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

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2381074 A1 2001/03/01

(21) 2 381 074

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(86) Date de dépôt PCT/PCT Filing Date: 2000/08/25
(87) Date publication PCT/PCT Publication Date: 2001/03/01
(85) Entrée phase nationale/National Entry: 2002/02/25
(86) N° demande PCT/PCT Application No.: US 2000/023466
(87) N° publication PCT/PCT Publication No.: 2001/015094
(30) Priorité/Priority: 1999/08/25 (60/150,650) US

(51) Cl.Int.^{7}/Int.Cl.^{7} G06K 5/00

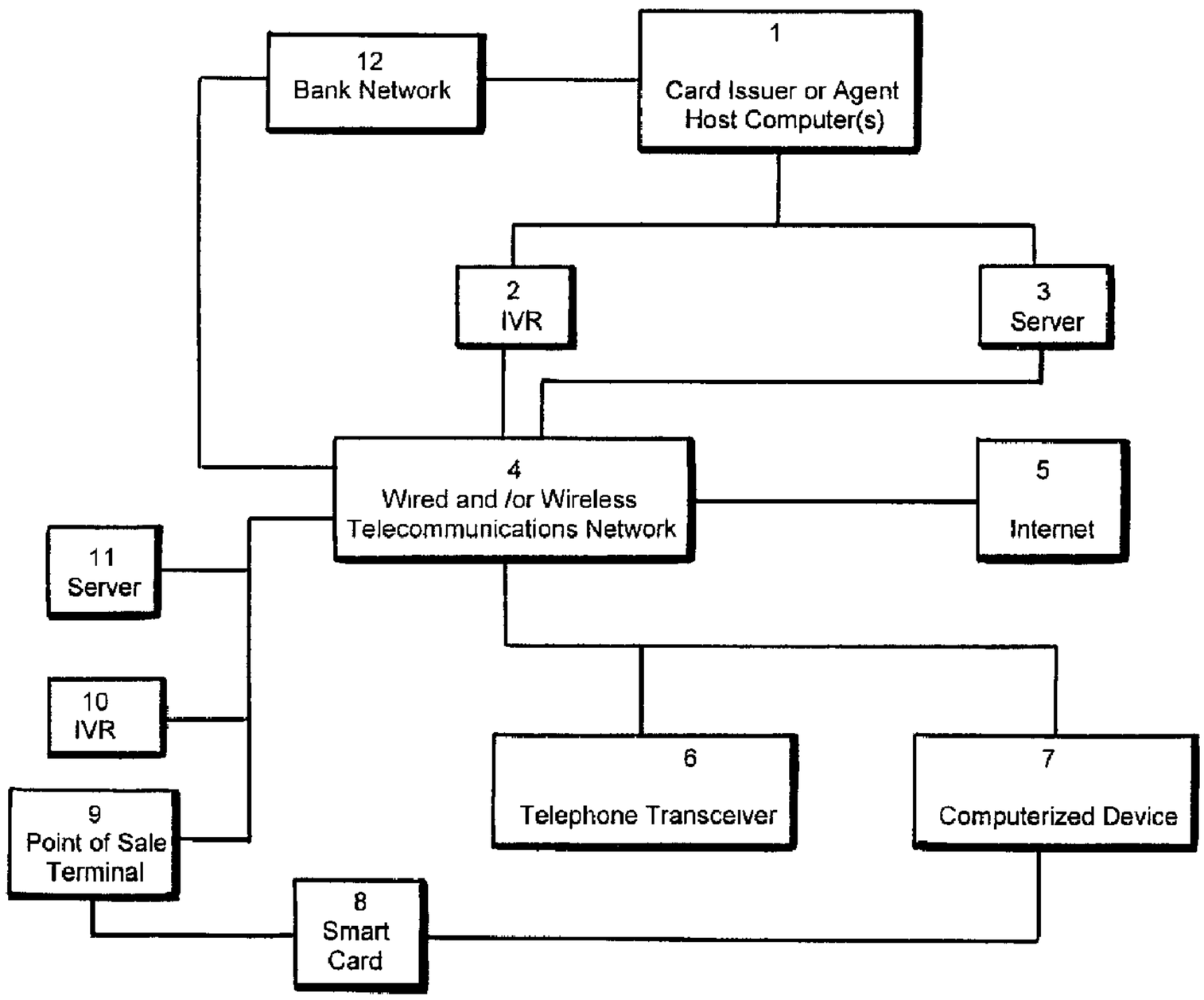
(71) Demandeur/Applicant:
FRIEND, JEFFREY EDWARD, US

(72) Inventeur/Inventor:
FRIEND, JEFFREY EDWARD, US

(74) Agent: DIMOCK STRATTON CLARIZIO LLP

(54) Titre : SYSTEME DE SECURITE POUR TRANSACTIONS ELECTRONIQUES ET PROCEDE D'UTILISATION CORRESPONDANT

(54) Title: SECURE SYSTEM FOR CONDUCTING ELECTRONIC TRANSACTIONS AND METHOD FOR USE THEREOF



(57) Abrégé/Abstract:
A system for conducting transactions with electronic verification of the status of a requesting party. A host microprocessor (1) with an associated memory containing a limited-use transaction identification number corresponding to user personal identification information. The limited-use transaction identification number includes a random generated number and a time

(21) 2 381 074

(13) A1

(57) Abrégé(suite)/Abstract(continued):
generated stamp. A communication device (4) for communicating with the host computer (1) to activate the transaction identification number.

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

REVISED VERSION

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 March 2001 (01.03.2001)

PCT

(10) International Publication Number
WO 01/15094 A3

(51) International Patent Classification[7]: G06K 5/00

(21) International Application Number: PCT/US00/23466

(22) International Filing Date: 25 August 2000 (25.08.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/150,650 25 August 1999 (25.08.1999) US

(71) Applicant and
(72) Inventor: **FRIEND, Jeffrey, Edward** [US/US]; 350 East Henry Clay Street, Suite 5, Whitefish Bay, WI 53217 (US).

(74) Agents: **NEUNER, George, W.** et al.; Dike, Bronstein, Roberts & Cushman, Intellectual Property Group, Edwards & Angell, LLP, 130 Water Street, Boston, MA 02109 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

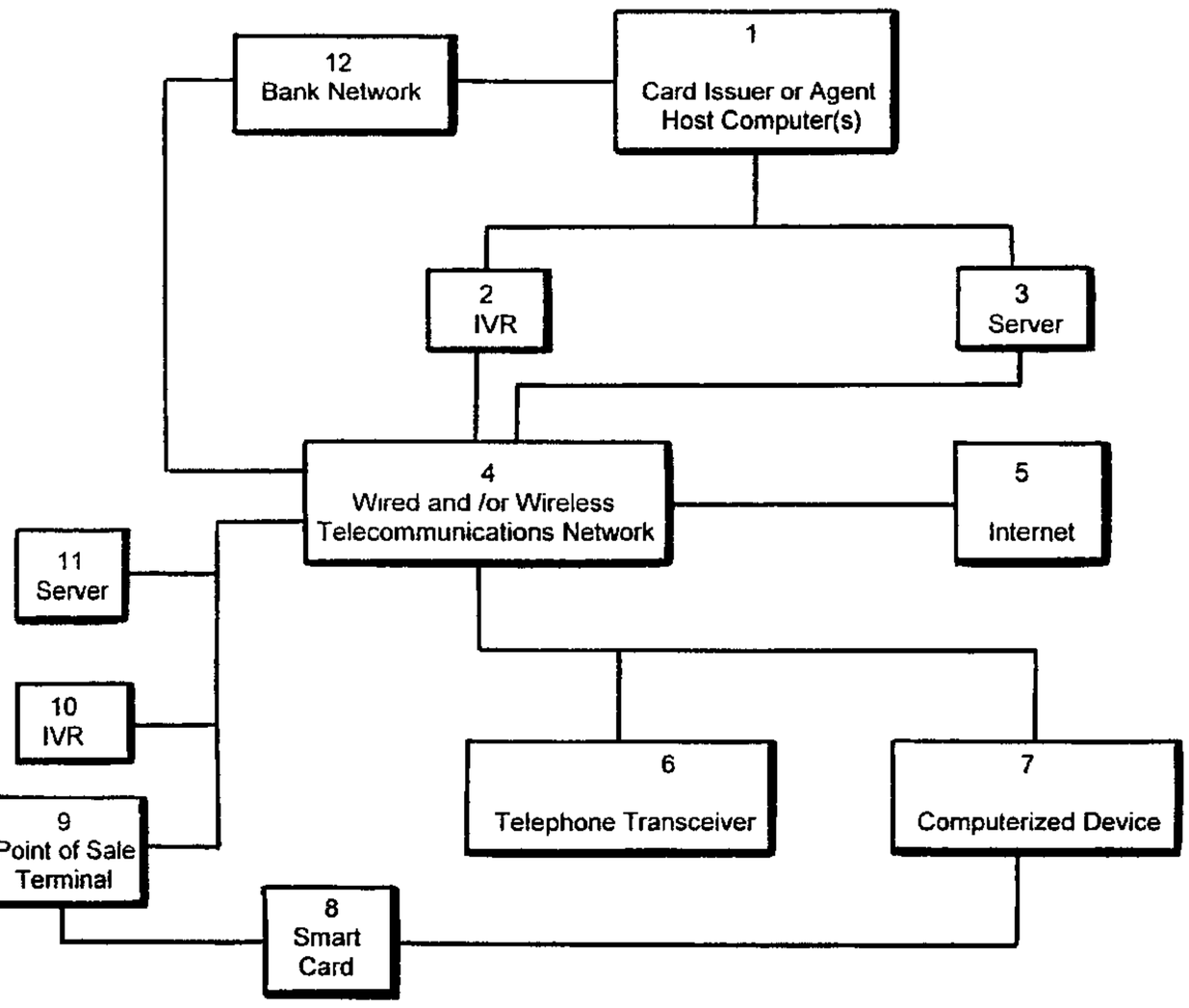
Published:
— *with international search report*

(88) Date of publication of the international search report:
20 September 2001

Date of publication of the revised international search report:
13 December 2001

[Continued on next page]

(54) Title: SECURE SYSTEM FOR CONDUCTING ELECTRONIC TRANSACTIONS AND METHOD FOR USE THEREOF



(57) Abstract: A system for conducting transactions with electronic verification of the status of a requesting party. A host microprocessor (1) with an associated memory containing a limited-use transaction identification number corresponding to user personal identification information. The limited-use transaction identification number includes a random generated number and a time generated stamp. A communication device (4) for communicating with the host computer (1) to activate the transaction identification number.

WO 01/15094 A3

SECURE SYSTEM FOR CONDUCTING ELECTRONIC TRANSACTIONS AND METHOD FOR USE THEREOF

FIELD OF INVENTION

The present invention is related to a system and associated method for conducting an electronic transaction, e.g., a bank card service involving the electronic distribution of credit and debit card numbers "on demand." More particularly, the invention relates to a system and method in which transaction identification numbers are electronically created, assigned and issued on demand at the request of consumers, e.g., credit or debit cardholders, and/or at regular frequency as determined by number issuers, e.g., card issuers, or their agents. The transaction identification numbers can be electronically transferred across wired and wireless telecommunications links for use in various transactions including but not limited to electronic payment transactions.

BACKGROUND OF THE INVENTION

In the case of credit and debit card numbers, the process today involves forwarding by mail numbers to cardholders in the form of an embossed plastic card having an expiration date. The assigned credit and debit card numbers are static numbers intended for repeated use by cardholders over extended periods of time. Typically, at the expiration date, a new plastic card is issued having the very same number and a new expiration date.

This is an inferior process and practice that sustains an environment of inconvenience and potential fraud for both cardholders and card issuers.

The inconvenience occurs in situations where cardholders order new cards or find their existing cards have been lost, stolen or damaged to the point of becoming non-functional. The cardholder has no recourse but to wait until new cards are delivered through the mail, a process usually requiring at the least several days.

Inconvenience also occurs as a result of today's practice of treating assigned credit and debit card numbers as static numbers for repeated use over extended periods of time.

It has been found that merchants, either mistakenly or willfully, use credit or debit card numbers they had previously been provided to obtain subsequent payment authorizations from the card issuer without the knowledge of cardholders and against their intended wishes. Cardholders often do not learn about these authorizations until weeks later when they receive their account statement and discover the unauthorized use.

The growing popularity of debit cards has made this an even worse problem by the fact that these "unauthorized" payment authorizations cause unexpected withdrawals to be made from deposit accounts. For many debit cardholders with limited funds, this sets in motion a domino effect due to overdrawn accounts and the returned checks, reversed automatic payments and transfers that can result.

Card issuers are also inconvenienced by having to investigate and resolve disputes on behalf of those cardholders affected.

The practice of treating credit and debit card numbers as static numbers can have considerable negative impact on cardholders and card issuers when the card numbers are used fraudulently, i.e., without proper authorization.

In the case of cardholders, the impact of credit and debit card theft also is a matter of inconvenience, but also can cause more serious consequences such as a damaged credit history. When theft of the card is involved, the total amount of charges to credit accounts or withdrawals from deposit accounts often is far greater than that occurring as a result of the unauthorized payments obtained by merchants who originally had obtained the card number legitimately for an authorized transaction and payment. It is not uncommon to find credit and debit card thieves running up charges or debits in the hundreds or even thousands of dollars before the available limit of credit or funds is reached or cardholders finally come to realize their cards are missing and report them lost or stolen.

Often, cardholders find that they have been victims of theft without their cards actually being stolen, only their credit and debit card numbers. Thieves seem to lack no creativity when it comes to conspiring new ways of stealing the numbers of unsuspecting cardholders. They also are finding an increasing number of ways in which to use stolen numbers, thanks to the

proliferation of commerce conducted over the internet and the telephone and to the expanding range of services and software products that can be purchased without need for physical delivery. This provides the means for thieves to skirt the protections provided by the credit card industry's requirements that goods purchased with credit and debit cards be shipped only to the addresses associated with the cardholders of record.

For card issuers, the impact of credit and debit card fraud primarily comes in the way of cost. Federal law requires that consumer liability be limited for unauthorized electronic transactions. Card issuers have voluntarily exceeded those requirements in an effort to further assure cardholder confidence when it comes to using credit and debit cards as a means for payment. Many issuers have made a public commitment to limiting cardholder liability to fifty dollars. As a matter of practice, issuers go further in many instances to totally cover any losses incurred by cardholders.

Card issuers view the burden of covering loss as the cost of doing business. In cases involving the Internet or other remote transactions when the physical card is not present, card issuers usually make the merchant cover any losses due to fraud. However, the sum total of the burden continues to grow and, of course, the costs ultimately are passed on to the consumer.

Attempts have been made to solve the above described problems. In US Patent No. 5,826,245, a method is described for providing verification

information with respect to a transaction wherein the customer generates first and second tokens based on certain confidential information. Each token contains some (but not all) of the confidential information and, in addition, certain information in common, such as a transaction identification tag that may be, for example, a randomly generated four digit number . The first token is sent by non-secure communication to the merchant. The second token is sent by non-secure communication to the card issuer. The card issuer then transmits verification information (i.e., the portion of confidential information already provided to the merchant accompanied by the transaction identification tag) via non-secure communication to the merchant. Thus, the entire confidential information is not transmitted at any time, and only the customer and the card issuer have knowledge of the total confidential information.

US Patent No. 5,627,355 describes a transaction device, equipment and method for protecting account numbers and their associated personal identification numbers. The equipment includes a host computer and a remote portable transaction device that interact. The card issuer generates an account number and a series of unique personal identification numbers for each account number. This information is stored in the host computer memory and is assigned as a reference series to an individual customer account number. An identical series of numbers in the same sequence is stored in the memory of the remote portable transaction device. During the use of the remote device, a unique personal identification number (the next number in the stored series) is added to the customer account number and transmitted to the host computer where it is compared to the account

number and personal identification number in the reference series. Authorization is granted if the number in the stored series from the remote device is identical to the number in the reference series.

US Patent No. 5,317,636 also describes a method and apparatus for securing credit card transactions. A so-called "smart" credit card is used. The card produces a verification number that is based on a transaction sequence number and an encrypted algorithm stored in the card. The verification number is transmitted to a verification computer, which uses the verification number together with a de-encryption algorithm to produce a computed transaction sequence number. If the computed transaction sequence number corresponds to a transaction sequence number stored in the computer memory, authorization will be provided.

US Patent No. 5,870,476 describes a process for a secure data exchange protocol in which a first party produces a seed applied to a pseudo-random generator to produce a pseudo-random word, combines this pseudo-random word in a one to one and reversible manner with a pledged data item to produce a check word, and transmits the check word to the second party. In a subsequent step, the first party transmits to the second party the seed together with the plain pledged data item. The second party then applies the seed to a pseudo-random generator similar to that of the first party to produce another pseudo-random word, combines the pseudo-random word and the check word in the same manner as the first party to produce a check data item, and checks the consistency of the check data item with the plain pledged data item received from the first party.

US Patent No. 5,478,994 describes a secure credit card for preventing unauthorized transactions. The card has a microprocessor coupled to a PROM that has been programmed with a series of random numbers in a predetermined sequence. The random numbers are identical to random numbers in a host computer, which is accessible upon each use of the card. The PROM accesses the next random number in sequence with each use of the card to permit verification by comparing it with the next random number in sequence as indicated by the host computer.

US patent No. 5,068,894 describes a method for generating a unique number for a smart card and its use in cooperation with a host computer. The smart card includes a random access memory RAM and a read only memory PROM that incorporates a production key PK, a distributor key MK, a bearer code CP and a serial number NS, which generates a unique number NU which is stored in RAM after execution of a series of steps that is specific to the card.

US Patent No. 4,965,827 describes an authenticator for digital data. The authenticator is derived by generating a numerical array, using a secret key to controllably shift the relative positions of the elements of the array, and applying the scrambled array to a message to create an authenticator for that message.

Accordingly, it is desirable to provide a means of avoiding the inconvenience caused by fraudulent use of credit card numbers particularly

when using the conventional process of forwarding credit and debit card numbers to cardholders in the form of an embossed plastic card. Further, it is desirable to provide a means of averting the threat of unauthorized authorizations caused by the conventional practice of treating newly assigned credit and debit card numbers as static numbers.

For the purpose of this application, terms such as "credit card" and "debit card", "cardholder", "card issuer" and "card service" are used as a matter of convenience for clarity of describing examples. However, it is likely that these terms will lose relevance over time and, in fact, the present invention helps bring that about in light of the advancements it offers for electronic transactions involving credit and debit card numbers and numerous other varieties of transactions such as, e.g., electronic check numbers processed through an automated clearinghouse, telephone numbers processed through a central switch, Internet protocol addresses and Uniform Resource Identifiers transferred across a computer network, digital certificates and signatures, and the like.

SUMMARY OF THE INVENTION

The present invention provides a new and improved system and methodology of conducting transactions with electronic verification of the status of the requesting party (e.g., customer) by the providing party (e.g., merchant) and authorization for the transaction payment, if required. For example, in a bank card service in which credit and debit card numbers can be issued electronically and transferred across wired and wireless telecommunications links, newly assigned credit and debit card numbers

can be regularly issued for use in electronic payment transactions at the request of cardholders and/or at regular frequency as determined by card issuers or their agents. Such numbers are electronically posted in conjunction with personally identifiable information such as, e.g., the mailing address of cardholder who has been assigned the number, or with non-personally identifiable information, e.g., demographic or financial profile information of the cardholder who has been assigned the number, or a digital certificate or signature, or even a random or selected alphanumeric string known to the cardholder, as a means for merchants or their agents to quickly verify such information presented at the point of sale (or by telecommunications, or the like) to identify the presenter as the authorized user of the number and, if required, confirm authorization for payment in the transaction.

In accord with the present invention, a system for conducting transactions with electronic verification of the status of the requesting party by the providing party comprises a host microprocessor with an associated memory and a communication device for communicating with the host computer, wherein the memory contains a limited use transaction identification number linked with personal identification information (e.g., personally identifiable information (i.e., personal information) and/or non-personally identifiable information) of the number holder (e.g., cardholder) who has been assigned the number, wherein the limited use transaction identification number comprises a randomly generated number and a time generation or activation stamp. The transaction identification number can be used for a wide variety of purposes such as, for example, authorizing

payment for purchases of goods or services in a transaction, for authorizing access to information, or for authorizing transfer of information, etc.

In accord with the present invention, a method for electronically providing a transaction identification number to a requestor comprises forming a telecommunications connection between the requestor at a first location and a host microprocessor of the number issuer (e.g., card issuer or card issuer agent) at a second location, said host microprocessor being connected to a data storage system with memory, providing personal identification information by the requestor to the host microprocessor, issuing a transaction identification number and assigning it to the requestor, storing the transaction identification number in conjunction with the personal identification information in the memory and transferring the transaction identification number to the requestor by the telecommunications connection.

In a preferred embodiment of the invention, a transaction identification number is issued to a user by the following steps: opening a communication link between the user and a host microprocessor having an associated memory storage device; verifying the identity of the user by a predetermined protocol; requesting a transaction identification number to be generated for limited use by the user in accord with a specified limitation; providing the transaction identification by the host microprocessor from a pool of available numbers, the transaction identification number comprising a random portion and a time stamp portion indicating the time of activating the transaction identification number for use by the requesting user;

transmitting the transaction identification number to the user; storing the transaction identification number in the associated memory with a link to associated personal identification information of the authorized user and to the specified limitations; and notifying the transaction processing network (e.g., bank network) of the activated transaction identification number. Further, when the specified limitation has been satisfied, the transaction identification number is deactivated and the random portion of the number is returned to the pool of available numbers for subsequent selection and association with subsequent user. When the random portion is subsequently used, the transaction identification number will be different due to the time stamp portion and the personal identification information associated therewith will be different. Thus, fraudulent use of a transaction identification number is highly unlikely. Typically, the time stamp portion will provide the date and also can provide other desired indicia of the time of activation of the transaction identification number.

Further, in accord with the present invention, a transaction is consummated using a transaction identification number comprising a random portion and a time stamp portion indicating the time of generating or activating the transaction identification number for use by the requesting user by the following steps: presenting the transaction identification number by the requesting user to a provider to obtain a product or service; transmitting the transaction identification number by the provider to a host microprocessor for verification of the user and of the status of the transaction identification number; receiving from the host microprocessor personal identification information for verification of the user; obtaining

information from the user to compare with the personal identification information obtained from the host microprocessor; confirming to the host microprocessor that the user has been verified; and receiving authorization from the host microprocessor, if required, for payment for the transaction. Where the transaction identification number is used only to confirm identification of the user and no payment is required, e.g., where access to information is sought for a club member, the final step can be omitted. Also, the personal identification information can be transmitted to the host microprocessor as part of the transaction for comparison with user information stored in memory and the host computer transmit a confirmation signal verifying the user.

To achieve the objective of averting unauthorized use, the invention takes full advantage of the inherent randomness of a pool of numbers. It creates the means for these numbers to be regularly assigned and issued for use for a limited period of time or limited circumstances and to be re-circulated among user populations with the assurance that any one number is assigned to only one user at any given point in time.

In preferred embodiments of the invention, users and number issuers (e.g., cardholders and card issuers) or their agents can exercise regular systematic control over the "life span" of individually assigned numbers (e.g., credit and debit card numbers). The range of this control can vary such that assigned numbers are limited in use to only a certain total number of authorized transactions, to only a specified period of time, to a series of transactions only in conjunction with specific merchant or other

specific providers of goods and services, to "one-time-use" whereby newly-issued numbers are good for a only a single transaction, and the like, etc.

Whatever the specified limitation, once the life span of an individually assigned transaction identification number comes to an end, a change in activity status is immediately made by the host microprocessor. The random portion of the number is removed from circulation and earmarked for return to the available number pool and eventual re-assignment. The length of time before a number is actually returned to the pool can depend on specific legal requirements or specific guidelines adhered to by the number issuer (e.g., card issuer) or its agent. However, no transaction identification number can be ever duplicated in accord with preferred embodiments of this invention.

According to a preferred embodiment of the invention, number issuers (e.g., card issuers) or their agents will be able to electronically post newly activated transaction identification numbers (e.g., credit or debit card numbers) to a secure web server and or other host server in conjunction with personal identification information, (e.g., personal information of the user such as the mailing address) of users (e.g., cardholders), to whom the numbers have been assigned. This offers further protection against unauthorized use of any transaction identification number by enabling merchants and other providers of goods and services or their agents to quickly verify, either over the Internet or by telephone, the personal identification information presented in conjunction with the transaction

identification number at the point of sale should that information not otherwise be readily available.

Thus, the present invention provides a process for issuing credit and debit card numbers by electronically transferring them across wired and wireless telecommunications networks. This makes it possible to execute real-time delivery of the newly assigned numbers for use by cardholders in electronic transactions.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 illustrates components of a system in accord with one embodiment of the present invention for the electronic distribution of credit and debit card numbers "on demand."

FIG. 2 illustrates an inherent randomness of typical 16-digit credit and debit card numbers.

FIG. 3 illustrates more detailed components of a system in accord with an embodiment of the present invention for the electronic transfer of newly assigned credit or debit card numbers across wired and/or wireless telecommunications links.

FIG. 4 illustrates the process by which the method of the present invention takes full advantage of the inherent randomness of typical 16-digit credit and debit card numbers.

FIG. 5 illustrates that part of a system in accord with one embodiment of the present invention involved with electronically posting newly assigned credit and debit card numbers in conjunction with the mailing addresses of cardholders, to whom the numbers have been assigned, as a means for merchants or their agents to quickly verify addresses presented at the point of sale.

DETAILED DESCRIPTION OF THE INVENTION INCLUDING THE PREFERRED EMBODIMENTS

FIG. 1 provides an overview of one embodiment of a system for the electronic distribution of credit and debit card numbers "on demand" in accord with a preferred method of electronically transferring newly assigned credit and debit card numbers from the card issuer or its agent to cardholders. In addition, it portrays those components of the conventional bank card network infrastructure involved with processing the numbers for the purpose of obtaining authorizations and completing electronic payment transactions.

At the center of the system is a host computer 1 of the card issuer or its agent. The host computer includes a microprocessor and memory that are used for generating new credit and debit card numbers, updating the bank network regarding card number activation and status changes, managing assigned and previously assigned card numbers, maintaining cardholder accounts, granting authorizations and executing all other functions associated with card-based electronic payment transactions. The functions of the host computer can be divided among several computers or servers. An interactive voice response unit 2 (IVR) or other computerized

device is provided for interactions with cardholders accessing the host computer primarily by way of a telephone or other audio transceiver 6. A server 3 is provided for interactions with cardholders using a computerized device for communication and accessing the host computer either directly by modem connection or by Internet connections 5. A wired and/or wireless telecommunications network 4 is used for communications.

Typically, the system includes additional computerized devices 7, including personal or network computers, digital phones or other remote devices, used for direct dial-up or Internet connections by the merchant or service provider. A smart card 8 can be used for portable storage of credit and debit card numbers in advance of electronic payment transactions conducted at the point of sale or over the Internet. A point of sale terminal 9 can be used in conjunction with card based electronic payment transactions initiated at the merchant site. Additional IVRs or other computerized devices 10 can be used in conjunction with electronic payment transactions initiated by cardholders accessing primarily by way of telephone transceiver. Further, additional servers 11 can be used in conjunction with electronic payment transactions initiated by cardholders accessing either by way of direct dial-up or Internet connections. A conventional bank network 12 is used for processing payment authorization for card based electronic payment transactions.

In accord with the invention, cardholders access the system by either a telephone transceiver 6 or a computerized device 7. In the case of access by way of telephone transceiver 6, the cardholder dials into IVR 2 over a

wired and/or wireless telecommunications network 4. Upon connection, the cardholder undergoes the process of authorized user identification or authentication in accord with the application and standards prescribed by the card issuer or card issuer agent. In its simplest form, authorized user identification can involve keying in a password or personal identification number (PIN). More advanced forms of identification can involve voice print technology or digital confirmation provided that the call emanates from an enhanced phone network connection permitting such identification.

Following authentication of the authorized user, the IVR 2 retrieves the cardholder information file that is stored within the card issuer or agent host computer 1. Retrieval involves transferring the file a server operating in conjunction with IVR 2 and host 1. This provides an acceptable level of security by restricting cardholder access to outside the firewall.

Once the cardholder file has been retrieved, the cardholder can initiate a new credit or debit card number request. The request is processed back through the server to host 1. Upon receiving the request, host 1 exercises a status change to the number previously assigned to the cardholder effectively deactivating the number and removing that number from circulation. An enhanced feature application of the methods of this invention can provide for cardholders to be simultaneously assigned more than one active credit or debit card number and allow individual numbers to retain active status until their specified limitations have been met. Such specified limitations can include, for example, a single authorization per the operational regulations of specific card programs, card issuers and their

agents. In such case, the fulfillment of a request for a new credit or debit card number would not necessarily demand that a change in status occur for a previously assigned number.

In this more simplified embodiment, coinciding with or after exercising the change of status for the previous cardholder number, host computer 1 randomly generates and assigns a new number from all the possible combinations available in the credit and debit number pool and issues that number to the cardholder. At this time, host computer 1 also notifies bank network 12 of the activation of the new number and the change of status to the previous number.

The issuance of the newly assigned credit or debit card number involves having the number transferred back to the server then on to IVR 2. Then, the newly assigned number is electronically transferred across the wired and/or wireless telecommunications network 4 as IVR 2 relays the new number in the form of audio waves to the cardholder through telephone transceiver 6.

Upon receiving the number, the cardholder can make a record of the newly assigned number and use the number in an upcoming electronic payment transaction. Although the cardholder can use the transaction identification or credit card number at a merchant site simply by having it keyed in to point of sale terminal 9, the cardholder also can use the number as part of a mail order/telephone order (MOTO) transaction. For such transaction, a direct person-to-person connection over the telephone or a

voice connection in conjunction with IVR 10 can be used where the number is keyed into or spoken aloud for interpretation by a virtual assistant employing voice recognition technology. Whichever the case, once the number is conveyed to a merchant, it is handled in the same manner as a transaction involving conventional credit and debit card numbers.

A difference between the method of the present invention and conventional credit card numbers can be found in the handling of any subsequent attempts by the merchant to obtain additional payment authorizations through use of the number. Whether a particular number can be used for additional payment authorizations depends upon the operational limitations specified by the cardholder when obtaining the new credit card number or the specific card program of the card issuer or agent.

In the case of access to the host computer 1 by way of computerized device 7, the cardholder can dial directly into server 3 over a wired and/or wireless telecommunications network 4 or can access server 3 over a wired and/or telecommunications network 4 in combination with the Internet using a web browser. Upon connection, the cardholder undergoes the process of authentication in accord with the application and standards prescribed by the card issuer or card issuer agent. As described above, the simplest form can involve simply keying in a password or PIN in combination with the issuance of a digital certificate. More enhanced forms of authentication can involve more advanced applications of digital certificates or signatures and/or some form of biometrics.

Following successful authentication, server 3 retrieves the cardholder file stored within host computer 1. Retrieval involves transferring the file to the server, possibly by way of another server operating in conjunction with the server 3 and host computer 1. This again provides an acceptable level of security by restricting cardholder access to outside the firewall.

Once the cardholder file has been retrieved, the cardholder initiates a new credit or debit card number request. The request is transferred from server 3 to host computer 1. Upon receiving the request, host computer 1 exercises a status change to the number previously assigned to the cardholder effectively deactivating the number and removing that number from circulation, provided that another specified limitation is not in effect in which case the previously assigned number can be deactivated already or can be permitted to stay active as the new number is assigned. In other words, preferred embodiments of the invention permit the user to have a plurality of active transaction identification numbers. Coinciding with exercising the change of status, if desired, host computer 1 randomly generates and assigns a new number from all the possible combinations available in the credit and debit number pool and issues that number to the cardholder. Also, at this time, host computer 1 notifies bank network 12 of the activation of the new number and the change of status to the previous number.

The issuance of the newly assigned credit or debit card number further involves transferring the number back to server 3. Then, the newly assigned number is electronically transferred across the wired and/or

wireless telecommunications network 4 as server 3 relays the new number to the cardholder in the form of data to computerized device 7 either through download to the hard drive or use of the browser. This transfer also can involve the use of an electronic wallet residing either on computerized device 7 or on a web server, perhaps server 3. In addition, a smart card 8 also can be employed in which the electronic transfer of the credit or debit card number culminates with the number being delivered to smart card 8 via computerized device 7. Alternatively, the new number can be delivered to smart card 8 via point of sale terminal 9, IVR 10 or server 11 (FIG. 1).

Upon receiving the number, the cardholder can immediately use the number for an upcoming electronic payment transaction, for example, for a transaction conducted either by way of direct dial up or Internet connection to server 11. The process can involve transferring the transaction identification number to the merchant's server 11 with the aid of an electronic wallet or transferring it by other means, including a page request as initiated through a browser or a simple key entry. The transaction identification number also can be transferred to the merchant's server 11 or IVR 10 via smart card 8. Whichever the case, once the transaction identification number is conveyed to a merchant, it is handled no differently than conventional credit and debit card numbers.

There are various alternative processes by which newly assigned credit and debit card numbers can be electronically transferred within the established bank network or through other channels across wired and/or wireless telecommunications links for use in electronic payment

transactions. For example, the numbers can be delivered directly to server 11 or to IVR 10 immediately before, during, or in the course of completing such transactions. Such processes are made possible by the advancements offered by this invention.

The inherent randomness of typical 16-digit credit and debit card numbers is illustrated in FIG. 2. A 16-digit number is used, although the exact number of total digits can vary, as may the exact number of digits allocated for the Bank Identification Number or other specific functions contained in the credit or debit card number. Looking at this example, the first digit at the left identifies the type of card, for instance "5" for MasterCard and "4" for Visa. The next series of digits comprises the Bank Identification Number (BIN). This is a static number that relates information specific to the card issuer. It is common that the first digit identifying the card type is included when references are made to the BIN. It is also common that card issuers will be assigned more than one BIN as a matter of meeting cardholder demand for either credit or debit card numbers. The last digit to the far right is what is commonly called the "check digit." It results from the application of a special algorithm and is used for ensuring the integrity of the entire credit or debit card number.

The series of digits between the BIN and the check digit constitute what is mostly a "random" string. It is a string often randomly selected by the card issuer host computer from the pool of available combinations (i.e. those not currently assigned or previously assigned) as a matter of creating and assigning a new credit or debit card number. It is not always the case

that the number is randomly selected. As a matter of conventional practice, the string can be a variation of the original number assigned to the cardholder.

However, in accord with this invention, the seven-digit string shown in the example in FIG 2 is treated as a randomly generated number. The present invention takes full advantage of this random feature, creating the means for these numbers to be regularly re-circulated among cardholder populations with assurance that any one random portion number is assigned to only one cardholder at any given point in time.

FIG. 3 illustrates a more detailed view of the components involved with the preferred method of electronically transferring newly assigned credit or debit card numbers across wired and/or wireless telecommunications links. A host computer 1, which includes a microprocessor and a memory storage unit, is operated by the card issuer or card issuer agent. It is linked via a wired and/or wireless telecommunications network 4 to a telephone transceiver 6, a server 3 or IVR 2, and a computerized device such as, for example device 7 or smart card 8. Server 3 and/or IVR 2 include the following components: custom written application 13, microprocessor 14, hard disk 15 and random access memory 16. Likewise, the computerized device 7 and/or smart card 8 also include the following components: custom written application 17, microprocessor 18, hard disk 19 and random access memory 20.

In operation, RAM 20 or telephone transceiver 6 is connected with the memory of host computer 1 across wired and/or wireless telecommunications links 4 by way of RAM 16. The cardholder request for a new credit or debit card number is relayed from computerized device 7 or telephone transceiver 6 to host computer 1 by way of IVR 2 or server 3 and/or a server working in conjunction with IVR 2. A digital replica of a newly assigned credit or debit card number is electronically transferred from the memory of host computer 1 to RAM 20 or telephone transceiver 6 by way of RAM 16.

Contributing to the method of electronic transfer are also custom written application 13 and custom written application 17. Custom written application 13 is stored on hard disk 15 and operates in conjunction with microprocessor 14. Such application software can be required for transfers done either by access to IVR 2 or server 3 and serves to smooth the operation of sessions conducted in conjunction with host computer 1. Custom written application 17 is stored on hard disk 19 and operates in conjunction with microprocessor 18. It can be required for transfers done with the aid of a locally stored electronic wallet, an Internet browser, or those transfers culminating with storage to a smart card 8. Such application software may not be required for transfers involving the use of an electronic wallet residing on a web server, perhaps server 3. In any event such application software can be written as necessary by those of ordinary skill in the art to facilitate communications between components in the system and storage of desired records at appropriate locations.

A custom written application generally also will be required for host computer 1. This application can be included as part of the application suite residing within host computer 1 as required for performing all functions associated with carrying out the functions required to implement the present invention, as well as keeping suitable financial and historical records for the card issuer. Such application software is readily provided by the skilled programmer.

In the case where the cardholder chooses to locally store the credit or debit card number following transfer, the digital replica is moved from temporary storage in RAM 20 to more permanent storage on hard disk 19.

A system in accord with the invention also can be configured in a way that would eliminate RAM 16 as an intermediary memory for access made through IVR 2. However, at present it is understood that this configuration may lessen the degree of security offered by the system.

FIG. 4 illustrates a process by which the invention takes full advantage of the inherent randomness of typical 16-digit credit and debit card numbers. To the right of host computer 1 is a representation of the credit or debit number pool comprised of all possible combinations of 7-digit strings available for selection in conjunction with an individual BIN. The size of this pool can be varied to adequately meet demand within prescribed cardholder populations. To the bottom of host computer 1 is a newly generated 16-digit number consisting of the random portion of the string, i.e., "0104905", which has been randomly selected from the pool in response

to a cardholder request. According to a preferred embodiment of the invention, the number is assigned and then issued by being electronically transferred across wired and/or wireless telecommunications links 4 by way of IVR 2 or server 3 depending on the means by which the cardholder has accessed the system (see FIGs. 1 and 3).

Above the selected 16-digit number and to the left of the host computer 1 is a depiction of notification being sent to the bank network that the number has been assigned and activated. The contents of this notification can include other information consistent with the operational regulations of specific card programs, card issuers and their agents. Next above the bank network block 13 is a depiction of the database maintained in conjunction with host computer 1 consisting of previously assigned 16-digit numbers which have undergone a status change and subsequently have been removed from circulation for return to the available number pool and reassignment in accordance with the specific legal requirements and/or specific guidelines adhered to by the card issuer or its agent.

FIG. 5 illustrates activation of newly assigned credit and debit card numbers by application of a time stamp indicating the time of activation. The time stamp can consist of any appropriate indication of the activation time, e.g., day, month and year of activation; preferably, the hour, day month and year of activation; and more preferably, the minute, hour, day month and year of activation. The time stamp can be incorporated into the number string in a variety of ways inhabiting various data fields or combinations of data fields available in the number string (for example, it

can conveniently be set as at least part of the data fields currently used for the expiration date). For exceptional security, even the "seconds" of a chronometer can be included in the time stamp. With the time stamp showing time of activation, the transaction identification number is electronically posted in conjunction with personal identification information (e.g., the mailing address, or other unique information) of the cardholder to whom the number has been assigned as a means for merchants or their agents to quickly verify such personal identification information presented at the point of sale to confirm an authorized user. Such personal information need not be presented directly to the merchant. It can be entered by the cardholder for comparison in the system with only a confirmation or verification signal provided to the merchant.

This aspect of the invention involves the posting of transaction identification number and the personal identification information in a manner that will provide merchants or their agents a means to access the information without comprising cardholder security. The personal identification information preferably can be posted to either IVR 2 or server 3, or to other appropriate IVRs or servers in the system. The posting can take place automatically as a matter of normal process following cardholder application and acceptance into the specific card program. This same information may be required from the requesting cardholders as they receive a new limited use credit or debit card number in accord with the invention.

The information required for access to cardholder personal information by a merchant (or to request confirmation of the authorized

user) is the newly assigned credit or debit card number in conjunction with the time stamp, which preferably is a simple derivative resulting from the time at which the number was officially activated or issued. The time stamp, for example, can take the form of "mmddyyyyhhmm" denoting a sequence of numbers pertaining to the month, day, year, hour and minute of issuance. A more extended form might include "ss" for the exact second at which issuance occurred.

The combination of the 16-digit number and the time stamp is illustrated in FIG. 5. In actuality, the two come together to form a "super string," which is the transaction identification number (e.g., credit card number). In the illustrated case, the transaction identification number is the 28-digit string "5410940001049055081119991200," which includes the random portion "0104905" and the time stamp "081119991200" depicting the official date and time of issuance as being noon on August 11, 1999.

An important feature of the transaction identification number in accord with the invention is that the time stamp indicates the time of generation, activation or issuance (which in preferred embodiments will indicate essentially the same time), not the expiration date. Thus, one looking at the time stamp has no idea whether it is valid. Validation must occur through the bank network or through other user verification and transaction authorization. However, there is no preclusion of the use of an expiration time or date. Indeed, there may be occasions where the combination of an activation time and an expiration time is desirable. As used herein, the term "time" includes date.

The delivery of the super string to cardholders takes place within the framework described above for the electronic transfer of the credit and debit card numbers to cardholders as part of the issuance process. The posting of the super string to the IVR or server for use by merchants or their agents also occurs simultaneously within the same framework as a step, preferably during the issuance process.

Once posted, the super string serves as a unique password for access to the file containing the cardholder identification information on the IVR or server. Of course, merchants or their agents must first acquire the date/time derivative in conjunction with the electronically issued transaction identification number in order to complete the super string. Further, once the number is deactivated, access to the personal identification information can be denied.

There are various ways in which the "super string" can be provided to the merchant or agent. The cardholder simply can convey the super string to the merchant at the point of sale by physical presence or by telephone. Also, the super string can be electronically conveyed (as with the presentment of the credit or debit card numbers) for use in electronic transactions as a matter of the transaction process. This can be done through the variety of means described above (e.g., voice recognition, electronic wallet, browser, smart card, or other similar type means). However, by whatever means they receive the transaction identification number, the merchant or agent then can use it for authorized access to the

cardholder personal information for the purpose of verifying that information provided in conjunction with the use of credit and debit card numbers at the point of sale or for accessing or transferring additional personal information that was not presented. This can be carried out either over the Internet or by telephone. In each case, the merchant or agent simply presents the super string at the IVR or server for access to the particular information in the file of the cardholder of record for the random portion of the number and time stamp at that time. To ensure cardholder security, steps can be taken to allow an individual super string to be used only once for access to the cardholder information. Further, such security measures can provide that once a particular number is deactivated, access to personal information is denied.

A wide variety of limitations on the use of a super string can be envisioned readily. In one embodiment, the super string can be augmented with an additional data field that identifies a particular merchant, e.g., an electronically issued digital certificate that permits use only by the specified merchant and, if payment is involved, provides payment only to an account previously specified by that merchant. The various ways to limit the use is subject only to practical considerations and the writing of application software to operate the system with such limitations.

Thus, the present invention provides a new and improved system and methodology for conducting transactions particularly where at least a portion of the transaction is conducted electronically, for example, a bank card service in which credit and debit card numbers are generated, activated

and issued by electronic transfer across wired and wireless telecommunications links, credit and debit card numbers are time stamped upon activation so as to create unique numbers for limited use, newly-assigned limited use credit and debit card numbers are regularly issued for use in electronic payment transactions at the request of cardholders and/or at regular frequency as determined by card issuers or their agents, and transaction identification numbers are electronically securely posted in conjunction with personal identification information (e.g., personal information such as mailing address or demographic or financial profile information) of cardholders who have been assigned those numbers as a means for merchants or their agents to quickly verify the personal information presented at the point of sale to confirm an authorized user. The confirmation of the authorized user can involve providing access to additional personal information or transferring additional personal information to the merchant or other providers of goods and services.

The hardware components needed for implementing this invention are currently in existence. However, it is expected that some custom written applications can be desired to assure smooth flow within the system. Such software can be readily written be a skilled programmer. An example may be an application allowing the card issuer or agent host computer(s) to automatically execute status changes to credit and debit card numbers in circulation after a specified event has occurred limiting use of the card.

One aspect of the invention involves the method of creating a "super string" for the purpose of facilitating transactions and permitting cardholder

verification by merchants or their agents. The super string is frequently utilized in the form of a credit or debit card or a pseudo credit or debit card. However, the super string can be utilized in a wide variety of transactional situations.

Although the invention has been described in detail, it is to be understood that variations therein and modifications thereto may be made by those skilled in the art without departing from the spirit and scope of the invention as set forth in the following claims. For example, the functions of the host computer can be provided by various microprocessors, servers, and memory storage devices working together in a distributed system. The time stamp, when used, only needs to provide an indication of the time of activation or issuance. The sequence of steps in obtaining a number and using it can be varied according to the circumstances. The number can be provided directly from the issuer to the merchant under circumstances selected by the user. The transaction identification number or "super string" can take other forms and be more than one number or string, or can be presented in the form of a table, etc. The time stamp can be provided as a separate number or in any manner conceivable. The invention is not limited by the terminology used to describe the invention or various embodiments herein.

I claim:

1. A system for conducting transactions with electronic verification of the status of the requesting party by the providing party comprises:

a host microprocessor with an associated memory, and

a communication device for communicating with the host computer,

wherein the memory contains a limited use transaction identification number and personal identification information corresponding to the limited use transaction identification number,

wherein the limited use transaction identification number comprises a randomly generated number and a time generation stamp.

2. The system for conducting transactions according to claim 1, further comprising a pool of available numbers for random selection as the randomly generated number.

3. The system for conducting transactions according to claim 1, wherein the memory contains a list of deactivated transaction identification numbers available for reuse.

4. The system for conducting transactions according to claim 2, wherein the memory contains a list of deactivated transaction identification numbers for return to the pool of available numbers.

5. The system for conducting transactions according to claim 1, wherein the transaction identification number is a credit card number.

6. The system for conducting transactions according to claim 1, wherein the transaction identification number is a debit card number.

7. A method for issuing a limited use transaction identification number to a user, the method comprising:

opening a communication link between the user and a microprocessor having an associated memory storage device;

verifying the identity of the user by a predetermined protocol;

requesting a transaction identification number to be generated for limited use by the user in accord with a specified limitation;

providing the transaction identification number from a pool of available numbers, wherein the transaction identification number comprises a random portion and a date stamp portion indicating the time of activating the transaction identification number for use by the requesting user;

transmitting the transaction identification number to the user;

storing the transaction identification number in the associated memory with a link to associated personal identification information and to the specified limitation; and

providing notification of the activated transaction identification number.

8. The method according to claim 7, further comprising:

deactivating the transaction identification number when the specified limitation has been satisfied, and

returning the random portion of the number to a pool of available numbers for subsequent selection and association with subsequent user.

9. The method according to claim 7, wherein the transaction identification number is a credit card number.

10. The method according to claim 7, wherein the transaction identification number is a debit card number.

11. The method according to claim 7, wherein the transaction identification number further comprises an additional data field that identifies a particular merchant

12. A method for consummating a transaction, the method comprising:

providing a transaction identification number comprising a random portion and a time stamp portion indicating the time of activating the transaction identification number for use by the requesting user;

presenting the transaction identification number by the requesting user to a provider to obtain a product or service;

transmitting the transaction identification number by the provider to a host microprocessor for verification of the user and of the status of the transaction identification number;

receiving from the host microprocessor personal identification information for verification of the user;

obtaining information from the user to compare with the personal identification information obtained from the host microprocessor; and

confirming to the host microprocessor that the user has been verified.

13. The method of claim 12, further comprising receiving authorization from the host microprocessor for payment for the transaction.

14. The method according to claim 12, wherein the transaction identification number is a credit card number.

15. The method according to claim 12, wherein the transaction identification number is a debit card number.

16. The method according to claim 11, wherein the transaction identification number further comprises an additional data field that identifies a particular merchant

17. The method of claim 12, wherein the step of providing a transaction identification number comprises:

opening a communication link between the user and a microprocessor having an associated memory storage device;

verifying the identity of the user by a predetermined protocol;

requesting a transaction identification number to be generated for limited use by the user in accord with a specified limitation;

providing the transaction identification number from a pool of available numbers, wherein the transaction identification number comprises

a random portion and a time stamp portion indicating the time of activating the transaction identification number for use by the requesting user;

transmitting the transaction identification number to the user;

storing the transaction identification number in the associated memory with a link to associated personal identification information and to the specified limitation; and

providing notification of the activated transaction identification number.

18. The method according to claim 17, wherein the transaction identification number is a credit card number.

19. The method according to claim 17, wherein the transaction identification number is a debit card number.

20. A method for electronically providing a transaction identification number to a requestor, the method comprising the steps of:

forming a telecommunications connection between a the requestor at a first location and a host microprocessor of a transaction number issuer at a second location, said host microprocessor being connected to a data storage system with memory;

providing personal identification information by the requestor to the host microprocessor;

issuing a transaction identification number and assigning it to the requestor;

storing the transaction identification number in conjunction with the personal identification information in the memory; and

transferring the transaction identification number to the requestor by the telecommunications connection.

21. The method according to claim 20, wherein the transaction identification number is a credit card number.

22. The method according to claim 20, wherein the transaction identification number is a debit card number.

23. The method according to claim 20, wherein the step of issuing a transaction identification number includes activating the number by addition of a time stamp indicating the time of activation.

24. The method according to claim 23, wherein the transaction identification number is a credit card number.

25. The method according to claim 23, wherein the transaction identification number is a debit card number.

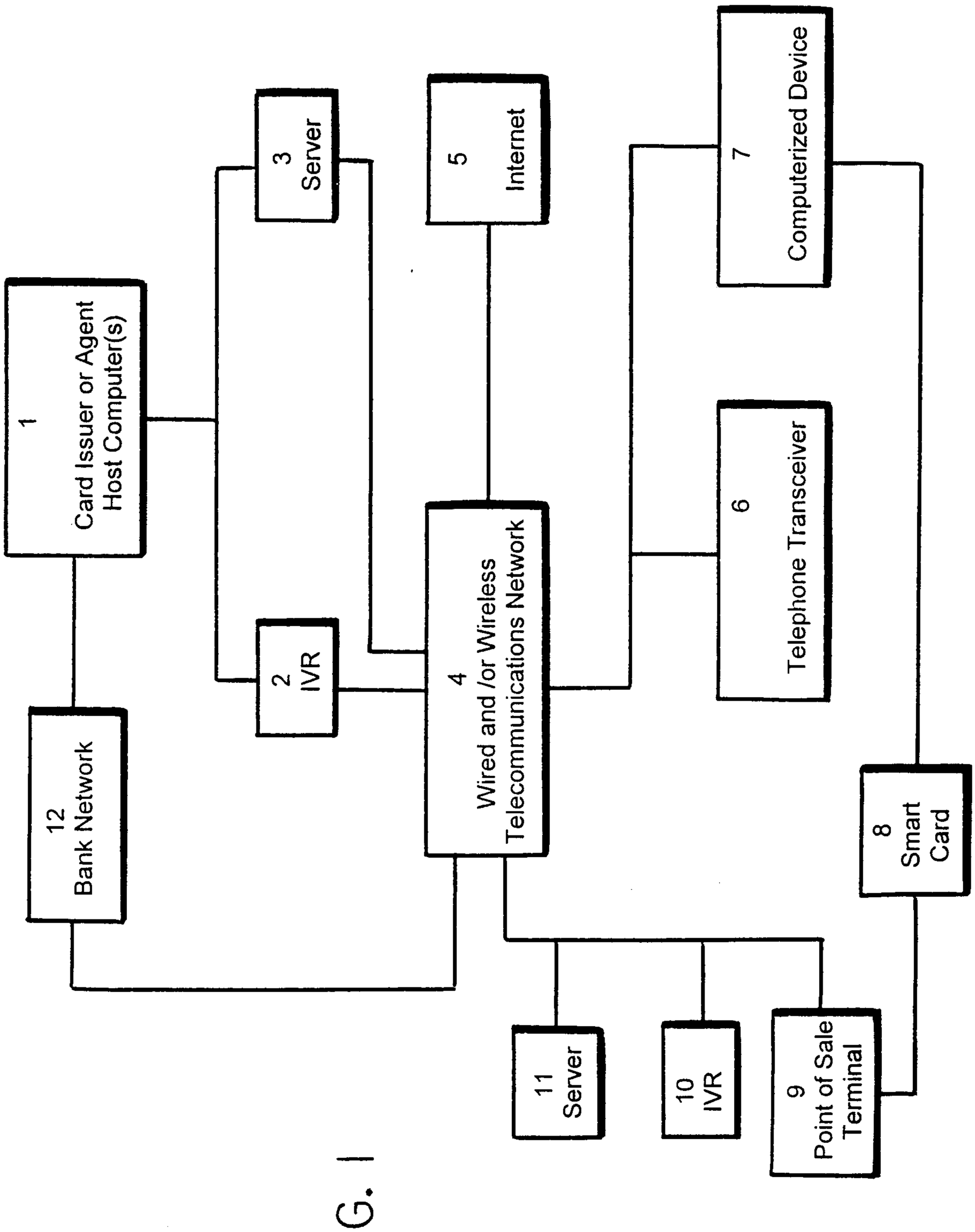

1
Card Issuer or Agent
Host Computer(s)
2
IVR
3
Server
4
Wired and /or Wireless
Telecommunications Network
5
Internet
6
Telephone Transceiver
7
Computerized Device
8
Smart
Card
9
Point of Sale
Terminal
10
IVR
11
Server
12
Bank Network

FIG. 1

Anatomy of Typical 16-Digit Credit or Debit Card Number

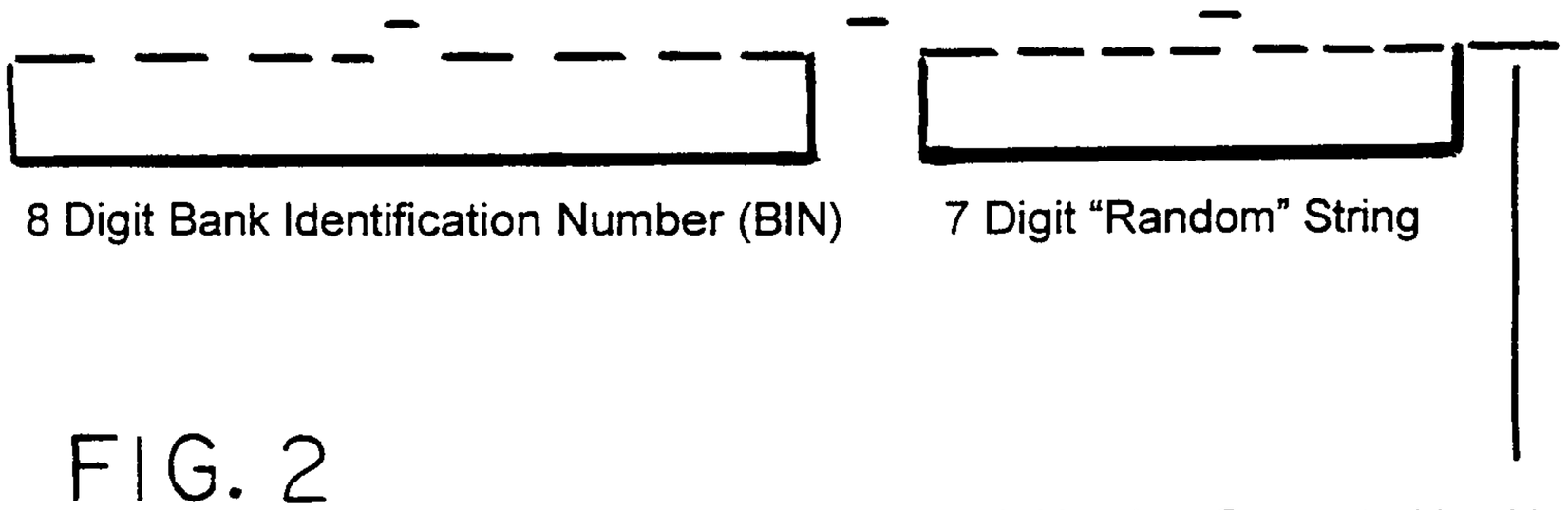


FIG. 2

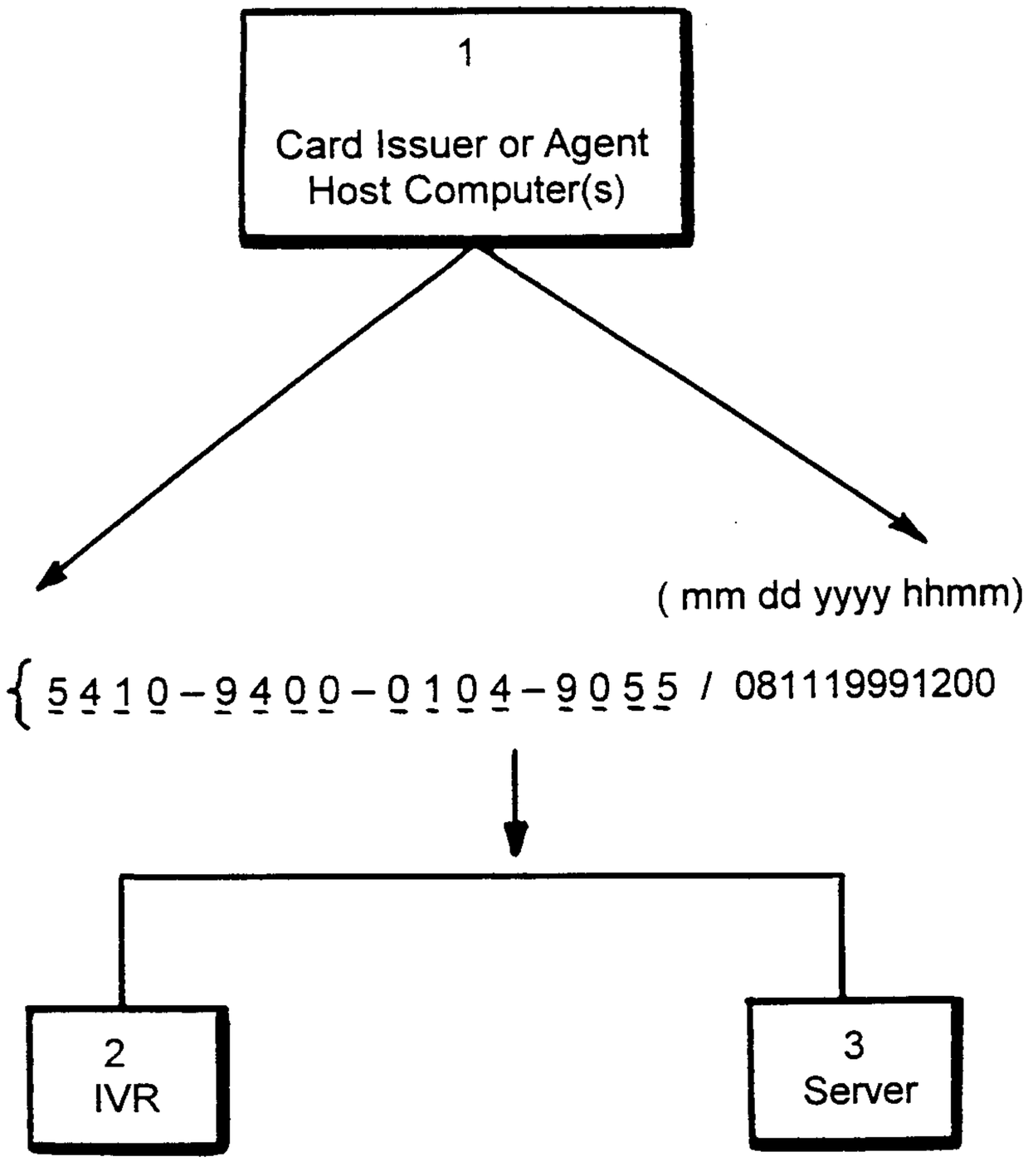


FIG. 5

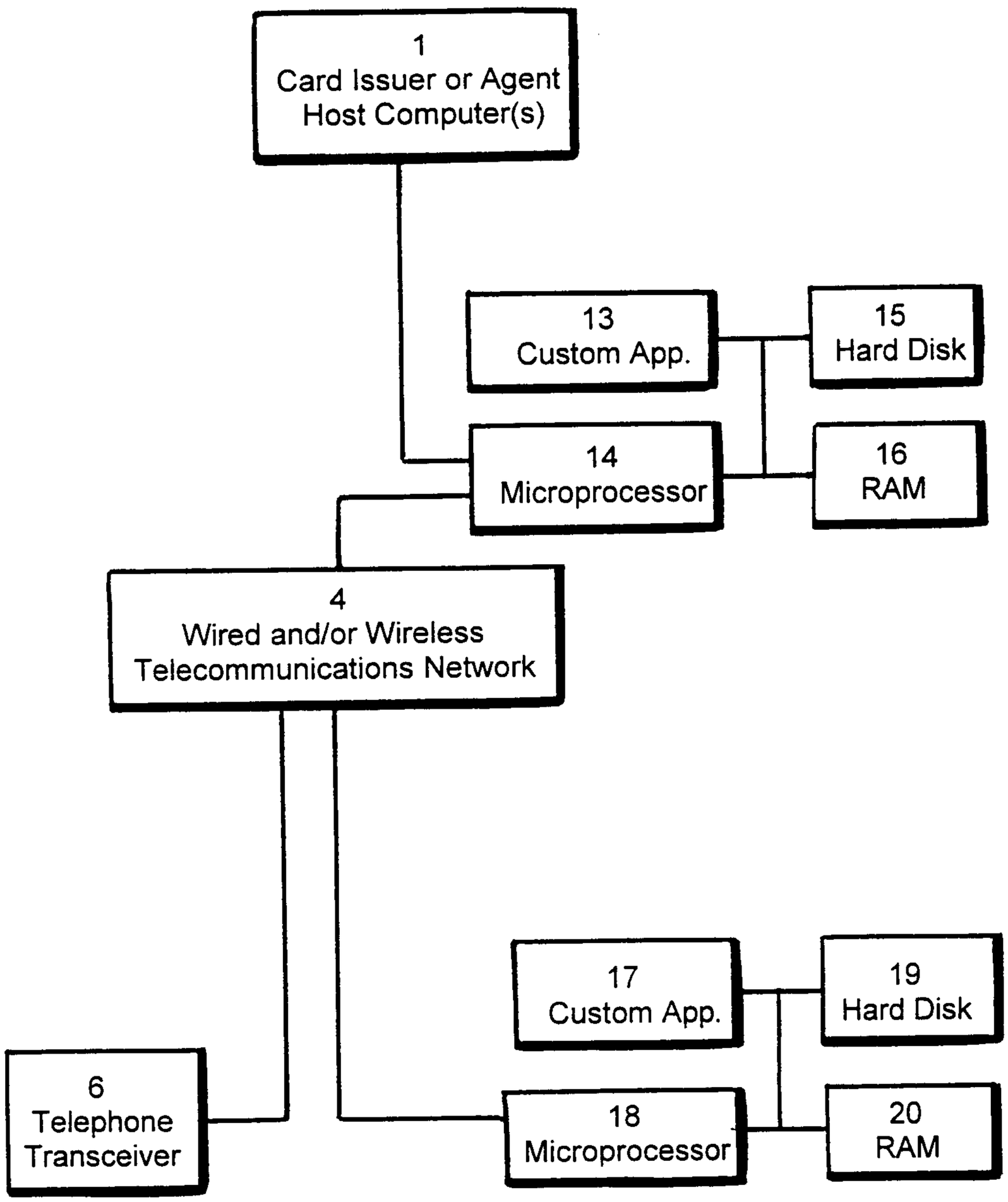

1
Card Issuer or Agent
Host Computer(s)
13
Custom App.
15
Hard Disk
14
Microprocessor
16
RAM
4
Wired and/or Wireless
Telecommunications Network
6
Telephone
Transceiver
17
Custom App.
19
Hard Disk
18
Microprocessor
20
RAM

FIG. 3

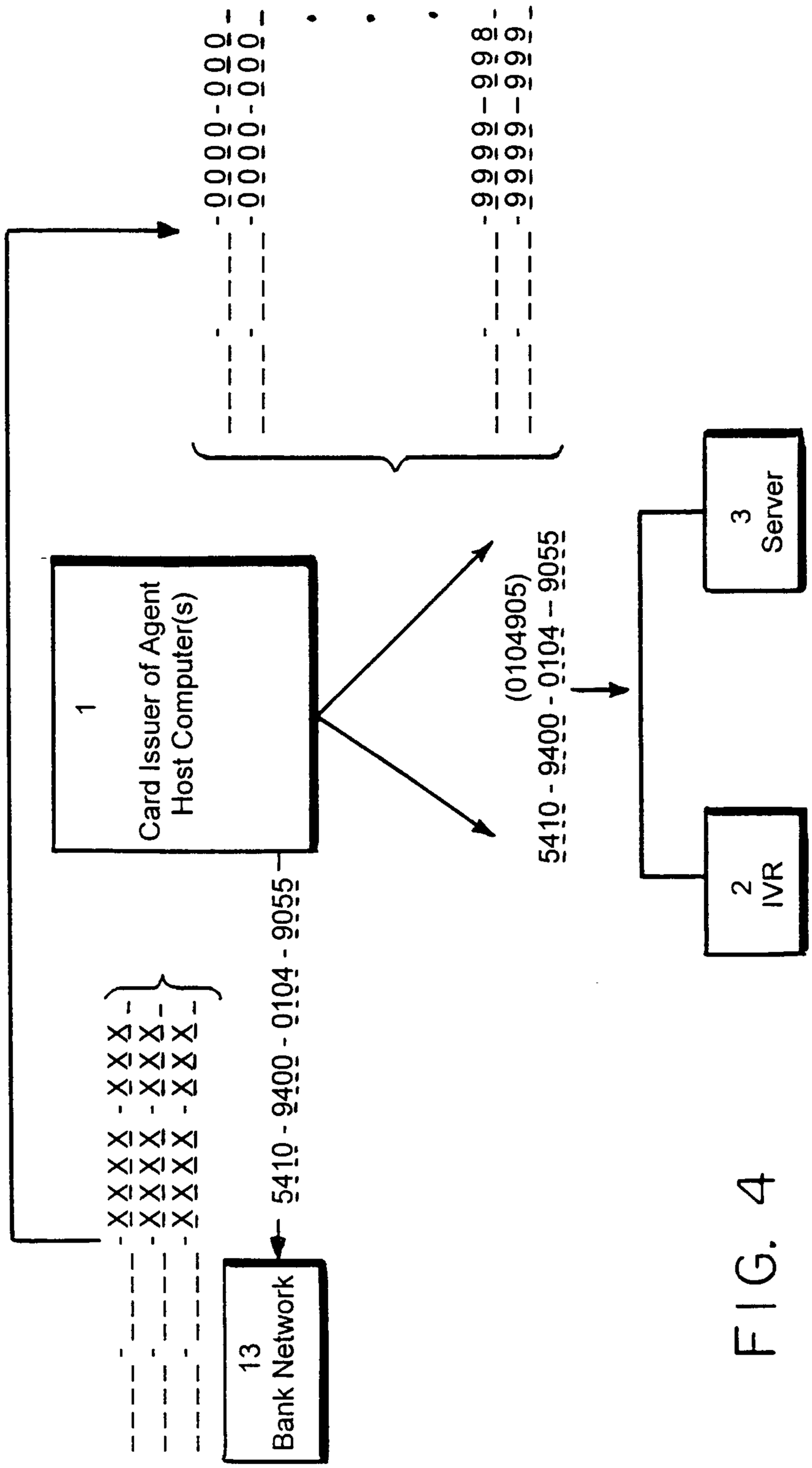
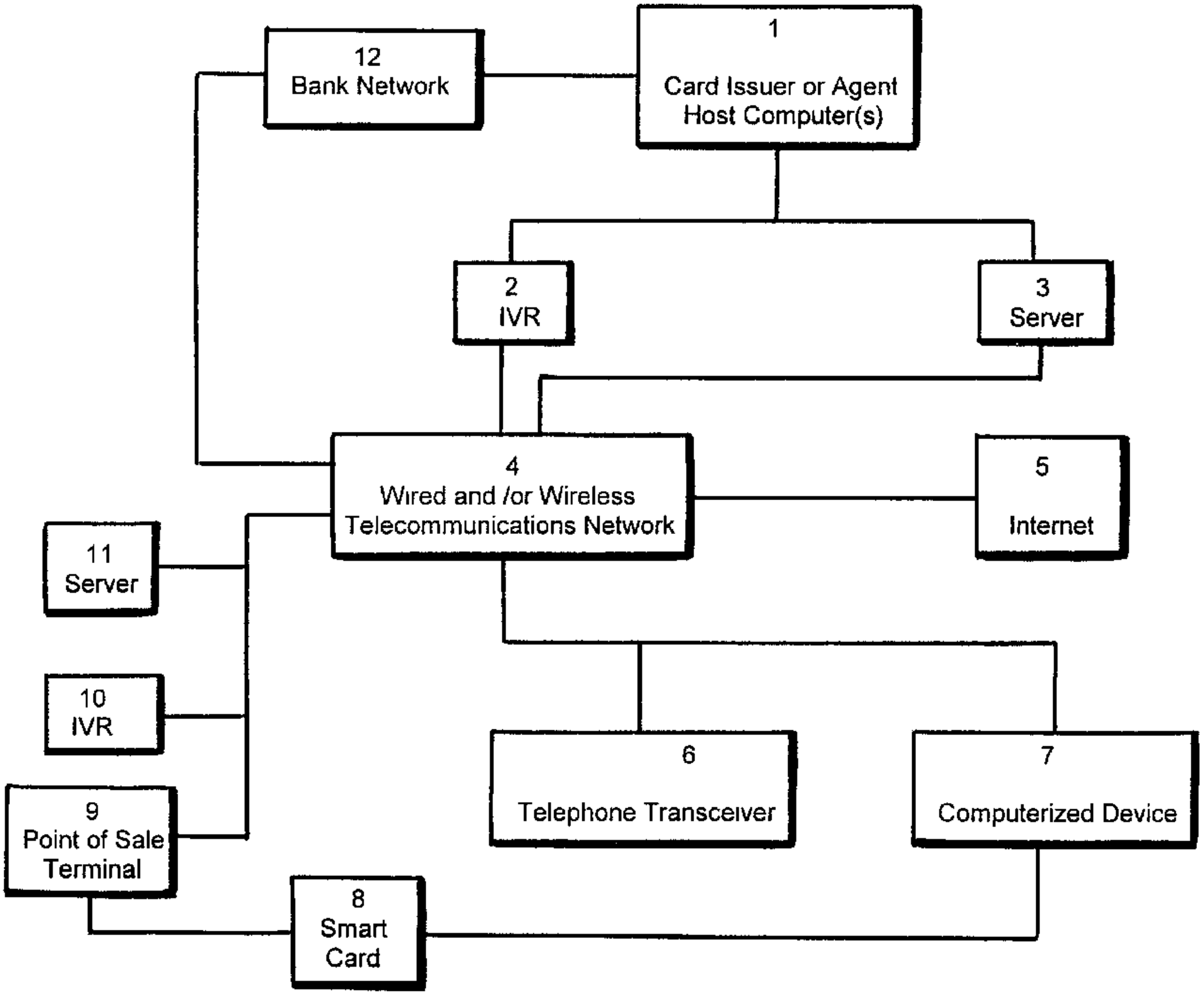

1
Card Issuer of Agent
Host Computer(s)
3
Server
2
IVR
13
Bank Network
5410 - 9400 - 0104 - 9055
(0104905)
5410 - 9400 - 0104 - 9055
XXXX - XXXX - XXXX - XXXX
9999 9999 9999 9999
0000 0000 0000 0000

FIG. 4


12
Bank Network
1
Card Issuer or Agent
Host Computer(s)
2
IVR
3
Server
4
Wired and /or Wireless
Telecommunications Network
5
Internet
11
Server
10
IVR
9
Point of Sale
Terminal
6
Telephone Transceiver
7
Computerized Device
8
Smart
Card