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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 March 2008 (06.03.2008)

PCT

(10) International Publication Number
WO 2008/027998 A2

(51) International Patent Classification: Not classified

(21) International Application Number:
PCT/US2007/077158

(22) International Filing Date: 29 August 2007 (29.08.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/823,803 29 August 2006 (29.08.2006) US

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

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **DOMINGUEZ, Benedicto** [US/US]; 2830 Merion Drive, SAN Bruno, CA 94066 (US).

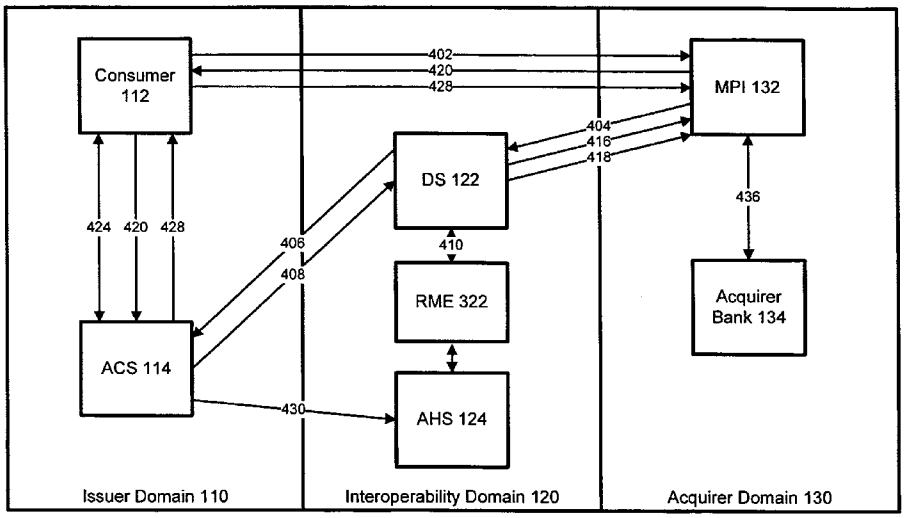
(74) Agent: **MAHONEY, Joseph, A.**; Mayer Brown LLP, P.O. Box 2828, Chicago, IL 60690-2828 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, 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, ME, 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).

Published:
— *without international search report and to be republished upon receipt of that report*

(54) **Title:** METHOD AND SYSTEM FOR PROCESSING INTERNET PURCHASE TRANSACTIONS



(57) **Abstract:** A method for minimizing risk of a consumer performing a fraudulent Internet purchase transactions using a transaction card is disclosed herein, the method comprising receiving an enrollment verification request for a transaction from a merchant's website, transmitting the enrollment verification request to an access control server; receiving an enrollment verification response from the access control server, determining whether the transaction is risky based on at least a portion of the enrollment verification request, if the transaction is not risky, forwarding the enrollment verification response to the merchant website and, if the transaction is risky, modifying the enrollment verification response to denote the transaction is risky and forwarding the modified enrollment verification response to the merchant's website.

WO 2008/027998 A2

METHOD AND SYSTEM FOR PROCESSING INTERNET PURCHASE TRANSACTIONS

REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority to U.S. Provisional Patent Application No. 60/823,803, filed August 29, 2006, entitled METHOD AND SYSTEM FOR PROCESSING INTERNET PURCHASE TRANSACTIONS.

BACKGROUND

[0002] 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 that the account is owned 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.

[0003] 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 transportation 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.

[0004] "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 volume increase, fraudulent transactions and the monetary losses due to such transactions are increasing as well.

[0005] **Figure 1** depicts a system diagram for a conventional transaction processing system according to the prior art. As shown in **Figure 1,** a transaction processing system is logically divided into an issuer domain **110**, an interoperability domain **120** and an acquirer domain **130.** The issuer domain **110** includes a consumer **112** and an access control server **114** ("ACS"). The interoperability domain **120** includes a directory server **122** ("DS") and an authentication history server **124** ("AHS"). The acquirer domain **130** includes a merchant purchase interface **132** ("MPI") and an acquirer bank **134.** The lines represent data transfers performed between the connected entities. Such data transfers are described more fully below in reference to **Figure 2**.

[0006] **Figure 2** depicts a conventional CNP transaction flow according to the prior art. As shown in **Figure 2**, a consumer adds items to a shopping cart and finalizes **205** a transaction. The MPI **132** sends **210** an enrollment verification request to a DS **122** to verify enrollment of the consumer **112.** If the consumer's card number is within a card range participating in authentication, the DS **122** forwards **215** the request to the ACS **114.** The ACS **114** responds **220** to the DS **122** with an enrollment verification response indicating whether authentication is available for the card number. The DS **122** then forwards **225** the enrollment verification response to the MPI **132.** If the consumer's card number is not within a participating card range, the DS **122** creates and sends **230** a response to the MPI **132.**

[0007] If card authentication is available, the MPI **132** sends **235** a request for payer

authentication to the ACS **114** via the consumer's Internet browser **112.** The ACS **114** receives **240** the payer authentication request and authenticates **245** the consumer **112** as appropriate for the card number. For example, the consumer **112** could be authenticated using a password, chip cryptogram, personal identification number or the like. The ACS **114** formats **250** and, optionally, digitally signs a response to the payer authentication request. The ACS **114** then transmits **255** the response to the MPI **132** via the consumer's Internet browser **112.** In addition, the ACS **114** can transmit **260** a copy of the response (in the form of a payer authentication transaction request) to an AHS **124.**

[0008] The MPI **132** then receives **265** the payer authentication response and validates **270** the response signature if the response signature was signed by the ACS **114.** The MPI **132** then commences **275** an authorization exchange with its acquirer **134.**

[0009] One problem with addressing fraud is determining how to provide early warning to merchants and issuers that fraud is occurring with a particular consumer's account number. Without an alert that fraud is taking place, the fraudster can continuously submit fraudulent transactions using the account number.

[0010] A need exists for methods and systems for providing early warning detection for suspicious activity.

[0011] A need exists for methods and systems for reporting suspicious activity related to CNP transactions.

[0012] A further need exists for methods and systems for providing an alert to an issuer that is not actively managing its CNP transaction processing system or authorization logic.

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

SUMMARY

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

[0015] It must be noted that as used herein and in the appended claims, the singular forms "a," "an," and "the" include plural reference unless the context clearly dictates otherwise. Thus, for example, reference to a "transaction" is a reference to one or more transactions and equivalents thereof known to those skilled in the art, and so forth. Unless defined otherwise, all technical and scientific terms used herein have the same meanings as commonly understood by one of ordinary skill in the art. Although any methods and materials similar or equivalent to those described herein can be used in the practice or testing of the present invention, the preferred methods, devices, and materials are now described. All publications mentioned herein are incorporated herein 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 minimizing risk of fraudulent Internet purchase transactions may include receiving an enrollment verification request for a transaction from a merchant website, transmitting the enrollment verification request to an access control server, receiving an enrollment verification response from the access control server, determining whether the transaction is risky based on at least a portion of the enrollment verification request,

forwarding the enrollment verification response to the merchant website if the transaction is not risky, and modifying the enrollment verification response to denote the transaction is risky and forwarding the modified enrollment verification response to the merchant website if the transaction is risky.

[0017] In an embodiment, a method for minimizing risk of fraudulent Internet purchase transactions may include receiving a transaction request that pertains to a user account and contains information pertaining to the transaction, comparing the transaction request information with information contained in a historical database to determine whether the transaction is at risk for being fraudulent, modifying a response to the transaction request, if the comparison determines the transaction is risky, to note that the transaction is risky, and updating the information contained in the historical database with the transaction request information.

BRIEF DESCRIPTION OF THE DRAWINGS

[0018] Aspects, features, benefits and advantages of the present invention will be apparent with regard to the following description and accompanying drawings, of which:

[0019] **Figure 1** depicts a system diagram for a conventional transaction processing system according to the prior art.

[0020] **Figure 2** depicts a flow diagram for a conventional CNP transaction flow according to the prior art.

[0021] **Figure** 3 depicts a system diagram for an exemplary transaction processing system according to an embodiment.

[0022] **Figure 4** depicts a flow diagram for an exemplary transaction flow according to an embodiment.

[0023] Figure 5 depicts an alternate system diagram for an exemplary transaction processing system according to an embodiment.

[0024] Figure 6 depicts an alternate flow diagram for an exemplary transaction flow according to an embodiment.

DETAILED DESCRIPTION

[0025] Figure 3 depicts a system diagram for an exemplary transaction processing system according to an embodiment. **Figure 3** differs from the prior art transaction processing system in **Figure 1** at least because of the introduction of a risk management engine **322** ("RME"). The RME **322** may be used to determine whether a transaction is risky. The RME **322** may receive transaction information such as the card number used in a transaction, one or more items purchased, a merchant at which the items are being purchased, a total cost for the transaction, information pertaining to the consumer's Internet browser (e.g., the IP address), and the like. Based on the transaction information, the RME **322** may use one or more risk processing criteria to determine whether the transaction is risky (i.e., potentially fraudulent). Exemplary risk processing criteria may include, without limitation, identifying whether the consumer's account number has been previously used at the same merchant for the same amount ("velocity checking"), determining whether a dollar amount limit for the consumer's account number has been exceeded ("limit checking") and/or checking the IP address of the consumer's computer ("geo-location checking"). The RME **322** may use transaction data stored in the AHS **124** to assist in determining whether the transaction is risky. In an embodiment, the RME **322** may use different criteria based on the region, country, member and/or the like for which the transaction is processed. If a transaction and/or an account are determined to be risky, the RME **322** may transmit an alert to an issuer and/or a merchant system to warn the

issuer/merchant of the potential risk. In an embodiment, the transaction may be permitted to complete, but subsequent transactions that satisfy one or more of the criteria may be denied.

[0026] Figure 4 depicts a flow diagram for an exemplary transaction flow according to an embodiment. As shown in **Figure 4**, a consumer may select one or more items for purchase via an MPI **132** and finalize **402** purchased items. The MPI **132** may transmit **404** an enrollment verification request ("VEReq") to a DS **122** to verify enrollment of the consumer **112.** If the consumer's card number is within a card range participating in authentication, the DS **122** may forward **406** the VEReq to an appropriate ACS **114.** The ACS **114** may provide **408** an enrollment verification response ("VERes") to the DS **122** that indicates whether authentication is available for the card number. The DS **122** may invoke **410** the RME **322** to determine whether the transaction is risky. If the RME **322** determines that the transaction is non-risky, the DS **122** may forward **412** the VERes provided **408** by the ACS **114** to the MPI **132.** If the RME **322** determines that the transaction is risky, the VERes provided **408** by the ACS **114** may be modified **414** to denote that the transaction is risky and/or unauthorized. In an embodiment, a current transaction may be allowed to complete without modification **414** regardless of the determination of risk. In such an embodiment, if the transaction is determined to be risky and/or unauthorized, future transactions having, for example, the same account number may be modified **414** to be denoted as risky and/or unauthorized transactions. The modified VERes may then be forwarded **416** to the MPI **132.** If the consumer's card number is not within the participating card range, the DS **122** may create a VERes and transmit **418** it to the MPI **132.**

[0027] If authentication is available for the consumer's card, the MPI **132** may transmit **420** a payer authentication request ("PAReq") to the ACS **114** via the consumer's Internet

browser **112.** The ACS **114** may receive **422** the PAReq and may authenticate **424** the consumer **112** in a manner that is appropriate based on the card number. For example, the consumer **112** may be authenticated **424** using a password, chip cryptogram, personal identification number or the like. The ACS **114** may format **426** and digitally sign a payer authentication response ("PARes") to the PAReq. The ACS **114** may then transmit **428** the PARes to the MPI **132** via the consumer's Internet browser **112.** In addition, the ACS **114** may transmit **430** a payer authentication transaction request ("PATransReq") to an AHS **124.** The AHS **124** may be a repository of information pertaining to previously performed transactions. The PATransReq may include, for example and without limitation, a merchant name, a transaction identifier, an description of purchased goods and/or services, a purchase amount, a purchase currency, a purchase date, a purchase time and the like. The MPI **132** may receive **432** the PARes and validate **434** the PARes signature. The MPI **132** may then commence **436** an authorization exchange with its acquirer **134.**

[0028] Figure 5 depicts an alternate system diagram for an exemplary transaction processing system according to an embodiment. **Figure 5** may differ from **Figure 3** in the manner in which an alert is provided. Accordingly, different entities may communicate with each other during transaction processing.

[0029] Figure 6 depicts an alternate flow diagram for an exemplary transaction flow according to an embodiment. As shown in **Figure 6,** a consumer may select one or more items for purchase via an MPI **132** and finalize **602** purchased items. The MPI **132** may transmit **604** a VEReq to a DS **122** to verify enrollment of the consumer. If the consumer's card number is within a participating card range, the DS **122** may forward **606** the VEReq to an appropriate ACS **114.** The ACS **114** may provide **608** a VERes to the DS **122** that indicates

whether authentication is available for the card number. The DS **122** may forward **610** the VERes to the MPI **132**. If the consumer's card number is not within the participating card range, the DS **122** may create a VERes and transmit **612** it to the MPI **132.**

[0030] If authentication is available for the consumer's card, the MPI **132** may transmit **614** a PAReq to the ACS **114** via the consumer's Internet browser **112.** The ACS **114** may receive **616** the PAReq. The DS **122** may invoke **618** the RME **322** to determine whether the transaction is from a risky account. If the RME **322** determines the account to be risky, the RME may transmit **620** data instructing the ACS **114** to respond **622** to the MPI denying payer authentication for the account. Otherwise, the ACS **114** may authenticate **624** the consumer in a manner that is appropriate based on the card number. For example, the consumer may be authenticated **624** using a password, chip cryptogram, personal identification number or the like. The ACS **114** may format **626** and digitally sign a PARes to the PAReq. The ACS **114** may then transmit **628** the PARes to the MPI **132** via the consumer's Internet browser **112.** In addition, the ACS **114** may transmit **630** a PATransReq to an AHS **124.** The PATransReq may include, for example and without limitation, a merchant name, a transaction identifier, an description of purchased goods and/or services, a purchase amount, a purchase currency, a purchase date, a purchase time and the like. The MPI **132** may receive **632** the PARes and validate **634** the PARes signature. The merchant **132** may then commence **636** an authorization exchange with its acquirer **134.**

[0031] 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 which are also intended to be encompassed by the disclosed embodiments.

CLAIMS

1. A method for minimizing risk of a consumer performing a fraudulent Internet purchase transaction using a transaction card, the method comprising:

receiving an enrollment verification request for a transaction from a merchant's website;

transmitting the enrollment verification request to an access control server;

receiving an enrollment verification response from the access control server;

determining whether the transaction is risky based on at least a portion of the enrollment verification request;

if the transaction is not risky, forwarding the enrollment verification response to the merchant website; and

if the transaction is risky:

modifying the enrollment verification response to denote the transaction is risky, and

forwarding the modified enrollment verification response to the merchant's website.

2. The method of claim 1, wherein the enrollment verification request comprises an account number.

3. The method of claim 2, wherein the enrollment verification response indicates whether cardholder authentication is available for the account number.

4. The method of claim 1, wherein determining whether the transaction is risky comprises at least one of:

identifying whether the account number has been previously used at the same merchant for the same amount;

determining whether a dollar amount limit for the account number has been exceeded; and

comparing a geographic location corresponding to an IP address of the consumer's computer.

5. The method of claim 1, further comprising transmitting, if the transaction is risky, an alert to the transaction card's issuer warning the issuer that the transaction is risky.

6. The method of claim 2, wherein the enrollment verification request further comprises one or more items to be purchased by the consumer, a total cost for the transaction, an identity of the merchant, and information pertaining to the consumer's internet browser.

7. A method for minimizing risk of a consumer performing a fraudulent Internet purchase transaction with a merchant using a transaction card, the method comprising:

receiving a transaction request, wherein the transaction request contains information pertaining to the transaction, and wherein the transaction request pertains to a consumer account;

comparing the transaction request information with information contained in a historical database to determine whether the transaction is at risk for being fraudulent;

if the comparison determines the transaction is risky, transmitting a response to the transaction request, wherein the response to the transaction request notes that the transaction is

risky; and

updating the information contained in the historical database with the transaction request information.

8. The method of claim 7, wherein the transaction request comprises one or more items to be purchased by the consumer, a total cost for the transaction, an identity of the merchant, and information pertaining to the consumer's internet browser.

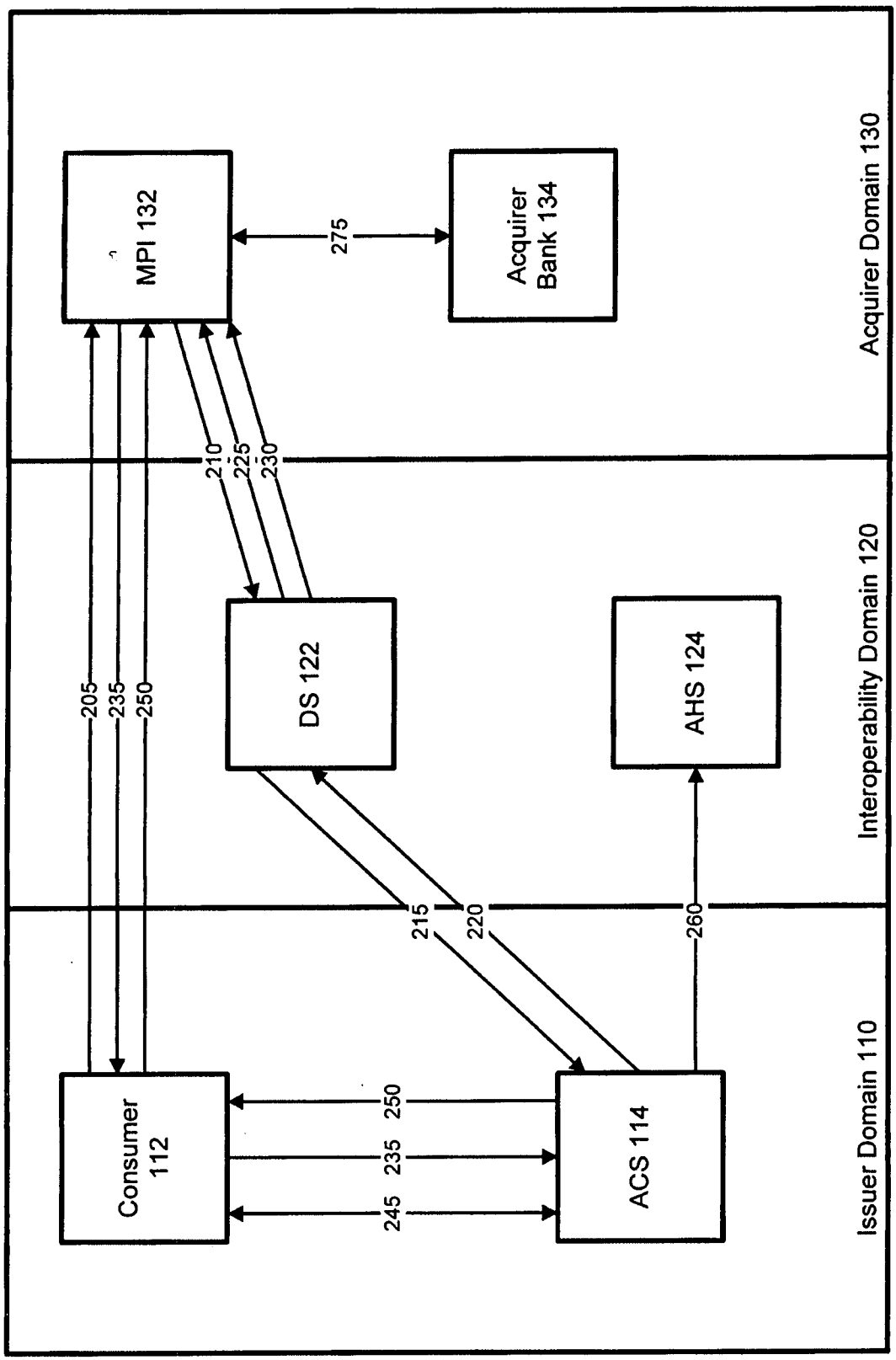


Figure 1
(Prior Art)

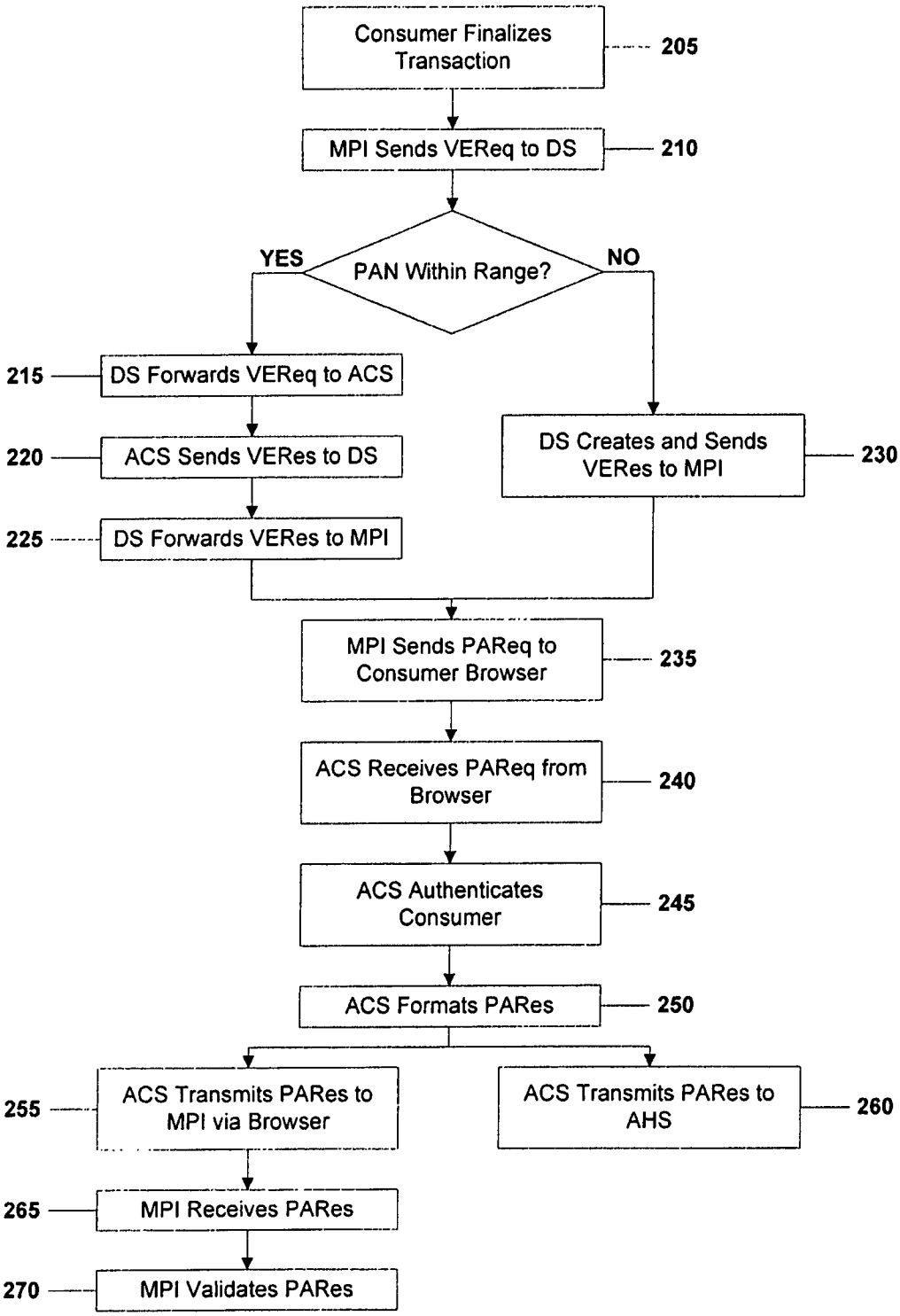


Figure 2
(Prior Art)

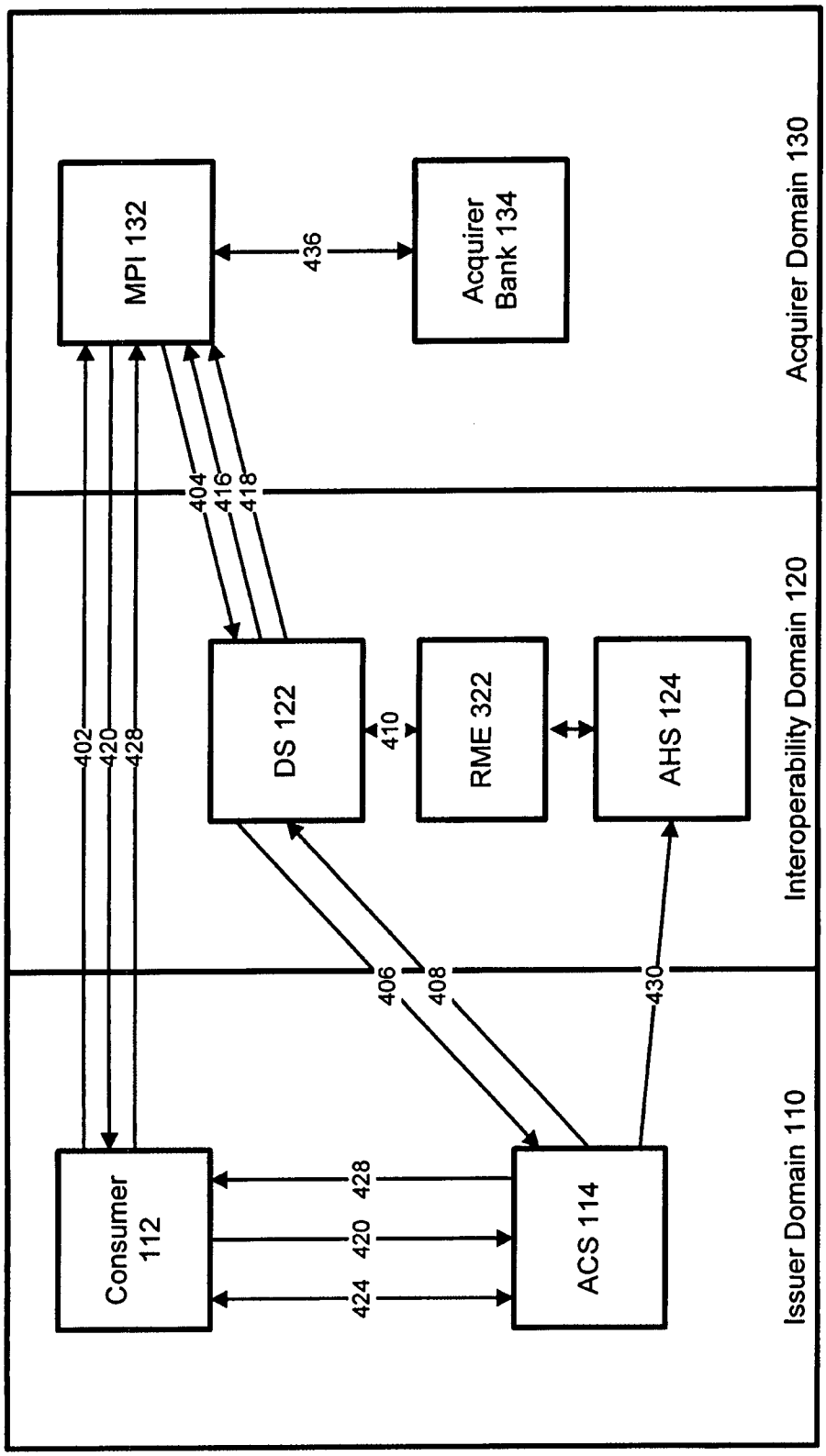

Acquirer Domain 130
Interoperability Domain 120
Issuer Domain 110
MPI 132
Acquirer Bank 134
436
404
416
418
402
420
428
DS 122
410
RME 322
AHS 124
406
408
430
Consumer 112
428
420
424
ACS 114

Figure. 3

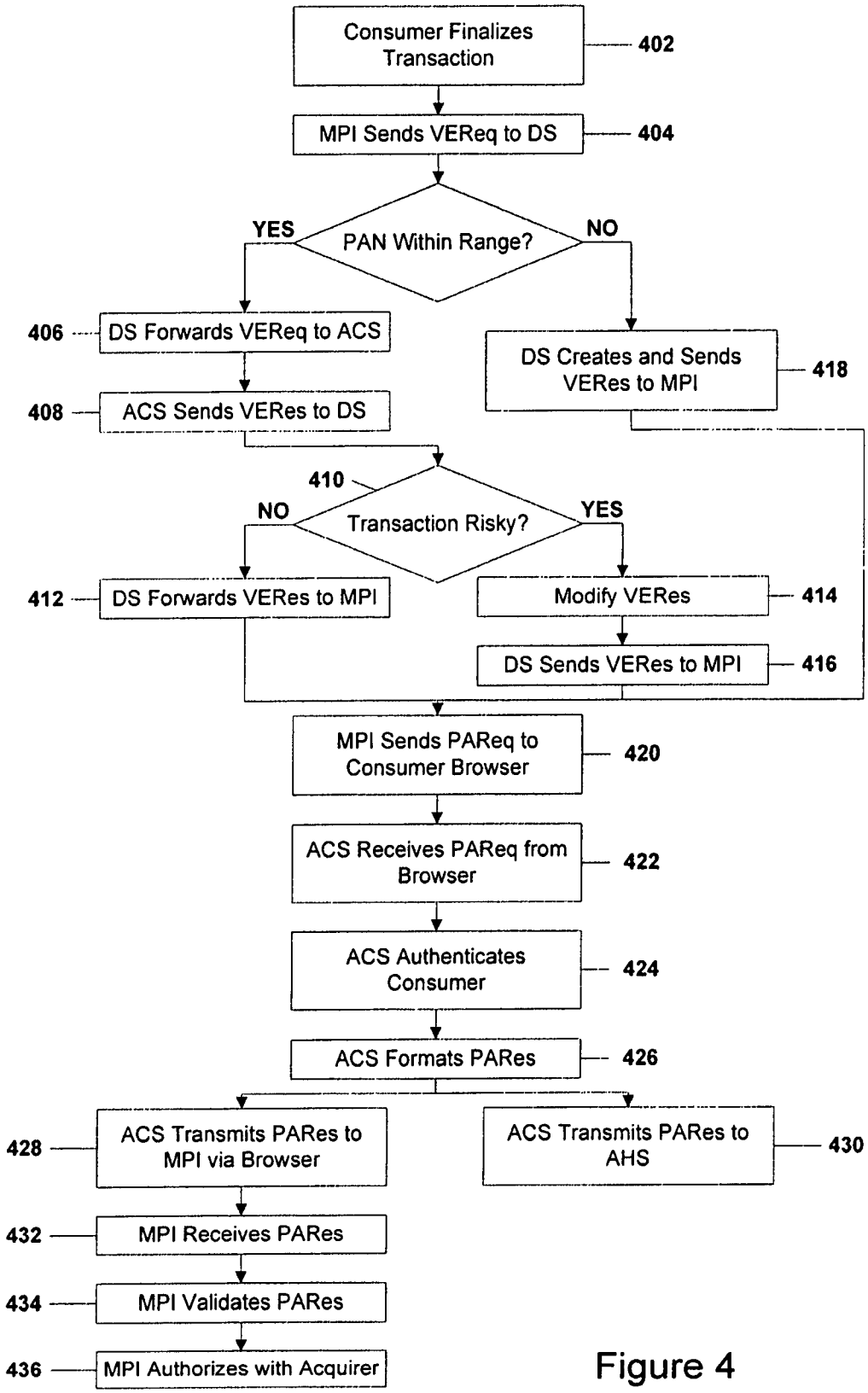

Consumer Finalizes Transaction
402
MPI Sends VEReq to DS
404
PAN Within Range?
YES
NO
406
DS Forwards VEReq to ACS
408
ACS Sends VERes to DS
DS Creates and Sends VERes to MPI
418
410
Transaction Risky?
NO
YES
412
DS Forwards VERes to MPI
Modify VERes
414
DS Sends VERes to MPI
416
MPI Sends PAReq to Consumer Browser
420
ACS Receives PAReq from Browser
422
ACS Authenticates Consumer
424
ACS Formats PARes
426
428
ACS Transmits PARes to MPI via Browser
ACS Transmits PARes to AHS
430
432
MPI Receives PARes
434
MPI Validates PARes
436
MPI Authorizes with Acquirer

Figure 4

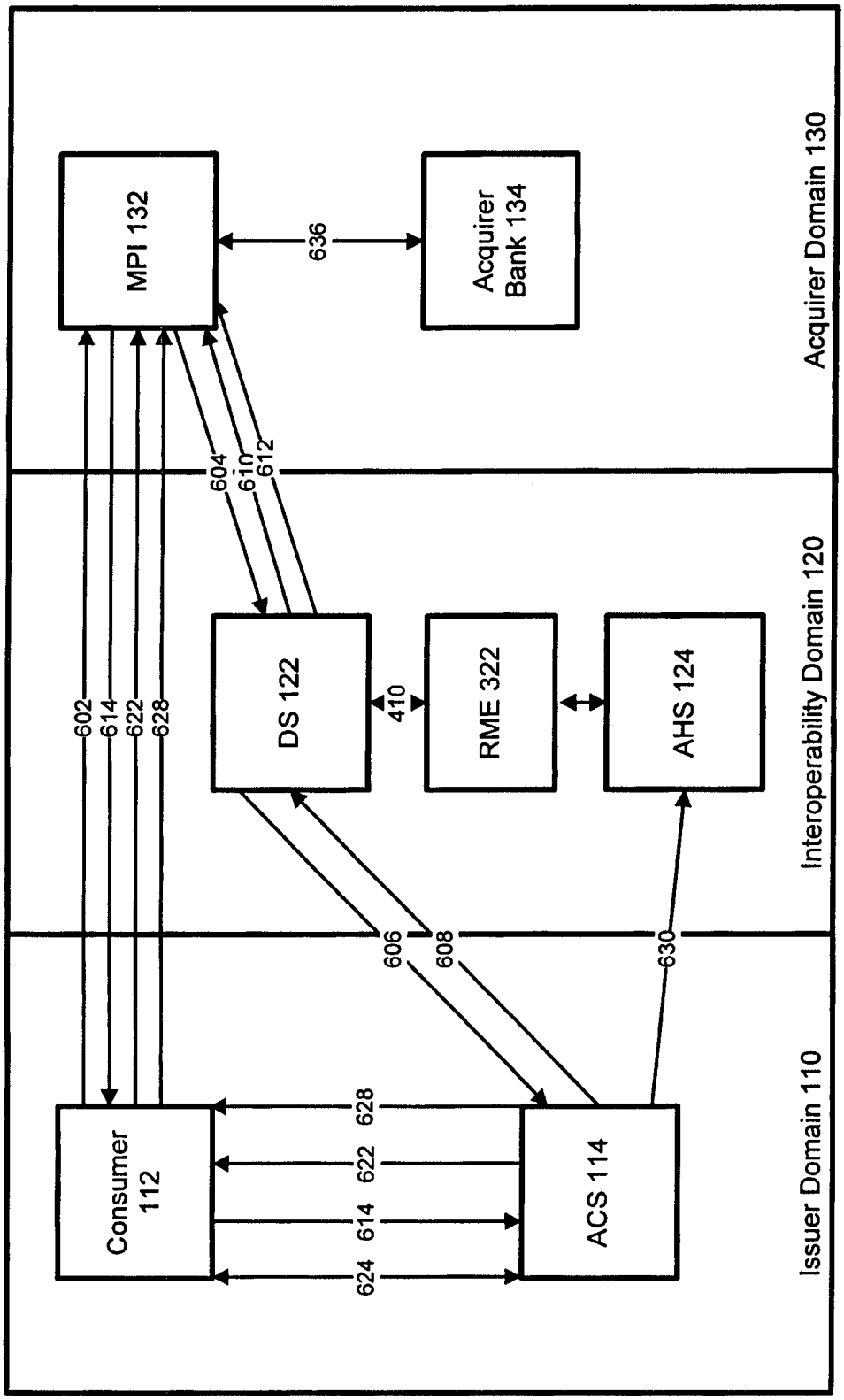

Acquirer Domain 130
Interoperability Domain 120
Issuer Domain 110
MPI 132
Acquirer Bank 134
636
604
610
612
DS 122
410
RME 322
AHS 124
602
614
622
628
606
608
630
Consumer 112
ACS 114
628
622
614
624

Figure 5

6/6

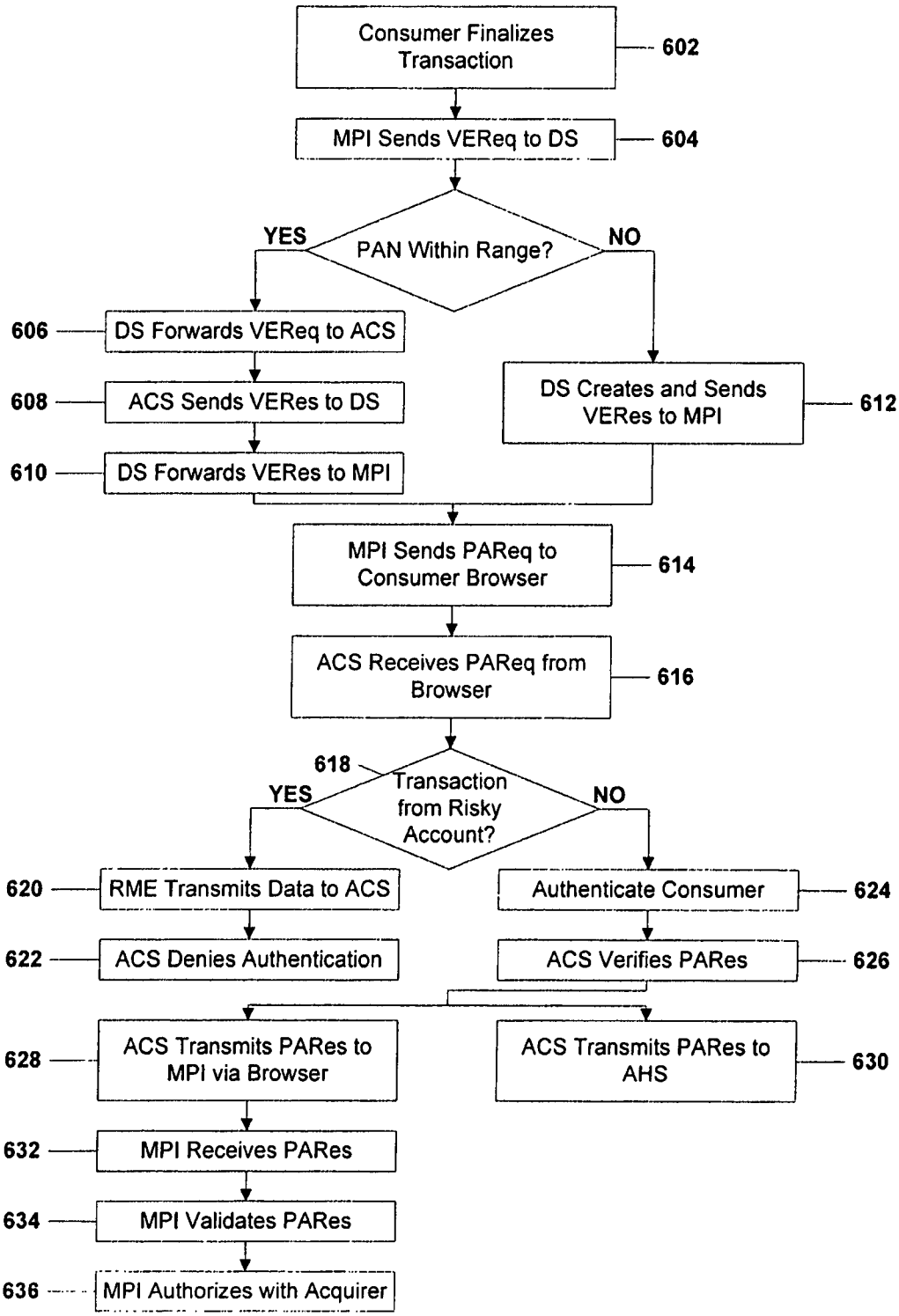

Consumer Finalizes Transaction
602
MPI Sends VEReq to DS
604
YES
PAN Within Range?
NO
606
DS Forwards VEReq to ACS
608
ACS Sends VERes to DS
610
DS Forwards VERes to MPI
DS Creates and Sends VERes to MPI
612
MPI Sends PAReq to Consumer Browser
614
ACS Receives PAReq from Browser
616
618
YES
Transaction from Risky Account?
NO
620
RME Transmits Data to ACS
622
ACS Denies Authentication
Authenticate Consumer
624
ACS Verifies PARes
626
628
ACS Transmits PARes to MPI via Browser
ACS Transmits PARes to AHS
630
632
MPI Receives PARes
634
MPI Validates PARes
636
MPI Authorizes with Acquirer

Figure 6