, for example by text message or email using contact details stored by or accessible by the issuing bank server 140.

[0042] Figure 4 shows a block diagram of a data processing system for processing a transaction authorization request according to an embodiment of the present invention. The system 400 shown in Figure 4 processes a transaction authorization request which corresponds to an online or electronic commerce transaction.

[0043] As shown in Figure 4, a customer device 410 such as a computer, smart phone, or tablet device executes a browser or app 412 which allows a user to access electronic commerce websites via the internet. The browser or app 412 allows the user to access an electronic commerce website provided by an online merchant server 420. The online merchant server 420 is connected via a network to an acquiring bank server 430 and the acquiring bank server 430 is connected via a payment network to an issuing bank server 440. The processing of transaction authorization requests by the online merchant server 420 and the acquiring bank server 430 is as described above with reference to Figure 1.

[0044] Further, as shown in Figure 4, the browser or app 414 running on the customer device 410 provides booking or order information 414 to the issuing bank server 440. The booking or order information 414 may comprise an indication of a basket content comprising a list of items which the customer is purchasing with the transaction being processed. If the purchase relates to a booking for a service such as a travel ticket or hotel booking, the booking or order information may comprise details of the times and dates of travel, number of passengers, class of travel, airline, name of hotel, room facilities, star level of the hotel and other details of the booking in addition to cost.

[0045] The issuing bank server 460 stores indications of cardholder preferences 442. The cardholder preferences specify how the method will progress in the event that the initial transaction authorization request is declined. For example, the cardholder preferences 442 may specify whether the customer should be provided with details of alternative merchants or whether the issuing bank server 440 should automatically execute a transaction at an alternative merchant in the event that the initial transaction authorization request is declined. The customer preferences may also specify how alternative merchants are selected. For example when the transaction relates to a hotel booking, the cardholder preferences 442

may specify for example how close to the location of the hotel in the initial transaction authorization request the alternative hotels must be. The cardholder preferences 442 may also specify other parameters of the booking which may be varied and by how much those parameters may be varied. Similarly, when the transaction relates to the purchase of an airline ticket, the cardholder preferences may specify parameters of the booking such as the name of the airline, the travel times and dates, the class of travel and by how much these parameters may be varied.

[0046] While the cardholder preferences 442 are shown in Figure 4 as being stored on the issuing bank server 440, it is envisaged that in embodiments of the present invention the cardholder preferences 442 may be stored on another server and accessed by the issuing bank server 440 when required.

[0047] The issuing bank server 440 is coupled to a merchant rating / review database 452 and a merchant fraud database 545. The merchant rating / review database 452 stores indications of ratings and reviews of merchants. The merchant fraud database 454 stores indications of fraud risks associated with merchants.

[0048] The issuing bank server 460 is also coupled to an alternative merchant database 460. The alternative merchant database 460 stores products and / or offers 462 for merchants.

[0049] Various operations of an exemplary method 500 will now be described with reference to Figure 5 in respect of processing a transaction authorization request. In the embodiment described with reference to Figure 5, the transaction authorization request relates to an online transaction. It should be noted that enumeration of operations is for purposes of clarity and that the operations need not be performed in the order implied by the enumeration.

[0050] In step 502, the issuing bank server 440 receives a transaction authorization request. As described above, the transaction authorization request relates to a transaction between a customer associated with a customer device 410 and a merchant 420. In this embodiment the merchant 420 is an online merchant. The transaction authorization request includes an indication of the merchant 420 and also other details of the transaction.

[0051] In step 504, the merchant validation information look up module 224a of the issuing bank server 440 looks up merchant validation information for the merchant 420. The merchant validation information look up module 224a may use the indication of the merchant included in the transaction authorization request to identify the merchant and look

up validation information for the merchant in the merchant rating / review database and / or the merchant fraud database 454.

[0052] In step 506, the merchant validation information analysis module 224b of the issuing bank server 440 analyses the merchant validation information. The analysis carried out in step 506 may comprise comparing a fraud risk rating with a threshold or determining if a fraud risk flag is present for the merchant 420. Alternatively, or additionally, the analysis may comprise comparing a review rating with a threshold. The threshold may be set by the issuer or may be set by the cardholder. In some embodiments this threshold may be stored as part of the cardholder preferences 442 stored on the issuing bank server 440.

[0053] If in step 506 the merchant validation information analysis module 224b of the issuing bank server 440 determines that the merchant 420 has a positive merchant validation indication, the method moves to step 508.

[0054] In step 508, the transaction authorization response generation module 224c of the issuing bank server 440 generates a transaction response indicating that the transaction is approved. As discussed above, in some embodiments the status of the account of the cardholder is checked to ensure that sufficient funds are available or that there is sufficient remaining credit before the response indicating that the transaction is approved is generated.

[0055] If in step 506 the merchant validation information analysis module 224b of the issuing bank server 440 determines that the merchant 420 has a negative merchant validation indication, the method moves to step 510.

[0056] In step 510, the transaction authorization response generation module 224c of the issuing bank server 440 generates a transaction response indicating that the transaction is declined. The method then moves to step 511.

[0057] In step 511, the issuing bank server 440 receives customer booking / order information 414 corresponding to the transaction authorization request from the app / browser running on the customer device 410. As described above, the customer booking / order information 414 indicates details of the booking made by the customer or the basket content of the order made by the customer.

[0058] In step 512, the alternative merchant determination module 224d of the issuing bank server 440 determines an alternative merchant. The alternative merchant determination module 224d uses the alternative merchant database 460 to identify an alternative merchant

or a selection of alternative merchants. In step 512, the alternative merchant determination module 224d of the issuing bank server 440 searches the products / offers 462 stored in the alternative merchant database 460 to find products or offers that match the booking / order of the customer as indicated by the booking order information 414 within the variation indicated by the cardholder preferences 442. For example, if the purchase relates to a hotel booking, the alternative merchant determination module 224d of the issuing bank server 440 may search the alternative merchant database 460 for hotels within a distance of, for example 5km of the location of the hotel in the initial booking; having a star rating that matches the star rating of the hotel of the initial booking; for a stay matching the stay of the initial booking; with a price within +/- 10% of the price of the initial booking.

[0059] For different types of purchase, different parameters may be defined in the cardholder preferences 462. For example, the cardholder preferences 462 may define like attributes such as reviews, ratings, discount, cost, distance, delivery time when the purchase relates to a goods purchase, and / or an indication of merchant credibility etc. The purchase types may include goods, for example from an on-line retailer, hotels, restaurant, movies and entertainment, tours and travel.

[0060] In step 514, the alternative merchant indication generation module 224e of the issuing bank server 540 generates an indication of the alternative merchant or alternative merchants and sends this to the cardholder; alternatively, the transaction execution module 224f of the issuing bank server 440 may execute a transaction at the alternative merchant.

[0061] The cardholder preferences 442 may indicate whether a transaction is executed by the transaction execution module 224f or whether an indication of the alternative merchant is sent to the cardholder. The indication of the alternative merchant may be sent as a link to a webpage which includes details of the order / booking at the alternative merchant so that the cardholder can quickly accept the transaction. In some embodiments where more than one alternative merchant is identified or where multiple possible alternative bookings or orders at the same merchant are identified, these may be presented to the cardholder to select one.

[0062] Whilst the foregoing description has described exemplary embodiments, it will be understood by those skilled in the art that many variations of the embodiment can be made within the scope and spirit of the present invention.

Claims

1. A computer implemented method of processing a transaction authorization request, the method comprising:

receiving a transaction authorization request at an issuer server, the transaction authorization request comprising a merchant identifier indicating a merchant associated with the transaction authorization request;

looking up merchant validation information associated with the merchant in a merchant validation database using the merchant identifier;

analyzing the merchant validation information to identify if the merchant has a negative validation indication; and

if the merchant has a negative validation indication:

generating a transaction authorization response indicating that the transaction is declined;

receiving booking or order information indicating parameters of a purchase relating to the transaction authorization request; and

determining an alternative merchant using the booking or order information, cardholder preferences indicating acceptable variations to the parameters of the purchase, and an alternative merchant database coupled to the issuer server.

2. The computer-implemented method according to claim 1, wherein the transaction authorization request relates to an electronic commerce transaction, and wherein the booking or order information comprises an indication of a customer order associated with the transaction authorization request.

3. The computer-implemented method according to claim 2, wherein the indication of the customer order comprises an indication of a parameter of the customer order and wherein determining an alternative merchant comprises searching the alternative merchant database using the parameter of the customer order.

4. The computer-implemented method according to claim 3 wherein searching the alternative merchant database using the parameter of the customer order comprises searching the alternative merchant database for merchants having a product offer having a parameter which matches the parameter of the customer order within an acceptable variation.

5. The computer-implemented method according to any preceding claim wherein the merchant validation information indicates a risk of fraud at the merchant.
6. The computer-implemented method according to any preceding claim wherein the merchant validation information indicates a rating of the merchant.
7. The computer-implemented method according to claim 6, wherein analyzing the merchant validation indication to identify if the merchant has a negative validation indication comprises comparing the rating with a threshold.
8. The computer-implemented method according to any preceding claim, further comprising sending an indication of the alternative merchant to a customer associated with the transaction authorization request.
9. The computer-implemented method according to any one of claims 1 to 7, further comprising executing a transaction with the alternative merchant.
10. A non-transitory computer readable medium having stored thereon program instructions for causing at least one processor to perform the computer-implemented method according to any preceding claim.
11. A system for processing a transaction authorization request, the system comprising:
 - a computer processor and a data storage device, the data storage device having a merchant validation information look up module; a merchant validation information analysis module; a transaction authorization response generation module; and an alternative merchant determination module comprising non-transitory instructions operative by the processor to:
 - receive a transaction authorization request at an issuer server, the transaction authorization request comprising a merchant identifier indicating a merchant associated with the transaction authorization request;
 - look up merchant validation information associated with the merchant in a merchant validation database using the merchant identifier;
 - analyze the merchant validation information to identify if the merchant has a negative validation indication; and

if the merchant has a negative validation indication:

generate a transaction authorization response indicating that the transaction is declined;

receive booking or order information indicating parameters of a purchase relating to the transaction authorization request; and

determine an alternative merchant using the booking or order information, cardholder preferences indicating acceptable variations to the parameters of the purchase, and an alternative merchant database coupled to the issuer server.

12. The system according to claim 11, wherein the transaction authorization request relates to an electronic commerce transaction, and wherein the booking or order information comprises an indication of a customer order associated with the transaction authorization request.

13. The system according to claim 12, wherein the indication of the customer order comprises an indication of a parameter of the customer order and wherein the alternative merchant determination module further comprises non-transitory instructions operative by the processor to: determine an alternative merchant by searching the alternative merchant database using the parameter of the customer order.

14. The system according to claim 13, wherein the searching the alternative merchant database using the parameter of the customer order comprises searching the alternative merchant database for merchants having a product offer having a parameter which matches the parameter of the customer order within an acceptable variation.

15. The system according to any one of claims 11 to 14 wherein the merchant validation information indicates a risk of fraud at the merchant.

16. The system according to any one of claims 11 to 15 wherein the merchant validation information indicates a rating of the merchant.

17. The system according to claim 16, wherein the merchant validation information analysis module further comprises non-transitory instructions operative by the processor to: analyze the merchant validation indication to identify if the merchant has a negative validation indication by comparing the rating with a threshold.

18. The system according to any one of claims 11 to 17, further comprising an alternative merchant indication generation module comprising non-transitory instructions operative by the processor to: send an indication of the alternative merchant to a customer associated with the transaction authorization request.

19. The system according to any one of claims 11 to 17, further comprising a transaction execution module comprising non-transitory instructions operative by the processor to: execute a transaction with the alternative merchant.