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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
26 September 2013 (26.09.2013)

(10) International Publication Number
WO 2013/142334 A1

(51) International Patent Classification: *G06Q 20/00* (2012.01)

(21) International Application Number: PCT/US2013/032130

(22) International Filing Date: 15 March 2013 (15.03.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/612,897 19 March 2012 (19.03.2012) US

(71) Applicant: PAYNET PAYMENTS NETWORK, LLC [US/US]; 601 Riverside Avenue, Jacksonville, FL 32204 (US).

(72) Inventors: MARCOUS, Neil; 62 Egbert Street, Bay Head, NJ 08742 (US). WOODBURY, Robert; 7 Johnston Drive, Flemington, NJ 08822 (US). GORDON, Peter; 26 Knob Hill Street, Sharon, MA 02067 (US).

(74) Agent: GARRETT, Arthur, S.; Finnegan, Henderson, Farabow, Garrett & Dunner LLP, 901 New York Avenue, N.W., Wahington, DC 20001-4413 (US).

(81) Designated States (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

**Published**:

— *with international search report (Art. 21(3))*

(54) Title: SYSTEMS AND METHODS FOR REAL-TIME ACCOUNT ACCESS

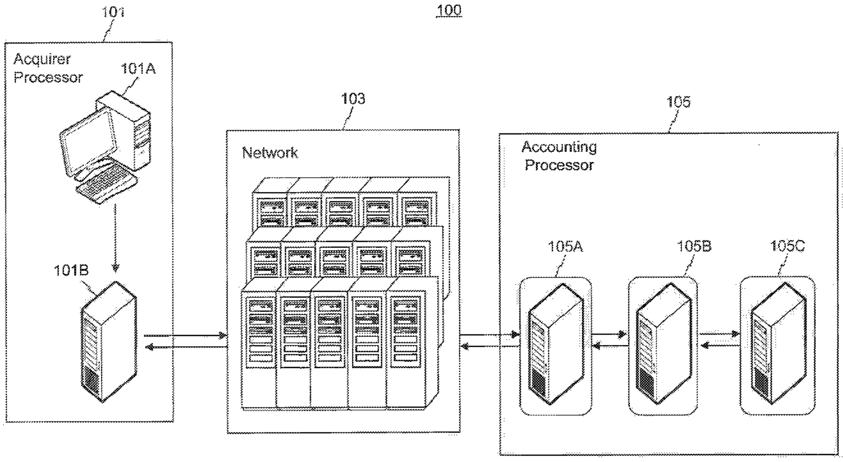


FIG. 1

(57) Abstract: Systems and methods for real-time account access, allowing access to accounts (such as deposit, credit, or debit accounts) through network processing infrastructures such as Electronic Funds Transfer (EFT). In some embodiments, consumers and/or merchants are able to effect transaction requests against accounts, using a pseudo-identifier or other identifier, and without the need to provide an account number or card number. In other embodiments, payment networks are able to route and process transaction requests against accounts, without having a card number or account number. In other embodiments, account processing systems are able to determine an appropriate account based on transaction requests that do not contain card numbers or account numbers.

# SYSTEMS AND METHODS FOR REAL-TIME ACCOUNT ACCESS

## CROSS-REFERENCE TO RELATED APPLICATIONS

[001] This application claims the benefit of prior-filed U.S. Provisional Application 61/612,897, filed March 19, 2012, which is hereby incorporated by reference in the present application.

## FIELD OF DISCLOSURE

[002] The disclosed embodiments are generally directed to systems and methods for real-time account access.

## BACKGROUND

[003] Network processing infrastructures, such as EFT (Electronic Funds Transfer) network processing, are used to process payments from traditional credit or debit card transactions. EFT enables quick provisioning of account information and other related information for purchases and other purposes. For example, when a cardholding customer seeks to purchase an item at a store, the customer will generally hand her card to the merchant and the merchant will swipe the card through a magnetic stripe machine to read the card information, including the card number. Card numbers are typically 13-19 digits long, and uniquely identify the user's credit or debit account.

[004] After the card number is received by the merchant, the merchant sends the card number, along with other information associated with the transaction, such as price, date, time, location, cardholder name, to a payment network. The payment network will typically route that information to the appropriate card issuer based on the card number. The first digits typically identify the "issuer," that is, the entity, such as a company, that issued the card. So, for example, a card number beginning with a '4,' e.g., 4000 1234 5678 9012, will typically identify VISA as the card provider/issuer. Each issuer typically has a numeric identifier that is associated with and represents their cards.

[005] The appropriate issuer, for example, a credit or charge card company, will then typically consult its records to determine the appropriate account and verify whether that account contains sufficient funds or credit to make a transaction (e.g., a purchase). The result of this determination will typically be returned to inform the merchant whether the user is able to purchase the item. The entire process, from the original capturing of the card data to the response providing funds verification may happen in a relatively short period of time. In some situations, this process happens in real-time or in near real-time.

[006] However, in some situations, a card number for accessing a customer's account is not available. For example, if a customer decides to pay by check, the merchant must capture the RTN (Routing Transit Number) for the bank that issued the check and the customer's personal account number. The merchant must then use a system such as the Automated Clearing House (ACH) to process the payment. ACH typically operates in batches and thus the process to authorize a purchase can take much longer than a card-based transaction. Thus, using ACH increases the amount of time for the merchant to acquire the funds promised. ACH use further includes a possibility of accepting payments that are later found to be uncollectable (also known as a "bounced check").

[007] In other situations, a customer may not wish to provide his account details to the merchant, for reasons of privacy or otherwise. This can cause issues in payment acceptance because a user will typically need to provide his payment card information. Without this information, the merchant is typically unable to accept payment.

[008] Still in other situations, such as with commercial accounts, there is no card number that can be used to effect purchases. Thus, commercial purchases may need to rely on the ACH system to make purchases, which (as mentioned before) is slow, costly, and inefficient.

[009] It would thus be desirable to provide for improved systems and methods for processing transactions to accounts using existing network processing infrastructure with real-time or near real-time access. It would also be desirable for these systems and methods to support routing, processing, settling, and reporting of payment transactions. Advantages of such systems and methods include increased speed for transaction processing, reliable account management and accounting,

and/or a drop in uncollectable accounts. Further advantages will be recognized by one skilled in the art after considering the remainder of the disclosure.

## SUMMARY OF THE DISCLOSURE

[010] In accordance with example embodiments, a method for processing payment transactions by a device (such as a payment network device) comprises receiving transaction requests from an acquirer and determining that the transaction request represents a transaction that does not require a card or account number. The method further comprises selecting an accounting processor based on the contents of the transaction request, providing the transaction request to the selected accounting processor, and receive a response from the accounting processor. In some example embodiments, the response received may comprise at least one of a selected account for the transaction request based at least in part on the contents of the transaction request or an account balance associated with the selected account. The method further comprises, approving, denying, or taking further action on the transaction request. Similarly, in some example embodiments, a computer system comprises at least one processor and a memory containing instructions that, when executed by the processor, cause the processor to perform the operations of this method.

[011] In accordance with example embodiments, a method for processing payment transactions by an accounting processor device comprises receiving, at the accounting processor device (e.g., from a network device), a transaction request determined by the network device to not require a card or account number. The method further comprises selecting an account for the transaction request based at least in part on the contents of the transaction request, determining a balance of the selected account, and generating a response based on the contents of the transaction request and the balance. The response comprises information for determining whether to approve or deny the transaction request. Similarly, in some example embodiments, a computer system comprises at least one processor and a memory containing instructions that, when executed by the processor, cause the processor to perform the operations of this method.

[012] In accordance with example embodiments, a method for processing a payment transaction by an acquirer processor device comprises a step of receiving

information using at least one computer system for conducting a payment transaction. In some example embodiments, the information does not include a card or account number. The method further comprises the computer system generating a transaction request including at least one identifier based on the information, sending the transaction request to a payment network for processing, and receiving at least one response to the transaction request based on at least one account associated with the identifier. Similarly, in some example embodiments, a computer system comprises at least one processor and a memory containing instructions that, when executed by the processor, cause the processor to perform the operations of this method.

[013] It is to be understood that both the foregoing general description and the following detailed description are examples and explanatory only and are not restrictive of the disclosed embodiments, as claimed.

## BRIEF DESCRIPTION OF THE DRAWINGS

[014] The accompanying drawings, which are incorporated in and constitute a part of this specification, illustrate several embodiments of the disclosed embodiments and together with the description, serve to explain principles of the disclosed embodiments.

[015] FIG. 1 is an example network 100 in accordance with some embodiments;

[016] FIG. 2 is an example network communication diagram 200 displaying some portions of communications usable in accordance with some embodiments;

[017] FIG. 3 is an example message format 300 for use with in accordance with some embodiments;

[018] FIG. 4 is an example diagram 400 of some data fields for use with in accordance with some embodiments; and

[019] FIG. 5 is an example computer system 500 for use with in accordance with some embodiments.

## DETAILED DESCRIPTION

[020] Reference will now be made in detail to the disclosed embodiments, examples of which are illustrated in the accompanying figures. Wherever possible, the same reference numbers will be used throughout the drawings to refer to the same or like parts.

[021] The disclosed embodiments employ multiple modes of operation to process a payment transaction (also referred to herein as a "transaction"). A first mode of operation is known as "native mode." In native mode, a message (also referred to herein as a transaction request or payment request) may be passed between devices. The message, in some embodiments, may conform to or be based upon the ISO 8583 message. The ISO 8583 standard defines a format for messages so, among other things, different systems can exchange data and effect transactions.

[022] A native mode message allows a transaction to utilize existing payment card transaction channels even without a payment card. For example, an ISO 8583 message could be used to effect these transactions. In some embodiments, the native mode system would construct one of these messages using particular information. At least part of this information may signify that the message is going to be used for a purpose different from its ordinary purpose (*i.e.* different from a payment card transaction).

[023] Another mode of operation is known as "non-native mode" or "X-REF mode." This mode may be similar to the above native mode but with messages constructed in a different manner. In some embodiments, a data store or database may be consulted to determine an account number based on data stored in the messages. Both of these modes will be described later with respect to at least FIGS. 3 and 4.

[024] Both modes of operation enable the conducting of a transaction that does not require a card number or account number. For example, in the situation of a user who does not wish to disclose her payment card number or account number to a merchant, a transaction can still be processed, using the above modes of operation.

[025] FIG. 1 is a representation of an example network 100 for use with the disclosed systems and methods. Network 100 contains, in some embodiments, at least one of Acquirer Processor 101, at least one of Network 103, and at least one of Issuer 105. These individual elements may be implemented, in some embodiments, using one or multiple computer systems as will be referenced with respect to FIG. 5. The particular components or devices used to implement each of these elements may vary.

[026] Acquirer Processor 101, in some embodiments, includes a Front-End System 101A and a Back-End System 101B. Front-End System 101A is used to capture payment details. In some embodiments, Front-End System 101A may be a merchant device for capturing data - including a cash register, an online shopping cart system, a credit card reader, a check-scanning machine (*e.g.* for reading MICR data), a computer, or the like. In other embodiments, Front-End System 101A is operated by an acquiring bank. This may be, for example, the bank that processes payments for a merchant who has accepted payment details from a customer.

[027] In some embodiments, Back-End System 101B can be a system for processing transactions passed through Front-End System 101A. Back-End System 101B can be run by the same acquiring bank that runs Front-End system 101A. In other embodiments Back-End System 101B may be run by a different entity. Back-End System 101B, in some embodiments, can generate a transaction request based in part on the payment details captured by Front-End System 101A. Back-End System 101B can then send this transaction request to a Network 103 for processing. In some embodiments, Front-End System 101A and Back-End System 101B may be a single distinct computer system. In others, they may be multiple computer systems. In further embodiments, Front-End System 101A and Back-End System 101B may be any of an ATM/ATM Processor, a merchant/POS Processor, a Bill Pay Merchant/Biller Processor, an Internet merchant/Internet merchant Processor, or the like.

[028] In some embodiments, Front-End System 101A or Back-End System 101B may acquire customer credentials in order to effect a purchase or other transaction. In some embodiments, these acquired credentials may be used to create a constructed value. The constructed value may comprise information identifying a unique deposit account or other kind of account. For example, accounts

may comprise any of a deposit account, a checking account, a debit account, a credit account, a brokerage account, a business account, a personal account, or the like. One of ordinary skill will recognize that one particular type of account is not necessarily essential to the disclosed embodiments.

[029] In some embodiments, the constructed value may be unique. For example, in constructing a payment request including a constructed value, the constructed value could refer only to the institution holding the account, with other information in the payment request referring to the particular account. In some embodiments, this constructed value may include any of a number of data types, including (but not limited to) a special value indicating the presence of a constructed value, identifiers (e.g., pre-agreed upon identifiers) for an account or institution (such as an International Bank Account Number (IBAN – used primarily outside of the United States), a Routing Transit Number (RTN or R&T Number – used primarily inside of the United States), a Canadian transit number, a bank code, a branch code, a sort code, or any other identifier that at least partially identifies the account or the institution that holds it), a time and date for the payment request, or the like.

[030] In some embodiments, the constructed value may include a number resembling a deposit account number, a card account number, or another type of account number (also known as a Primary Account Number (PAN)). PANs may comply with or be based on ISO 7812, which may, in part, assign specific first digits of PANs to specific issuers.

[031] In still other embodiments, the constructed value and/or the payment request may include a number of other identifiers that can uniquely identify a customer or his accounts. For example, a customer's email address, phone number (cellular/mobile, work, home, pager, etc.), username, social network identity (such as a Facebook or Twitter account), or the like, may be included. Additionally, these identifiers can be used to generate another identifier (such as a hexadecimal or encrypted value) for use in the payment request. Further, other identifiers may be used in some embodiments.

[032] Network 103 can be an Interbank Network (such as NYCE, INTERAC, or the like). Interbank Networks allow money systems (such as ATMs or payment terminals) to access deposit or other accounts. In some embodiments, Network 103 enables the use of ATM cards issued by a bank to be used at a point of sale through

an EFTPOS (Electronic Fund Transfer at Point Of Sale) system. Rather than operating as a credit card transaction, which would typically need to go through a credit card issuer system, an EFTPOS transaction could be received by Network 103 and routed to the appropriate bank holding the account. Network 103 can be national, international, or both. Network 103, in some embodiments, may be configured to send messages to Accounting Processor 105, to request Accounting Processor 105 to move funds associated with a transaction.

[033] Accounting Processor 105 represents systems used in processing payment transactions. For example, in some embodiments, Accounting Processor 105 may be a computer system that receives a transaction request, attempts to process the transaction request (e.g., by debiting or crediting accounts referenced in the request), and provides the status of the attempt to process the transaction request. Accounting Processor 105 may be operated by, for example, an issuer, a bank, a credit union, a commercial bank, a company operating deposit accounts, or the like. Accounting Processor 105 may differ based on, for example, which kind of transaction is being attempted. For example, a transaction on a credit card not tied to a particular bank could be processed at a card issuer's servers. However, a debit card transaction that is tied to a deposit account at a bank may be processed at least in part by the bank. In any case, the group or organization operating Accounting Processor 105 typically stores information on accounts, such as lines of credit, account balances, credit worthiness, payment history, and the like. In some embodiments, the accounts managed by Accounting Processor 105 are known as Demand Deposit Accounts (DDAs). Accounting Processor 105 may deposit funds into accounts, withdraw funds from accounts, request balances of accounts, or perform other accounting transactions when requested by, for example, Network 103.

[034] In some embodiments, Acquirer Processor 101, Network 103, and/or Accounting Processor 105 may employ a set of rules for initiating and processing transaction requests, such as EFTPOS transactions. In some embodiments, any or all of these devices may be configured to comply with these rules. For example, Accounting Processor 105 may be configured to move funds between accounts when requested by Network 103. Accounting Processor 105 may also be configured to process credit transactions, debit transactions, micro-transactions, or other

transactions, when requested by Network 103 and/or Acquirer Processor 101. Accounting Processor 105 may also be configured to provide account balance or status (e.g., open, closed, suspended) when requested by Acquirer Processor 101. Accounting Processor 105 may also be configured to settle transactions at the end of a business day. One of ordinary skill will recognize that other rules for processing transactions are possible as well.

[035] FIG. 2 discloses an example method 200 for implementing portions of the disclosed systems and methods. Method 200 begins with step 201A with Acquirer Processor 201 receiving credentials from a customer or purchaser. These credentials (or “payment details”) could include payment account information - such as an RTN (Routing Transit Number), an account number, a credit card number, a payment card number, a debit card number, an identifier tied to an account, a pseudo-identifier that when referenced in a data store or database resolves to an account number, or the like. The payment details, in some embodiments, can uniquely represent a customer's deposit, credit, debit, or other account. For example, payment details can comprise a customer's account number. The payment details, in still other embodiments, can comprise another unique identifier that is associated with customer's account. For example, the payment details can comprise a pseudo-identifier made of numeric, hexadecimal, or another coding scheme, to identify the customer's account. In other embodiments, the payment details can comprise a pseudo-card number or a constructed value. The first few digits of the constructed value could be a '59,' but other values and constructions are possible as well. A ‘59’ may be used to signify that the characters following it contain an ABA value. These values may be provided by the customer attempting to purchase a good or make a transaction, may be generated by Acquirer Processor 101 based on information received from the customer, or the like.

[036] In still other embodiments, the constructed value and/or the payment details may include a number of other identifiers that can uniquely identify a customer or account. For example, a customer's email address, phone number (cellular/mobile, work, home, pager, etc.), username, social network identity (such as a Facebook or Twitter account), or the like. Additionally, these identifiers can be used to generate another identifier (such as a hexadecimal or encrypted value) for

use in the payment request. Further, other identifiers may be used in some embodiments.

[037] In step 201B, Acquirer Processor 201 generates a transaction request. In some embodiments, these transaction requests will be in the form of a balance inquiry transaction. A balance inquiry transaction may occur when an entity operating Acquirer Processor 201 (*e.g.* a merchant, a bank, or the like) desires to find out whether the customer's account contains the funds required to make a purchase. In other embodiments, these transaction requests will be in the form of debiting or crediting instructions. In some embodiments, transaction requests generated in step 201B can be in the form of, or based on, the ISO 8583 message standard, as will be described later with respect to figures 3 and 4. Such messages may also contain information such as the type of transaction, the amount of the transaction, the date, the time, the location information, or the like. In step 201C, Acquirer Processor 201 can submit the generated transaction request to Network 203.

[038] In some embodiments, Network 203 (which, in some embodiments, may be implemented as described above with respect to Network 103) is chosen by Acquirer Processor 201 for processing transactions. Network 203, in some embodiments, can be an Interbank Network (such as NYCE, INTERAC, or the like) as mentioned previously. Network 203 may be enabled to provide proper routing of received transaction requests. This can be done, for example, by determining the RTN and/or other information about the payment type. This is represented in steps 203A and 203B, and can be done in part by determining the existence of a particular value in the transaction request. In some embodiments, this may involve determining the existence of the numbers '59' (or another particular piece of data) at a particular position in the transaction request. A '59' signifies that the characters following it contain an ABA value.

[039] In other embodiments, for example, those involving a pseudo identity of the user (such as usernames, social network identities, phone numbers, or e-mail addresses), Network 203 may determine the appropriate routing by consulting a data store. After determining the existence of a particular value in the transaction request, Network 203 may determine that the characters following the particular value represent an RTN, and may route the transaction as represented in step 203B to

EFT Processing 205. In some embodiments, step 203B may be performed shortly after a routing process (e.g., step 203A) is performed. In other embodiments, the process of routing in step 203B may be performed on a batch or bulk basis. For example, if the transaction was submitted to Payment Network 203 during the afternoon of a first business day (e.g., step 201C), determining the proper routing in step 203A and/or routing that transaction request in step 203B may be performed later that evening, along with determining and routing of other transaction requests received the same day.

[040] EFT Processing 205, as well as Authorization Processing 207 and Core Processing 209, can, in some embodiments, be part of a broader Accounting Processor system 211. (In some embodiments, Accounting Processor system 211 may be implemented as described above with respect to Accounting Processor 105.) In FIG. 2, these Processing systems are represented as three separate systems, but any or all may be implemented on a single computer or multiple computers. In step 205A, EFT Processor 205 may determine the transaction parameters present in the forwarded transaction request in order to determine the proper Authorization Processing system 207 to send the request to for processing. Again, this may involve determining the routing based on a particular value that is present in the transaction request (such as the RTN).

[041] Once Authorization Processing 207 receives the transaction request in step 205B, the process continues to step 207A for account determination. Authorization Processing 207 may then determine the proper account. This could be accomplished by inspecting the transaction request (and extracting an account number), consulting a cross-reference database (not pictured) to determine the proper account number/identifier based on information in the transaction, or the like. Once this account number/identifier is determined, a request may be sent to Core Processing 209 with that account number/identifier. This request, in some embodiments, comprises a request for the current balance of the account referenced by that account number/identifier. In other embodiments, the request can comprise other operation requests, such as debiting, crediting, or the like.

[042] When Core Processing 209 receives the request in step 207B, it may take some or all of a number of actions. Core Processing 209 may provide the balance associated with the account referenced in the transaction request back to

Authorization Processing 207. Core Processing 209 may debit or credit based on the amount of money referenced in the transaction request, and provide the new balance (*i.e.* after the debit/credit) back to Authorization Processing 207. In other embodiments, based on the particular transaction request, Core Processing 209 may respond differently, such as with an indication that the available balance is less than (or more than) the amount in the transaction request; an indication that the ledger balance is less than (or more than) the amount in the transaction request; an indication of the health of the account (such as whether the account is open and/or in good standing; an indication of how long the account has been open for; an indication of any negative history associated with the account, average balance ranges, or the like); the account owner's name, address, date the account was opened, or other information; or the like. Any or all of these items may make up a part of the response by Core Processing 209 in step 207C.

[043] Upon receiving the response in step 207C, Authorization Processing 207 may determine, based on the content of the request, whether the transaction should be approved or denied. For example, if the response in 207C indicates that the account has less money than is required to effect the purchase transaction referenced by the original transaction request, Authorization Processing 207 may deny the transaction, and may construct a denial message for sending back to Acquirer Processor 201, via steps 205C, 203C, and 201D. If the account has enough money to cover the transaction, Authorization Processing 207 may approve the transaction, and send back an approval message via the same steps.

[044] Authorization Processing 207 may also send back other messages, such as messages indicating the amount of money available in an account, a status of the account (such as whether the account is open or closed), an owner of the account, or a request for more information from the user. Other messages may also be sent, as will be appreciated by those having ordinary skill in the art.

[045] FIG. 3 is an example message format 300 for use with the disclosed systems and methods, in accordance with disclosed embodiments. Messages based on message format 300, in some embodiments, are used to transmit data between the devices in FIGS. 1 and 2. In some embodiments, the data elements in message format 300 may be based on the ISO 8583 message standard. Any of the revisions of this standard may be used, as well as other standards. In other embodiments,

other messages may be used and the particular data sizes and fields in FIG. 3 may vary. Furthermore, in some embodiments, the particular data fields in FIG. 3 may contain data as described in FIG. 3. For example, the DE12 data element may contain 6 bytes indicating the local time at a terminal where a transaction is taking place.

[046] In some embodiments, a message as described with respect to message format 300 could include DE2 304 (*i.e.* "Data Element 2" 304) storing a "constructed PAN." As mentioned above, PANs are generally used in the art to represent credit card numbers. PANs may comply with or be based on ISO 7812, which defines which card issuers use the first digits of the PAN. For example, a '4' in the first position of the PAN may signify VISA, while a value of '53' may signify MasterCard.

[047] In some embodiments, the PAN can be constructed of multiple portions. The PAN may comprise a pseudo card number, which may be constructed based on pre-agreed identifiers for an account (*e.g.* the above-mentioned RTN or IBAN). In some embodiments, a '59' is used in the first two spaces to signify that the PAN is a constructed value. A nine-digit RTN or other identifier may follow, and following that would be an eight digit value indicating time and date. This mode of operation has been previously referred to in this disclosure as "native mode."

[048] In order to identify the particular account used by the customer, other portions of message 300 can store the actual account number. For example, in some embodiments, the user's particular deposit account could be stored in another portion of the message; for example, in DE102 323.

[049] In other embodiments, the PAN can be constructed as a pseudo-identifier. That is, the PAN itself could be constructed as a cross-reference to an account number. So, upon receiving the PAN, an issuing bank could consult a table, database, or other data store, in order to determine the account number associated with the pseudo-identifier. The account number could then be used to debit the account or perform other actions. In some embodiments, the PAN may be constructed as a single- or limited-use string of numbers (for example, composed of 19 decimal digits or hexadecimal numbers), a hash of the account number, an encrypted string representing the account number, or the like. This mode of

operation has been previously referred to in this disclosure as "non-native mode" or "X-REF mode."

[050] After identifying the account associated with either the account number stored in message 300 or the pseudo-identifier stored in 300, an issuer would be able to determine the proper account and process payment transactions. For example, this could include returning a balance, authorizing a payment, or the like, as previously mentioned with respect to FIG. 2.

[051] FIG. 4 represents some data elements that make up the message described in FIG. 3 above. To start, Data Element 2 (DE2) is represented as 401 in FIG. 4. In some embodiments, DE2 is used to store a constructed PAN. The first two spaces indicate how many characters will follow (in example FIG. 4, this is '19'). Thus, DE2 is 21 characters long in total, including the '19' at the beginning. Each of these characters, in some embodiments, may be a single digit (*i.e.* 0-9); however, in other embodiments, a larger character set is usable (e.g. hexadecimal code). After the '19,' a PAN will follow. In example FIG. 4, a constructed PAN is represented as characters 3-21 in DE2. A '59' signifies that the characters following it contain an ABA value. (However, other characters, including other numbers, letters, or the like, may be used to signify that the following value is an ABA value.) The 'R' characters represent the previously mentioned RTN, and the string 'DDHHMMSS' represents the time of the transaction (*i.e.* Day, Hour, Minute, Second).

[052] Data Element 32 (DE32) 402, in some embodiments, is used to identify the Acquiring institution, for example, Acquirer Processor 101, in order to properly route the response back to sending party. DE32 enables a network, such as Network 103, to recognize transactions as coming from a particular acquirer, such as a merchant. The first two digits ('11') signify the length of the data, and the second two digits ('59') represent that a non-card based transaction will take place. The final 9 'I' characters represent an institution ID, that is, the ID of the institution that originated the message.

[053] Continuing to Data Element 52 (DE58) 403, this data element contains a number of bits signifying attributes of the transaction. In some embodiments, DE58 may be constructed as follows:

| | |
|---|---|
| 011 | signifying the length of the field – in this case, 11 characters long |
| 0 | signifying whether a transaction was attended – in this case, not at a stand-alone terminal |
| 1 | signifying whether a merchant operated the terminal – in this case, that a merchant operated the terminal |
| 1 | signifying whether the transaction was made at a physical location associated with the acquirer institution – in this case, that the transaction was made at a device not at a location associated with the acquirer institution, such as at an ATM device not located at an associated bank's branch |
| 0 | signifying whether the customer is present – in this case, that the customer is not present |
| 0 | signifying whether a card is present – in this case, that the card is not present, and that the R&T number should be checked |
| 0 | signifying whether the merchant's terminal has "card retention" capability, e.g., the ability to keep a physical plastic card if instructed by an issuer (such as an ATM keeping a card in response to the issuer recognizing a stolen card) – in this case, that the merchant's terminal does not have this capability |
| 0 | signifying whether this is the first time that the transaction has been attempted, e.g., because the first attempt to process this transaction did |

| | |
|---|---|
| | not work properly – in this case, that this is not the first attempt at this transaction |
| 0 | signifying whether a security check was performed (e.g., whether a driver's license or other identification document was checked by a merchant) – in this case, that no security check was performed |
| 00 | signifying whether the terminal is an "administrative" terminal (e.g., a merchant terminal directly or indirectly operated by a merchant or cashier, such as a checkout line at a supermarket) or a "non-administrative" terminal (e.g., a non-merchant operated terminal, such as a stand-alone terminal operated by a customer, a website, an Automated Teller Machine, etc.) was used to effect the transaction request – in this case, that the terminal was a non-administrative terminal |
| 1 | signifying whether transaction data for this transaction was manually entered by a merchant (e.g., using a keypad) or automatically entered (e.g., using a magnetic card or other device to receive the transaction data) |

[054] However, other values are possible for each of the data elements, based on the individual characteristics of each transaction.

[055] Moving on to Data Element 102 (DE102) 404, this data element may, in some embodiments, be used to signify the purchaser's account information. In the ISO 8583 specification, this is referred to as the "Account ID 1." In some embodiments, this may signify, as mentioned previously, the account data for the user's deposit account. As depicted in FIG. 4, DE102 consists of '028', signifying that

a 28-character string will follow. In some embodiments, these 28 characters may consist of digits from the MICR (Magnetic Ink Character Recognition) line of a check given to the merchant by the customer.

[056] FIG. 5 discloses an example computer system 500 for use with the disclosed systems and methods, in accordance with disclosed embodiments. Example computer system 500 may power any of the methods, systems, devices, or computer-readable media mentioned above, in addition to those disclosed in FIGS. 1-3.

[057] In some embodiments, computer system 500 may be implemented as a cellular phone, a mobile device, a POS (point-of-sale) device, a server, a wireless device, or any other system that includes at least some of the components of FIG. 5. Computer system 500 contains a Central Processing Unit 501, which enables data to flow between the other components and otherwise manages the operation of the other components in computer system 500. CPU 501, in some embodiments, may be any of a general-purpose processor (such as an Intel- or AMD-branded consumer/business/enterprise processor), a special-purpose processor (for example, a graphics-card processor), or any other kind of processor that enables input and output of data.

[058] Also part of Computer system 500 is Input Device 502. In some embodiments, Input Device 502 may be any device that enables a user or other entity to input data. For example, Input Device 502 could be a keyboard, a mouse, or the like. Input Device 502 can be used to control the operation of the other components of FIG. 5.

[059] Computer system 500 also includes Storage Device 503. Storage Device 503 stores data that is usable by the other components in computer system 500, including data that has previously been referenced and referred to in FIGS. 1-4. Storage Device 503 may, in some embodiments, be implemented as any or all of a hard drive, temporary memory, permanent memory, optical memory, or any other type of permanent or temporary storage device.

[060] Computer system 500 also includes Power Unit 506. Power Unit 506 provides the electricity necessary to power the other components in computer system 500. For example, in some embodiments, CPU 501 may need power to

operate; Power Unit 506 can provide the necessary electric current to power this component.

[061] Computer System 500 also includes Network Adapter 505. Network Adapter 505, in some embodiments, enables communication with other devices that are implemented in the same or similar way as computer system 500. Network Adapter 500, in some embodiments, may allow communication to and/or from a network such as the Internet; other networks are possible as well. Network Adapter 500 may be implemented using any or all of known or as-yet-unknown wired or wireless technologies (such as Ethernet, 802.11a/b/g/n (aka Wi-Fi), cellular (e.g. GSM, CDMA, LTE), or the like).

[062] Additionally, any of the components in FIG. 5 may be implemented as one or more of the illustrated components. For example, in some embodiments, CPU 501 may be implemented as any of multiple computer processors, a processor and a co-processor, or a single processor. For example, in some embodiments, Storage Device 503 may be implemented as any of Random Access Memory (RAM), Read-Only Memory, a hard drive, USB storage, a CD/DVD/Blu-Ray disk, or the like. The particular number of each component as illustrated in FIG. 5 is not controlling and a person skilled in the art will understand the appropriate number of each component for each particular implementation of the disclosed embodiments.

[063] Other embodiments of the disclosed embodiments will be apparent to those skilled in the art from consideration of the specification and practice of the disclosed embodiments disclosed herein. It is intended that the specification and examples be considered as examples only, with a true scope and spirit of the disclosed embodiments being indicated by the following claims.

[064] Furthermore, the disclosed embodiments may be implemented in part or in full on various computers, electronic devices, computer-readable media (such as CDs, DVDs, flash drives, hard drives, or other storage), or other electronic devices or storage devices.

WHAT IS CLAIMED IS:

1. A method for processing payment transactions via a network, comprising:

when a received transaction request is determined to represent a transaction that does not require a card number or account number:

providing the transaction request to a selected accounting processor;

receiving a response from the selected accounting processor, the received response comprising a selected account for the transaction request, and an account balance associated with the selected account; and

based on the received response, determining whether to (i) approve the transaction request, (ii) deny the transaction request, or (iii) take further action other than to approve the transaction request or to deny the transaction request.

2. The method of claim 1, wherein:

the transaction request comprises a pseudo-identifier;

the selected account is selected based at least in part on the pseudo-identifier; and

the selecting of the accounting processor is based at least in part on the pseudo-identifier.

3. The method of claim 1, wherein:

the transaction request includes at least one of an ABA number, a Routing Transit Number (RTN), a Canadian Transit Number, a sort code, a branch code, a bank code, or a date, time, or day; and

the selecting of the accounting processor is based at least in part on the least one of an ABA number, a Routing Transit Number (RTN), a Canadian Transit Number, a sort code, a branch code, a bank code, or a date, time, or day, in the transaction request.

4. The method of claim 1, wherein the transaction request is formatted to comply with ISO 8583.

5. The method of claim 1, wherein the transaction request comprises at least one of:

a request for a current balance of the account;

a request for whether the available balance is more than, less than, or equal to an amount in the transaction request;

a request for whether the ledger balance is more than, less than, or equal to an amount in the transaction request;

a request for an indication of the health of the account; or

a request for information about the owner of the account.

6. The method of claim 1, wherein the network is an interbank network comprising one or more banks.

7. The method of claim 1, wherein taking further action comprises at least one of:

approving a transaction requested by the transaction request;

denying the transaction requested by the transaction request;

returning a monetary amount contained in the account;

requesting further information; or

returning other information.

8. A method for processing payment transactions via a network, comprising:

receiving, from the network, a request associated with a transaction determined not to require a card number or account number;

selecting an account for the transaction, based at least in part on information in the request;

determining a balance of the selected account; and

generating a response based on the request, comprising information for the determination of whether to approve or deny the request.

9. The method of claim 8, wherein:

the transaction request comprises a pseudo-identifier; and

the selecting an account is based at least in part on the pseudo-identifier.

10. The method of claim 9, wherein the pseudo-identifier identifies an account and selecting an account further comprises:

identifying the account from among a group of deposit accounts using the pseudo-identifier; and

retrieving information on the identified account.

11. The method of claim 8, wherein the transaction request is formatted to comply with ISO 8583.

12. The method of claim 8, wherein the transaction request comprises at least one of:

a request for a current balance of the account;

a request for whether the available balance is more than, less than, or equal to an amount in the transaction request;

a request for whether the ledger balance is more than, less than, or equal to an amount in the transaction request;

a request for an indication of the health of the account; or

a request for information about the owner of the account.

13. The method of claim 8, wherein the network is an interbank network.

14. A method for processing a payment transaction, comprising:

receiving information by at least one computer system for conducting a payment transaction that does not require a card number or account number, wherein the information does not include a card number or account number;

generating a transaction request based on the information, including at least one identifier;

sending the transaction request to a payment network for processing;

receiving at least one response to the transaction request, based on at least one account associated with the identifier.

15. The method of claim 14, wherein the identifier comprises a pseudo-identifier, such that the pseudo-identifier allows determination of the at least one account associated with the identifier.

16. The method of claim 14, wherein:

the transaction request includes at least one of an ABA number, a Routing Transit Number (RTN), a Canadian Transit Number, a sort code, a branch code, a bank code, or a date, time, or day; and

the selecting of the accounting processor is based at least in part on the least one of an ABA number, a Routing Transit Number (RTN), a Canadian Transit Number, a sort code, a branch code, a bank code, or a date, time, or day, in the transaction request.

17. The method of claim 14, wherein the transaction request is formatted to comply with ISO 8583.

18. The method of claim 14, wherein the transaction request comprises at least one of:

a request for a current balance of the at least one account;

a request for whether the available balance in the at least one account is more than, less than, or equal to an amount in the transaction request;

a request for whether the ledger balance in the at least one account is more than, less than, or equal to an amount in the transaction request;

a request for an indication of the health of the at least one account; or

a request for information about the owner of the at least one account.

19. The method of claim 14, wherein the at least one response comprises at least one of:

a message approving the transaction request;

a message denying the transaction request;

a message returning a monetary amount contained in the at least one account;

a message requesting further information; or

a message returning other information.

20. The method of claim 14, wherein the at least one computer system is operated by at least one of a bank or a merchant.

21. A computer system for processing payment transactions via a network, comprising:

at least one processor; and

memory containing instructions that, when executed by the at least one processor, cause the at least one processor to perform a method comprising:

when a received transaction request is determined to represent a transaction that does not require a card number or account number:

providing the transaction request to a selected accounting processor;

receiving a response from the selected accounting processor, the received response comprising a selected account for the transaction request, and an account balance associated with the selected account; and

based on the received response, determining whether to (i) approve the transaction request, (ii) deny the transaction request, or (iii) take further action other than to approve the transaction request or to deny the transaction request.

22. The system of claim 21, wherein:

the transaction request comprises a pseudo-identifier;

the selected account is selected based at least in part on the pseudo-identifier; and

the selecting of the accounting processor is based at least in part on the pseudo-identifier.

23. The system of claim 21, wherein:

the transaction request includes at least one of an ABA number, a Routing Transit Number (RTN), a Canadian Transit Number, a sort code, a branch code, a bank code, or a date, time, or day; and

the selecting of the accounting processor is based at least in part on the least one of an ABA number, a Routing Transit Number (RTN), a Canadian Transit Number, a sort code, a branch code, a bank code, or a date, time, or day, in the transaction request.

24. The system of claim 21, wherein the transaction request is formatted to comply with ISO 8583.

25. The system of claim 21, wherein the transaction request comprises at least one of:

a request for a current balance of the account;

a request for whether the available balance is more than, less than, or equal to an amount in the transaction request;

a request for whether the ledger balance is more than, less than, or equal to an amount in the transaction request;

a request for an indication of the health of the account; or

a request for information about the owner of the account.

26. The system of claim 21, wherein the network is an interbank network comprising one or more banks.

27. The system of claim 21, wherein the step of taking further action comprises at least one of:

approving a transaction requested by the transaction request;

denying the transaction requested by the transaction request;

returning a monetary amount contained in the account;

requesting further information; or

returning other information.

28. A computer system for processing payment transactions via a network, comprising:

at least one processor; and

memory containing instructions that, when executed by the at least one processor, cause the at least one processor to perform a method comprising:

receiving, from the network, a request associated with a transaction determined not to require a card number or account number;

selecting an account for the transaction, based at least in part on information in the request;

determining a balance of the selected account; and generating a response based on the request, comprising information for the determination of whether to approve or deny the request.

29. The system of claim 28, wherein:

the transaction request comprises a pseudo-identifier; and

the selecting an account is based at least in part on the pseudo-identifier.

30. The system of claim 29, wherein the pseudo-identifier identifies an account and the step of selecting an account further comprises:

identifying the account from among a group of deposit accounts using the pseudo-identifier; and

retrieving information on the identified account.

31. The system of claim 28, wherein the transaction request is formatted to comply with ISO 8583.

32. The system of claim 28, wherein the transaction request comprises at least one of:

a request for a current balance of the account;

a request for whether the available balance is more than, less than, or equal to an amount in the transaction request;

a request for whether the ledger balance is more than, less than, or equal to an amount in the transaction request;

a request for an indication of the health of the account; or

a request for information about the owner of the account.

33. The system of claim 28, wherein the network is an interbank network.

34. A computer system for processing a payment transaction, comprising:

at least one processor; and

memory containing instructions that, when executed by the at least one processor, cause the at least one processor to perform a method comprising:

receiving information for conducting a payment transaction that does not require a card number or account number, wherein the information does not include a card number or account number;

generating a transaction request based on the information, including at least one identifier;

sending the transaction request to a payment network for processing;

receiving at least one response to the transaction request, based on at least one account associated with the identifier.

35. The system of claim 34, wherein the identifier comprises a pseudo-identifier, such that the pseudo-identifier allows determination of the at least one account associated with the identifier.

36. The system of claim 34, wherein:

the transaction request includes at least one of an ABA number, a Routing Transit Number (RTN), a Canadian Transit Number, a sort code, a branch code, a bank code, or a date, time, or day; and the selecting of the accounting processor is based at least in part on the least one of an ABA number, a Routing Transit Number (RTN), a Canadian Transit Number, a sort code, a branch code, a bank code, or a date, time, or day, in the transaction request.

37. The system of claim 34, wherein the transaction request is formatted to comply with ISO 8583.

38. The system of claim 34, wherein the transaction request comprises at least one of:

a request for a current balance of the at least one account;

a request for whether the available balance in the at least one account is more than, less than, or equal to an amount in the transaction request;

a request for whether the ledger balance in the at least one account is more than, less than, or equal to an amount in the transaction request;

a request for an indication of the health of the at least one account; or

a request for information about the owner of the at least one account.

39. The system of claim 34, wherein the at least one response comprises at least one of:

a message approving the transaction request;

a message denying the transaction request;

a message returning a monetary amount contained in the at least one account;

a message requesting further information; or

a message returning other information.

40. The system of claim 34, wherein the system is operated by at least one of a bank or a merchant.

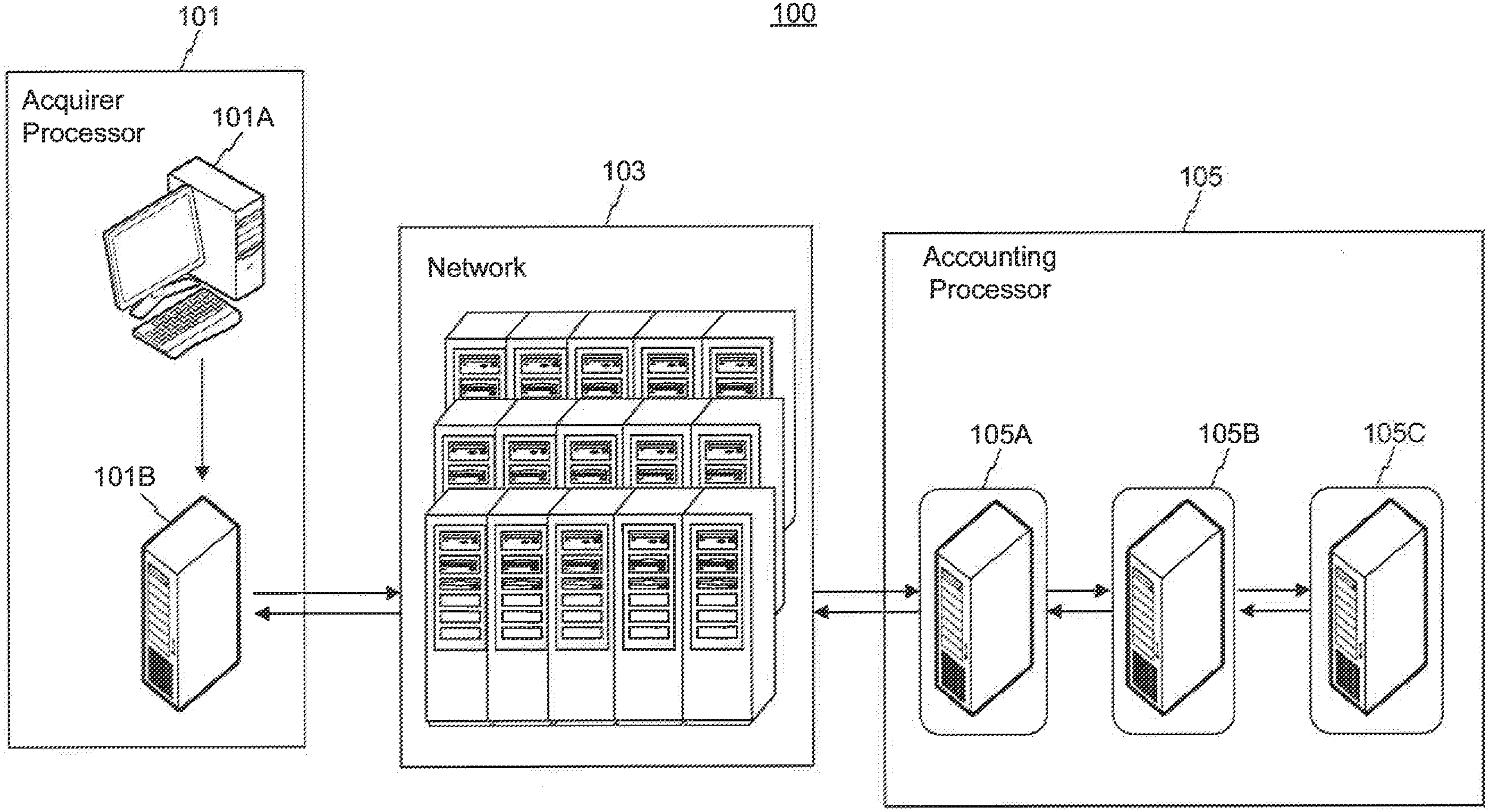

100
101
Acquirer
Processor
101A
101B
103
Network
105
Accounting
Processor
105A
105B
105C

FIG. 1

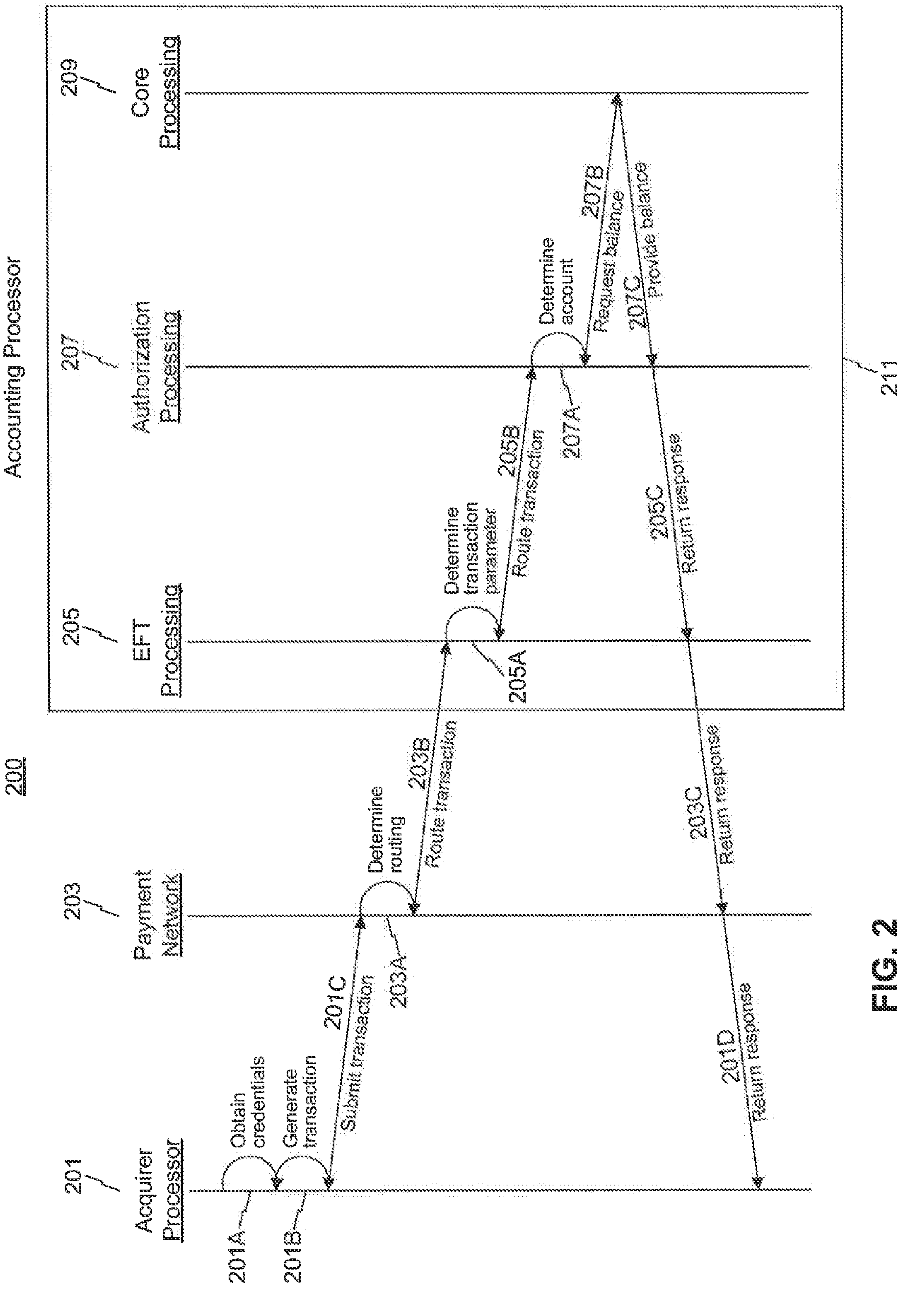
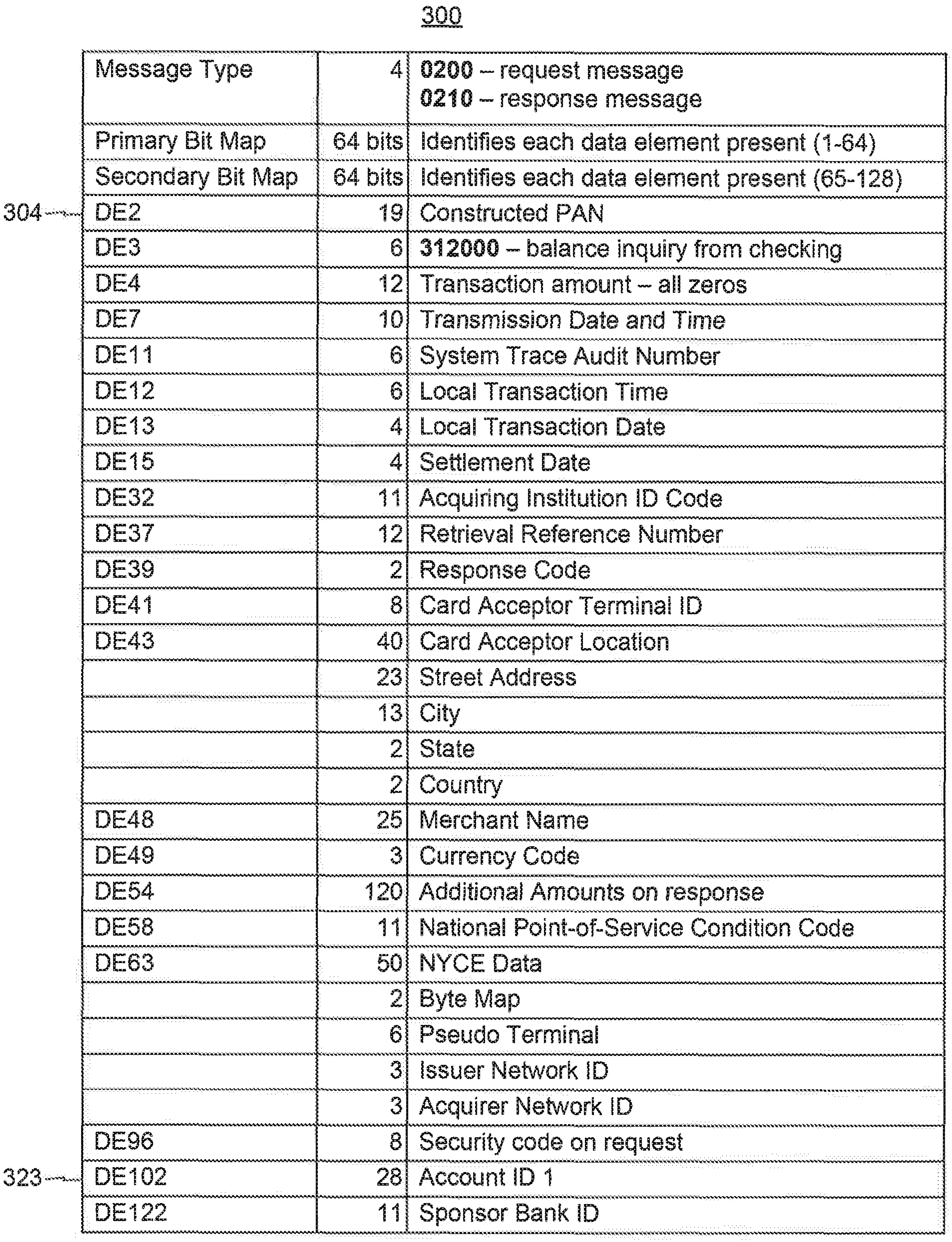

200
Accounting Processor
211
201
Acquirer Processor
203
Payment Network
205
EFT Processing
207
Authorization Processing
209
Core Processing
201A
201B
Obtain credentials
Generate transaction
201C
Submit transaction
203A
Determine routing
203B
Route transaction
205A
Determine transaction parameter
205B
Route transaction
207A
Determine account
207B
Request balance
207C
Provide balance
205C
Return response
203C
Return response
201D
Return response

FIG. 2



| | | |
|---|---|---|
| Message Type | 4 | **0200** – request message<br>**0210** – response message |
| Primary Bit Map | 64 bits | Identifies each data element present (1-64) |
| Secondary Bit Map | 64 bits | Identifies each data element present (65-128) |
| DE2 | 19 | Constructed PAN |
| DE3 | 6 | **312000** – balance inquiry from checking |
| DE4 | 12 | Transaction amount – all zeros |
| DE7 | 10 | Transmission Date and Time |
| DE11 | 6 | System Trace Audit Number |
| DE12 | 6 | Local Transaction Time |
| DE13 | 4 | Local Transaction Date |
| DE15 | 4 | Settlement Date |
| DE32 | 11 | Acquiring Institution ID Code |
| DE37 | 12 | Retrieval Reference Number |
| DE39 | 2 | Response Code |
| DE41 | 8 | Card Acceptor Terminal ID |
| DE43 | 40 | Card Acceptor Location |
| | 23 | Street Address |
| | 13 | City |
| | 2 | State |
| | 2 | Country |
| DE48 | 25 | Merchant Name |
| DE49 | 3 | Currency Code |
| DE54 | 120 | Additional Amounts on response |
| DE58 | 11 | National Point-of-Service Condition Code |
| DE63 | 50 | NYCE Data |
| | 2 | Byte Map |
| | 6 | Pseudo Terminal |
| | 3 | Issuer Network ID |
| | 3 | Acquirer Network ID |
| DE96 | 8 | Security code on request |
| DE102 | 28 | Account ID 1 |
| DE122 | 11 | Sponsor Bank ID |

FIG. 3

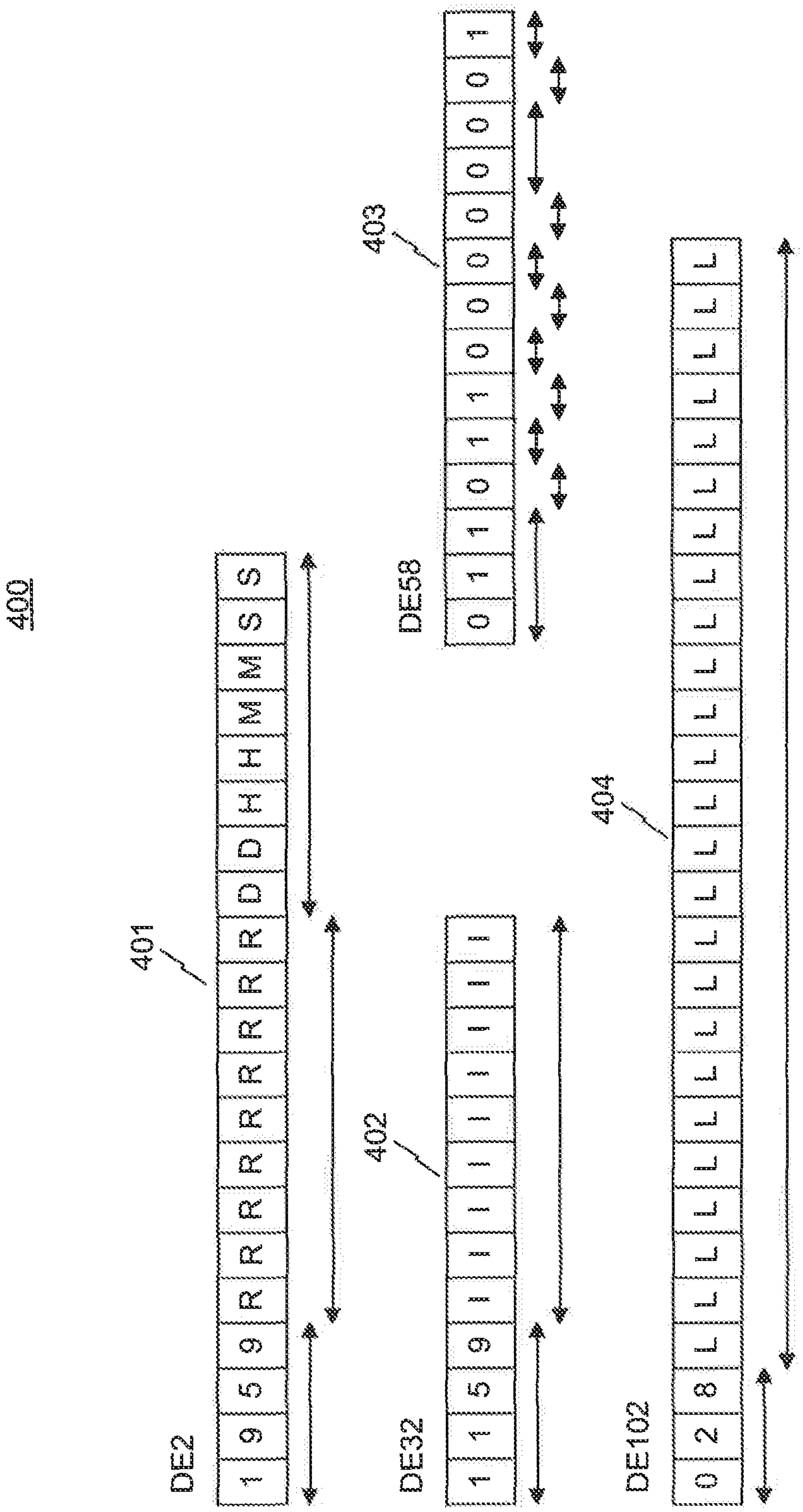

400
401
402
403
404
DE2
1 9 5 9 R R R R R R R R R D D H H M M S S
DE32
1 1 5 9 I I I I I I I I I
DE58
0 1 1 0 1 1 0 0 0 0 0 0 0 1
DE102
0 2 8 L L L L L L L L L L L L L L L L L L L L L L L L L

FIG. 4

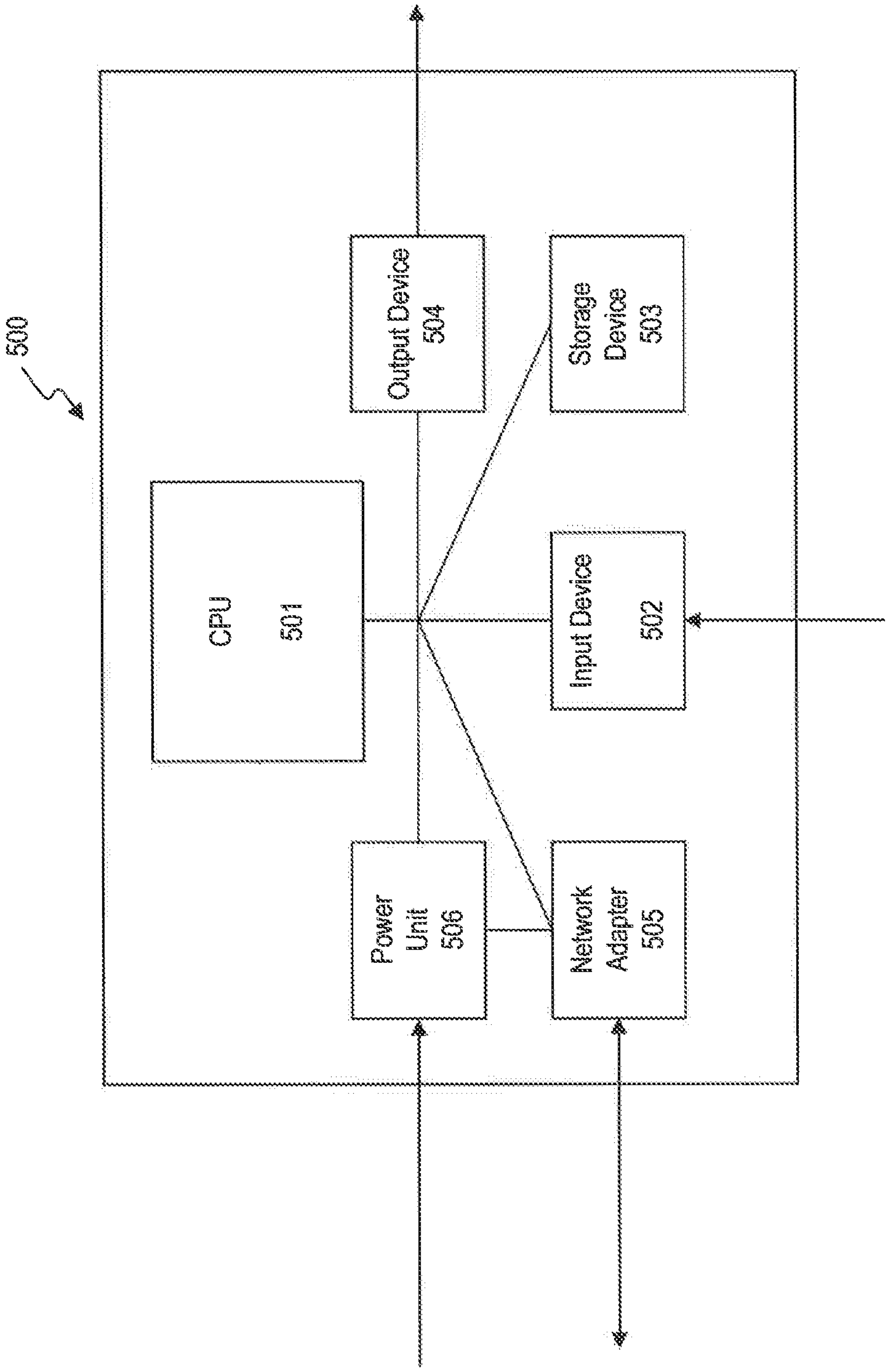

500
CPU
501
Output Device
504
Storage
Device
503
Input Device
502
Power
Unit
506
Network
Adapter
505

FIG. 5

# INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2013/032130

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06Q 20/00 (2013.01)
USPC - 705/39
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC(8) - G07F 7/02; G06Q 20/00; 20/04 (2013.01)
USPC - 235/380; 705/35, 39

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
CPC- G07F 7/02; G06Q 20/00; 20/04 (2013.01)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Orbit.com, Google Patents, Google.com

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X<br>-----<br>Y | WO 01/43084 A2 (PIELEMEIER et al) 14 June 2001 (14.06.2001) entire document | 14, 15, 19, 20, 34,35, 39, 40<br>-----<br>1-13, 16-18, 21-33, 36-38 |
| Y | US 2008/0167017 A1 (WENTKER et al) 10 July 2008 (10.07.2008) entire document | 1-13, 18, 21-33, 38 |
| Y | US 2012/0041876 A1 (NOSEK et al) 16 February 2012 (16.02.2012) entire document | 3, 10, 16, 23, 30, 36 |
| Y | US 2012/0016799 A1 (KILLIAN et al.) 19 January 2012 (19.01.2012) entire document | 4, 11, 17, 24, 31, 37 |
| A | WO 2009/003030 A2 (CARLSON) 31 December 2008 (31.12.2008) entire document | 1-40 |
| A | US 2008/0319869 A1 (CARLSON et al) 25 December 2008 (25.12.2008) entire document | 1-40 |

□ Further documents are listed in the continuation of Box C. □

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

| | |
|---|---|
| Date of the actual completion of the international search<br>20 May 2013 | Date of mailing of the international search report<br>05 JUN 2013 |
| Name and mailing address of the ISA/US<br>Mail Stop PCT, Attn: ISA/US, Commissioner for Patents<br>P.O. Box 1450, Alexandria, Virginia 22313-1450<br>Facsimile No. 571-273-3201 | Authorized officer:<br>Blaine R. Copenheaver<br>PCT Helpdesk: 571-272-4300<br>PCT OSP: 571-272-7774 |

(19) 中华人民共和国国家知识产权局

(12) 发明专利申请

(10) 申请公布号 CN 104303197 A
(43) 申请公布日 2015.01.21

(21) 申请号 201380026008.9

(22) 申请日 2013.03.15

(30) 优先权数据
61/612,897 2012.03.19 US

(85) PCT国际申请进入国家阶段日
2014.11.18

(86) PCT国际申请的申请数据
PCT/US2013/032130 2013.03.15

(87) PCT国际申请的公布数据
WO2013/142334 EN 2013.09.26

(71) 申请人 派奈特支付网络有限责任公司
地址 美国佛罗里达州

(72) 发明人 N·马库斯 R·伍德伯里 P·戈登

(74) 专利代理机构 北京三友知识产权代理有限公司 11127
代理人 吕俊刚 刘久亮

(51) Int. Cl.
*G06Q 20/10* (2012.01)
*G06Q 20/40* (2012.01)

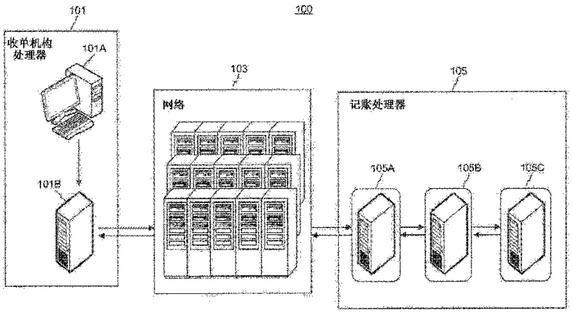
权利要求书5页 说明书9页 附图5页

(54) 发明名称

用于实时的账户访问的系统和方法

(57) 摘要

用于实时的账户访问的系统和方法允许通过诸如电子资金转账(EFT)这样的网络处理架构来访问账户(诸如存款账户、信用账户或借记账户)。在某些实施方式中,消费者和/或商家能够使用伪标识符或其它标识符并且在无需提供账号或卡号的情况下实现针对账户的交易请求。在其它实施方式中,支付网络能够在无需卡号或账号的情况下路由和处理针对账户的交易请求。在其它实施方式中,账户处理系统能够基于不包含卡号或账号的交易请求来确定适当的账户。



1. 一种用于经由网络处理支付交易的方法，该方法包括：

当接收到的交易请求被确定为表示不需要卡号或账号的交易时：

向选择的记账处理器提供所述交易请求；

从所选择的记账处理器接收响应，接收到的响应包括针对所述交易请求而选择的账户和与所选择的账户相关联的账户余额；以及

根据接收到的响应，确定是 (i) 批准所述交易请求，(ii) 拒绝所述交易请求，还是 (iii) 采取除了批准所述交易请求或拒绝所述交易请求以外的进一步行动。

2. 根据权利要求 1 所述的方法，其中：

所述交易请求包括伪标识符；

所选择的账户至少部分地基于所述伪标识符来选择；并且

选择所述记账处理器至少部分地基于所述伪标识符。

3. 根据权利要求 1 所述的方法，其中：

所述交易请求包括 ABA 号码、路由转账号码 RTN、加拿大转账号码、分类代码、分支机构代码、银行代码、或者日期、时间或天中的至少一个；并且

选择所述记账处理器至少部分地基于所述交易请求中的 ABA 号码、路由转账号码 RTN、加拿大转账号码、分类代码、分支机构代码、银行代码、或者日期、时间或天中的至少一个。

4. 根据权利要求 1 所述的方法，其中，所述交易请求被格式化以符合 ISO 8583。

5. 根据权利要求 1 所述的方法，其中，所述交易请求包括以下至少一项：

对所述账户的当前余额的请求；

对可用余额是大于、小于还是等于所述交易请求中的金额的请求；

对分类账余额是大于、小于还是等于所述交易请求中的金额的请求；

对所述账户的健康状况的指示的请求；或者

对与所述账户的所有者有关的信息的请求。

6. 根据权利要求 1 所述的方法，其中，所述网络是包括一个或更多个银行的同业银行网络。

7. 根据权利要求 1 所述的方法，其中，采取进一步行动包括以下至少一项：

批准所述交易请求所请求的交易；

拒绝所述交易请求所请求的所述交易；

返回所述账户中包含的货币金额；

请求另外的信息；或者

返回其它信息。

8. 一种用于经由网络处理支付交易的方法，该方法包括：

从所述网络接收与被确定为不需要卡号或账号的交易相关联的请求；

至少部分地基于所述请求中的信息，选择用于所述交易的账户；

确定所选择的账户的余额；以及

基于所述请求生成响应，所述响应包括用于确定是批准还是拒绝所述请求的信息。

9. 根据权利要求 8 所述的方法，其中：

所述交易请求包括伪标识符；并且

选择账户至少部分地基于所述伪标识符。

10. 根据权利要求 9 所述的方法，其中，所述伪标识符标识账户，并且选择账户还包括：

使用所述伪标识符从一组存款账户中识别出所述账户；以及

检索关于所识别的账户的信息。

11. 根据权利要求 8 所述的方法，其中，所述交易请求被格式化以符合 ISO 8583。

12. 根据权利要求 8 所述的方法，其中，所述交易请求包括以下至少一项：

对所述账户的当前余额的请求；

对可用余额是大于、小于还是等于所述交易请求中的金额的请求；

对分类账余额是大于、小于还是等于所述交易请求中的金额的请求；

对所述账户的健康状况的指示的请求；或者

对与所述账户的所有者有关的信息的请求。

13. 根据权利要求 8 所述的方法，其中，所述网络是同业银行网络。

14. 一种用于处理支付交易的方法，该方法包括：

由进行不需要卡号或账号的支付交易的至少一个计算机系统接收信息，其中，所述信息不包括卡号或账号；

基于所述信息生成交易请求，所述交易请求包括至少一个标识符；

将所述交易请求发送至支付网络进行处理；

基于与所述标识符相关联的至少一个账户，接收对所述交易请求的至少一个响应。

15. 根据权利要求 14 所述的方法，其中，所述标识符包括伪标识符，使得所述伪标识符允许确定与所述标识符相关联的所述至少一个账户。

16. 根据权利要求 14 所述的方法，其中：

所述交易请求包含 ABA 号码、路由转账号码 RTN、加拿大转账号码、分类代码、分支机构代码、银行代码、或者日期、时间或天中的至少一个；以及

选择所述记账处理器至少部分地基于所述交易请求中的 ABA 号码、路由转账号码 RTN、加拿大转账号码、分类代码、分支机构代码、银行代码、或者日期、时间或天中的至少一个。

17. 根据权利要求 14 所述的方法，其中，所述交易请求被格式化以符合 ISO 8583。

18. 根据权利要求 14 所述的方法，其中，所述交易请求包括以下至少一项：

对所述至少一个账户的当前余额的请求；

对所述至少一个账户中的可用余额是大于、小于还是等于所述交易请求中的金额的请求；

对所述至少一个账户中的分类账余额是大于、小于还是等于所述交易请求中的金额的请求；

对所述至少一个账户的健康状况的指示的请求；或者

对与所述至少一个账户的所有者有关的信息的请求。

19. 根据权利要求 14 所述的方法，其中，所述至少一个响应包括以下至少一项：

批准所述交易请求的消息；

拒绝所述交易请求的消息；

返回所述至少一个账户中包含的货币金额的消息；

请求另外信息的消息；或者

返回其它信息的消息。

20. 根据权利要求 14 所述的方法，其中，所述至少一个计算机系统由银行或商家中的至少一方来操作。

21. 一种用于经由网络处理支付交易的计算机系统，该计算机系统包括：

至少一个处理器；以及

存储器，该存储器包含指令，当所述指令由所述至少一个处理器执行时，所述指令使得所述至少一个处理器执行一方法，所述方法包括：

当接收到的交易请求被确定为表示不需要卡号或账号的交易时：

将所述交易请求提供至选择的记账处理器；

从所选择的记账处理器接收响应，接收到的响应包括针对所述交易请求而选择的账户和与所选择的账户相关联的账户余额；以及

基于接收到的响应，确定是 (i) 批准所述交易请求，(ii) 拒绝所述交易请求，还是 (iii) 采取除了批准所述交易请求或拒绝所述交易请求以外的进一步行动。

22. 根据权利要求 21 所述的系统，其中：

所述交易请求包括伪标识符；

所选择的账户至少部分地基于所述伪标识符来选择；并且

选择所述记账处理器至少部分地基于所述伪标识符。

23. 根据权利要求 21 所述的系统，其中：

所述交易请求包括 ABA 号码、路由转账号码 RTN、加拿大转账号码、分类代码、分支机构代码、银行代码、或者日期、时间或天中的至少一个；以及

选择所述记账处理器至少部分地基于所述交易请求中的 ABA 号码、路由转账号码 RTN、加拿大转账号码、分类代码、分支机构代码、银行代码、或者日期、时间或天中的至少一个。

24. 根据权利要求 21 所述的系统，其中，所述交易请求被格式化以符合 ISO 8583。

25. 根据权利要求 21 所述的系统，其中，所述交易请求包括以下至少一项：

对所述账户的当前余额的请求；

对可用余额是大于、小于还是等于所述交易请求中的金额的请求；

对分类账余额是大于、小于还是等于所述交易请求中的金额的请求；

对所述账户的健康状况的指示的请求；或者

对与所述账户的所有者有关的信息的请求。

26. 根据权利要求 21 所述的系统，其中，所述网络是包括一个或更多个银行的同业银行网络。

27. 根据权利要求 21 所述的系统，其中，采取进一步行动的步骤包括以下至少一项：

批准所述交易请求所请求的交易；

拒绝所述交易请求所请求的所述交易；

返回所述账户中包含的货币金额；

请求另外的信息；或者

返回其它信息。

28. 一种用于经由网络处理支付交易的计算机系统，该计算机系统包括：

至少一个处理器；以及

存储器，该存储器包含指令，当所述指令由所述至少一个处理器执行时，所述指令使得

所述至少一个处理器执行一方法，所述方法包括：

从所述网络接收与被确定为不需要卡号或账号的交易相关联的请求；

至少部分地基于所述请求中的信息选择用于所述交易的账户；

确定所选择的账户的余额；以及

基于所述请求生成响应，所述响应包括用于确定是批准还是拒绝所述请求的信息。

29. 根据权利要求 28 所述的系统，其中：

所述交易请求包括伪标识符；并且

选择账户至少部分地基于所述伪标识符。

30. 根据权利要求 29 所述的系统，其中，所述伪标识符标识账户，并且选择账户的步骤还包括：

使用所述伪标识符从一组存款账户中识别出所述账户；以及

检索有关所识别的账户的信息。

31. 根据权利要求 28 所述的系统，其中，所述交易请求被格式化以符合 ISO 8583。

32. 根据权利要求 28 所述的系统，其中，所述交易请求包括以下至少一项：

对所述账户的当前余额的请求；

对可用余额是大于、小于还是等于所述交易请求中的金额的请求；

对分类账余额是大于、小于还是等于所述交易请求中的金额的请求；

对所述账户的健康状况的指示的请求；或者

对与所述账户的所有者有关的信息的请求。

33. 根据权利要求 28 所述的系统，其中，所述网络是同业银行网络。

34. 一种用于处理支付交易的计算机系统，该计算机系统包括：

至少一个处理器；以及

存储器，该存储器包含指令，当所述指令由所述至少一个处理器执行时，所述指令使得所述至少一个处理器执行一方法，所述方法包括：

接收用于进行不需要卡号或账号的支付交易的信息，其中，所述信息不包括卡号或账号；

基于所述信息生成交易请求，所述交易请求包括至少一个标识符；

将所述交易请求发送至支付网络进行处理；

基于与所述标识符相关联的至少一个账户，接收对所述交易请求的至少一个响应。

35. 根据权利要求 34 所述的系统，其中，所述标识符包括伪标识符，使得所述伪标识符允许确定与所述标识符相关联的所述至少一个账户。

36. 根据权利要求 34 所述的系统，其中：

所述交易请求包含 ABA 号码、路由转账号码 RTN、加拿大转账号码、分类代码、分支机构代码、银行代码、或者日期、时间或天中的至少一个；以及

选择所述记账处理器至少部分地基于所述交易请求中的 ABA 号码、路由转账号码 RTN、加拿大转账号码、分类代码、分支机构代码、银行代码、或者日期、时间或图中的至少一个。

37. 根据权利要求 34 所述的系统，其中，所述交易请求被格式化以符合 ISO 8583。

38. 根据权利要求 34 所述的系统，所述交易请求包括以下至少一项：

对所述至少一个账户的当前余额的请求；

对所述至少一个账户中的可用余额是大于、小于还是等于所述交易请求中的金额的请求；

对所述至少一个账户中的分类账余额是大于、小于还是等于所述交易请求中的金额的请求；

对所述至少一个账户的健康状况的指示的请求；或者

对与所述至少一个账户的所有者有关的信息的请求。

39. 根据权利要求 34 所述的系统，其中，所述至少一个响应包括以下至少一项：

批准所述交易请求的消息；

拒绝所述交易请求的消息；

返回所述至少一个账户中包含的货币金额的消息；

请求另外的信息的消息；或者

返回其它信息的消息。

40. 根据权利要求 34 所述的系统，其中，所述系统由银行或商家中的至少一方操作。

# 用于实时的账户访问的系统和方法

[0001] 相关申请的交叉引用

[0002] 本申请要求2012年3月19日申请的在先申请的美国临时申请61/612,897的权益，该美国临时申请通过引用的方式并入本申请中。

## 技术领域

[0003] 所公开的实施方式总体上针对用于实时的账户访问的系统和方法。

## 背景技术

[0004] 诸如EFT（电子资金转账）网络处理的网络处理架构被用于处理来自传统的信用卡或借记卡交易的付款。EFT使得能够快速地提供账户信息和用于购买或其它目的的其它相关信息。例如，当持卡顾客打算在商店购买物品时，该顾客通常会将她的卡交给商家，而该商家会将这张卡刷过磁条机以读取包括卡号在内的该卡信息。卡号通常长度为13至19位数，并且唯一地标识用户的信用账户或借记账户。

[0005] 在商家接收到卡号之后，商家将该卡号连同诸如价格、日期、时间、地点、持卡人姓名这样的与交易相关联的其它信息一起发送至支付网络。支付网络通常会根据卡号将这些信息路由至适当的发卡机构。第一个数字通常标识了“发卡机构”，即，诸如公司这样的发行卡的实体。因此，例如，以‘4’开头的卡号，例如4000123456789012通常会标识VISA为卡提供商/发卡机构。每家发卡机构通常都具有与它们的卡相关联并且表示这些卡的数字标识符。

[0006] 适当的发卡机构（例如信用卡或签账卡公司）然后通常会查阅它的记录以确定适当的账户，并且验证该账户是否包含足够的资金或信用来进行交易（例如，购买）。该判断的结果通常会被返回以告知商家该用户是否有能力购买该商品。从最初获取卡的数据到提供资金验证的响应的整个过程可能发生在一段相对短的时间内。在某些情况下，该过程实时地或者接近实时地发生。

[0007] 然而，在某些情况下，无法获得用于访问顾客账户的卡号。例如，如果顾客决定使用支票来支付，则商家必须获取发行该支票的银行的RTN（交换码）和该顾客的个人账号。商家随后必须使用诸如自动清算所(ACH)这样的系统来处理支付。ACH通常批量地操作，因此用于授权购买的过程能够耗费比基于卡的交易长得多的时间。因此，使用ACH增加了商家获得资金保证的时间量。ACH的使用还包括收到后来被发现是无法收回的付款（也称为“空头支票”）的可能性。

[0008] 在其它情况下，出于隐私或其它方面的原因，顾客可能不愿意将他的账户详细信息提供给商家。这可导致支付接收方面的问题，这是因为用户将通常需要提供他的支付卡信息。没有该信息，商家通常无法收到付款。

[0009] 在诸如具有商业账户这样的其它情况下，也不存在能够被用于实现购买的卡号。因此，商业购买可能需要依靠ACH系统来进行购买，这（正如前面所描述的）是缓慢的、费用高的并且效率低的。

[0010] 因此，期望提供用于使用现有的网络架构在实时的或接近实时的访问的情况下处理对于账户的交易的改进的系统和方法。同样期望这些系统和方法支持支付交易的路由、处理、结算和报告。这样的系统和方法的优点包括交易处理速度加快、可靠的账户管理和记账、和／或无法收回的账户减少。本领域技术人员将在考虑到本公开的其余部分之后认识到进一步的优点。

## 发明内容

[0011] 根据示例实施方式，一种用于通过设备（诸如支付网络设备）处理支付交易的方法包括：从收单机构接收交易请求，并且确定该交易请求表示不需要卡号或账号的交易。该方法还包括：基于交易请求的内容选择记账处理器，将所述交易请求提供给所选择的记账处理器，并且接收来自所述记账处理器的响应。在某些示例实施方式中，接收到的响应可以包括至少部分地基于所述交易请求的内容而针对所述交易请求选择的账户或者与所选择的账户相关联的账户余额中的至少一项。该方法还包括：批准所述交易请求，拒绝所述交易请求，或者针对所述交易请求采取进一步的行动。类似地，在某些示例实施方式中，计算机系统包括至少一个处理器以及包含指令的存储器，当所述指令由所述处理器执行时，所述指令使所述处理器执行该方法的操作。

[0012] 根据示例实施方式，一种用于通过记账处理器设备处理支付交易的方法包括：在所述记账处理器设备（例如，从网络设备）处接收所述网络设备确定的不需要卡号或账号的交易请求。该方法还包括：至少部分基于所述交易请求的内容选择用于所述交易请求的账户，确定所选择的账户的余额，并且基于所述交易请求的内容和所述余额生成响应。所述响应包括用于确定批准还是拒绝所述交易请求的信息。类似地，在某些示例实施方式中，计算机系统包括至少一个处理器以及包含指令的存储器，当由所述处理器执行所述指令时，所述指令使所述处理器执行该方法的操作。

[0013] 根据示例实施方式，一种用于通过收单机构处理器设备处理支付交易的方法包括以下步骤：使用用于进行支付交易的至少一个计算机系统来接收信息。在某些示例实施方式中，所述信息不包括卡号或账号。该方法还包括：所述计算机系统基于所述信息生成包括至少一个标识符的交易请求，将所述交易请求发送至支付网络进行处理，并且基于与所述标识符相关联的至少一个账户接收对所述交易请求的至少一个响应。类似地，在某些示例实施方式中，计算机系统包括：至少一个处理器和以及包含指令的存储器，当所述指令由所述处理器执行时，所述指令使所述处理器执行该方法的操作。

[0014] 要理解的是，正如所声称的，前面的一般描述和下面的详细描述都是示例并且仅是示例性的，而不是对所公开的实施方式的限制。

## 附图说明

[0015] 附图被并入并构成本说明书的一部分，附图示出了所公开的实施方式中的数个实施方式，并且与本说明书一起用于解释所公开的实施方式的原理。

[0016] 图 1 是根据某些实施方式的示例网络 100 ；

[0017] 图 2 是显示了根据某些实施方式的可用的通信系统中的某些部分的示例网络通信图 200 ；

[0018] 图 3 是根据某些实施方式的用于与其一起使用的示例消息格式 300 ;

[0019] 图 4 是根据某些实施方式的用于与其一起使用的某些数据字段的示例图 400 ;以及

[0020] 图 5 是根据某些实施方式的用于与其一起使用的示例计算机系统 500。

## 具体实施方式

[0021] 现在将详细地描述所公开的实施方式,这些实施方式的示例被示出在附图中。只要可能,在整个附图用中相同的附图标记将被用于表示相同或相似的部分。

[0022] 所公开的实施方式使用多种操作模式来处理支付交易(在本文中也称为“交易”)。第一种操作模式被称为“本机模式(native mode)”。在本机模式中,可以在设备之间传递消息(在本文中也称为交易请求或支付请求)。在某些实施方式中,该消息可以符合或者基于 ISO 8583 消息。ISO 8583 标准定义了消息的格式,因此,除了其它方面外,不同的系统能够交换数据并且实现交易。

[0023] 本机模式消息允许交易即使在没有支付卡的情况下也能够利用现有的支付卡交易渠道。例如,可以使用 ISO 8583 消息来实现这些交易。在某些实施方式中,本机模式系统将使用特定信息来构建这些消息中的一个。该信息的至少一部分可以表示该消息将被用于不同于其通常用途(即,不同于支付卡交易)的用途。

[0024] 另一种操作模式被称为“非本机模式”或“X-REF 模式”。该模式可以类似于上述的本机模式,但是使用不同的方式来构造消息。在某些实施方式中,可以查询数据存储器或数据库,以基于存储在这些消息中的数据来确定账号。稍后将至少参照图 3 和图 4 来描述这两种模式。

[0025] 这两种操作模式使得能够不需要卡号或账号来进行交易成为可能。例如,在用户不希望将她的支付卡号或账号公开给商家的情况下,仍然能够使用上述的操作模式来处理交易。

[0026] 图 1 示出了用于与所公开的系统和方法一起使用的示例网络 100。在某些实施方式中,网络 100 包含至少一个收单机构处理器 101、至少一个网络 103 和至少一个发卡机构 105。在某些实施方式中,可以使用如图 5 所引用的一个或更多个计算机系统来实现这些单个单元。用于实现这些单元中的每一个的特定部件或设备可能改变。

[0027] 在某些实施方式,收单机构处理器 101 包括前端系统 101A 和后端系统 101B。前端系统 101A 被用于获取支付明细。在某些实施方式中,前端系统 101A 的可以是用于获取数据的商家设备,包括现金出纳机、在线购物车系统、信用卡读卡器、支票扫描仪(例如,用于读取 MICR 数据)、计算机等。在其它实施方式中,由收单银行操作前端系统 101A。例如,这可以是为已经接收到来自顾客的支付明细的商家处理支付的银行。

[0028] 在某些实施方式中,后端系统 101B 能够是用于处理已通过前端系统 101A 的交易的系统。能够由运行前端系统 101A 的同一收单银行来运行后端系统 101B。在其它实施方式中,可以由不同的实体来运行后端系统 101B。在某些实施方式中,后端系统 101B 能够部分地基于由前端系统 101A 获取的支付明细来生成交易请求。后端系统 101B 随后能够将该交易请求发送至网络 103 进行处理。在某些实施方式中,前端系统 101A 和后端系统 101B 可以是单个不同的计算机系统。在其它方面,它们可以是多个计算机系统。在进一步的实

施方式中，前端系统 101A 和后端系统 101B 可以是任何的 ATM/ATM 处理器、商家 /POS 处理器、账单支付 (Bill Pay) 商家 / 账单机 (Biller) 处理器、因特网商家 / 因特网商家处理器等。

[0029] 在某些实施方式中，前端系统 101A 或后端系统 101B 可以获取顾客凭证，以便实现购买或其它交易。在某些实施方式中，这些获得的凭证可以被用来创建构造值 (constructed value)。该构造值可包括标识唯一的存款账户或者其它类型的账户的信息。例如，账户可以包括存款账户、支票账户、借记账户、信用账户、经纪账户、商业账户、个人账户等中的任一个。普通技术人员将认识到，一种特定类型的账户对于所公开的实施方式不一定是必不可少的。

[0030] 在某些实施方式中，构造的值可以是唯一的。例如，在构造包括构造值的支付请求时，该构造值只能够表示持有该账户的机构，而支付请求中的其它信息表示特定账户。在某些实施方式中，该构造值可以包括多个数据类型中的任一种，包括（但不限于）指示构造值的存在的特殊值、账户或机构的标识符（例如，预先约定的识别符）（诸如国际银行账号 (IBAN- 主要用于美国境外）、路由转账代码 (RTN 或 R&T 号码 - 主要用于美国境内）、加拿大转账号码、银行代码、分支机构代码、分类代码、或者至少部分地标识账户或持有它的机构的任何其它标识符）、支付请求的时间和日期等。

[0031] 在某些实施方式中，构造值可以包括像存款账号、信用卡账号或另一种类型的账号（也称为主账号 (PAN)）的号码。PAN 可以符合或者基于 ISO 7812，这可以在某种程度上将 PAN 的特定的第一个数字分配给特定的发卡机构。

[0032] 在其它的实施方式中，构造值和 / 或支付请求可包括能够唯一地标识顾客或他的账户的多个其它的标识符。例如，可以包括顾客的电子邮件地址、电话号码（蜂窝 / 移动、工作、家庭、寻呼机等）、用户名、社交网络身份（诸如 Facebook 或 Twitter 账户）等。此外，这些标识符可用于生成在支付请求中使用的另一个标识符（诸如十六进制的或加密的值）。此外，可以在某些实施方式中使用其它标识符。

[0033] 网络 103 可以是同业银行网络（如 NYCE、INTERAC 等）。同业银行网络允许货币系统（诸如 ATM 或支付终端）访问存款账户或其它账户。在某些实施方式中，网络 103 使得能够通过 EFTPOS（销售点电子资金转账）系统在销售点处使用由银行发行的 ATM 卡。不同于作为信用卡交易来操作，这通常会需要通过信用卡发卡机构系统，EFTPOS 交易能够网络 103 来接收并且被路由到保持该账户的适当银行。网络 103 能够是国内网络、国际网络、或者二者。在某些实施方式中，网络 103 可以被配置为将消息发送到记账处理器 105，以请求记账处理器 105 转移与交易相关联的资金。

[0034] 记账处理器 105 表示在处理支付交易中使用的系统。例如，在某些实施方式中，记账处理器 105 可以是接收交易请求、尝试处理该交易请求（例如，通过借记或贷记请求中提及的账户）、并且提供处理该交易请求的尝试的状态的计算机系统。例如，可以由发卡机构、银行、信用社、商业银行、经营存款账户的公司等来操作记账处理器 105。记账处理器 105 例如可以基于正在尝试的交易的类型而不同。例如，能够在发卡机构的服务器上处理未被绑定到特定银行的信用卡的交易。然而，被绑定到银行的存款账户的借记卡交易可以至少部分地由该银行处理。在任何情况下，操作记账处理器 105 的集团或组织通常存储诸如信贷额度、账户余额、信誉、支付历史记录等这样的与账户有关的信息。在某些实施方式中，由记

账处理器 105 管理的账户被称为活期存款账户 (DDA)。记账处理器 105 可以将资金存入账户中，从账户中提取资金，请求账户余额，或者例如当通过网络 103 请求时执行其它记账业务。

[0035] 在某些实施方式中，收单机构处理器 101、网络 103 和 / 或记账处理器 105 可以使用一组规则来发起和处理诸如 EFTPOS 交易这样的交易请求。在某些实施方式中，任何或者所有的这些设备可以被配置为遵守这些规则。例如，记账处理器 105 可以被配置为在被网络 103 请求时在账户之间转移资金。记账处理器 105 还可以被配置为在被网络 103 和 / 或收单机构处理器 101 请求时处理信用卡交易、借记卡交易、小额交易或其它交易。记账处理器 105 还可以被配置为在被收单机构处理器 101 请求时提供账户余额或状态（例如，正常、销户、冻结）。记账处理器 105 还可以被配置为在工作日结束时结算交易。普通技术人员将认识到，用于处理交易的其它规则是可能的。

[0036] 图 2 公开了用于实现所公开的系统和方法的一部分的示例方法 200。方法 200 开始于步骤 201，收单机构处理器 201 从顾客或购买者接收凭证。这些凭证（或“支付明细”）可以包括支付账户信息 - 诸如 RTN（路由转账号码）、账号、信用卡号、支付卡号、借记卡号、绑定到账户的标识符、当在数据存储器或数据库中引用时用于解析账号的伪标识符 (pseudo-identifier) 等。在某些实施方式中，支付明细能够唯一地表示顾客的存款账户、信用账户、借记账户或其它账户。例如，支付明细能够包括顾客的账号。在其它的实施方式中，支付明细可包括与顾客的账户关联的另一个唯一的标识符。例如，支付明细可包括由数字、十六进制数或其它的编码方案组成的伪标识符，以标识顾客的账户。在其它实施方式，支付明细能够包括伪卡号 (pseudo-card number) 或构造值。该构造值的前几个数字可以是“59”，但是其它的值和结构也是可能的。“59”可以被用来表示其之后的字符包含 ABA 值。这些值可以由试图购买商品或进行交易的用户提供，可以由收单机构处理器 101 基于从顾客接收到的信息来生成等。

[0037] 在其它的实施方式中，构造值和 / 或支付明细可以包括能够唯一地标识顾客或账户的多个其它的标识符。例如，顾客的电子邮件地址、电话号码（蜂窝 / 移动、工作、家庭、寻呼机等）、用户名、社交网络身份（诸如 Facebook 或 Twitter 账户）等。此外，这些标识符能够被用来生成在支付请求中使用的另一标识符（诸如十六进制的或加密的值）。此外，在某些实施方式中可以使用其它的标识符。

[0038] 在步骤 201B 中，收单机构处理器 201 生成交易请求。在某些实施方式中，这些交易请求将具有余额查询交易的形式。当操作收单机构处理器 201 的实体（例如，商家、银行等）希望找出顾客的账户是否包含进行购买所需要的资金时，可发生余额查询交易。在其它实施方式中，这些交易请求将具有借记或贷记指令的形式。在某些实施方式中，在步骤 201B 中生成的交易请求能够是具有如随后将针对图 3 和图 4 进行描述的 ISO 8583 消息标准的形式或者基于该 ISO 8583 消息标准。这样的消息也可以包含诸如交易类型、交易金额、日期、时间、位置信息等这样的信息。在步骤 201C 中，收单机构处理器 201 可将生成的交易请求提交给网络 203。

[0039] 在某些实施方式中，由用于处理交易的收单机构处理器 201 选择网络 203（在某些实施方式中，网络可以如上所述的网络 103 那样实现）。在某些实施方式中，网络 203 能够是如前所述的同业银行网络（诸如 NYCE、INTERAC 等）。网络 203 可以被使能以提供接收

到的交易请求的适当路由。这例如能够通过确定 RTN 和 / 或有关支付类型的其它信息来完成。这在步骤 203A 和步骤 203B 中得到表示，并且能够部分地通过确定在交易请求中存在特定值来完成。在某些实施方式中，这可以涉及确定在交易要求中的特定位置处存在数字"59"（或者另一个特定的数据）。"59"表示其后的字符包含 ABA 值。

[0040] 在其它实施方式，例如，涉及用户的伪身份 (pseudo identity)（诸如用户姓名、社交网络身份、电话号码或电子邮件地址）的那些实施方式中，网络 203 可以通过查询数据库来确定适当的路由。在确定交易请求中存在特定值之后，网络 203 可以确定该特定值后面的字符表示 RTN，并且可以将在步骤 203B 中表示的交易路由至 EFT 处理 205。在某些实施方式中，步骤 203B 可以在路由过程（例如，步骤 203A) 被执行之后立即执行。在其它实施方式中，步骤 203B 中的路由处理可以成批地或批量地执行。例如，如果交易是在第一个工作日的下午被提交给支付网络 203（例如，步骤 201C)，则在步骤 203A 中确定适当的路由和 / 或在步骤 203B 中路由交易请求可以稍后与同一天接收到的其它交易请求的确定和路由一起在当天晚上执行。

[0041] 在某些实施方式中，EFT 处理 205 以及授权处理 207 和核心处理 209 可以是更广义的记账处理器系统 211 的一部分。（在某些实施方式中，记账处理器系统 211 可以实现为如上所述的记账处理器 105。）在图 2 中，这些处理系统被表示为三个独立的系统，但是任一个或全部都可以实现在单个计算机或多个计算机上。在步骤 205A 中，EFT 处理器 205 可以确定存在于所转发的交易请求中的交易参数，以便确定用于发送该请求以进行处理的适当的授权处理系统 207。此外，这可涉及基于存在于交易请求中的特定值（诸如 RTN) 来确定路由。

[0042] 一旦授权处理 207 接收到步骤 205B 中的交易请求，则该过程继续到步骤 207A 用于账户确定。授权处理 207 随后可确定适当的账户。这可通过检查交易请求（和提取账号），查阅交叉引用数据库（未示出）以基于该交易中的信息等确定正确的账号 / 标识符来实现。一旦确定了该账号 / 识别符，就可利用该账号 / 标识符将请求发送到核心处理 209。在某些实施方式中，该请求包括对由该账号 / 标识符表示的账户中的当前余额的请求。在其它实施方式中，该请求可包括其它操作请求，诸如借记、贷记等。

[0043] 当核心处理 209 接收到步骤 207B 中的请求时，该核心处理 209 可以采取多个行动中的某些或全部。核心处理 209 可以将与交易请求所提及的账户相关联的余额提供回授权处理 207。核心处理 209 可以基于交易请求中提及的金额借记或借贷，并且将新的余额（即，在借记 / 贷记之后）提供回授权处理 207。在其它实施方式中，基于特定的交易请求，核心处理 209 可以不同地响应，诸如通过可用余额小于（或大于）在交易请求中的数额的指示；分类账余额小于（或大于）交易请求中的数额的指示；账户的健康状况的指示（诸如该账户是否开通和 / 或信誉良好；该账户已开通多久的指示；与该账户相关联的任何负面历史记录的平均余额范围的指示等）；账户所有者的姓名、地址、开户日期或其它资料等。这些项目中的任一个或全部可以在步骤 207C 中由核心处理 209 组成响应的一部分。

[0044] 在步骤 207C 中接收到响应后，授权处理 207 可基于请求的内容来确定应当批准还是拒绝该交易。例如，如果 207C 中的响应指示该账户具有的钱比实现由原始的交易请求所提及的购买交易所需要的钱少，则授权处理 207 可以拒绝该交易，并且可以构建拒绝消息以通过步骤 205C、步骤 203C 和步骤 201D 发回至收单机构处理器 201。如果该账户具有足

够的钱来支付交易，则授权处理 207 可以批准该交易，并且经由相同的步骤发回批准消息。

[0045] 授权处理 207 还可以发回其它消息，诸如指示账户中的可用金额、账户的状态（诸如该账户是否开通或注销）、账户的所有者或者请求用户的更多信息的消息。如本领域技术人员将理解的，也可以发送其它消息。

[0046] 图 3 是根据所公开的实施方式的、用于与所公开的系统和方法一起使用的示例消息格式 300。在某些实施方式中，基于消息格式 300 的消息用于在图 1 和图 2 中的设备之间传送数据。在某些实施方式中，消息格式 300 中的数据元素可以基于 ISO 8583 消息标准。可以使用该标准的任何修订版本以及其它标准。在其它实施方式中，可以使用其它的消息，并且可以改变图 3 中的特定的数据大小和字段。此外，在某些实施方式中，图 3 中的特定数据字段可以包含如图 3 中所描述的数据。例如，DE12 数据元素可以包含指示正在发生交易的终端处的本地时间的 6 个字节。

[0047] 在某些实施方式中，参照消息格式 300 所描述的消息可以包括存储“构建的 PAN”的 DE2304（即，“数据元素 2”304）。如上所述，PAN 通常被用于本领域中以表示信用卡号。PAN 可以符合或基于 ISO 7812，其限定了哪些发卡机构使用 PAN 的第一个数字。例如，在 PAN 的第一位置上的‘4’可以表示 VISA，而值‘53’可以表示万事达卡。

[0048] 在某些实施方式中，PAN 可由多个部分构成。PAN 可包括伪卡号，所述伪卡号可基于针对账户预先约定的标识符（例如，上述的 RTN 或 IBAN）来构造。在某些实施方式中，‘59’被用在最前面的两个空格中以表示 PAN 是构造值。随后可跟随九位的 RTN 或其它标识符，并且随后是指示时间和日期的 8 位的值。这种操作模式先前已经在本公开中被称为“本机模式”。

[0049] 为了标识顾客所使用的特定账户，消息 300 的其它部分可存储实际的账号。例如，在某些实施方式中，用户的特定存款账户可以被存储在该消息的另一部分中；例如，存储在 DE102323 中。

[0050] 在其它实施方式中，PAN 可被构造为伪标识符。即，PAN 本身可以被构造为对账号的交叉引用。因此，在接收到 PAN 后，发卡银行能够查阅表、数据库或其它数据存储，以便确定与该伪标识符相关联的账号。所述账号随后可被用于借记账户或执行其它动作。在某些实施方式中，PAN 可以被构造为单次使用或有限使用的数字串（例如，由 19 个十进制数字或十六进制数组成）、账号的散列值、表示账号的加密的字符串等。这种操作模式先前已在本公开中被称为“非本机模式”或“X-REF 模式”。

[0051] 在识别出与存储在消息 300 中的账号或存储在 300 中的伪标识符相关联的账户之后，发卡机构将能够确定正确的账户并且处理支付交易。例如，这可以包括返回余额、授权支付等，如之前图 2 提到的。

[0052] 图 4 表示组成以上在图 3 中所描述的消息的某些数据元素。为了开始，数据元素 2(DE2) 在图 4 中被表示为 401。在某些实施方式中，DE2 被用来存储构造的 PAN。前两个空间指示后面将跟随多少个字符（在示例图 4 中，为‘19’）。因此，DE2 总计为 21 个字符长，包括开始处的“19”。在某些实施方式中，这些字符中的每一个可以是单个数字（即，0-9）；然而，在其它实施方式中，可用较大的字符集（例如，十六进制码）。在‘19’之后，将跟随 PAN。在示例图 4 中，构建的 PAN 被表示为 DE2 中的字符 3-21。‘59’表示随后的字符包含 ABA 值。（然而，可以使用包括其它数字、字母等这样的其它字符表示跟随的值是 ABA 值。‘R’

字符表示先前提到的 RTN,并且字符串‘DDHHMMSS’表示交易的时间(即,日、时、分、秒)。

[0053] 在某些实施方式中,数据元素 32(DE32)402 被用于标识收单机构,例如收单机构处理器 101,以便将该响应正确地路由回发送方。DE32 使得诸如网络 103 这样的网络能够辨认出交易来自特定的收单机构,诸如商家。前两个数字(‘11’)表示数据的长度,并且其次的两个数字(‘59’)表示将发生基于无卡的交易。最后 9 个‘I’字符表示机构 ID,即发起该消息的机构的 ID。

[0054] 继续数据元素 52(DE58)403,该数据元素包含表示交易的属性的若干比特。在某些实施方式中,DE58 可以被构造如下:

[0055]

| | |
|---|---|
| 011 | 表示字段的长度 - 在这种情况下，表示 11 个字符长 |
| 0 | 表示是否参加交易 - 在这种情况下，表示不是在独立终端处 |
| 1 | 表示商家是否操作终端 - 在这种情况下，表示商家操作终端 |
| 1 | 表示是否在与收单机构相关联的物理位置处进行交易 - 在这种情况下，表示在不位于与收单机构相关联的位置处的设备处进行交易，诸如在不位于相关联的银行分支机构处的 ATM 设备处 |
| 0 | 表示顾客是否在场 - 在这种情况下，表示顾客不在场 |
| 0 | 表示未出示卡 - 在这种情况下，表示未出示卡，并且应当核对 R&T 号码 |
| 0 | 表示商家的终端是否具有“卡扣留”能力，例如，如果由发卡机构指示，用于保留实体塑料卡的能力（诸如 ATM 响应于发卡机构辨识出被盗的卡而扣留卡） - 在这种情况下，表示商家的终端不具有这种能力 |
| 0 | 表示这是否是第一次尝试交易，例如，由于处理该交易的第一次尝试没有正常工作 - 在这种情况下，表示这不是该交易的第一次尝试 |
| 0 | 表示是否执行安全检查（例如，商家是否核对驾照或其他证明文件） - 在这种情况下，表示不执行安全检查 |
| 00 | 表示终端是否是用于实现交易请求的“管理”终端（例如，由商家或收银员直接或间接地操作的商家终端，诸如超市处的付款台）或“非管理”终端（例如，非商家操作的终端，诸如由顾客操作的独立终端、网站、自动柜员机等） - 在这种情况下，表示该终端是非管理终端 |
| 1 | 表示针对该交易的交易数据是否由商家手动地输入（例如，使用键盘）或者自动地输入（例如，使用磁卡或用于接收该交易数据的其他设备） |

[0056] 然而,基于每个交易的个体特征,每个数据元素的其它值是可能的。

[0057] 移动到数据元素 102(DE 102)404,在某些实施方式中,该数据元素可以被用于表示购买者的账户信息。在 ISO 8583 规范中,这被称为“账户 ID 1”。在某些实施方式中,如先前提到的,这可以表示用户的存款账户的账户数据。如图 4 中示出的,DE 102 包含‘028’,表示后面将跟随 28 个字符的字符串。在某些实施方式中,这 28 个字符可以由来自顾客提供给商家的支票的 MICR(磁性墨水字符识别)线的数字组成。

[0058] 图 5 公开了根据所公开的实施方式的、用于与所公开的系统和方法一起使用的示例计算机系统 500。除了在图 1 至图 3 中所公开的内容以外，示例计算机系统 500 还可以为上面提到的任何的方法、系统、设备或计算机可读介质供电。

[0059] 在某些实施方式中，计算机系统 500 可以被实现为蜂窝电话、移动设备、POS（销售点）设备、服务器、无线设备、或者包括图 5 中的至少某些部件的任何其它系统。计算机系统 500 包括中央处理单元 501，中央处理单元 501 使得数据能够在其它部件之间流动，并且在其他方面管理计算机系统 500 中的其它部件的操作。在某些实施方式中，CPU 501 可以是通用处理器（诸如 Intel 或 AMD 品牌的消费者 / 商业 / 企业处理器）、专用处理器（例如，图形卡处理器）或者使得输入和输出数据成为可能的任何其它类型的处理器中的任一种。

[0060] 此外，计算机系统 500 的一部分是输入设备 502。在某些实施方式中，输入设备 502 可以是使得用户或其它实体能够输入数据的任何设备。例如，输入设备 502 可以是键盘、鼠标等。输入设备 502 能够被用于控制图 5 中的其它部件的操作。

[0061] 计算机系统 500 还包括存储设备 503。存储设备 503 存储计算机系统 500 中的其它部件可以使用的数据，包括先前已经提及并且在图 1 至图 4 中提到的数据。在某些实施方式中，存储设备 503 可以被实现为硬盘驱动器、临时存储器、永久存储器、光学存储器或任何其它类型的永久或临时存储设备中的任一个或全部。

[0062] 计算机系统 500 还包括电源单元 506。电源单元 506 提供了向计算机系统 500 中的其它部件供电所必要的电力。例如，在某些实施方式中，CPU 501 可需要电力来工作；电源单元 506 能够提供必要的电流来为该部件供电。

[0063] 计算机系统 500 还包括网络适配器 505。在某些实施方式中，网络适配器 505 使得与以计算机系统 500 相同或类似的方式实现的其它设备通信成为可能。在某些实施方式中，网络适配器 500 可以允许到诸如因特网这样的网络和 / 或来自所述网络的通信；其它网络也是可能的。网络适配器 500 可以使用任何或所有的已知或尚未已知的有线或无线技术（诸如以太网、802.11a/b/g/n（也称为 Wi-Fi）、蜂窝电话（例如，GSM、CDMA、LTE）等）来实现。

[0064] 此外，图 5 中的任何部件可以被实现为一个或更多个示出的部件。例如，在某些实施方式中，CPU 501 可以被实现为多个计算机处理器、处理器和协处理器或单个处理器中的任一种。例如，在某些实施方式中，存储设备 503 可以被实现为随机存取存储器 (RAM)、只读存储器、硬盘驱动器、USB 存储器、CD/DVD/ 蓝光光盘等中的任一种。图 5 中所示的每个部件的具体数目不受控制，并且本领域技术人员将理解对于所公开的实施方式中的每个特定的实现方式而言的各个部件的适当数目。

[0065] 通过考虑本说明书和本文中所公开的实施方式的实践，所公开的实施方式中的其它实施方式对于本领域技术人员将是显而易见的。意在本说明书和示例仅被视为示例，而所公开的实施方式的真正范围和精神由所附的权利要求书来指出。

[0066] 此外，所公开的实施方式可以部分或全部地在各种计算机、电子设备、计算机可读介质（诸如 CD、DVD、闪存驱动器、硬盘驱动器或其它存储器）、或者其它的电子设备或存储设备来实现。

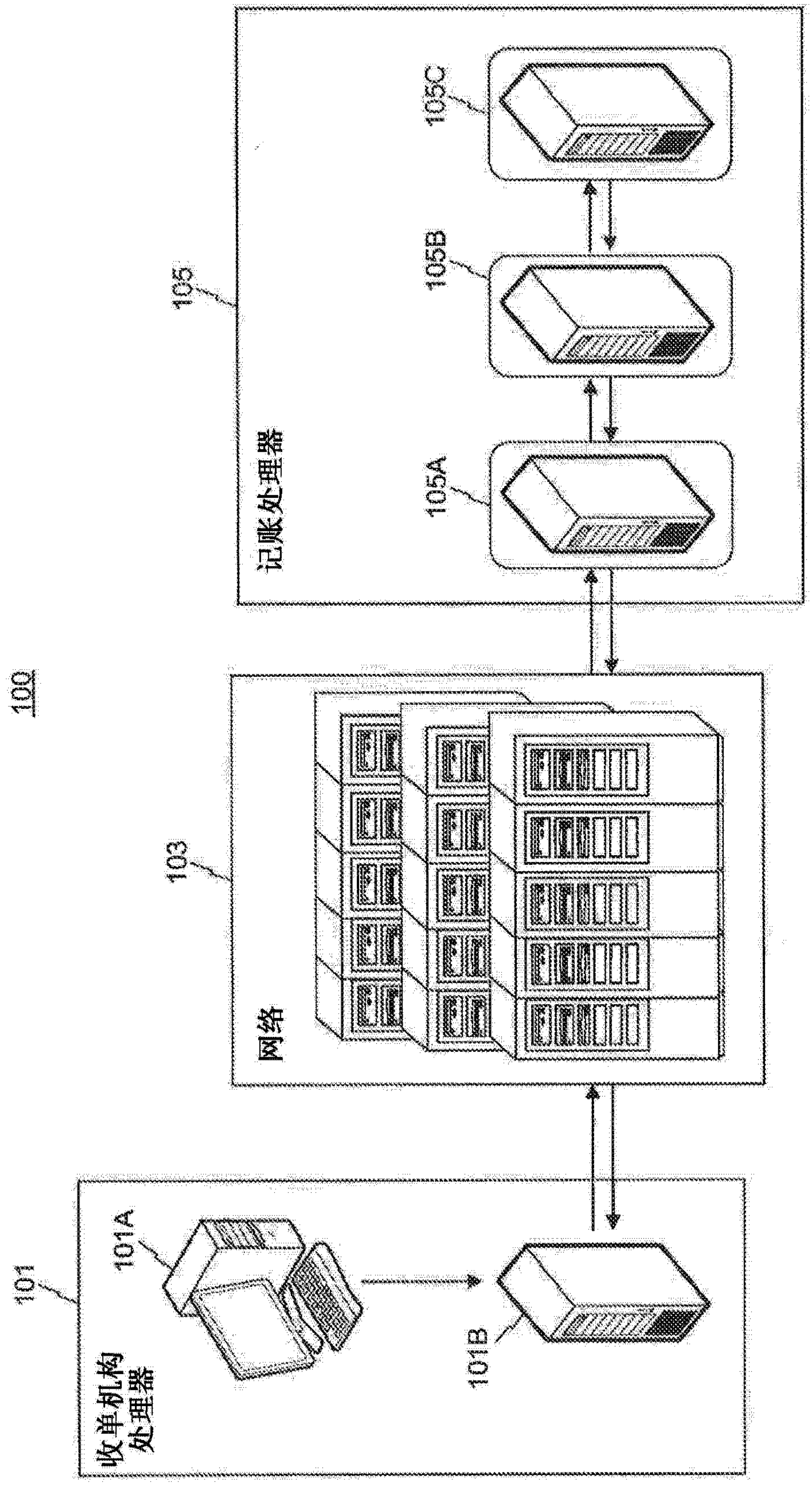


图 1

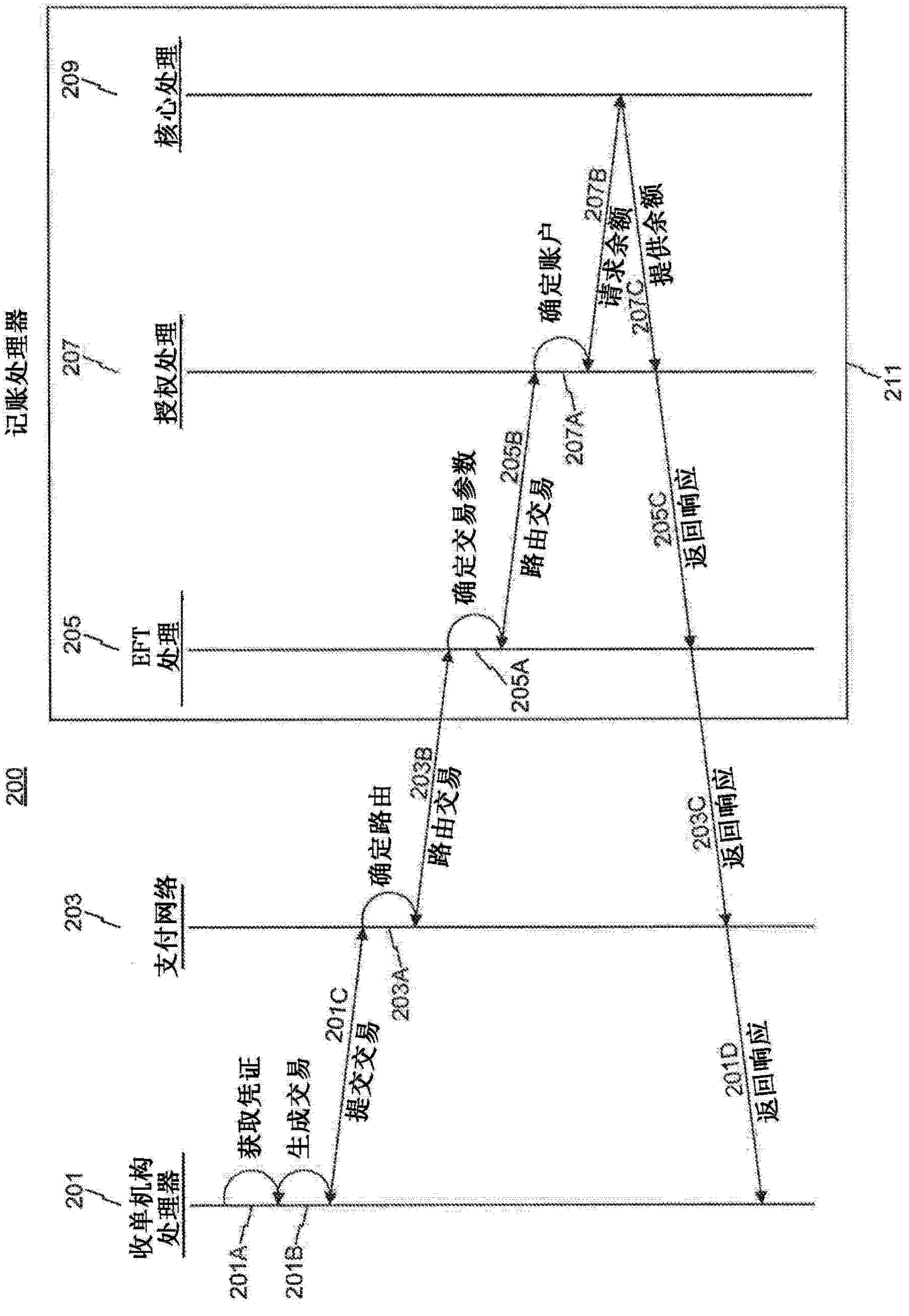
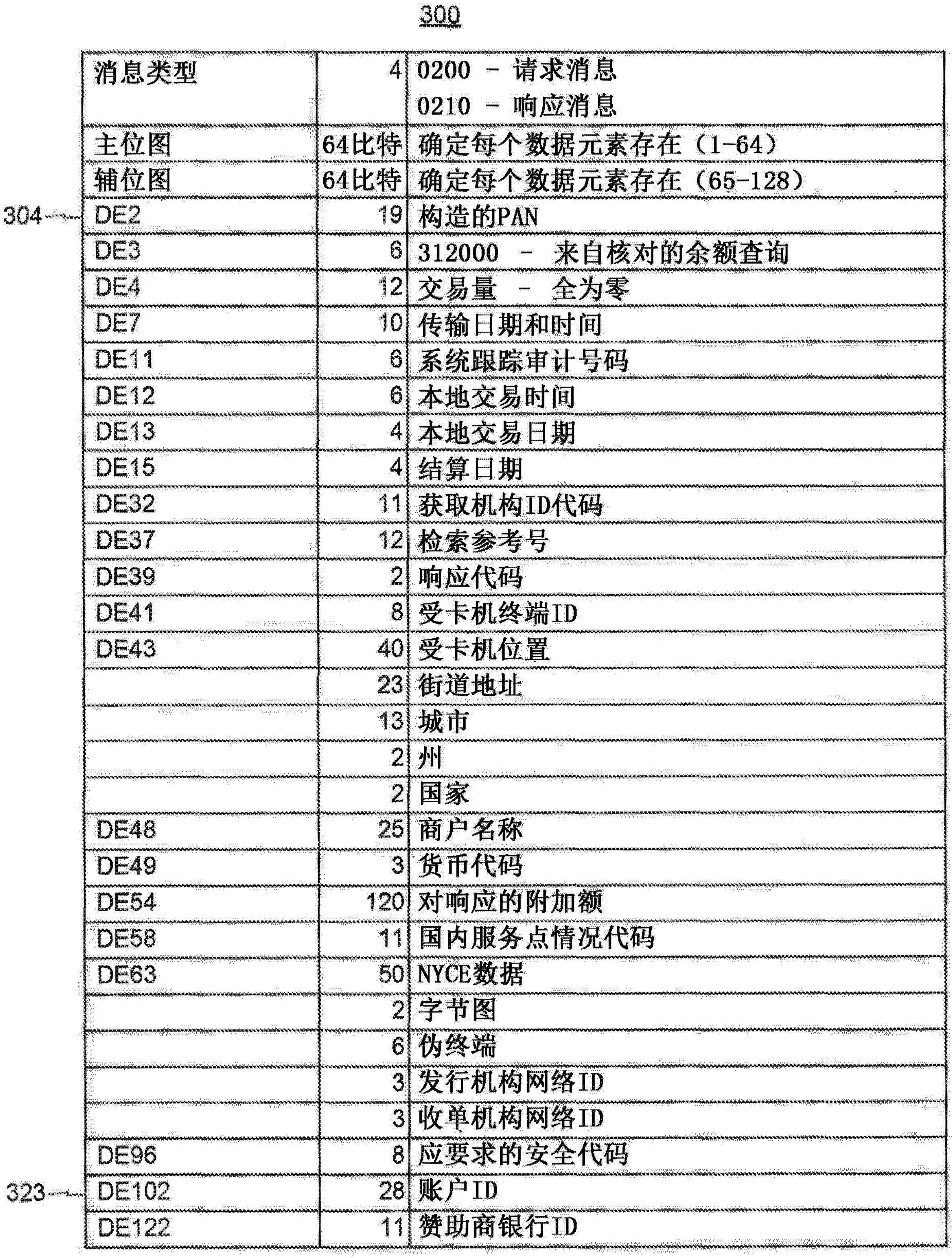

200
记账处理器
211
201
收单机构处理器
203
支付网络
205
EFT处理
207
授权处理
209
核心处理
201A
获取凭证
201B
生成交易
201C
提交交易
203A
确定路由
203B
路由交易
205A
确定交易参数
205B
路由交易
207A
确定账户
207B
请求余额
207C
提供余额
205C
返回响应
203C
返回响应
201D
返回响应

图 2



| | | |
|---|---|---|
| 消息类型 | 4 | 0200 - 请求消息<br>0210 - 响应消息 |
| 主位图 | 64比特 | 确定每个数据元素存在（1-64） |
| 辅位图 | 64比特 | 确定每个数据元素存在（65-128） |
| DE2 | 19 | 构造的PAN |
| DE3 | 6 | 312000 - 来自核对的余额查询 |
| DE4 | 12 | 交易量 - 全为零 |
| DE7 | 10 | 传输日期和时间 |
| DE11 | 6 | 系统跟踪审计号码 |
| DE12 | 6 | 本地交易时间 |
| DE13 | 4 | 本地交易日期 |
| DE15 | 4 | 结算日期 |
| DE32 | 11 | 获取机构ID代码 |
| DE37 | 12 | 检索参考号 |
| DE39 | 2 | 响应代码 |
| DE41 | 8 | 受卡机终端ID |
| DE43 | 40 | 受卡机位置 |
| | 23 | 街道地址 |
| | 13 | 城市 |
| | 2 | 州 |
| | 2 | 国家 |
| DE48 | 25 | 商户名称 |
| DE49 | 3 | 货币代码 |
| DE54 | 120 | 对响应的附加额 |
| DE58 | 11 | 国内服务点情况代码 |
| DE63 | 50 | NYCE数据 |
| | 2 | 字节图 |
| | 6 | 伪终端 |
| | 3 | 发行机构网络ID |
| | 3 | 收单机构网络ID |
| DE96 | 8 | 应要求的安全代码 |
| DE102 | 28 | 账户ID |
| DE122 | 11 | 赞助商银行ID |

图 3

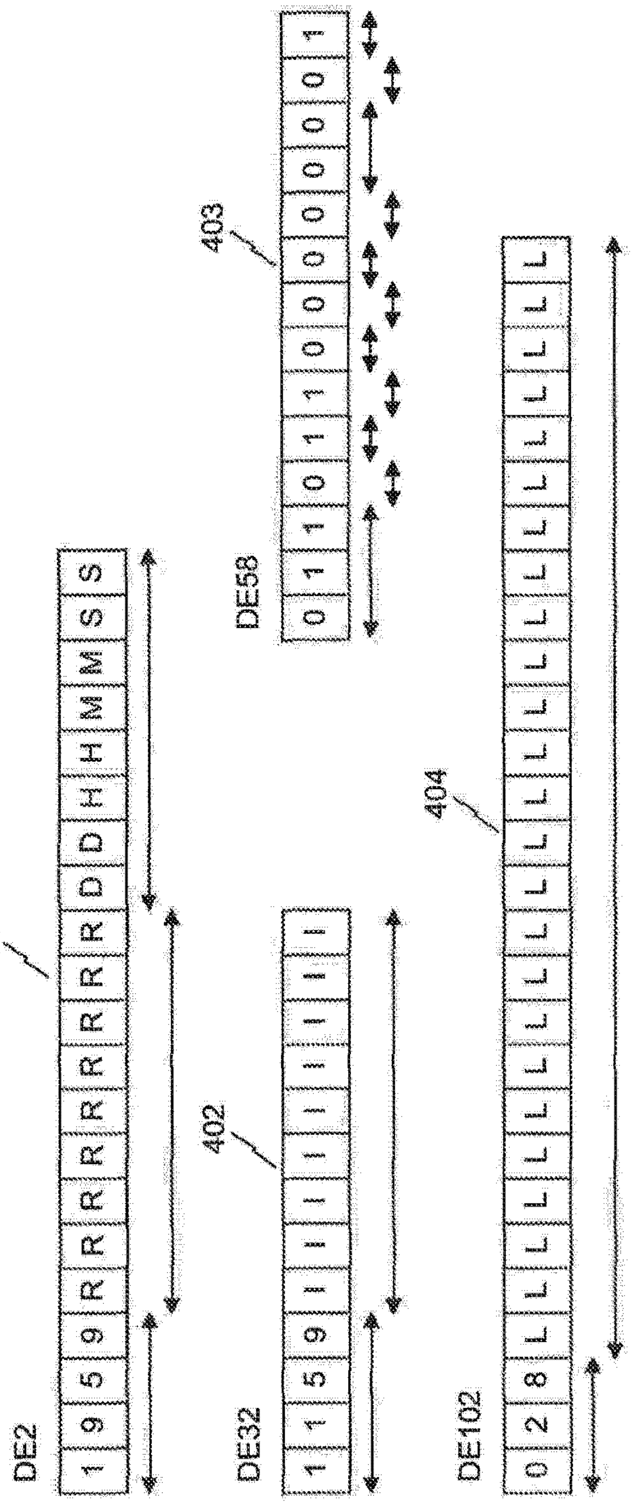


图 4

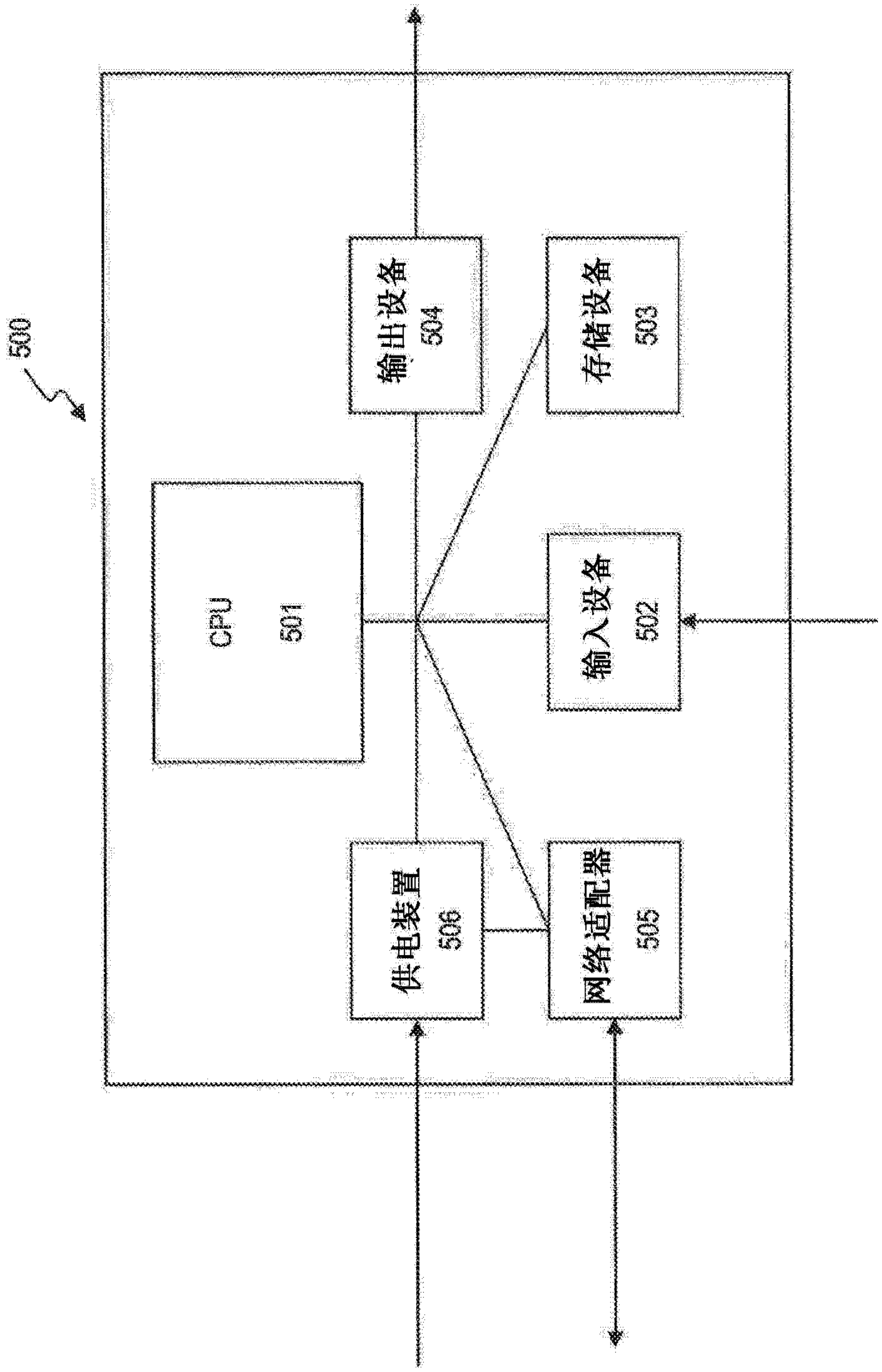


图 5

# Abstract

Systems and methods for real-time account access, allowing access to accounts (such as deposit, credit, or debit accounts) through network processing infrastructures such as Electronic Funds Transfer (EFT). In some embodiments, consumers and/or merchants are able to effect transaction requests against accounts, using a pseudo-identifier or other identifier, and without the need to provide an account number or card number. In other embodiments, payment networks are able to route and process transaction requests against accounts, without having a card number or account number. In other embodiments, account processing systems are able to determine an appropriate account based on transaction requests that do not contain card numbers or account numbers.