(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)

WIPO | PCT

(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

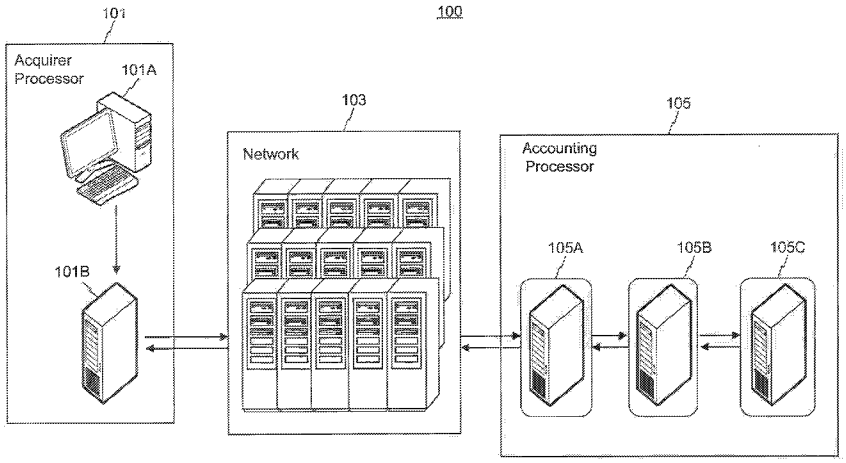

FIG. 1

(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.

WO 2013/142334 A1

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.

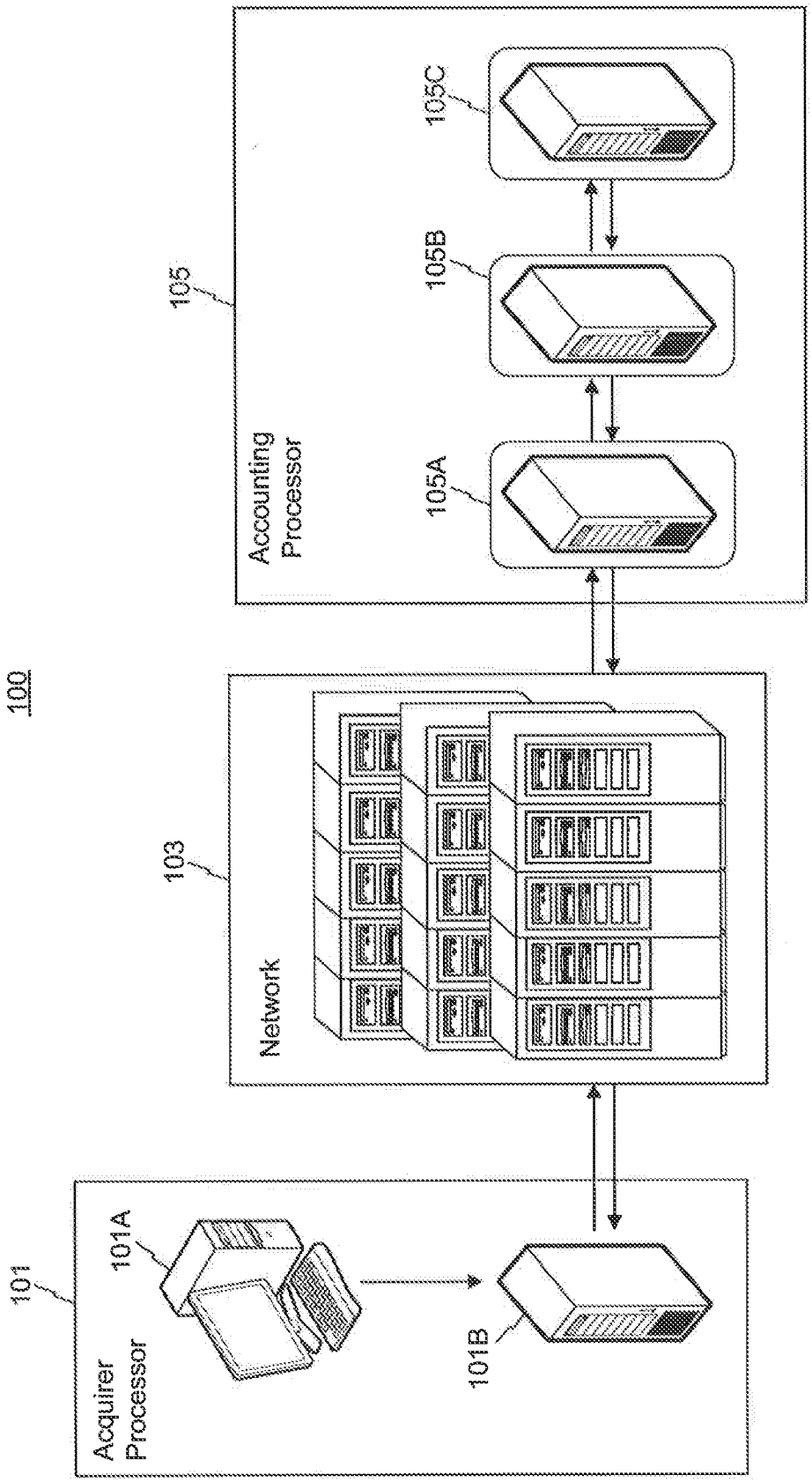
100
101
Acquirer Processor
101A
101B
103
Network
105
Accounting Processor
105A
105B
105C

FIG. 1

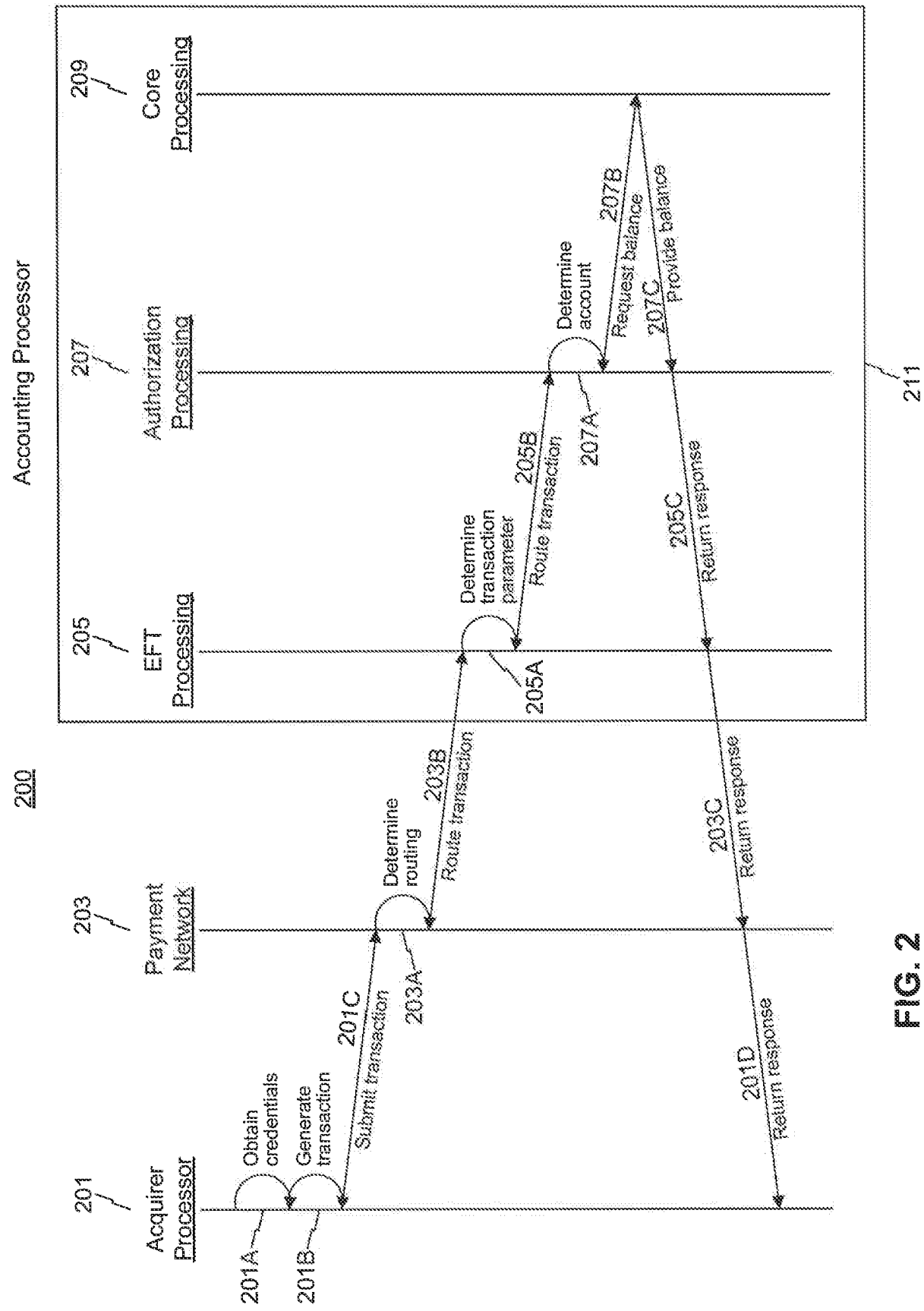
200
Accounting Processor
211
201
Acquirer Processor
203
Payment Network
205
EFT Processing
207
Authorization Processing
209
Core Processing
Obtain credentials
Generate transaction
Determine routing
Determine transaction parameter
Determine account
201A
201B
201C
Submit transaction
201D
Return response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

FIG. 2

300

	Message Type	4	**0200** – request message **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)
304	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
323	DE102	28	Account ID 1
	DE122	11	Sponsor Bank ID

FIG. 3

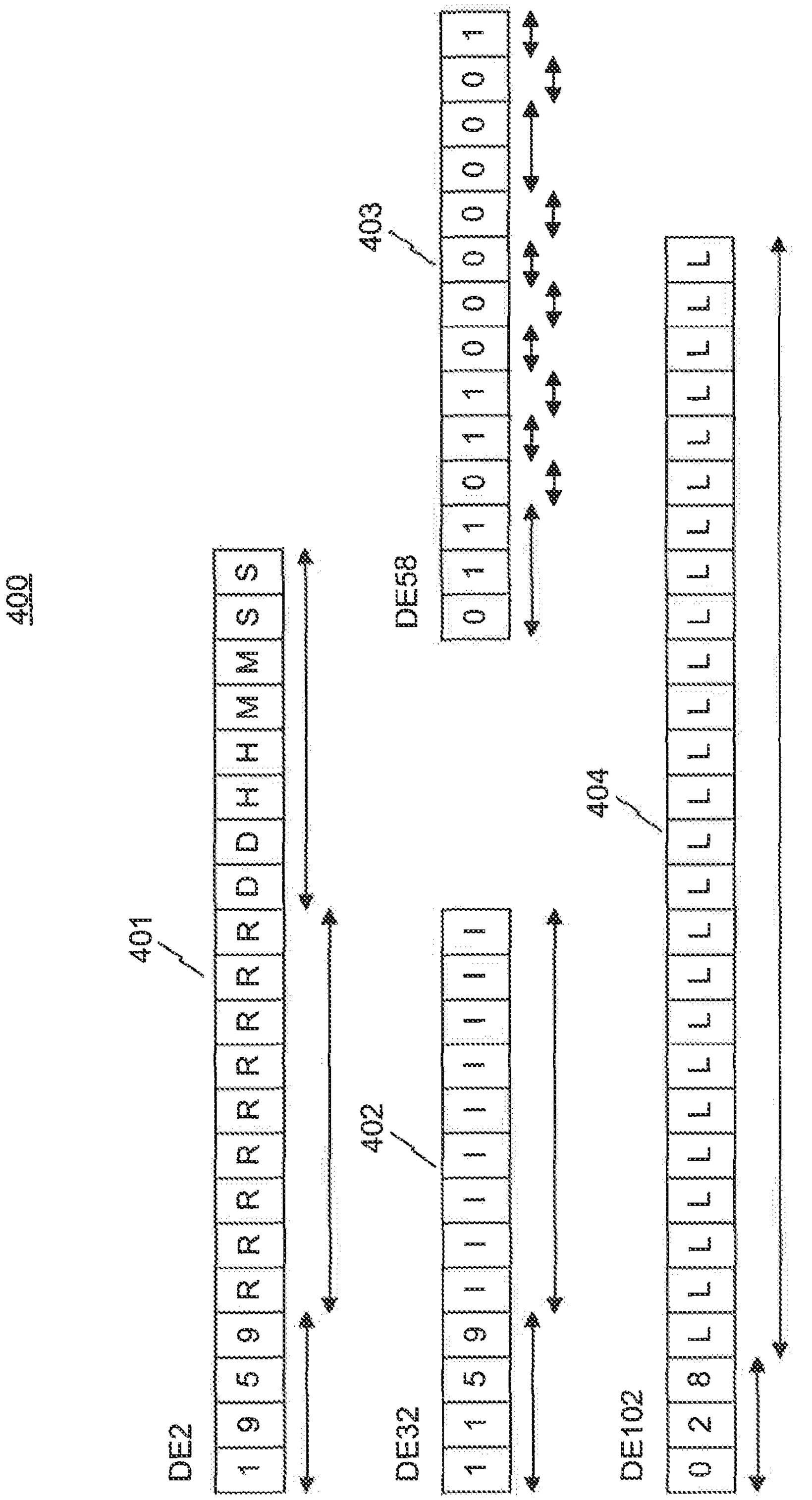

FIG. 4

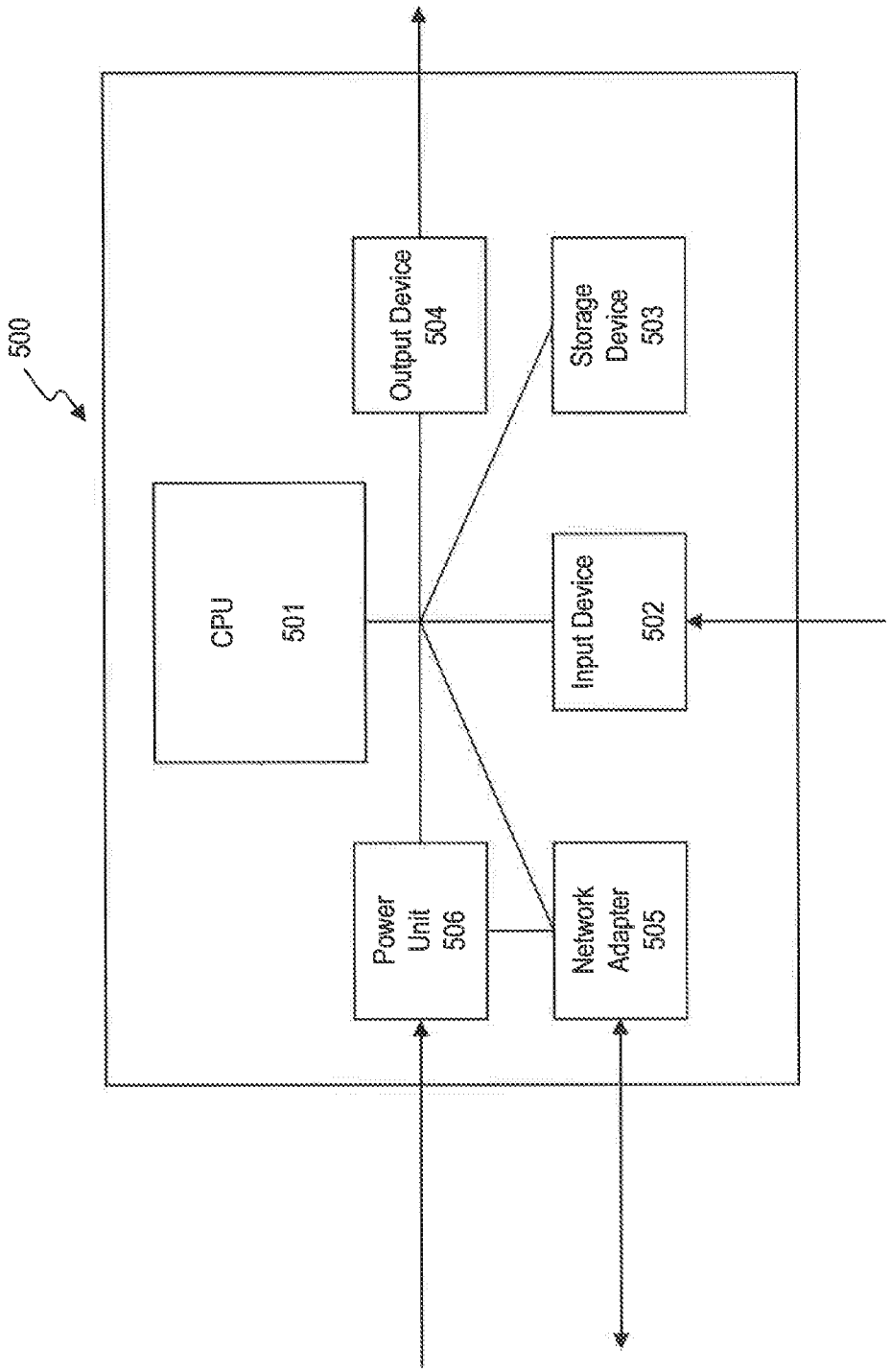
500
Output Device
504
Storage
Device
503
CPU
501
Input Device
502
Power
Unit
506
Network
Adapter
505

FIG. 5