Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2641676 A1 2007/09/13

(21) 2 641 676

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(86) Date de dépôt PCT/PCT Filing Date: 2007/03/02
(87) Date publication PCT/PCT Publication Date: 2007/09/13
(85) Entrée phase nationale/National Entry: 2008/08/06
(86) N° demande PCT/PCT Application No.: US 2007/063239
(87) N° publication PCT/PCT Publication No.: 2007/103831
(30) Priorité/Priority: 2006/03/02 (US60/778,282)

(51) Cl.Int./Int.Cl. *G06Q 99/00* (2006.01),
H04L 9/00 (2006.01)

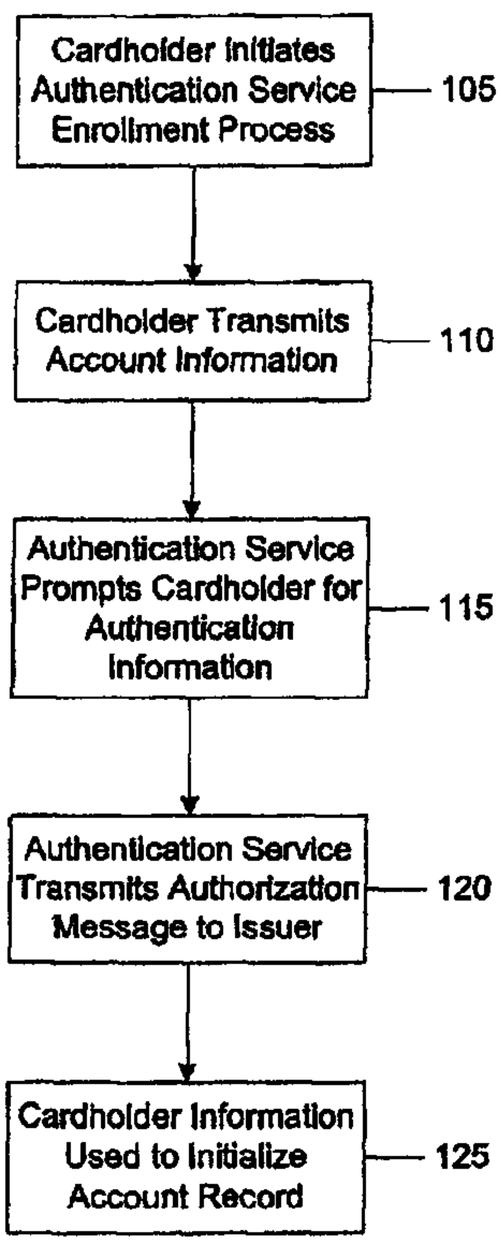
(71) Demandeur/Applicant:
VISA INTERNATIONAL SERVICE ASSOCIATION, US

(72) Inventeurs/Inventors:
DOMINGUEZ, BENEDICTO H., US;
FISHER, DOUGLAS, US;
LEE, TIMOTHY MU-CHU, SG

(74) Agent: DE FAZEKAS, ANTHONY

(54) Titre : PROCEDE ET SYSTEME DE REALISATION D'AUTHENTIFICATION A DEUX FACTEURS DANS DES TRANSACTIONS DE VENTE PAR CORRESPONDANCE OU DE VENTE PAR TELEPHONE

(54) Title: METHOD AND SYSTEM FOR PERFORMING TWO FACTOR AUTHENTICATION IN MAIL ORDER AND TELEPHONE ORDER TRANSACTIONS



(57) Abrégé/Abstract:
The method for authenticating a mail order or telephone order transaction according to the present invention includes receiving authentication information from a cardholder, providing authentication information to an issuer, and determining whether the authentication information is valid. If the authentication information is valid, the issuer informs the merchant that the transaction is valid. In an embodiment, the issuer may not supply a personal assurance message and/or other confidential cardholder information previously supplied by the cardholder in response to the authentication information.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 September 2007 (13.09.2007)

PCT

(10) International Publication Number
WO 2007/103831 A3

(51) International Patent Classification:
G06Q 99/00 (2006.01) *H04L 9/00* (2006.01)

(21) International Application Number:
PCT/US2007/063239

(22) International Filing Date: 2 March 2007 (02.03.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/778,282 2 March 2006 (02.03.2006) US

(71) Applicant *(for all designated States except US)*: **VISA INTERNATIONAL SERVICE ASSOCIATION** [US/US]; 900 Metro Blvd., Foster City, CA 94404 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **DOMINGUEZ, Benedicto, H.** [US/US]; 2830 Merion Drive, San Bruno, CA 94066 (US). **FISHER, Douglas** [US/US]; 1121 Bruckner Circle, Mountain View, CA 94040 (US). **LEE, Timothy, Mu-chu** [US/SG]; c/o Visa International Service Association, 30 Raffles Place #10-00, Singapore, 048622.

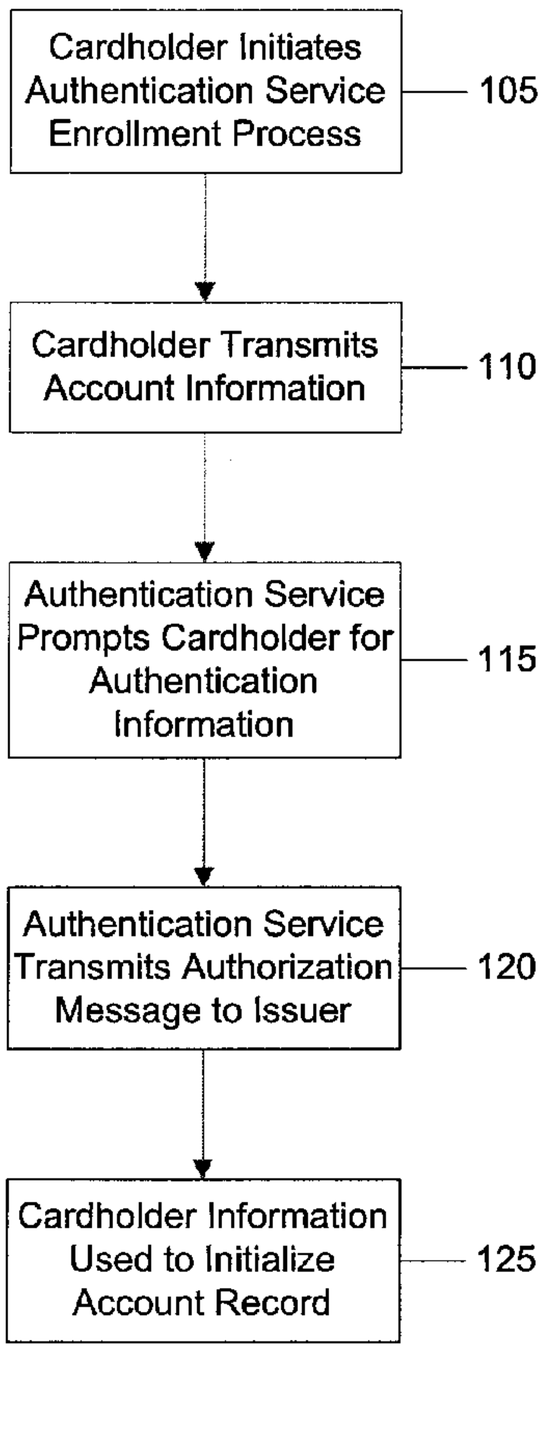
(74) Agent: **MOLANO, Michael, A.**; Mayer, Brown, Rowe & Maw Llp, P.O. Box 2828, Chicago, IL 60690-2828 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: METHOD AND SYSTEM FOR PERFORMING TWO FACTOR AUTHENTICATION IN MAIL ORDER AND TELEPHONE ORDER TRANSACTIONS



(57) Abstract: The method for authenticating a mail order or telephone order transaction according to the present invention includes receiving authentication information from a cardholder, providing authentication information to an issuer, and determining whether the authentication information is valid. If the authentication information is valid, the issuer informs the merchant that the transaction is valid. In an embodiment, the issuer may not supply a personal assurance message and/or other confidential cardholder information previously supplied by the cardholder in response to the authentication information.

WO 2007/103831 A3

WO 2007/103831 A3

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report:
15 November 2007

METHOD AND SYSTEM FOR PERFORMING TWO FACTOR AUTHENTICATION IN MAIL ORDER AND TELEPHONE ORDER TRANSACTIONS

REFERENCE TO RELATED APPLICATIONS

The application claims priority to U.S. Application Serial No. 60/778,282, entitled "Method and System for Performing Two Factor Authentication in Mail Order and Telephone Order Transactions," filed March 2, 2006.

BACKGROUND

[0001] During a transaction using a transaction card, such as a credit card, a debit card, a stored value card, a bank card, a loyalty card, a smart card and/or the like, it is important to verify a cardholder's ownership of an account to avoid a variety of problems, such as unauthorized use. Cardholder authentication is the process of verifying such ownership by the cardholder. For example, cardholder authentication during a "card present" transaction is performed when a merchant's representative verifies that the signature on a transaction card matches the cardholder's signature on a receipt.

[0002] Technological improvements have allowed businesses and individuals to engage in transactions in a plurality of environments. For example, cardholders can engage in traditional "in person" transactions, transactions via the Internet, transactions over the telephone and transactions through mail systems. In many cases, cardholders desire the convenience of performing transactions without having to directly visit a service provider. In doing so, the cardholder may seek to eliminate driving time and reduce the hassle associated with, for example, shopping in a retail environment or waiting in line at a bank by performing these transactions from the privacy of their own home.

[0003] "Card not present" ("CNP") transaction volumes are increasing at least in part because of such convenience provided to cardholders and the extra sales provided to merchants. However, as CNP transaction volumes increase, fraudulent transactions and the monetary losses due to such transactions are increasing as well.

[0004] Various solutions have been proposed to make ecommerce and/or online banking transactions more secure, such as two-factor authentication (e.g., by GPayment Pty. Ltd.), dynamic passcodes (e.g., by Barclay PLC) and token authentication (e.g., by MasterCard International Inc.). However, these technological solutions have not been implemented for mail order and telephone order ("MOTO") transactions due to unique challenges presented by such transactions.

[0005] For example, security weaknesses can arise when MOTO transactions use static passcodes. An unauthorized third party can obtain the static passcode by intercepting a transaction and reverse engineering the transmitted data to determine the account information and passcode. The unauthorized third party can be, for example, a person intercepting information passed between a cardholder and a merchant or between a merchant and an issuer. Alternatively, the unauthorized third party can be the merchant and/or its representative.

[0006] Solutions used to increase security include the use of static data, such as information stored in the Card Verification Value 2 ("CVV2") field of a transaction card, information from an address verification service, expiry dates, authorization controls and the like. The CVV2 field demonstrates that a cardholder is in possession of the transaction card. When the cardholder provides the CVV2 information to the merchant, the merchant includes the CVV2 in an authorization request to the issuer, and the authorization response advises the merchant whether the CVV2 information provided is valid.

[0007] One disadvantage of such static authentication measures is that the authentication value does not change for each transaction. Accordingly, a third party that has access to the card for even a short period of time may be able to copy the information and use it without the cardholder's knowledge.

[0008] Another disadvantage of static authentication measures is that such measures typically verify only the transaction card's presence as opposed to authenticating the cardholder. However, cardholder authentication provides stronger security than transaction card verification. For example, cardholder authentication provides card issuers with sufficient non-repudiation evidence to warrant providing merchant chargeback protection, while transaction card authentication does not.

[0009] Dynamic authentication technologies have also been devised to facilitate cardholder authentication in MOTO environments. Such technologies include voice authentication, sound authentication (i.e., transaction cards that generate dynamic sounds) and dynamic passcodes. One disadvantage of such dynamic authentication technologies is that they only represent one piece of the required solution needed to implement a MOTO authentication solution. Such technologies do not represent a solution to the infrastructure layer whereby merchants receive authentication data from cardholders and transmit such data to transaction card issuers. Merchants would need to implement systems to accept and forward the dynamic information. Moreover, acquirers would need to implement systems to pass dynamic information to the transaction card issuer.

[0010] Accordingly, cardholders and merchants are concerned that fraudulent MOTO transactions occur frequently and that information in non-fraudulent transactions can be stolen for fraudulent purposes. What is needed is a method and system for inhibiting unauthorized accesses to MOTO transactions.

[0011] A need exists for a method and system that permits a MOTO transaction to be performed securely.

[0012] A further need exists for a method and system of performing two-factor authentication in a MOTO environment to inhibit fraudulent access to MOTO transactions.

[0013] The present disclosure is directed to solving one or more of the above-listed problems.

SUMMARY

[0014] Before the present methods, systems and materials are described, it is to be understood that this invention is not limited to the particular methodologies, systems and materials described, as these may vary. It is also to be understood that the terminology used in the description is for the purpose of describing the particular versions or embodiments only, and is not intended to limit the scope of the invention which will be limited only by the appended claims.

[0015] It must also be noted that as used herein and in the appended claims, the singular forms "a," "an," and "the" include plural references unless the context clearly dictates otherwise. Thus, for example, reference to a "cardholder" is a reference to one or more parties involved in an exchange of value, data and/or information. Unless expressly stated otherwise, all undefined technical and scientific terms used herein have the same meanings as commonly understood by one of ordinary skill in the art, while all defined technical and scientific terms shall be deemed to include the same meaning as commonly understood by one of ordinary skill in the art with the stated definition. Although any methods, materials and devices similar or equivalent to those described herein can be used, the preferred methods, materials and devices are now described. All publications mentioned

herein are incorporated by reference. Nothing herein is to be construed as an admission that the invention is not entitled to antedate such disclosure by virtue of prior invention.

[0016] In an embodiment, a method for authenticating a mail order or telephone order transaction may include receiving authentication information by a merchant from a cardholder, providing authentication information to an issuer, and determining, by the issuer, whether the authentication information is valid. If the authentication information is valid, the issuer may inform the merchant that the transaction is valid. Otherwise, the issuer may inform the merchant that the authentication information is invalid. In an embodiment, the authentication information may include information such as a dynamic passcode, a static passcode, biometrics, or any other information that may be used to authenticate a transaction card, an account or a cardholder. For example, such information may include a sound, sound biometrics, a business identification, a country code, a card account number, a card expiration date, a cardholder name, issuer-specific authentication data specified in the "participating BIN" data (e.g., mother's maiden name), a billing address, a shipping address, a social security number, a telephone number, an account balance, a transaction history and/or a driver's license number. In an embodiment, the issuer may determine whether a merchant initiated the authentication as part of a MOTO transaction. In an embodiment, the issuer may not supply a personal assurance message and/or other cardholder information previously supplied by the cardholder in response to the authentication information if the merchant transmitted the information.

BRIEF DESCRIPTION OF THE DRAWINGS

[0017] Aspects, features, benefits and advantages of the embodiments of the present invention will be apparent with regard to the following description, appended claims and accompanying drawings where:

[0018] FIG. 1 illustrates an exemplary process for registering a cardholder with an authentication service according to an embodiment.

[0019] FIG. 2 depicts an exemplary process for an authenticated payment transaction according to an embodiment.

[0020] FIG. 3 depicts a flow diagram of an exemplary process for authenticating a MOTO transaction according to an embodiment.

[0021] FIG. 4 depicts a flow diagram of an exemplary process for authenticating a MOTO transaction according to a preferred embodiment.

DETAILED DESCRIPTION

[0022] Exemplary methods for setting up, authorizing, registering and securely transacting in an online environment will now be described. Initially, an authentication service may be set up. Setting up the authentication service may involve performing initialization procedures for each participant in a system. These participants may include a plurality of entities, such as merchants, financial institutions (i.e., issuers), acquirers and cardholders. A merchant who signs up with the authentication service may receive a merchant plug-in software module for an online environment. In an embodiment, the plug-in software module may be designed specifically for the merchant's computing platform and commerce server software. Issuers participating in the authentication service may provide bank logos and marketing designs for incorporation into a customized authentication service enrollment site template. Acquirers may also provide the merchant with a service organization certification authority ("CA") root certificate, a service organization certification authority SSL certificate for client authentication and/or integration support.

[0023] Before an issuer uses the authentication service, the issuer may obtain a copy of authentication software programs specified in the issuer domain and may install hardware

systems and the authentication service software. Issuers may also provide identity authentication policies and participating business identification number (BIN) information to the authentication service to be used in cardholder verification processes. In an embodiment, an issuer may provide authentication information to the authentication service. Pre-loading of authentication information may facilitate large volume support of cardholders. For example, when an issuer desires to activate all or most of its cardholders for the authentication service, the issuer may assign a Personal Identification Number ("PIN") to each of its cardholders. Each cardholder may then use the assigned PIN to access authentication information. In this manner, the enrollment process may be expedited because each cardholder may not be required to complete a formal enrollment process.

[0024] Authentication information may include information such as a dynamic passcode, a static passcode, biometrics, or any other information that may be used to authenticate a transaction card, an account or a cardholder. For example, such information may include a sound, sound biometrics, a business identification, a country code, a card account number, a card expiration date, a cardholder name, issuer-specific authentication data specified in the "participating BIN" data (e.g., mother's maiden name), a billing address, a shipping address, a social security number, a telephone number, an account balance, a transaction history and/or a driver's license number. Issuers may provide account number ranges for their card account portfolios and access control server ("ACS") IP addresses or Uniform Resource Locators ("URLs") to the directory server. In an embodiment, the authentication service may be offered through bank-branded Web sites, which allow cardholders to register with the authentication service. In an alternate embodiment, information may be transmitted via a mail service, over the telephone and/or via any other communication means.

[0025] FIG. 1 illustrates an exemplary process for registering a cardholder with an authentication service according to an embodiment. As shown in FIG. 1, a cardholder may visit **105** an enrollment Web site maintained by an issuer. In an alternate embodiment, a cardholder may contact an issuer by telephone, mail and/or other communication means. A cardholder may register with the authentication service by supplying one or more transaction card account numbers to the service. The cardholder may transmit **110** information, such as a primary account number ("PAN"), the cardholder's name, a card expiration date, an address, an e-mail address, a shopper identification value, an account verification value, a cardholder-specific password and/or authentication information.

[0026] After the cardholder sends the requested information to the authentication service, the service may verify that the cardholder's PAN falls within a card range registered by the issuer. The authentication service may further verify a cardholder's identity using, for example, an authentication database maintained by a third party and/or the issuer. In an embodiment, the issuer may verify a cardholder's identity using an issuer-provided file of approved cardholders. In an embodiment, the issuer may verify a cardholder's identity by analyzing status check authorizations. In an embodiment, the issuer may verify a cardholder's identity by comparing responses to pre-loaded information in the authentication database provided by the issuer.

[0027] If the specified PAN is not within the issuer-enrolled card range, the enrollment may be rejected, and the enrollment process may terminate. If the PAN is within an enrolled card range, an authorization for, for example, one dollar may be submitted through a service organization payment network, such as VisaNet, to the issuer. In an embodiment, the authorization of the one-dollar transaction may permit the issuer to verify the card account status, verify the address using the Address Verification Service, and verify the Card Verification Value 2 ("CVV2"). Alternate or additional information may be verified

during the authorization process. In an embodiment, the CVV2 field may be a 3-digit value that is typically printed on the signature strip of the transaction card.

[0028] If the card is approved, the authentication service may prompt **115** the cardholder for additional authentication information to verify the cardholder's identity. The cardholder may provide a password and a "hint question and response" pair to authenticate the cardholder during subsequent purchase transactions.

[0029] When the cardholder's identity is verified and the appropriate responses are returned, the authentication service may send **120** an authorization message to the issuer. An enrollment server may then pass **125** cardholder information to an ACS to initialize records in an account holder file. The account holder file may store information such as: financial institution BIN numbers, account numbers, expiration dates, first and last names, driver's license numbers, billing addresses, social security numbers, cardholder passwords, cardholder password questions, cardholder password responses, cardholder email addresses, third party identity scores and other information.

[0030] After the authentication service participants are initialized and a cardholder is registered, a payment transaction may be authenticated utilizing the authentication service. FIG. 2 depicts an exemplary process for authenticating an online payment transaction according to an embodiment. As shown in FIG. 2, a cardholder may visit **205** a merchant's ecommerce Web site. After the cardholder selects products or services for purchase, the cardholder may begin a checkout process, complete a checkout form and click on a "purchase" button **210**.

[0031] After the "purchase" button is selected **210**, the merchant plug-in software module may be activated. The merchant plug-in software may perform **215** a verification process to determine whether the cardholder-specified account is registered with the authentication service. Verification may be performed **215** using: i) a process in which a

directory server and the ACS associated with the cardholder are checked, ii) a process in which only the ACS is checked, and/or iii) a process in which the merchant checks a cache memory containing information similar to the directory server.

[0032] The merchant plug-in software module may identify the PAN and query a directory server to verify that the PAN falls within a range of numbers associated with an issuer bank that is an authentication service participant. If the account number does not fall within a range of PANs defined on the directory server, the cardholder is not registered with the authentication service. In this case, the merchant may be notified that the account number is not registered, and the merchant plug-in software module may return control of the transaction to the merchant storefront software. At this point, the merchant storefront software may proceed with the transaction, refuse further service to the cardholder, or proceed with alternative payment methods.

[0033] If the PAN is within a range of PANs accepted by the directory server, the directory may send the PAN to the ACS capable of authenticating the cardholder to determine whether the card is enrolled. If the card is not enrolled, the verification process may be terminated. If the ACS indicates that the card is enrolled, the ACS, via the directory server, may return its URL to the merchant plug-in software module. The merchant plug-in software may invoke the ACS via the cardholder client device and its resident browser. A plurality of ACS's may be stored in the authentication service.

[0034] In an embodiment, the merchant plug-in software may query the ACS to verify the cardholder's registration with the authentication service. In an embodiment, the merchant may access a cache memory containing substantially the same information stored at the directory server to verify the cardholder's registration with the authentication service. In an embodiment, the authentication server may include only one logical directory server, although more than one physical directory server may reside in the authentication service.

[0035] If the cardholder is an authentication service participant, the ACS may display an issuer-branded window to the cardholder. The issuer-branded window may include basic payment transaction information and may prompt the cardholder for authentication information. The cardholder may enter the authentication information for verification by the ACS.

[0036] The payment authentication may continue if the correct authentication information is immediately entered or the correct response is provided to a hint question within an allowed number of attempts. The ACS may digitally sign a receipt using the issuer's signature key and/or a service provider's key. This receipt may include the merchant name, card account number, payment amount and the payment date. A receipt file may store the merchant name, merchant URL, card account number, expiration date, payment amount, payment date, issuer payment signature and/or cardholder authentication verification value. The ACS may then redirect the cardholder to the merchant plug-in software module through the cardholder's browser and may pass the digitally signed receipt and its determination as to whether the cardholder has been authenticated to the merchant. The merchant plug-in software module may use a validation server to verify the digital signature used to sign the payment receipt. After verifying the digital signature, the cardholder may be deemed "authenticated." After the transaction is completed, the cardholder may re-register a transaction card account and/or create new authentication information to be used for future transactions.

[0037] After the cardholder is authenticated, the specific cardholder's account may be authorized. Specifically, the merchant, through the merchant plug-in software module, may send **220** an authorization message to a payment network, such as VisaNet. The payment network may forward the authorization message and an electronic commerce indicator ("ECI") to an issuer. The issuer may receive the authorization message so that the

issuer may verify to the merchant that a specific account is in good standing and has adequate credit available for the requested transaction. The ECI may indicate that the transaction was completed via the Internet so that an appropriate level of message security and authentication may be used.

[0038] After the issuer processes the authorization transaction, control of the purchase transaction may be returned to the merchant's storefront software via the payment network. The issuer may return **225** the authorization response via the payment network to the merchant. The authorization response may either authorize or decline the transaction.

[0039] For a MOTO transaction, a merchant may initiate authentication of the cardholder by redirecting the cardholder to the issuer for the exchange of authentication information. Since the cardholder does not have a direct connection to the issuer in a MOTO transaction, the cardholder may provide authentication information to the merchant. The merchant may then submit the information on behalf of the cardholder. Accordingly, for a MOTO transaction, the merchant may perform functions that a cardholder would typically perform in a "card present" or e-commerce transaction. In an embodiment, the authentication information may be dynamically generated to prevent the merchant from using the authentication information in a fraudulent manner and to otherwise prevent security from being compromised. The transaction system may determine whether a merchant is entering the information instead of the cardholder by requesting information from the merchant. Accordingly, when a MOTO transaction is being performed, sensitive cardholder information, such as a personal assurance message, may not be transmitted to the merchant. In an embodiment, an identifier may denote whether a MOTO transaction is performed.

[0040] Certain functions may not be appropriate to use when a merchant is acting on behalf of the cardholder in a MOTO transaction. For example, functionality that enables a cardholder to generate authentication information during a transaction to verify the

cardholder for future transactions may be disabled when processing a MOTO transaction. Such a feature may be inappropriate when a merchant is performing data entry for a transaction. Likewise, if an issuer tracks the location of the transaction originator for risk mitigation purposes, such functionality may be disabled for a MOTO transaction in which the merchant enters the authentication information.

[0041] FIG. 3 depicts a flow diagram of an exemplary process for authenticating a MOTO transaction according to an embodiment. As shown in FIG. 3, a cardholder may select items from a catalog and finalize **305** a purchase via, for example, a telephone or a mail service. The merchant may send **310** an enrollment request for the purchase to, for example, a directory server. A MOTO transaction indicator may be included with the enrollment request. The indicator may indicate that the transaction is a MOTO transaction and that the cardholder will not be directly providing authentication. If a card number offered by the cardholder to the merchant and transferred to the directory server is within a participating card range **315**, the directory server may transmit **320** the enrollment request to, for example, an appropriate ACS. The ACS may respond **325** to the directory server with an enrollment response that indicates whether authentication is available for the card. If the card number is not in the participating range, the directory server may create **330** an enrollment response denying the transaction. The enrollment response may be sent **335** to the merchant.

[0042] Assuming that authentication is available, the merchant may transmit **340** an authentication request to the ACS via the merchant's browser. The ACS may receive **345** the authentication request and authenticate **350** the cardholder as appropriate for the card number. For example, the cardholder may be required to provide authentication information, a chip cryptogram, a PIN and/or the like. The ACS may determine that the transaction is a MOTO transaction by comparing the cardholder's account identifier with the enrollment request. The ACS may further determine which cardholder information fields are not

confidential to the cardholder and are thus appropriate to display to the merchant. For example, a personal assurance message may not be appropriate for display to the merchant. The ACS may format and digitally sign an authentication response message before transmitting **355** the authentication response to the merchant via the merchant's browser. In an embodiment, the ACS may send the authentication response to an authentication history server for future verification. The merchant may receive **360** the authentication response and validate **365** the authentication response signature. If validated, the merchant may authorize **370** the transaction with its acquirer.

[0043] In an embodiment, the cardholder may be provided with a dynamic method of generating authentication information. The method by which authentication information is generated may vary and may not be explicitly constrained herein. For example, the cardholder may be provided with a printed sheet containing a list of one-time passcodes and/or limited duration passcodes. The cardholder may also be issued a dynamic passcode device, a transaction card and/or a reader that generates a dynamic passcode, and/or a transaction card that utilizes biometrics to generate a dynamic passcode.

[0044] Enhancements over previous methods of performing MOTO transactions may include the enablement of cardholder authentication without significant modifications to an underlying transaction system used in e-commerce and/or online banking environments. As such, the improved MOTO transaction described herein may enhance security without substantial modifications to the underlying infrastructure.

[0045] In an embodiment, a static passcode may be used. This may provide additional convenience for the cardholder. In an embodiment, static passcodes may be used in MOTO transactions for which the cardholder provides the passcode directly to the issuer instead of the merchant.

[0046] FIG. 4 depicts a flow diagram of an exemplary process for authenticating a MOTO transaction according to a preferred embodiment. As shown in FIG. 4, a MOTO operator, on behalf of a consumer, may perform **405** one or more functions using a merchant shopping cart on a merchant web site. In an embodiment, the one or more functions may include one or more of selecting merchandise; adding, removing and/or updating merchandise quantities; and maintaining a running total for selected merchandise. The MOTO operator may then perform **410** a check out process. For example, the MOTO operator, on behalf of the consumer, may enter shipping information, enter payment information, and/or finalize a transaction.

[0047] In an embodiment, a verification process may then be initiated. For example, merchant plug-in software may transmit **415** a Verify Enrollment Request ("VEReq") to an issuer ACS. In an embodiment, the VEReq may include a MOTO transaction indicator that is set for a MOTO transaction. The MOTO transaction indicator may indicate that the transaction is a MOTO transaction, and, thus, that the cardholder will not be directly providing authentication. The ACS may determine **420** whether the MOTO transaction indicator is set in the VEReq. If so, the ACS may respond **425** to the MOTO operator with a Verify Enrollment Response ("VERes") tailored to a MOTO transaction. In an embodiment, the VERes may include information indicating whether authentication is available for the transaction.

[0048] If authentication is available for the card, the MOTO operator may transmit **430** a Payer Authentication Request ("PAReq") to the ACS via the merchant's browser. The ACS may receive **435** the PAReq and may authenticate **440** the cardholder as appropriate based on the card number. In an embodiment, the ACS may recognize an account identifier as a MOTO transaction based on the VEReq/VERes process described above. The ACS may then generate **445** a Payer Authentication Response ("PARes") for transmission to the MOTO

operator. In an embodiment, for a MOTO transaction, the ACS may not transmit sensitive cardholder information, such as a personal assurance message, a password and/or the like. In an embodiment, for a MOTO transaction, the ACS may disable an Activation During Shopping feature that tracks the location of a customer's purchases for fraud detection purposes. The MOTO operator may receive **450** the PARes and, optionally, display information pertaining to the transaction that authenticates the issuer. The MOTO operator may then engage in a transaction authorization process in which monetary value is transferred to the MOTO operator as usual.

[0049] It will be appreciated that various of the above-disclosed and other features and functions, or alternatives thereof, may be desirably combined into many other different systems or applications. It will also be appreciated that various presently unforeseen or unanticipated alternatives, modifications, variations or improvements therein may be subsequently made by those skilled in the art.

1. A method for performing authentication in a mail order or telephone order (MOTO) transaction, the method comprising:

receiving a MOTO purchase order and information pertaining to a transaction card from a cardholder;

transmitting an enrollment request to an authentication server, the enrollment request comprising an indicator indicating that the enrollment request pertains to a MOTO transaction;

receiving an enrollment response from the authentication server, wherein the enrollment response indicates whether authentication is available for the transaction card;

receiving an authentication prompt from the authentication server if authentication is available for the transaction card, wherein the authentication prompt does not include or request sensitive cardholder information;

entering authentication information provided by the cardholder into the authentication prompt; and

receiving an authentication response from the authentication server, the authentication response indicating whether the cardholder is authenticated.

2. The method of claim 1, wherein the authentication response is digitally signed by the authentication server.

3. The method of claim 2, further comprising validating the authentication response.

4. The method of claim 1, wherein the authentication information comprises at least one of a chip cryptogram, a personal identification number, a static passcode, a one-time passcode, or a limited-duration passcode.

5. The method of claim 1, wherein the authentication information comprises a dynamic passcode.

6. The method of claim 1, wherein the transaction is not authorized if the cardholder is not authenticated.

7. The method of claim 1, wherein the sensitive cardholder information comprises a personal assurance message.

8. A method for performing authentication in a mail order or telephone order (MOTO) transaction, the method comprising:

receiving an enrollment request from a merchant, the enrollment request comprising information pertaining to a transaction card and an indicator indicating that the enrollment request pertains to a MOTO transaction;

transmitting an enrollment response to the merchant, the enrollment response indicating whether authentication is available for the transaction card;

transmitting an authentication prompt to the merchant if authentication is available for the transaction card, wherein the authentication prompt does not include or request sensitive cardholder information;

receiving authentication information entered into the authentication prompt; and

transmitting an authentication response to the merchant, the authentication response indicating whether the cardholder is authenticated.

9. The method of claim 8, wherein the authentication response is digitally signed.

10. The method of claim 8, wherein the sensitive cardholder information comprises a personal assurance message.

11. The method of claim 8, wherein the authentication information comprises at least one of a chip cryptogram, a personal identification number, a static passcode, a one-time passcode, or a limited-duration passcode.

12. The method of claim 9, wherein the authentication information comprises a dynamic passcode.

13. The method of claim 8, wherein the transaction is authorized.

14. The method of claim 8, wherein the transaction is not authorized if the cardholder is not authenticated.

15. A method for performing authentication in an online payment transaction using a transaction card in a system comprising a merchant system and an authentication server the method comprising:

receiving a checkout request from a cardholder to initiate a checkout process at the merchant system;

displaying an authentication window to the cardholder prompting the cardholder for authentication information, wherein the window does not include sensitive cardholder information;

transmitting an authentication request to the authentication server, the authentication request including authentication information entered into the window by the cardholder;

receiving an authentication response from the authentication server, the authentication response indicating whether the cardholder is authenticated;

transmitting an authorization request and an indicator indicating that the enrollment request pertains to an electronic commerce transaction to the authentication server; and

receiving an authorization response from the payment network, wherein the authorization indicates whether an account connected to the transaction card is authorized.

16. The method of claim 15, wherein the authentication request includes an account number.

17. The method of claim 15, wherein the authentication information comprises at least one of a chip cryptogram, a personal identification number, a static passcode, a one-time passcode, or a limited-duration passcode.

18. The method of claim 15, wherein the authentication information a dynamic passcode.

19. The method of claim 15, wherein the transaction is authorized.

20. The method of claim 15, wherein the sensitive cardholder information comprises a personal assurance message.

21. The method of claim 15, wherein the transaction is not authorized if the cardholder is not authenticated.

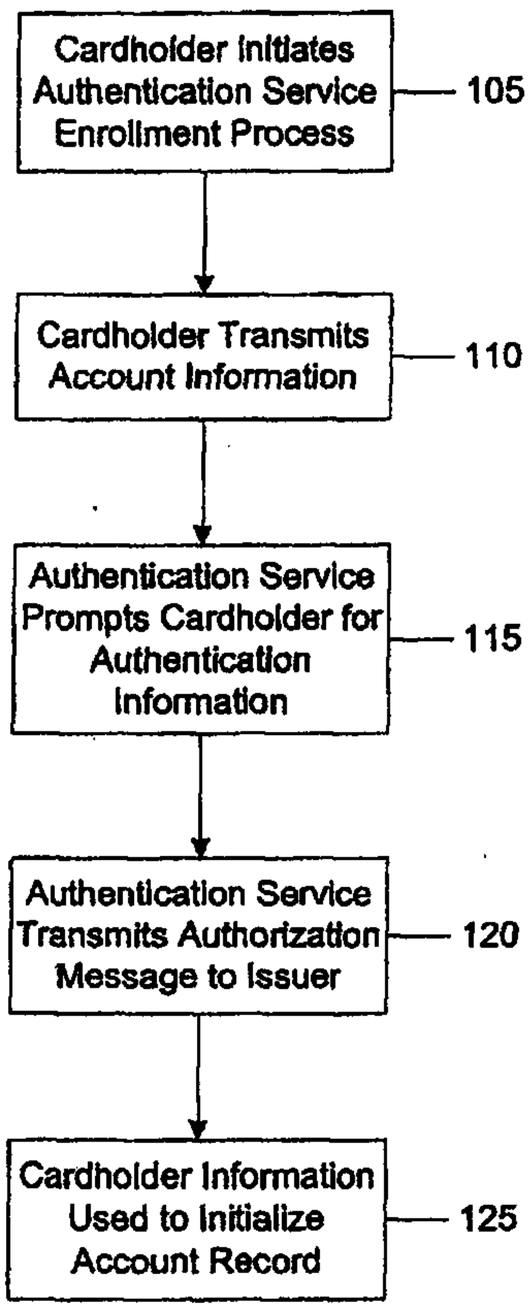

Cardholder Initiates Authentication Service Enrollment Process
105
Cardholder Transmits Account Information
110
Authentication Service Prompts Cardholder for Authentication Information
115
Authentication Service Transmits Authorization Message to Issuer
120
Cardholder Information Used to Initialize Account Record
125

FIG. 1

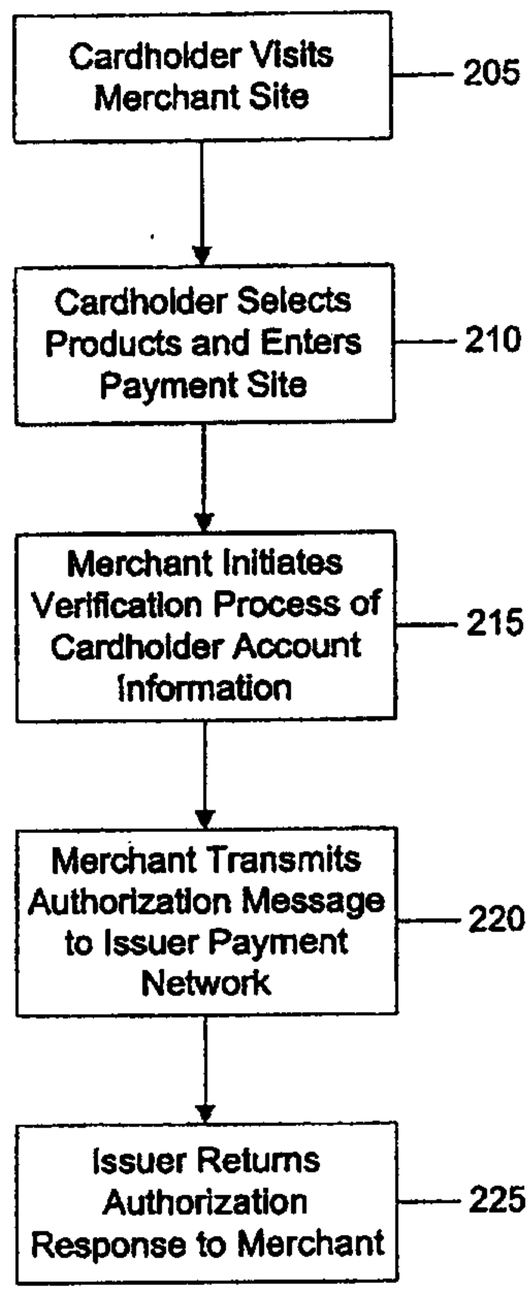

Cardholder Visits Merchant Site
205
Cardholder Selects Products and Enters Payment Site
210
Merchant Initiates Verification Process of Cardholder Account Information
215
Merchant Transmits Authorization Message to Issuer Payment Network
220
Issuer Returns Authorization Response to Merchant
225

FIG. 2

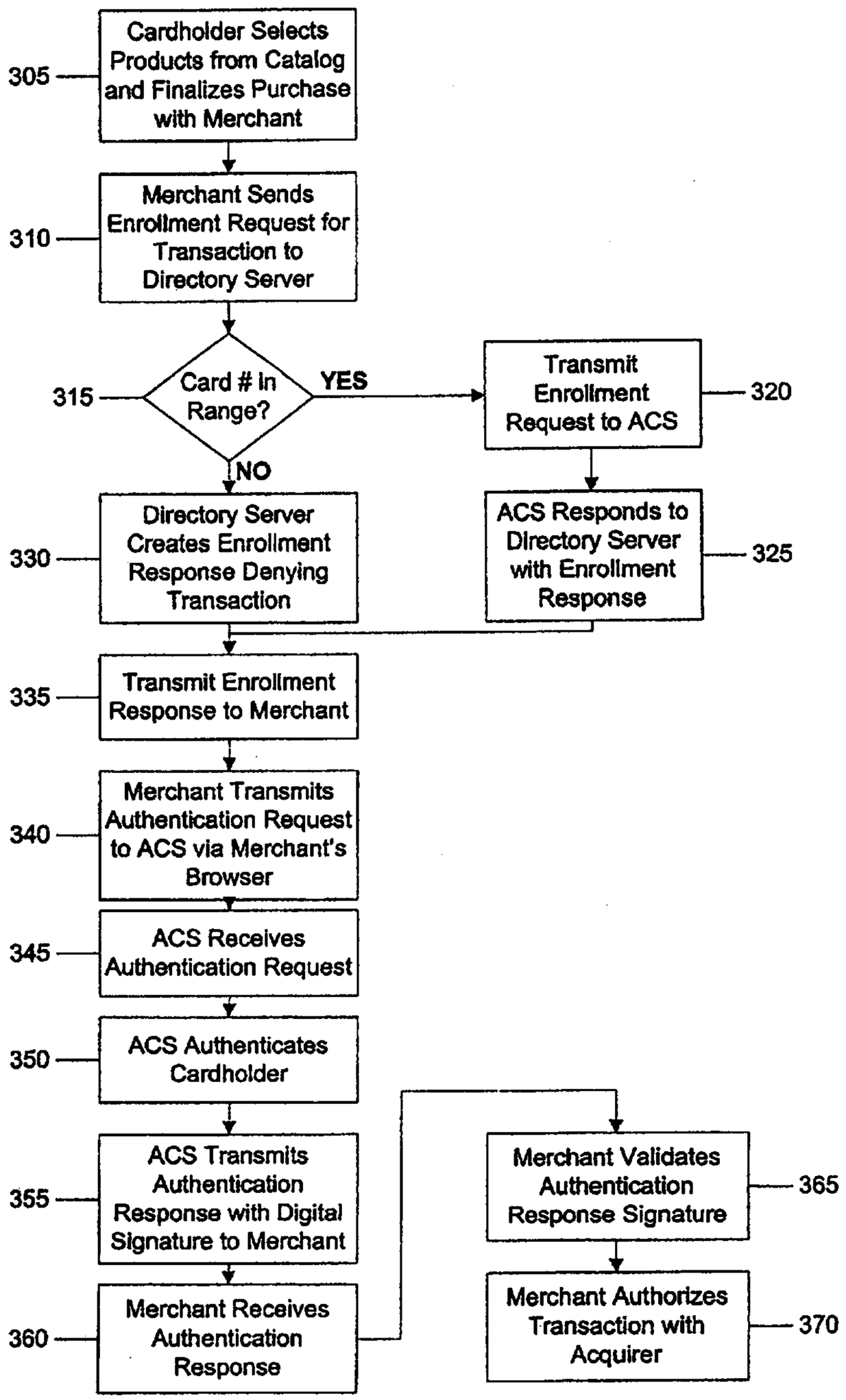

Cardholder Selects Products from Catalog and Finalizes Purchase with Merchant
305
Merchant Sends Enrollment Request for Transaction to Directory Server
310
Card # in Range?
315
YES
NO
Transmit Enrollment Request to ACS
320
ACS Responds to Directory Server with Enrollment Response
325
Directory Server Creates Enrollment Response Denying Transaction
330
Transmit Enrollment Response to Merchant
335
Merchant Transmits Authentication Request to ACS via Merchant's Browser
340
ACS Receives Authentication Request
345
ACS Authenticates Cardholder
350
ACS Transmits Authentication Response with Digital Signature to Merchant
355
Merchant Receives Authentication Response
360
Merchant Validates Authentication Response Signature
365
Merchant Authorizes Transaction with Acquirer
370

FIG. 3

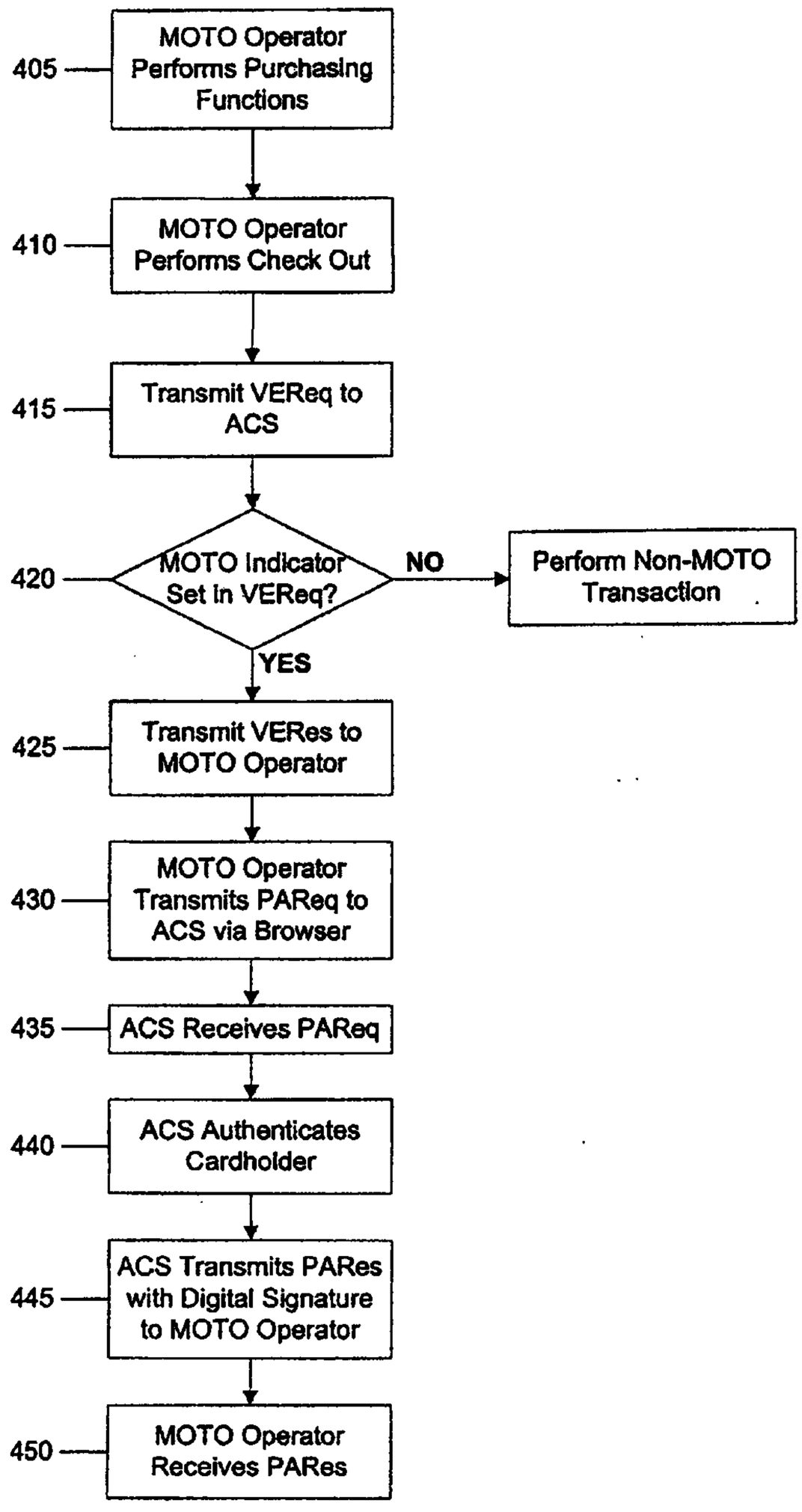
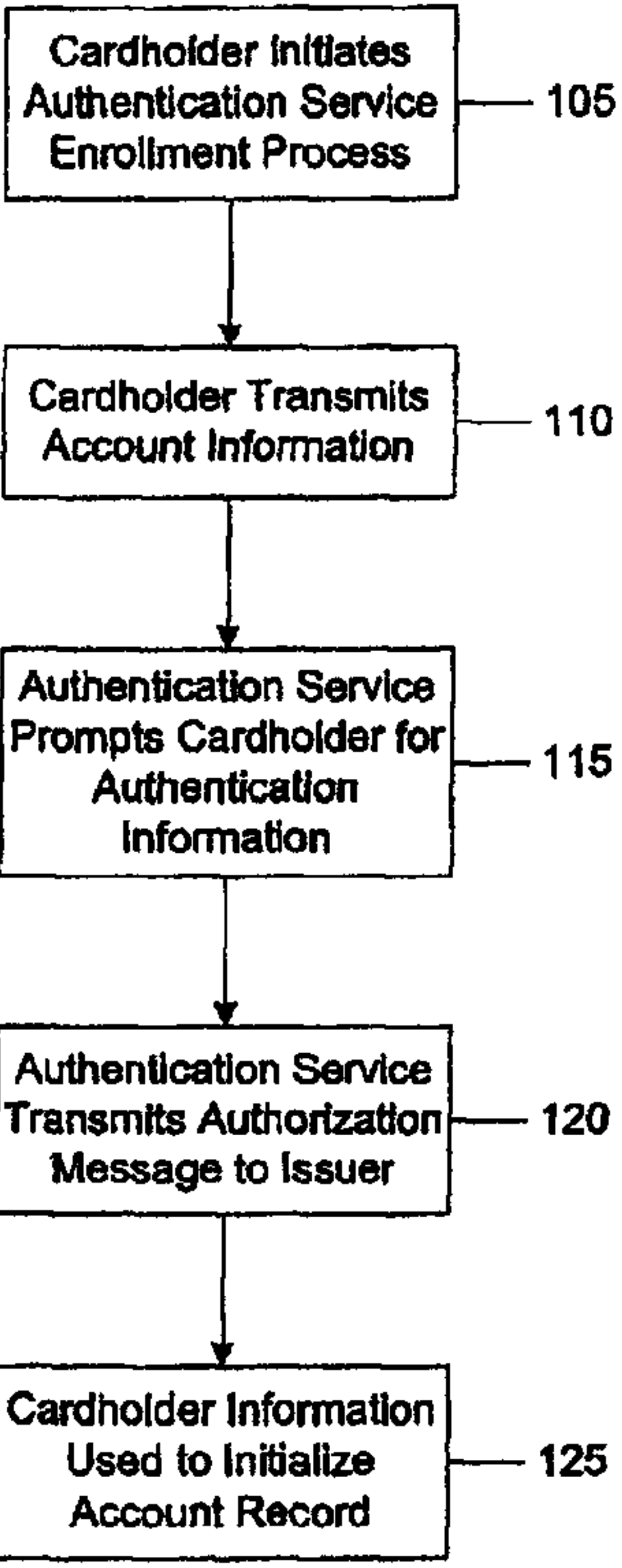

405
MOTO Operator Performs Purchasing Functions
410
MOTO Operator Performs Check Out
415
Transmit VEReq to ACS
420
MOTO Indicator Set In VEReq?
NO
Perform Non-MOTO Transaction
YES
425
Transmit VERes to MOTO Operator
430
MOTO Operator Transmits PAReq to ACS via Browser
435
ACS Receives PAReq
440
ACS Authenticates Cardholder
445
ACS Transmits PARes with Digital Signature to MOTO Operator
450
MOTO Operator Receives PARes

FIG. 4


Cardholder Initiates Authentication Service Enrollment Process
105
Cardholder Transmits Account Information
110
Authentication Service Prompts Cardholder for Authentication Information
115
Authentication Service Transmits Authorization Message to Issuer
120
Cardholder Information Used to Initialize Account Record
125