OPIC
Office de la propriété intellectuelle du Canada

CIPO
Canadian Intellectual Property Office

(12) (19) (CA) **Demande-Application**

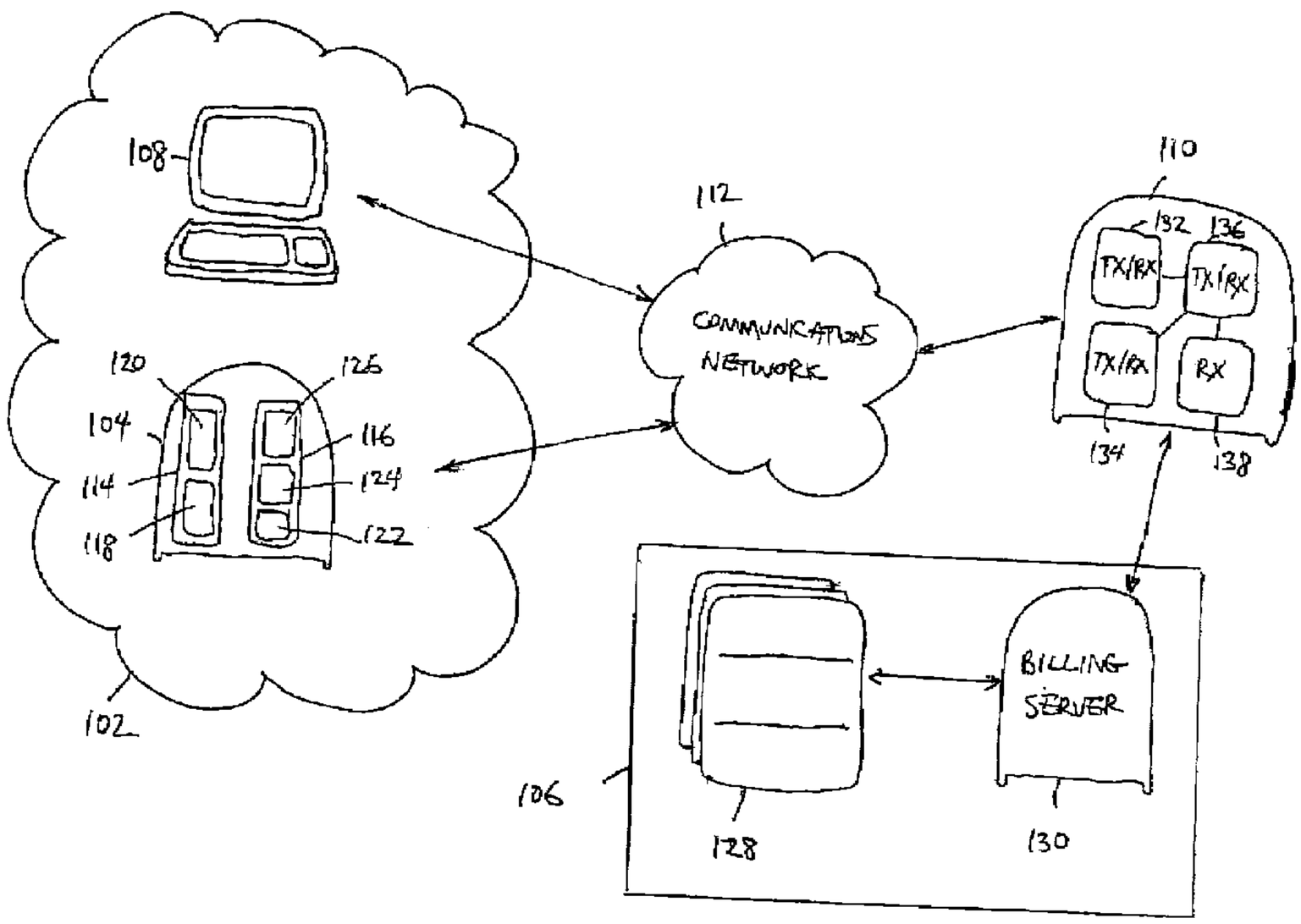
(21) (A1) **2,293,832**
(22) 1999/12/31
(43) 2001/02/05

(72) SHANNON, JOHN P., CA
(72) SOMERVILLE, JIM B., CA
(72) BOUFFARD, CLAUDE C., CA
(71) NORTEL NETWORKS CORPORATION, CA

(51) Int.Cl.[7] G06F 17/60, H04L 9/32
(30) 1999/08/05 (09/368,932) US

(54) **METHODE ET SYSTEME DE PROTECTION DES TRANSACTIONS DE COMMERCE ELECTRONIQUE**

(54) **METHOD AND SYSTEM FOR SECURE E-COMMERCE TRANSACTIONS**



(57) A system for facilitating e-commerce transactions includes a network including at least one subscriber, a virtual merchant, an authentication server, and a billing system associated with the network for obtaining payment from the subscribers. The virtual merchant includes input means for receiving a request for an e-commerce transaction, and an authorization signal for execution of the transaction. The authentication server includes a data receiver for receiving transaction information identifying the transaction, and for receiving along a first data channel subscriber billing data identifying a subscriber billing account for the transaction. The authentication server also includes an authentication transceiver for obtaining an indication of authenticity of the received billing data from the billing system along a second data channel. The authentication server further includes an authorizing transmitter for providing the merchant with the authorization signal. In operation, the virtual merchant receives a request from for an e-commerce transaction. The authorization server then receivers billing data for the transaction, and provides the merchant with an authorization signal responsive to the billing data for causing the merchant to respond to the request for the transaction in accordance with the authorization signal. The authorization server then causes the billing system to obtain payment for the transaction from the subscriber, the payment being responsive to the authenticity of the balling data. Preferably, the first and second data channels are secure at least from the virtual merchant to reduce the possibility of fraud, and the authorization signal is derived from the authenticity indication and excludes information identifying the subscriber so as to protect the anonymity of the subscriber relative to the virtual merchant.

ABSTRACT

A system for facilitating e-commerce transactions includes a network including at least one subscriber, a virtual merchant, an authentication server, and a billing system associated with the network for obtaining payment from the subscribers. The virtual merchant includes input means for receiving a request for an e-commerce transaction, and an authorization signal for execution of the transaction. The authentication server includes a data receiver for receiving transaction information identifying the transaction, and for receiving along a first data channel subscriber billing data identifying a subscriber billing account for the transaction. The authentication server also includes an authentication transceiver for obtaining an indication of authenticity of the received billing data from the billing system along a second data channel. The authentication server further includes an authorizing transmitter for providing the merchant with the authorization signal. In operation, the virtual merchant receives a request from for an e-commerce transaction. The authorization server then receivers billing data for the transaction, and provides the merchant with an authorization signal responsive to the billing data for causing the merchant to respond to the request for the transaction in accordance with the authorization signal. The authorization server then causes the billing system to obtain payment for the transaction from the subscriber, the payment being responsive to the authenticity of the billing data. Preferably, the first and second data channels are secure at least from the virtual merchant to reduce the possibility of fraud, and the authorization signal is derived from the authenticity indication and excludes information identifying the subscriber so as to protect the anonymity of the subscriber relative to the virtual merchant.

METHOD AND SYSTEM FOR SECURABLE E-COMMERCE TRANSACTIONS

FIELD OF THE INVENTION

The present invention relates to a system for electronic commerce over communications networks. In particular, the present invention relates to a method and system for maintaining the security of consumer billing information in e-commerce transactions.

BACKGROUND OF THE INVENTION

Communications networks, such as the Internet, provide consumers with the ability to engage in electronic commerce by purchasing both goods and services from the vantage point of a computer terminal interfacing with the network. Typically, a vendor or web merchant maintains a web site page, accessible over the Internet, offering for sale tangible goods or intangible goods (such as computer software) to consumers. A consumer selects from the goods offered by selecting a link on the web merchant's web page corresponding to the goods desired. The web merchant requests the consumer to provide the merchant with information to facilitate payment for the transaction, and then arranges to have the selected goods delivered to the consumer.

Various payment systems are known to facilitate such electronic commerce transactions. The most common payment system involves a consumer entering credit card details, such as the billing number and the expiry date, and the consumer's shipping address into a dialogue frame on a computer terminal. The web merchant then transmits the credit card details to the credit card provider for verification that the billing information is correct and that the cost of the transaction does not exceed any predetermined spending limit. Typically, the credit card details and the shipping information are transmitted through a secure connection over the Internet, such as an SSL (Secure Sockets Layer) connection, to reduce the possibility of the information being received by a party other than the web merchant. Despite the widespread use of SSL connections for e-commerce transactions however, the conventional credit card-based payment system is prone to fraud.

For instance, an unscrupulous web merchant or computer hacker may attempt to uncover a correct combination of credit card billing number and expiry date by sending a credit card vendor with credit card billing number and expiry date combinations. Once the credit card vendor indicates that the combination of billing number and expiry date are valid, the web merchant may use the combination to obtain revenue for fictitious transactions.

Also, typically the web merchant stores consumer credit card and shipping information in a database accessible by the web merchant's web page so that a consumer need only enter the information for the initial e-commerce transaction. Thereafter, the consumer need only enter a username and password unique to the consumer for subsequent e-commerce transactions. Although this system is advantageous in that it alleviates the need for the consumer to provide the web merchant with its credit card and shipping information for each transaction, the database is prone to espionage from computer hackers. Also, unscrupulous web merchants may use the information stored in the database to obtain revenue either by creating fictitious transactions with the information, or by selling the information to third parties.

The conventional credit card-based e-commerce payment system also exposes consumers to unauthorized use of transaction details and shipping information. For instance, the web merchant may retain the shipping information and the information on the goods purchased by each consumer for soliciting future sales either by the web merchant or third parties.

Further, the credit card holder may wish to allow other individuals, such as family members or employees, to engage in e-commerce with the credit card, but may also wish to place subject matter restrictions or monetary spending limits on each transaction. However, as the conventional credit card-based e-commerce system validates an e-commerce transaction based solely on the credit card information and the monetary spending limit set by the credit card vendor, the credit card holder is unable to set customized restrictions on e-commerce purchases.

Additional deficiencies include the price structure of credit card transactions. Although the credit card price structure is generally not problematic for conventional credit card transactions, web merchants who wish to provide small volumes of data, or charge small monetary amounts for data on a per-use basis or a timed-access basis may find the credit card price structure renders such transactions for small monetary amounts uneconomical.

Many attempts have been made to provide an e-commerce system which overcome the deficiencies of the conventional credit card-based e-commerce system. For instance, Ronen (US Patent 5,745,556) teaches an e-commerce system in which a merchant made a "900" telephone number available to consumers. To complete a sale, the consumer dials the "900" telephone number which causes the telephone company to place a charge on the user's telephone bill at a rate set by the web merchant. A portion of this charge is credited to the web merchant using the telephone company's billing system. In one variation, Ronen teaches an e-commerce system in which the consumer enters a password and its telephone number on a web page form generated by the web merchant. This information is then relayed to the telephone company to generate a charge on the consumer's telephone bill.

However, the e-commerce systems taught by Ronen have not been widely used. This may be due in part to the fact that if the consumer accesses the Internet via a telephone line connection, the consumer must maintain a second telephone line to initiate the "900" telephone call. Also, the web merchant loses control over the transaction at a crucial point. If the consumer finds the telephone number is busy or dials the wrong number, the web merchant cannot ascertain the source of the lost sale. Apart from over providing telephone access, the web merchant cannot ensure that all consumers successfully complete a transaction.

Therefore, there remains a need for an e-commerce system which is not prone to fraud or to misappropriation of consumer data, and is suitable for use with e-commerce transactions of small monetary value. Further, there remains a need for an e-commerce system which allows the consumer to set subject matter or monetary spending restrictions on transactions. Also, there remains a need for an e-commerce

system which facilitates transactions from consumers over a single communication line to the e-commerce telecommunication network.

SUMMARY OF THE INVENTION

According to the invention, there is provided a secure e-commerce transaction method and system which addresses the deficiencies of the prior art.

In accordance with a first aspect of the invention, there is provided an e-commerce transaction system comprising a network including at least one subscriber, a virtual merchant, a billing system associated with the network for obtaining payment for the e-commerce transaction, and an authentication server. The virtual merchant includes input means for receiving a request for the e-commerce transaction and for receiving an authorization signal for execution of the transaction. The authentication server includes a data receiver, an authentication transceiver, and an authorizing transmitter. The data receiver receives billing data associated with the at least one subscriber along a first data channel, and receives transaction information identifying the transaction. The authentication transceiver obtains an indication of authenticity of the received billing data from the billing system along a second data channel. The authorizing transmitter provides the merchant with the authorization signal, with the authorization signal being derived from the authenticity indication, and the payment being responsive to the authenticity indication. Preferably, the first and second data channels are secure at least from the virtual merchant to reduce the possibility of fraud, and the authorization signal excludes information identifying the subscriber so as to protect the anonymity of the subscriber relative to the virtual merchant.

In accordance with the first aspect, there is also provided a method, which is typically implemented by a virtual merchant, for conducting an e-commerce transaction between a consumer and the virtual merchant. The method comprises the steps of (1) receiving a request for the e-commerce transaction; (2) initiating transmission of billing data for the transaction to an authorization server; (3) responding to the request in accordance with an authorization signal received from the authorization server; and (4) causing a billing system to obtain payment for the

transaction, with the payment being responsive to the transaction information and the authorization signal. Preferably, the authorization signal is responsive to an authenticity of the billing data and excludes information identifying the consumer, and the billing data is transmitted over a communications channel which excludes the merchant.

In accordance with the first aspect, there is also provided a method, which is typically implemented by an authorization server, for conducting an e-commerce transaction between a virtual merchant and a consumer. The method comprises the steps of (1) receiving billing data for the transaction; (2) verifying an authenticity of the transaction billing data from the billing system; (3) providing the merchant with an authorization signal responsive to the billing data authenticity; and (4) causing the billing system to obtain payment from the subscriber for the transaction, with the payment being determined in accordance with the billing data authenticity. Preferably, the billing data is received over a communications channel which excludes the merchant, and the authorization signal excludes the billing data and information identifying the consumer.

According to a preferred embodiment of the invention, the virtual merchant comprises a web page form which offers for sale goods or services over the Internet. A consumer accessing the Internet through a web browser, and visiting the web site upon which the web page form is displayed, generates a request to purchase the goods or services offered by the web merchant selecting an appropriate link or virtual button displayed on the web page form. The web merchant responds to the request from the consumer by establishing a secure data channel between the web merchant and the authentication server via the consumer's web browser. Once the secure data channel is established, the web merchant transmits transaction information associated with the transaction to the authentication server over the first secure data channel. Typically, the transaction information includes a description of the goods or services requested, and the price to be billed for the requested goods or services.

Upon receipt of the transaction information, the authentication server determines whether the consumer had previously used the authentication server for e-commerce. Preferably, the authentication server performs the determining step by

checking the consumer's browser for the presence of a session identifier which the authentication server stored in the consumer's browser during a previous e-commerce session. If the authentication service determines that the consumer had not previously used the authentication server, or had not used the authentication server within a set time frame, the authentication server establishes a secure data channel between the authentication server and the consumer's web browser, but excluding the web merchant. Once this latter secure data channel is established, the authentication server transmits a login web page form to the consumer's browser over this latter secure data channel, prompting the consumer to enter financial data which identifies the network subscriber's billing account for the transaction. Typically, the network subscriber will be the consumer, but may also be another party such as the consumer employer. The consumer enters the requested financial data into the login web page form, and then transmits the entered information back to the authentication server over the secure data channel.

Upon receipt of the financial data, the authentication server transmits the financial data to the billing system. The billing system examines the transmitted financial data, and returns to the authentication server an indication of the validity of the financial data. The authentication server then transmits an authorization signal to the web merchant, responsive to the validity indication of the financial data, over a secure data channel established between the web merchant and the authentication server via the consumer's web browser. If the financial data is valid, preferably the validity indication includes a billing account identifier associated with the network subscriber. However, the authorization signal excludes the billing account identifier to protect the anonymity of the subscriber. The web merchant then provides or refuses to provide the requested goods or service based on the status of the authorization signal.

Preferably, once the requested transaction is completed successfully, the web merchant signals the authorization server of the successful completion, and the authorization server then transmits the billing account identifier and the transaction information to the billing system for payment via the subscriber's billing account.

In accordance with a second aspect of the invention, there is provided a billing system for billing for an e-commerce transaction between a consumer and a virtual merchant. The billing system interfaces with a billing network which includes at least one subscriber and with a subscriber database which includes billing data associated with the at least one subscriber. The billing system comprises a transaction data receiver for receiving transaction data identifying the transaction; a billing data receiver for receiving billing data for the transaction; and account transceiver in communication with the billing receiver for obtaining an account identifier from the subscriber database, the account identifier being associated with the received billing data; and a billing transmitter in communication with the account transceiver and the transaction data receiver for providing the billing network with the account identifier and the transaction data for receiving payment form the subscriber in accordance with the transaction data. Preferably, the billing data receiver includes means for establishing a first data channel secure at least from the virtual merchant for receiving the billing data, and the account transceiver includes means for establishing a second data channel secure at least from the virtual merchant for receiving the account identifier.

In accordance with the second aspect, there is also provided a method, which is typically implemented by a communications network or an authorization server, of billing for an e-commerce transaction between a virtual merchant and a consumer. The method comprises the steps of (1) receiving billing data for the transaction, the billing data being associated with a network; (2) verifying an authenticity of the transaction billing data with a billing system of the network; and (3) causing the billing system to obtain payment from the subscriber for the transaction, the payment being determined in accordance with the billing data authenticity. Preferably, the billing data is received via a communications channel which excludes the merchant.

In accordance with a third aspect of the invention, there is provided an authorization system for authorizing an e-commerce transaction between a consumer and a virtual merchant. The billing system interfaces with a network which includes at least one subscriber and with a subscriber database which includes billing data associated with the at least one subscriber. The authorization system comprises a

billing data receiver for receiving billing data identifying the transaction; an authentication transceiver in communication with the billing receiver for obtaining an indication from the subscriber database of an authenticity of the received billing data, the account identifier being associated with the received billing data; and an authorizing transmitter in communication with the authentication transceiver for providing the merchant with an authorization signal for execution of the transaction. Preferably, the billing data receiver includes means for establishing a first data channel secure at least from the virtual merchant for receiving the billing data, the authentication transceiver includes means for establishing a second data channel secure at least from the virtual merchant for receiving the authentication indication, and the authorization transmitter includes means for deriving the authorization signal from the authenticity indication and for excluding from the authorization signal information identifying the subscriber.

In accordance with the third aspect, there is also provided a method, which is typically implemented by a communications network or an authorization server, of authorizing an e-commerce transaction between a virtual merchant and a consumer. The method comprises the steps of (1) receiving billing data for the transaction, the billing data being associated with a network; (2) verifying an authenticity of the transaction billing data with a billing system of the network; and (3) providing an authorization signal responsive to the billing data authenticity, the authorization signal excluding the billing data. Preferably, the billing data is received over a communications channel which excludes the merchant.

BRIEF DESCRIPTION OF THE DRAWINGS

A preferred embodiment of the invention will now be described, by way of example only, with reference to the drawings, in which:

Fig. 1 is a schematic diagram showing an e-commerce transaction system, according to a first aspect of the invention;

Fig. 2 is a chart depicting one variation of the method steps implemented by the e-commerce transaction system shown in Fig. 1;

Fig. 3 is a chart depicting another variation of the method steps implemented by the e-commerce transaction system shown in Fig. 1; and

Fig. 4 is a chart depicting in detail the method steps implemented by the e-commerce transaction system shown in Fig. 1.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Turning to Fig. 1, an e-commerce transaction system, denoted generally as 100, for facilitating an e-commerce transaction between a consumer and a merchant, is shown comprising a network 102, a merchant server 104, a billing system 106 associated with the network 102 for obtaining payment for an e-commerce transaction involving a consumer 108, and an authentication server 110 for authorizing the transaction. The e-commerce transaction system 100 also includes a communications network 112, interconnecting the merchant server 104, the consumer 108 and the authentication server 110 for allowing communication between the merchant server 104, the consumer 108 and the authentication server 110.

The network 102 has at least one, and preferably a plurality of subscribers, to whom the cost of a requested e-commerce transaction may be billed. Preferably, the network 102 comprises a telephone network, and the cost of the requested e-commerce transaction is billed to the telephone account of one of the telephone network subscribers. The telephone account may be either an account to which invoices are sent, or may be a pre-paid account from which the cost of the transaction may be debited. As will be appreciated, the merchant server 104 may be credited with a corresponding credit to the telephone billing account associated with the merchant server 104, or through more direct means such as cash payment. The telephone network is a preferred form of the network 102 due to the recognized ability of such networks to rapidly, reliably and efficiently bill for transactions for small monetary amounts. However, other forms of the network 102 may be used. For instance, the network 102 may comprise a credit card billing network for billing credit card subscribers, or a banking network for transferring funds from the bank account of a consumer into the bank account associated with the merchant server 104. Alternately,

the network 102 may comprise a hybrid network which allows, for example, a debit to be made to the credit card account of the consumer and a corresponding credit to be made to the bank account associated with the merchant server 104. Further, the network 102 may comprise a non-monetary hybrid network which allows, for example, funds to be deposited to the bank account associated with the merchant server 104 and a corresponding number of points to be withdrawn from the AirMiles (trade-mark) account of the consumer. Alternately, the e-commerce transaction may take the form of a "pawn-shop-type" transaction with the network 102 allowing funds to be withdrawn from the bank account associate with the merchant server 104 and a corresponding number of AirMiles points to be provided to the consumer. Other variations of the network 102 will be apparent to those skilled in the art.

The merchant server 104 comprises a virtual merchant 114, and an authentication merchant 116 for communicating with the merchant server 104 and the authentication server 110. The virtual merchant 114 includes a virtual merchant transaction transceiver 118 for receiving and responding to a request for an e-commerce transaction, and a virtual merchant completion transceiver 120 for receiving from the authentication merchant 116 an authorization signal authorizing the transaction and for transmitting to the authentication merchant 116 a completion signal indicating completion of the transaction. Preferably, the communications network 112 comprises the Internet, and the virtual merchant 114 includes a web page form, accessible by consumers over the Internet, which allows consumers to engage in an e-commerce transaction with the virtual merchant 114. For instance, the virtual merchant 114 may offer for sale goods, such as software, or services, such as streaming video or audio, to consumers over the Internet. However, other e-commerce transactions may be offered, and other mechanisms may be used to conduct the e-commerce transactions without departing from the scope of the invention. For instance, consumers may elect to purchase tangible goods and have the goods shipped to a shipping address, or to obtain tangible services, such as the repaving of a driveway. Further, the merchant server 104 may be accessible over other forms of communications networks 112, and the consumer may elect to make an offer for a

transaction, rather than selecting a transaction offered by the merchant server 104. Other variations will be readily apparent.

The authentication merchant 116 comprises an authentication merchant transaction receiver 122 for receiving transaction information identifying the transaction, an authentication merchant authorization transceiver 124 for receiving from the authentication server 110 an authorization signal authorizing a transaction and for transmitting the transaction information to the authentication server 110, and an authentication merchant completion transceiver 126 for transmitting to the authentication server 110 a completion signal indicating completion of the transaction. Typically, the transaction information includes a description and the price of the goods or services which are the subject of the transaction, and a transaction identifier used by the merchant server 104 to record the transaction. Preferably, the authentication merchant authorization transceiver 124 is configured to transmit the transaction information and to receive the authorization signal over a secure data channel established between the authentication merchant 116 and the authentication server 110, such as a Secure Sockets Layer (SSL) channel, but which excludes the virtual merchant 114 to reduce the likelihood of computer hackers or third parties creating fictitious requests or fictitious authorizations for e-commerce transactions.

The billing system 106 comprises a network subscriber database 128 of subscribers to the network 102, and a network billing server (NBS) 130 in communication with the network subscriber database 128 for restricting access to the subscriber database 128 to authorized entities and for administering the allocation of credits and debits to the network billing accounts of the subscribers of the network 102. As will be appreciated, in the present invention preferably the NBS 130 administers payments between the consumer 108 and the virtual merchant 114 for the requested e-commerce transaction.

The subscriber database 128 includes subscriber data records associated with each subscriber of the network 102 for identifying the network billing account to which the cost of the e-commerce transaction is to be billed. Typically, each subscriber data record comprises a unique pair of identifier codes, and an associated network billing account identifier of a subscriber of the network 102. In the preferred

embodiment, where the network 102 comprises a telephone network, each subscriber data record comprises a calling card number of a calling card administered by the network 102, a personal identification number (PIN) associated with the calling card number, and the telephone network subscriber's telephone number associated with the calling card number and the PIN. However, it should be understood that the identifier codes are not limited to a calling card number and PIN, but may instead comprise a username and password or any other combination of codes which identify the network billing account number to which the e-commerce transaction is to be billed. For instance, if the network 102 is a credit card-based network, as discussed above, the identifier codes may comprise, for example, a credit card username and expiry date, or a credit card username and subscriber telephone number. Further, the subscriber data records may comprise any number of identifier codes, including a single identifier code. However, since the network billing account identifier is accessed by querying the subscriber database 128 with the identifier codes, to reduce the likelihood of fraud preferably the identifier codes comprise at least a primary code and a secondary code associated with each network billing account. In the event that the identifier codes are invalid, namely that the identifier codes are not associated with a known network billing account, the subscriber database 128 returns a code indicating the invalidity of the identifier codes, rather a network billing account identifier.

Also, in the preferred embodiment, where the network 102 comprises a telephone network, the subscriber database 128 comprises a Line Information Database (LIDB) for rapid access to the billing data records, and the NBS 130 comprises a digital multiplexed telephone switch (DMS). DMS switches are preferred since they are widely used by telephone companies (telcos) for call processing and therefore provide a reliable mechanism for the generation of telephone bills. Further, the LIDB is generally accessible only with the SS7 network of the associated telco, and the TCP/IP protocol commonly used with the Internet is not compatible with the SS7 protocol. Therefore, if the communications network 112 comprises the Internet, as in the preferred embodiment, the use of a telephone switch has the further advantage of simplifying access to the LIDB by the authentication server 110 by providing an interface between TCP/IP and SS7. As will be appreciated, however, the

telephone switch may be replaced with any other suitable TCP/IP - SS7 interface known to those skilled in the art.

The authentication server 110 may be provided as an element distinct from the billing system 106, or as an element integral with the billing system 106. The authentication server 110 comprises an authentication server transaction transceiver132, an authentication server billing data transceiver 134, an authentication server billing transaction transceiver 136, and an authentication server completion receiver 138. The authentication server 110 also includes a transient database, such as a RAM-based database, and a non-volatile database, such as a magnetic disk or ROM-based database, for management of the e-commerce transactions. The function of the transient database and the non-volatile database will be described below with reference to Fig. 4.

The authentication server transaction transceiver 132 receives transaction information from the authentication merchant 116, and transmits to the authentication merchant 116 an authorization signal authorizing the transaction. Preferably, the authentication merchant authorization transceiver 132 is configured to transmit the transaction information and to receive the authorization signal over a secure data channel, such as a Secure Sockets Layer (SSL) channel, established between the authentication merchant 116 and the authentication server 110 but excluding the virtual merchant 114 so as to reduce the likelihood of computer hackers or third parties creating fictitious requests or fictitious authorizations for e-commerce transactions.

The authentication server billing data transceiver 134 receives billing data records for the transaction. Preferably, the billing data records identify the billing account of a subscriber of the network 102 for billing for the e-commerce transaction. Also, preferably each billing data record comprises a pair of identifier codes which identify the network billing account number of the subscriber but which are recognized only by the billing system 106 of the network 102. As will be appreciated, in the preferred embodiment the billing data comprises a calling card number from a telephone calling card administered by the network 102, and a personal identification number (PIN) associated with the calling card number which, together with the calling

card number, is used by the billing system 106 to identify the telephone number account to which the e-commerce transaction is to be billed.

Preferably, the authentication server billing data transceiver 134 is configured to receive the billing data records over a secure data channel, such as a SSL channel, established between the consumer 108 and the authentication server 110 but excluding the merchant server 104 so as to reduce the likelihood that the merchant server 104, or any party other than the consumer 108 and the authentication server 110, may become privy to the billing data. Also, typically the consumer 108 requesting the e-commerce transaction and the network subscriber are the same entity, so that the cost of the e-commerce transaction between the consumer 108 and the merchant server 104 is billed to the consumer's billing account. However, the consumer 108 and the network subscriber need not be the same entity, so as to allow, for example, employees to engage in e-commerce transactions paid for by their employer, or to allow a family member to engage in e-commerce transactions paid for by another family member.

The authentication server billing transaction transceiver 136 is in communication with the authentication server billing data transceiver 134, and confirms the authenticity of the billing data. As will be explained below, the authentication server authorization transceiver 136 queries the billing system 106 for the network account identifier of the network account to which the transaction is to be billed. The authentication server authorization transceiver 136 then receives from the billing system 106 an indication of the authenticity of the received billing data. Preferably, the authentication server billing transaction transceiver 136 is configured to query the billing system 106 over a secure communications channel established with the billing system 106 but which excludes the merchant server 104 so as to reduce the likelihood that the merchant server 104, or any party other than the consumer and the authentication server 110, may become privy to the billing data or the network account identifier. If the billing data is valid, preferably the billing system 106 returns the network account identifier associated with the billing data, whereas if the billing data is invalid, the billing system 106 returns an error code.

Upon receipt of the network account identifier, the authentication server billing transaction transceiver 136 provides the authentication merchant 116 with an

authorization signal responsive to the validity of the billing data. Preferably, the authentication server billing transaction transceiver 136 is also in communication with the authentication server transaction transceiver 132 so as to transmit the authorization signal to the authentication merchant 116 with a reduced likelihood that any party other than the authentication merchant 116 and the authentication server 110 may become privy to the authorization signal, and to reduce the likelihood of computer hackers or third parties creating fictitious authorization signals for e-commerce transactions. However, alternately the authentication server billing transaction transceiver 136 may be configured to transmit the authorization signal over another secure data channel established between the authentication server 110 and the authentication merchant 116. Further, to prevent the virtual merchant 114, the authentication merchant 116, or any party other than the consumer 108, the authentication server 110 or the billing system 106 from being privy to the network account identifier, preferably the authentication server billing transaction transceiver 136 also includes a filter for excluding the network account identifier from the authorization signal.

Preferably, the authentication server billing transaction transceiver 136 queries the billing system 106 by querying the subscriber database 128 with a data record comprising the billing data received by the authentication server billing data transceiver 134. Further, in the preferred embodiment, where the network 102 comprises a telephone network, the NBS 122 comprises a telephone switch, and the billing data comprises a calling card number and PIN, the communications channel established with the billing system 106 comprises a SS7 data channel, and the data record for querying the subscriber database 120 also includes a fictitious "FROM" telephone number and a fictitious "TO" telephone number which identify the authorization server 110 as an entity entitled to access the LIDB. Further, as some telephone calling cards only allow subscribers to make a telephone call to a predetermined destination telephone number, such as the subscriber's home telephone number, the combination of the fictitious "FROM" and "TO" telephone numbers are set by the telco to ensure that the query with the subscriber database 128 always functions properly.

The authentication server billing transaction transceiver 136 is also in communication with the authentication server transaction transceiver 132 and the authentication server billing data transceiver 134 not only for confirming the authenticity of the billing data and for providing the authentication merchant 116 with a transaction authorization signal, but also for providing the billing system 106 with the network billing account identifier and the transaction data for initiating payment for the e-commerce transaction. In the preferred embodiment, where the network 102 comprises a telephone network and the NBS 122 comprises a telephone switch, preferably the billing system 106 enters a credit and a corresponding debit to the telephone billing accounts of the merchant server 104 and the consumer 108 for the e-commerce transaction. As will be appreciated, if the billing data is valid, the monetary value of the payment is determined in accordance with the transaction data and an optional transaction fee administered by the authentication server 110 and the billing system 106. The transaction fee may also include a nominal value for the costs of processing invalid billing data identifiers. Alternately, if the billing data is invalid, the merchant server 104 may be billed a nominal amount in accordance with a fee structure administered by the authentication server 110 and the billing system 106.

The authentication server completion receiver 138 receives from the authentication merchant 116 a completion signal indicating completion of the transaction for providing the billing system 106 with a completion signal for initiating payment for the transaction upon completion of the transaction. Preferably, the authentication server completion receiver 138 is in communication with the authentication server billing transaction transceiver 136 so as to allow the authentication server billing transaction transceiver 136 to transmit the completion signal to the billing system over a secure communications channel. However, the authentication server completion receiver 138 may also be configured to transmit the completion signal over another secure communications channel established with the billing system 106 but which excludes the merchant server 104. Further, it should be understood that the authentication server completion receiver 138 is not an essential element of the invention. Rather, the authentication server 110 may be configured to initiate payment prior to completion of the transaction, such as where the transaction

request relates to a flat-rate transaction which is billed whether or not the transaction is performed until completion.

A high-level overview of the operation of the e-commerce transaction system shown in Fig. 1 will now be described with reference to the charts shown in Fig. 2 and Fig. 3, followed by a more detailed overview with reference to the chart shown in Fig. 4. The chart shown in Fig. 2 depicts the communication of data between the merchant 104, the billing system 106, the consumer 108, and the authentication server 110. At step 202, the merchant 104 receives from the consumer 108 a request for an e-commerce transaction. Preferably, the request relates to a transaction between the merchant 104 and the consumer 108. However, the request may also relate to a transaction between the merchant 104 and a third-party, or between two parties other than the merchant 104 and the consumer 108.

At step 204, the authentication server 110 initiates transmission of billing data for the transaction from the consumer 108 to the authentication server 110. Preferably, the billing data is associated with the network 102 and is received over a communications channel excluding the merchant 104. As discussed above, the authentication server 110 may be provided as an element distinct from or integral with the billing system 106. Consequently, in the latter case, the billing system 106 initiates transmission of billing data for the transaction.

Upon receipt of the billing data, the authentication server 110 verifies the authenticity of the billing data with the billing system 106, at step 206. The authentication server 110 then provides the merchant 104 with an authorization signal responsive to the authenticity of the billing data, at step 208. Preferably, the authorization signal excludes the billing data and information identifying the consumer. At step 210, the merchant 104 responds to the request for the e-commerce transaction in accordance with the authorization signal. The billing system 106 then obtains payment for the transaction, with the payment being based on the transaction information and the authorization signal. Preferably, the billing system 106 obtains payment after completion of the transaction, with the request for payment being initiated by the merchant 104, the consumer 108, the party which participates with the merchant 104 in the transaction (in the case where the consumer 108 only initiates the

request for the transaction), or a third party to the transaction. However, as discussed above, the e-commerce transaction system 100 may be configured to obtain payment prior to completion of the transaction, such as where the transaction request relates to a flat-rate transaction, which is billed whether or not the transaction is performed until completion. In this latter variation, preferably the request for payment is initiated by the authentication server 110 upon verification of the billing data authenticity.

Fig. 3 again depicts the communication of data between the merchant 104, the billing system 106, the consumer 108 and the authentication server 110. As above, at step 302 the merchant 104 receives a request for an e-commerce transaction. However, in contrast to the previous embodiment, the billing data for the transaction is retained on the authentication server 110, preferably having been transmitted to the authentication server 110 in a previous transaction. Consequently, after the request for an e-commerce transaction is received at step 302, the authentication server 110 initiates transmission of the billing data to the billing system 106 at step 304. Preferably, the billing data is transmitted to the billing system 106 over a communications channel excluding the merchant 104, with the transmission of the billing data being initiated at the behest of the merchant 104 requesting confirmation to proceed with the transaction.

Upon receipt of the billing data, the billing system 106 verifies the authenticity of the billing data, at step 306. The authentication server 110 then provides the merchant 104 with an authorization signal responsive to the authenticity of the billing data, at step 308. At step 310, the merchant 104 responds to the request for the e-commerce transaction in accordance with the authorization signal. The billing system 106 then proceeds to obtain payment for the transaction. The foregoing methods will now be described in more detail with reference to Fig. 4.

The chart shown in Fig. 4 depicts the communication of data between the consumer 108, the authentication server 110, the virtual merchant 114, the authentication merchant 116, the subscriber database 128, and the NBS 130. As discussed above, preferably the virtual merchant 114 comprises a web page form which offers for sale goods or services over the Internet. At step 402, a consumer 108 accessing the Internet through a web browser, requests access to the web page form of

the virtual merchant 104 by entering the URL of the virtual merchant 114 into the web browser. The virtual merchant 114 receives the request via the virtual merchant transaction transceiver 118, and responds to the request from the consumer 108 by transmitting the requested web page form back to the consumer 108 through the virtual merchant transaction transceiver 118 at step 404, thereby providing the consumer 108 with a description of the items offered, the price associated with each item and a transaction identifier to identify the transaction. As will be discussed below, the virtual merchant 114 uses the transaction identifier, after the consumer billing data is authenticated, to identify which items the consumer 108 has requested, and to reconcile the billing statement received from the billing system 106 with the goods or services sold.

The consumer 108 views the list of goods or services offered by the virtual merchant 114, and identifies the items/services it wishes to purchase by selecting a "radio button", "check box" or other identifier associated with the desired items. The consumer then generates a request to purchase the identified items by selecting a virtual button provided on the web page form for that purpose. The virtual button is configured with the network address or URL of the authentication merchant 116 so as to transmit the list of selected items from the web browser of the consumer 108 to the authentication merchant transaction receiver 122, at step 406, rather than to the virtual merchant 114. Upon receipt of the itemized list from the consumer 108, the authentication merchant 116 compiles a transaction data list which includes a description of the selected items, the sale price of the selected items, and the transaction identifier which identifies the transaction.

After the transaction data list is complied, the authentication merchant 116 encrypts the transaction data list, preferably using a private key - public key encryption scheme, and is then transmitted to the authentication server 110 in a manner to be described below. According to the preferred encryption scheme, the authentication merchant 116 signs the transaction data list with a private key which is unique to and known only to the authentication merchant 116. The signed transaction data list can only be read using a key which corresponds to the private key. The corresponding key is publicly available and, when applied to the authentication server

110 to the signed transaction data list, verifies to the authentication server 110 that the transaction data list originated from the authentication merchant 116 and not from a third party such as a computer hacker intending to generate fictitious purchase requests.

After signing the transaction data list with the private key of the authentication merchant 114, the virtual merchant encrypts the signed data list with a key which is publicly available and is associated with the authentication server 110. The signed encrypted data list can only be read using a key which corresponds to the public key used to encrypt the signed data list. The key corresponding to the public key used to encrypt the signed data list is unique to and known only to the authentication server 110. Consequently, when the authentication merchant 116 signs the data list with its private key, and then encrypts the signed data list with the public key of the authentication server 110, the authentication merchant 116 has a degree of assurance that no entity other than the authentication server 110 will be able to read the data list and the authentication server 110 will have a degree of assurance that the data list originated from the authentication merchant 116. Other means of verifying the authenticity and confidentiality of the transaction data will be apparent to those skilled in the art.

After the transaction data list is compiled, signed and encrypted, the authentication merchant 116 establishes a secure data channel with the consumer 108 at step 408, and then transmits the transaction data list to the consumer 108 over the secure date channel via the authentication merchant authorization transceiver 124. The signed, encrypted data list is transmitted to the consumer 108 with the URL or network address of the authentication server 110. Consequently, when the web browser of the consumer 108 receives the transaction data from the authentication merchant 116, the web browser establishes a secure data channel with the authentication server 110 at step 410, and then transmits the received transaction data to the authentication server 110 over the secure data channel. The transaction data is received at the authentication server 110 via the authentication server transaction transceiver 132. Preferably, the secure data channels established at steps 408 and 410 each comprise a separate Secure Sockets Layer (SSL) data channel so that when

combined with the use of public and private key encryption technology, as discussed above, there is provided a high degree of assurance of the authenticity and confidentiality of the transaction data. However, other means of provide secure data channels may be used if desired. Further, it will be appreciated that the secure data channels and/or the encryption of the transaction data may be dispensed with if confidentiality and authenticity of the transaction data is not of significant concern.

Upon receipt of the signed, encrypted data list from the authentication merchant 116 (via the consumer 108), the authentication server 110 decrypts the encrypted data list with its private key, and then reads the resulting signed data list with the public key of the authentication merchant 116, as described above. The authentication server 110 then transmits a login page to the consumer 108 via the authentication server billing data transceiver 134, at step 412, over the secure data channel established at step 410, requesting that the consumer 108 provide billing data which will identify a billing account for the requested transaction. Typically, the billing account will be associated with the consumer 108, but may also be associated with another party such as the consumer's employer.

At step 414, the requested billing data is transmitted from the consumer 108 to the authentication server 110 over the secure data channel established at step 410. Preferably, the billing data comprises a telephone calling card number, the associated personal identification number (PIN) and the name of the telephone company which administers the telephone calling card. Alternately, the billing data may comprise a credit card number and the associated expiry date. However, it should be understood that the invention is not limited to any particular form of billing data. Rather, the billing data need only identify the billing account to which the cost of the desired transaction may be billed. Consequently, it will be apparent that the billing data may simply comprise a single alphanumeric sequence such as, for example, a bank account number or telephone account number. However, preferably the billing data comprises at least two billing account identifier codes which are cross-referenced so as to reduce the possibility of fraud.

Upon receipt of the billing data, the authentication server 110 establishes a secure data channel with the NBS 122, at step 416, and then transmits the billing data

to the NBS 122 over the secure data channel via the authentication server billing transaction transceiver 136. The NBS 130 queries the subscriber database 128 with the billing data at step 418, and in reply receives an indication from the subscriber database 128 of the authenticity of the transmitted billing data, at step 420. Specifically, if the subscriber database 128 includes a record whose billing account identifier codes match the transmitted billing account identifier codes, the subscriber database 128 replies to the NBS 130, at step 420, with the billing account identifier associated with the transmitted billing account identifier codes. On the other hand, if the subscriber database 128 does not include a record which billing account identifier codes match the transmitted billing identifier codes, the subscriber database 128 replies to the NBS 130, at step 420, with a signal indicating that the billing data is not associated with a valid billing account. In the preferred embodiment the billing data comprises a telephone calling card and PIN, the network 102 comprises a telephone network, the subscriber database 128 comprises a LIDB, and the NBS 130 comprises a telephone switch. Consequently, in these circumstances, the authentication server 110 establishes a secure data channel with the NBS 130 by making a telephone connection with the NBS 130. The authentication server 110 then transmits the calling card number and the associated PIN, at step 416, to the NBS 130 for verification by the LIDB at step 418. As discussed above, preferably the authentication server 110 also transmits, as part of the data package including the calling card number and PIN, fictitious "FROM" and " TO" telephone numbers established with the telco to ensure that the LIDB lookup returns valid data. The LIDB then replies to the NBS 130, at step 420, either with the telephone number associated with the calling card number and PIN, or a signal indicating that the calling card number does not correspond to the PIN provided.

At step 422, the NBS 130 provides the authentication server 110 with the indication of the authenticity of the billing data received from the subscriber database 128 at step 420. The authenticity indication is received at the authentication server 110 via the authentication server billing transaction transceiver 136. If the authentication server 110 is notified by the NBS 130 at step 422 that the billing data received from the consumer 108 is valid, preferably the authentication server 110 then

transmits to the consumer 108, at step 424, a web page over the secure data channel (established at step 410) via the authentication server billing data transceiver 134 asking the consumer 108 to confirm the transaction. The consumer 108 then responds by selecting a virtual button provided on the web page indicating whether the consumer 108 wishes to proceed with the transaction. The reply from the consumer 108 is transmitted over the secure channel, at step 426, and received by the authentication server billing data transceiver 134 of the authentication server 110.

On the other hand, if the authentication server 110 is notified by the NBS 130 at step 422 that the billing data received from the consumer 108 is invalid, the authentication server 110 transmits to the consumer 108, at step 424, a web page over the secure data channel (established at step 410) via the authentication server billing data transceiver 134 asking the consumer 108 to re-enter the billing data. The consumer 108 then responds with new billing data, as discussed above with respect to step 414. The authentication server 110 then attempts to authenticate the billing data, as discussed above with respect to steps 416 to 422. If the authenticity of the new billing data is verified, or if the authentication server 110 is unable to verify the authenticity of the billing data after a predetermined limit for unsuccessful login attempts, the authentication server 110 proceeds as set out in the follow paragraph. As will be appreciated, steps 424 and 426 may be eliminated if desired.

Upon receipt of the reply from the consumer 108 at step 426, preferably the authentication server 110 filters the indication of authenticity (and the optional confirmation reply received from the consumer 108) so as to obtain an authorization signal which excludes the billing data and any other information which the virtual merchant 114 could use to identify the subscriber associated with the network billing account. However, as will be appreciated, the authorization signal includes the transaction identifier associated with the transaction. Preferably, the authentication server 110 includes with the authorization signal a serial number for the transaction, which serial number is unique to the authentication merchant 116 to preclude a third party or computer hacker from intercepting the authorization signal and thereby generating multiple fictitious authorization signals. The authentication server 110 then signs the authorization signal with the private encryption key of the

authentication server 110 to provide the authentication merchant 116 with a degree of certainty that the authorization signal originated from the authentication server 110 and not from a third party such as a computer hacker intending to generate fictitious authorization signals, and then encrypts the signed authorization signal with the public key of the authentication merchant 116 to provide the authentication server 116 with a degree of certainty that the signed authorization signal can only be read by the authentication merchant 116. Other means of verifying the authenticity and confidentiality of the authentication signal will be apparent to those skilled in the art.

After the authorization signal is signed and encrypted, the authentication server 110 transmits the signed, encrypted authorization signal to the consumer 108, at step 428, over the secure data channel established at step 410 via the authentication server transaction transceiver 132. The signed, encrypted authorization signal is transmitted to the consumer 108 with the URL or network address of the authentication merchant 116. Consequently, when the web browser of the consumer 108 receives the authorization signal from the authentication server 110, the web browser establishes a secure data channel with the authentication merchant 116 at step 430, and then transmits the received authorization signal to the authentication merchant 116 over the secure data channel. The authorization signal is received at the authentication merchant 116 via the authentication merchant authorization transceiver 124. Preferably, the secure data channel established at step 430 comprises a SSL data channel so that when combined with the use of public and private key encryption technology, as discussed above, there is provide a high degree of assurance of the authenticity and confidentiality of the authorization signal. However, other means of provide secure data channels may be used if desired. Further, it will be appreciated that the secure data channels and/or the encryption of the authorization signal may be dispensed with if confidentiality and authenticity of the authorization signal is not of significant concern.

Upon receipt of the signed, encrypted authorization signal from the authentication merchant 116 (via the consumer 108), the authentication merchant 116 decrypts the encrypted authorization signal with its private key, and then reads the resulting signed data list with the public key of the authentication server 110. The

authentication merchant 116 then transmits the authorization signal (via the authentication merchant transaction transceiver 132) to the virtual merchant 114 (via the virtual merchant transaction completion transceiver 120), at step 432. If the authorization signal indicates that the billing data was valid (and the transaction was optionally confirmed by the consumer 108), the virtual merchant 114 then proceeds with the requested transaction at step 434. If, for example, the transaction request related to a software download, the transaction could be conducted via the virtual merchant transaction transceiver 118. On the other hand, if the authorization signal indicates that the billing data was invalid (or the transaction was not confirmed by the consumer 108), the virtual merchant 114 does not proceed with the transaction.

Upon completion of the transaction, the virtual merchant 114 transmits a completion signal (via the virtual merchant completion transceiver 120) to the authentication merchant 116 (via the authentication server completion transceiver 126) at step 436. The authentication merchant 116 then establishes a secure data channel with the authentication server 110, and transmits the completion signal (via the authentication merchant completion transceiver 126) to the authentication server 110 over the secure data channel (via the authentication merchant completion receiver 138), at step 438. Alternately, the consumer 108 may transmit a completion signal directly to the authentication server 110 over the secure data channel established at step 410 between the consumer 108 and the authentication server 110.

At step 440, the authentication server 110 transmits the transaction data (including a description of the goods or servers requested, the price to be billed for the requested goods or services, and the transaction identifier) and the network account identifier to the NBS 130 (via the authentication server billing transaction transceiver 136). The NBS 130 then proceeds to bill the network account for the transaction in accordance with the price established in the transaction data and an optional transaction fee administered by the authentication server 110 and the billing system 106. As discussed above, the transaction fee may comprise a fee to be paid by the virtual merchant 114 if the transaction was not confirmed by the consumer 108. Also, as discussed above, in the preferred embodiment where the network 102 comprises a telephone network, the network account identifier comprises a telephone number, and

the NBS 130 issues an invoice for the telephone account, including the description of the goods or services on the invoice. Alternately, the network account identifier may be associated with a pre-paid telephone account (such as a pre-paid telephone calling card), and the NBS 130 may debit the pre-paid telephone account for the transaction.

Thus far, it may appear that the foregoing embodiment is limited in being suitable only for a single discrete transaction. However, the invention is not so limited. For instance, if a consumer 108 requests an ongoing transaction, such as for "streaming audio" or "streaming video", preferably the virtual merchant 114 transmits completion signals (steps 436) to the authentication server 110 (via the authentication merchant 116) at periodic intervals throughout the transaction. Alternately, the authentication server 110 may transmit periodic confirmation web pages to the consumer 108 throughout the transaction (such as the confirmation web page transmitted at step 424), requesting the consumer 108 to verify that it wishes to continue with the transaction.

However, the foregoing embodiments are limited in that they do not allow the consumer 108 to customize the authorization process. For instance, the consumer 108 may wish to place a monetary limit on such transactions or restrict the subject matter of acceptable transaction. Accordingly, in one variation, rather than the authorization server 110 transmitting to the consumer 108 a web page asking the consumer 108 to confirm the transaction, at step 424, the authentication server 110 first accesses the non-volatile database of the authentication server to determine if any restrictions have been placed on transactions associated with the network billing account identifier. According to this latter variation, if restrictions have been placed on permitted transactions, the authorization server 110 transmits to the consumer 108 the confirmation web page at step 424 only if the requested transaction complies with these restrictions. Alternately, if the requested transaction does not comply with the predetermined restrictions, the web page transmitted at step 424 may allow the consumer 108 to proceed with the transaction if the consumer is able to provide a secondary "override" password previously established by the consumer 108. In either case, if the authentication server 110 is unable to locate any entry in the non-volatile database of the authentication server associated with the network billing account

identifier, the web page transmitted to the consumer 108 at step 424 prompts the consumer 108 to enter the transaction restrictions desired (if any). The restrictions are then retained in the non-volatile database upon confirmation of the validity of the billing data at step 422.

The foregoing embodiments are also limited in that they require the consumer 108 to "log in" or provide billing data for each transaction. This requirement can be bothersome to consumers, particularly if the consumer 108 wishes to visit multiple web merchants 114 within a single Internet session. Accordingly, in another variation, rather than transmitting a login page to the consumer 108 upon receipt of the signed, encrypted data list from the authentication merchant 116 at step 410, the authentication server 110 first determines whether the consumer 108 has previously used the authentication server 110 for e-commerce transactions. Further, it is desirable to allow the authentication server 110 to maintain a user list in the transient database identifying those consumers who are actively using the authentication server 110 (and identifying the network billing account for those consumers) so that the authentication server 110 will not have to verify the authenticity of the billing data for each transaction requested during a single Internet session. Consequently, in another variation the authentication server 110 determines whether the consumer 108 has previously used the authentication server 110 with a predetermined login period. The primary purpose of performing this latter more detailed check is to avoid the problem of the transient database being overrun by entries associated with consumers who left the authentication server 110 without logging out of the authentication server 110 (such as by turning off the consumer's computer or terminating the web browser of the consumer 108).

Since the authentication server 110 is now (at step 410) in direct communication with the web browser of the consumer 108, preferably the authentication server 10 determines whether the consumer 108 has previously used the authentication server 110 (or used the authentication server 110 within a predetermined login period) by searching the web browser memory of the consumer 108 for a "cookie" which the authentication server 110 deposited with the web browser during a previous session. Preferably, the cookies which the authentication

server 110 deposits with the web browser are transmitted to the consumer 108 at step 412 during a previous login attempt, are time-stamped, are encrypted with, for example, a simply encryption key, to preclude tampering, and include a login session identifier pointing to an entry in the transient database of the authentication server 110 identifying the network account identifier for the consumer 108. By transmitting such cookies, the authentication server 110 is also able to determine whether the web browser is capable of accepting cookies.

Preferably, the cookies are transient in nature, namely that they are stored in web browser memory rather than on a nonvolatile storage medium on the computer of the consumer 108, so that if the consumer 108 terminates the web browser, the cookies will be destroyed. This latter feature is advantageous since it prevents unauthorized users from initiating transactions with a virtual merchant 114 by accessing the web browser of the consumer 108 after the consumer 108 has provided the requisite billing data and then left the computer unattended. If the authentication server 110 is unable to locate any such cookie, or is unable to establish by other means whether the consumer 108 has previously used the authentication server 110, the authentication server 110 transmits the login page to the consumer 108, at step 412. According to this variation, if the consumer 108 logs out of the authentication server 110, the authentication server 110 removes the cookie from the web browser memory.

Further, the foregoing embodiments are limited in that they initiate billing only after completion of the transaction. This limitation may be problematic where the transaction has an associated "flat-rate" fee structure and involves a significant time delay between transmission of the authorization signal to the virtual merchant 114 (step 432) and transmission of the completion signal to the authentication server 110 (step 438). Accordingly, in another variation, rather than the authentication server 110 awaiting receipt of the completion signal at step 438 before initiating billing, the authentication server 110 transmits the transaction data and the network account identifier to the NBS 130 immediately after the authentication server 110 transmits the signed, encrypted authorization signal to the consumer 108, at step 428. As a result, steps 436 and 438 may be eliminated in this variation.

The foregoing description is intended to be illustrative of the preferred embodiments of the invention. Those of ordinary skill may envisage certain additions, deletions and/or modifications to the described embodiments which, although not expressly suggested by the foregoing embodiments, are nevertheless encompassed by the spirit or scope of the invention as defined by the appended claims.

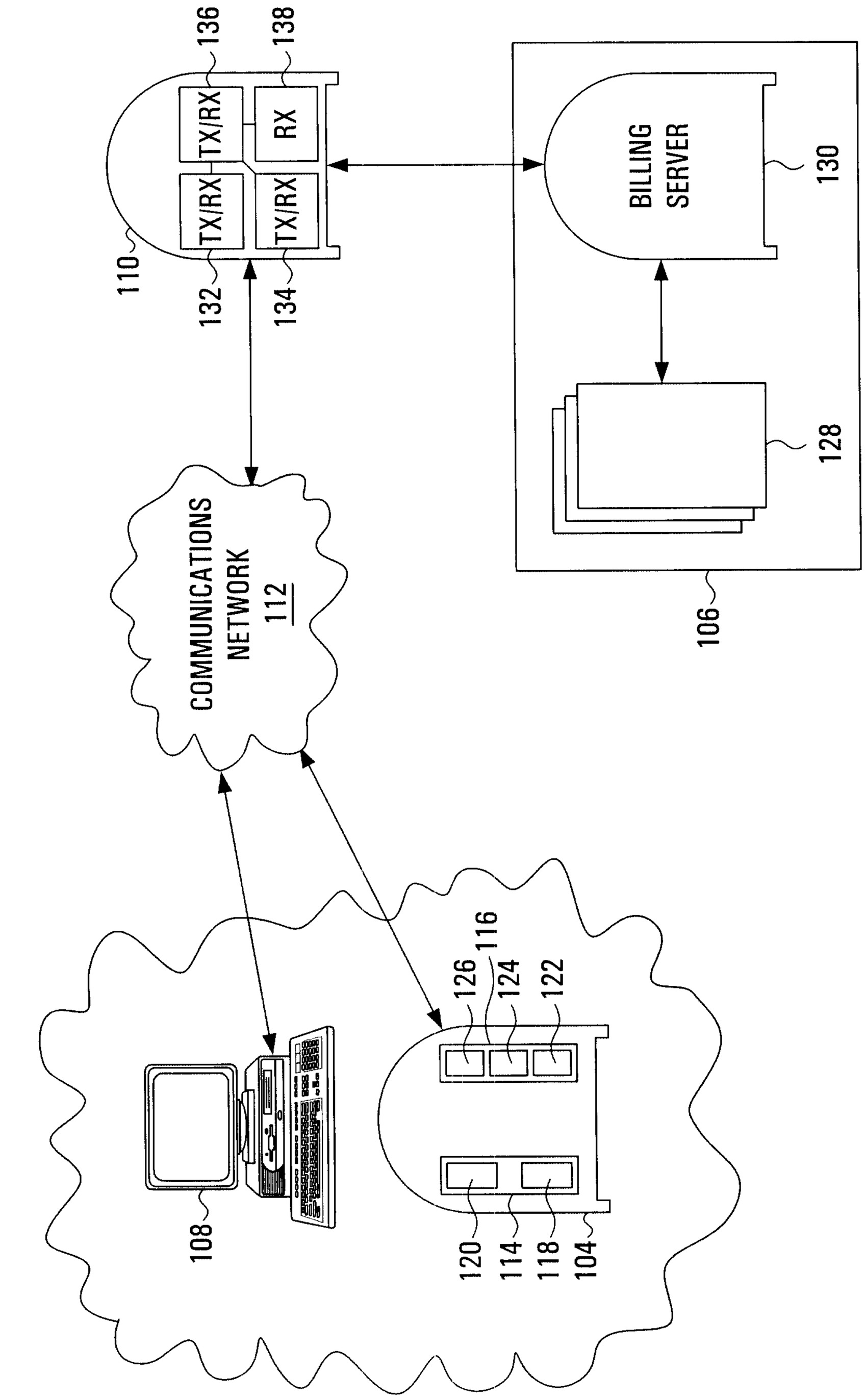

136
138
TX/RX
RX
TX/RX
RX
110
132
134
COMMUNICATIONS NETWORK 112
BILLING SERVER
130
128
106
126
116
124
122
108
120
114
118
104

FIG. 1

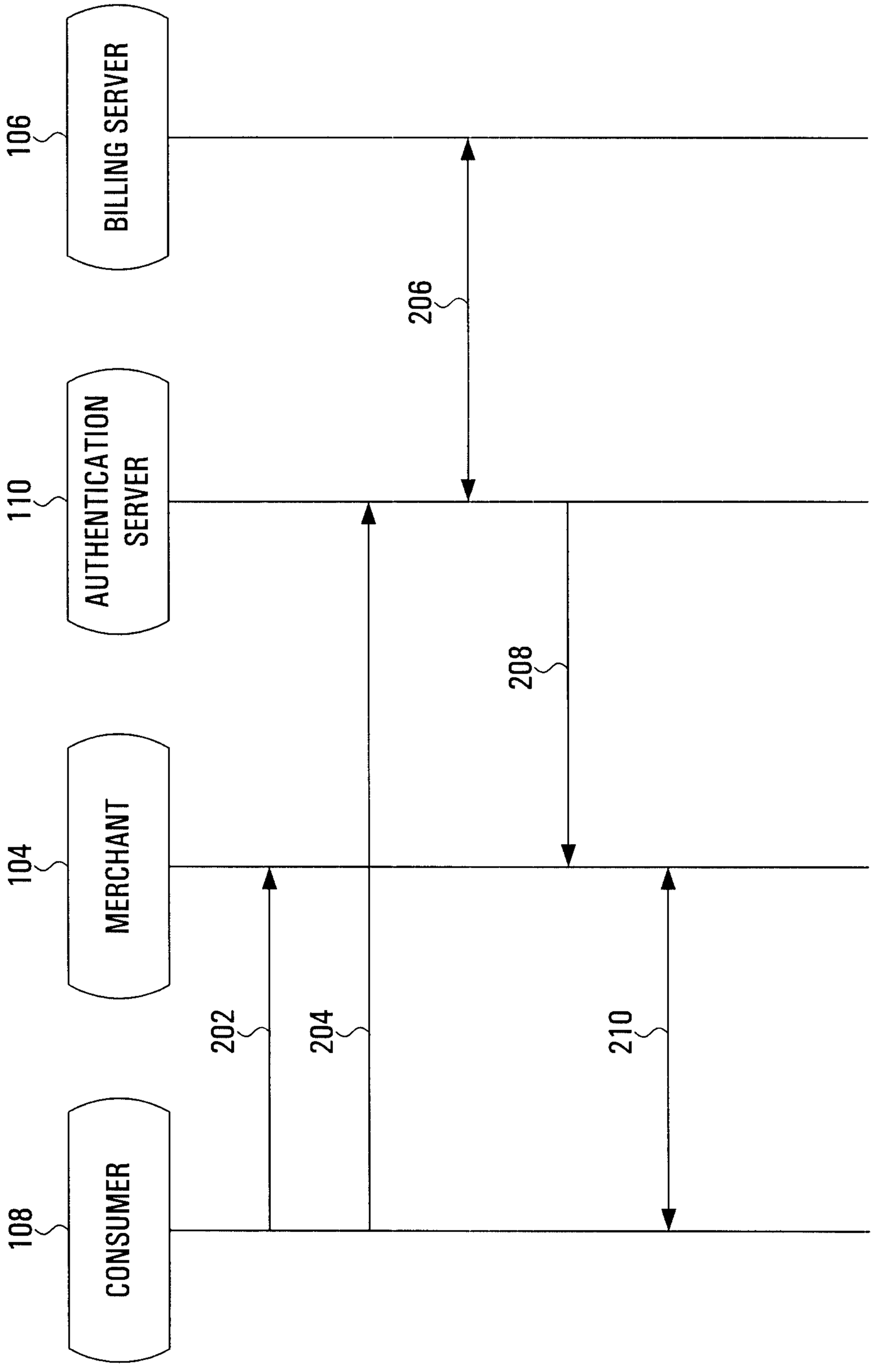

106
BILLING SERVER
206
110
AUTHENTICATION SERVER
208
104
MERCHANT
202
204
210
108
CONSUMER

FIG. 2

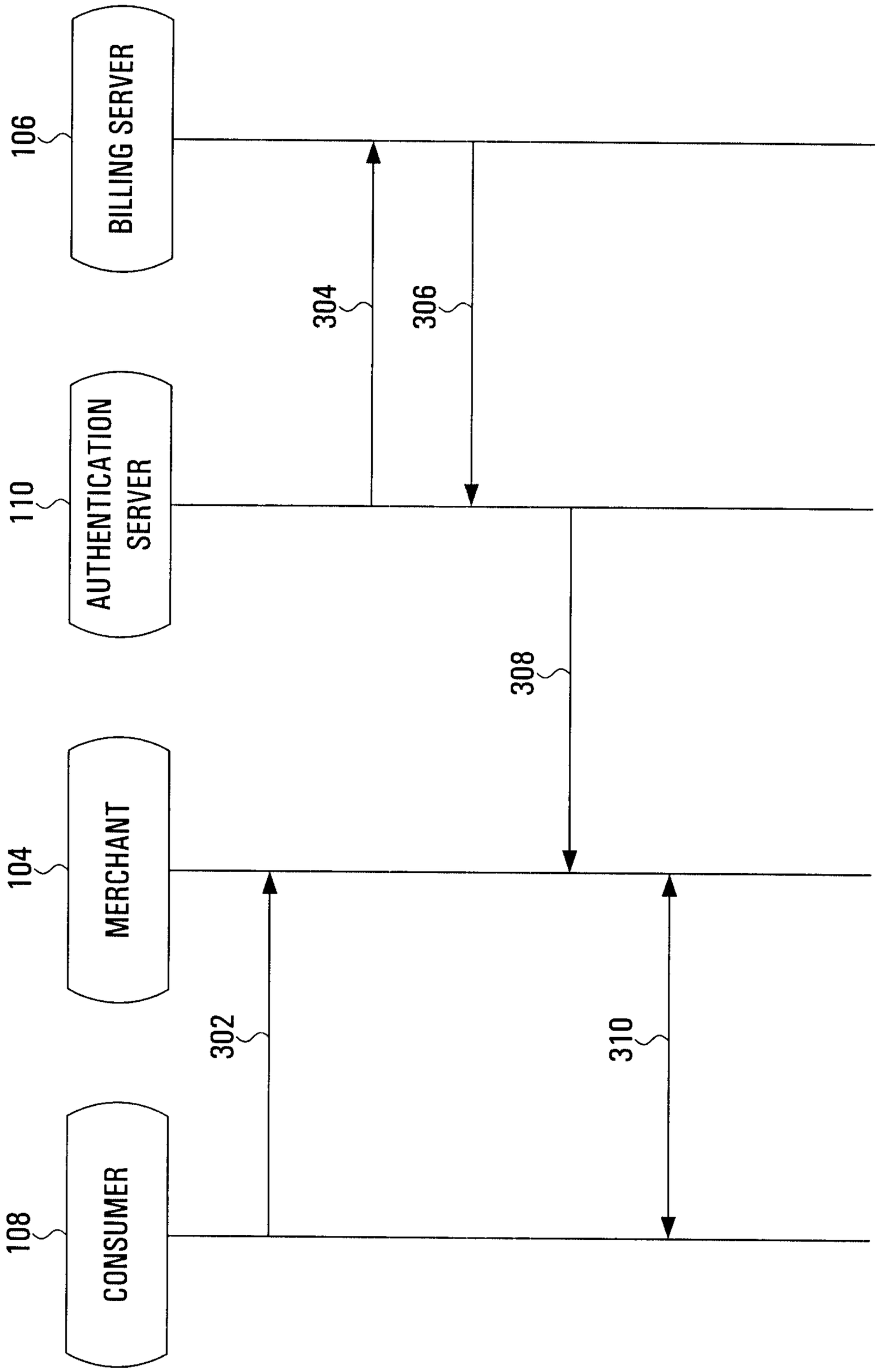

106
BILLING SERVER
304
306
110
AUTHENTICATION SERVER
308
104
MERCHANT
302
310
108
CONSUMER

FIG. 3

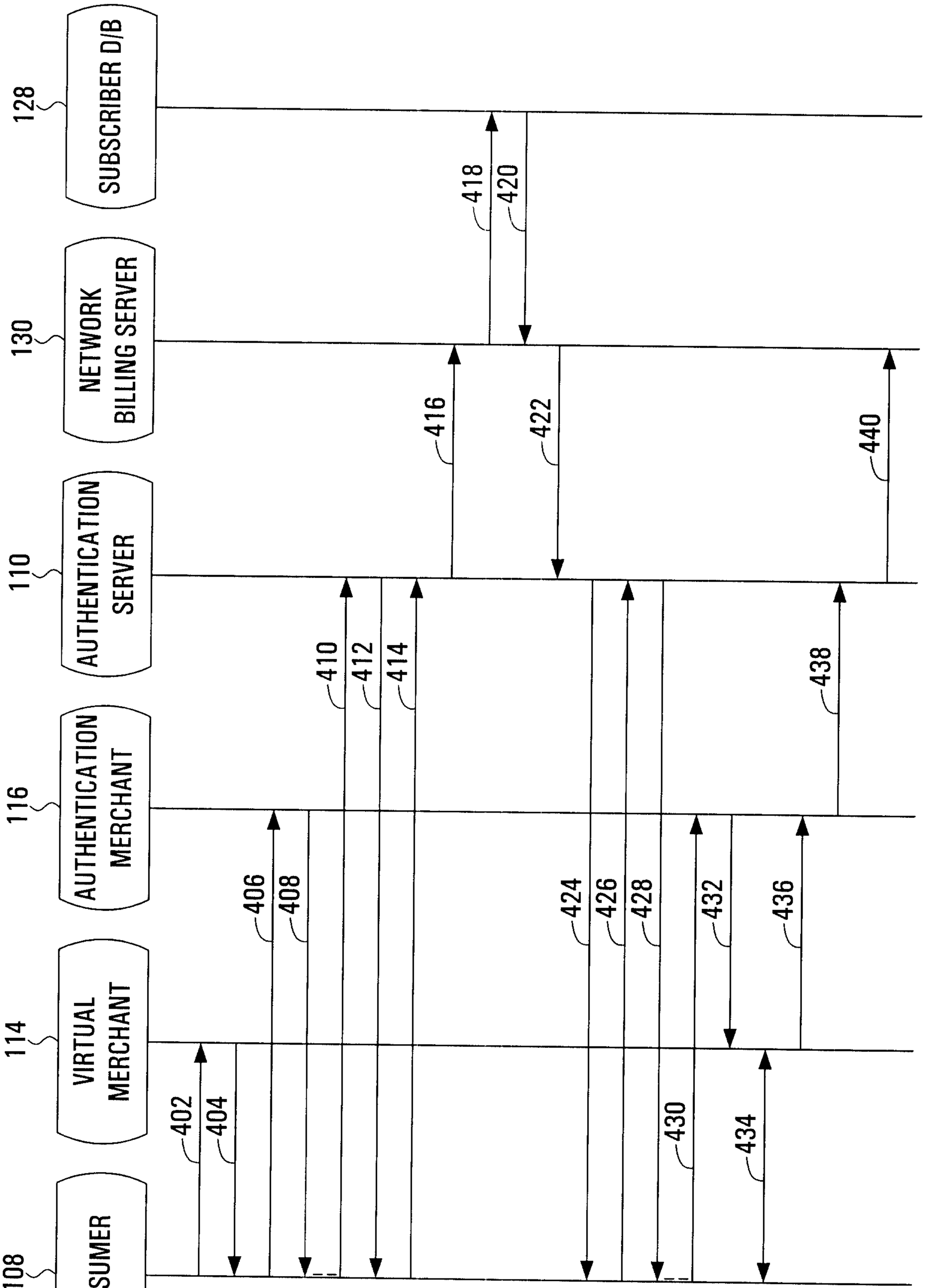

128
SUBSCRIBER D/B
130
NETWORK BILLING SERVER
110
AUTHENTICATION SERVER
116
AUTHENTICATION MERCHANT
114
VIRTUAL MERCHANT
108
CONSUMER
402
404
406
408
410
412
414
416
418
420
422
424
426
428
430
432
434
436
438
440

FIG. 4

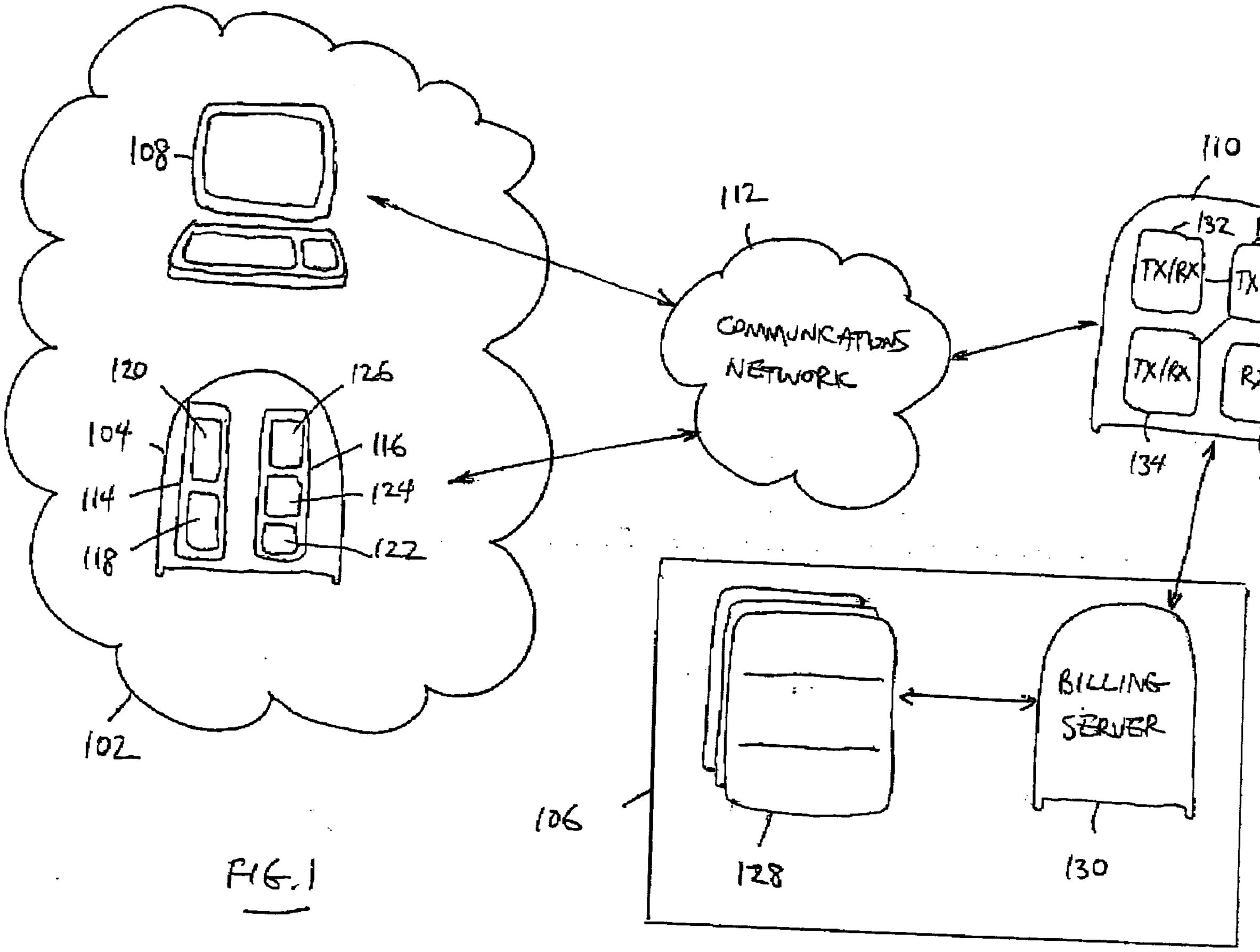


FIG. 1

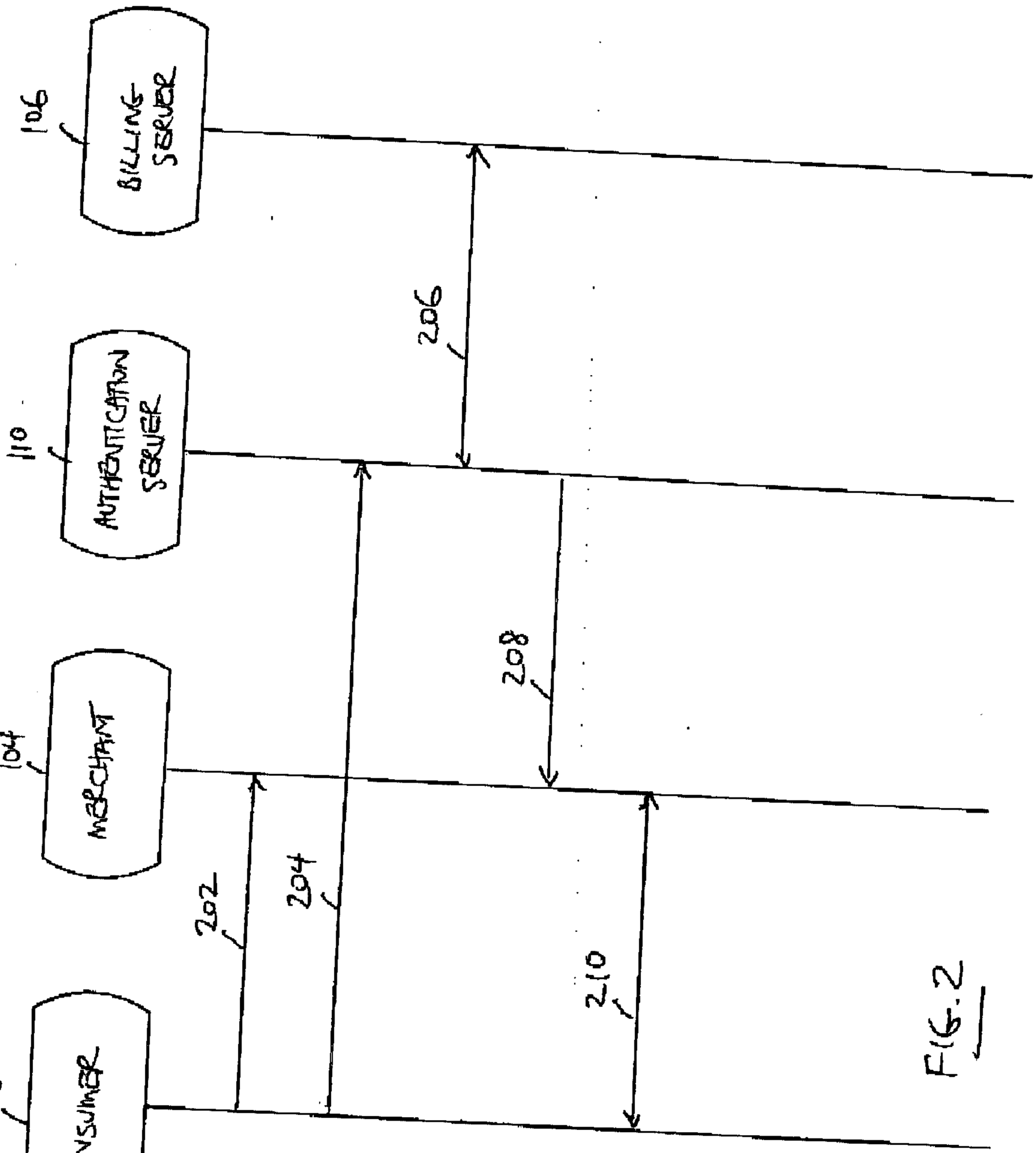

106
BILLING SERVER
110
AUTHENTICATION SERVER
104
MERCHANT
108
CONSUMER
206
208
202
204
210

FIG. 2

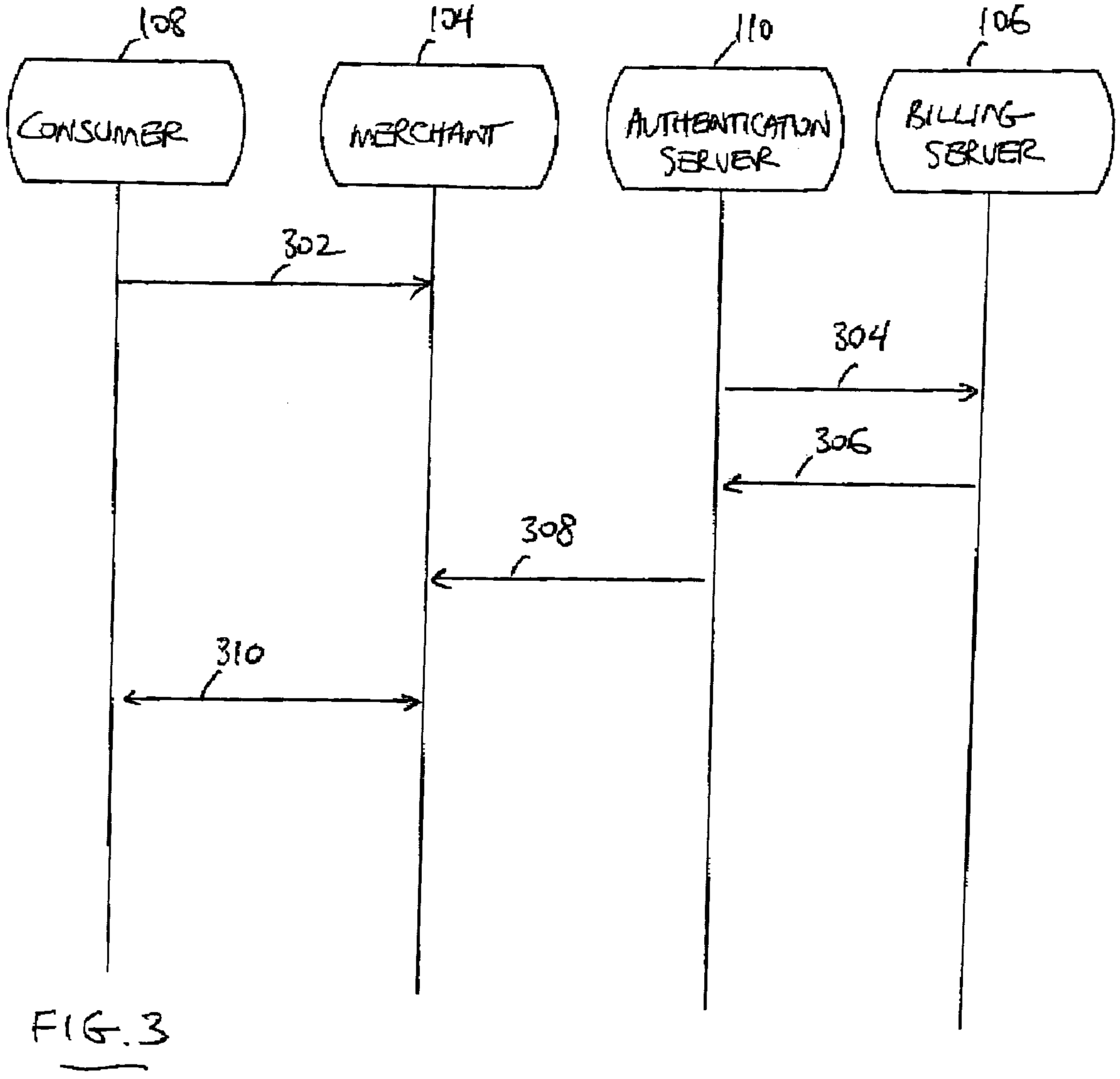


FIG. 3

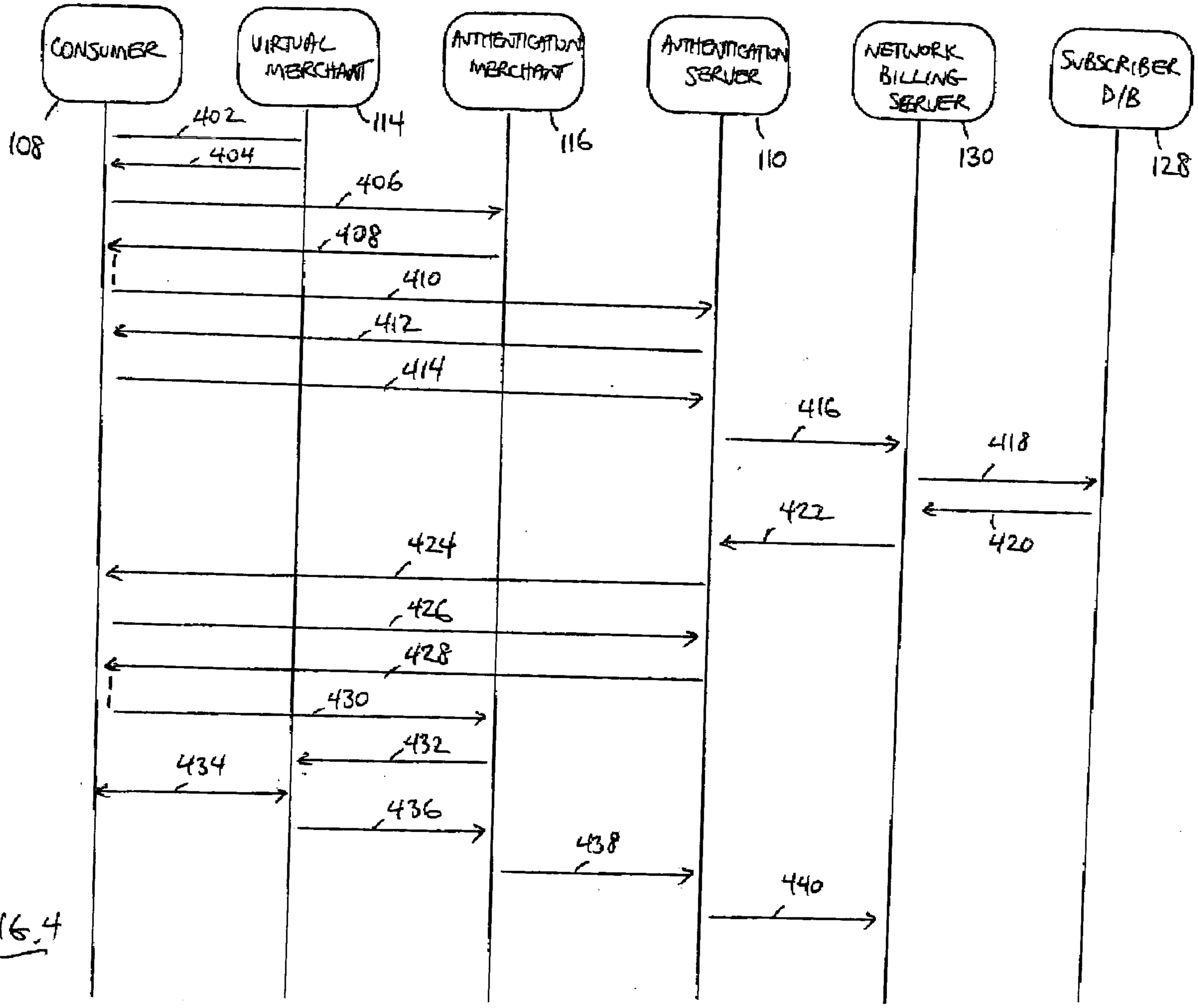
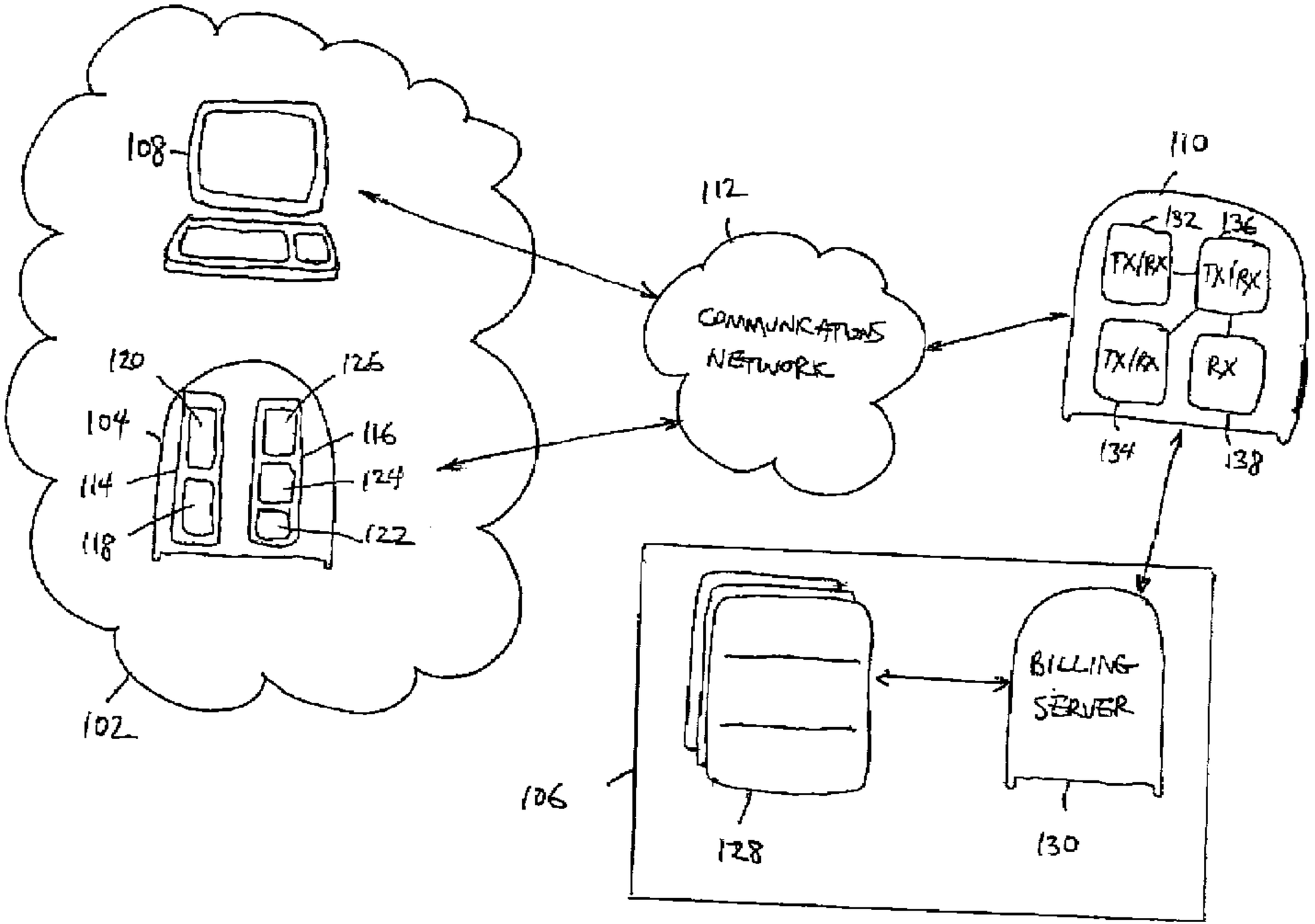


FIG. 4


108
120
126
104
116
114
124
118
122
102
112
COMMUNICATIONS NETWORK
110
132
136
TX/RX
TX/RX
TX/RX
RX
134
138
106
128
BILLING SERVER
130