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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 May 2002 (16.05.2002)

PCT

(10) International Publication Number
WO 02/39226 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number: PCT/US01/47155

(22) International Filing Date:
8 November 2001 (08.11.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/710,283 10 November 2000 (10.11.2000) US

(71) Applicant *(for all designated States except US)*: **PAYMATE.NET CORPORATION** [US/US]; 9420 Research Boulevard, Echelon III, Suite 160, Austin, TX 78759 (US).

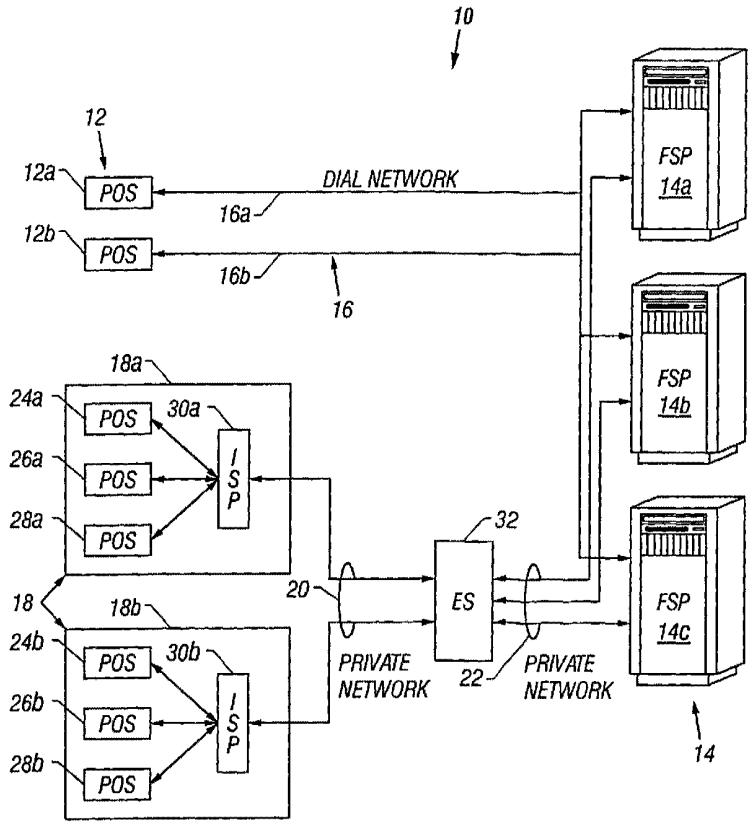
(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **THOMPSON, R., William** [US/US]; 9305 Scenic Bluff Drive, Austin, TX 78733 (US). **SPENCE, J., Standford** [US/US]; 7209 Valburn Drive, Austin, TX 78731 (US). **JONES, Alan, L.** [US/US]; 209 North Stone, Round Rock, TX 78664 (US). **MELLO, Mathew, R.** [US/US]; P.O. Box 200369, Austin, TX 78720 (US). **HEILVEIL, Andrew, L.** [US/US]; 13271 Kerrville Folkway, Austin, TX 78729 (US).

(74) Agents: **SKALE, Andrew, D.** et al.; Brobeck, Phleger & Harrison, 12390 El Camino Real, San Diego, CA 92130 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, 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, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR CONSUMMATING A FINANCIAL TRANSACTION AT A POINT-OF-SALE BASED ON SECURE ELECTRONICS COMMUNICATIONS OVER AN ACTIVE, FULL-TIME PUBLIC NETWORK



(57) Abstract: A system and method for consummating a financial transaction at a POS based on a secure electronic communication over an active, full-time public network such as the Internet. The invention comprises at least one POS, at least one network appliance, at least one primary server, and at least one financial service provider, the network appliance, primary server, and financial service provider being in electronic communication over an active, full-time public network, whereby a financial transaction is consummated at the POS based on the electronic communications over the network.

WO 02/39226 A2

(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, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

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

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SYSTEM AND METHOD FOR CONSUMMATING A FINANCIAL TRANSACTION AT A POINT- OF-SALE BASED ON SECURE ELECTRONICS COMMUNICATIONS OVER AN ACTIVE, FULL-TIME PUBLIC NETWORK

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates generally to authentication of non-cash payment methods and more specifically, to an e-commerce gateway system and method for consummating a financial transaction at a point-of-sale system ("POS") based on secure electronic communications over an active, full-time public network such as the Internet.

2. Description of Related Art

Today's POS environment can be considered broadly segmented into two primary types of businesses: those having a single or small number (i.e., approximately 2 to 5) of POSs within their confines ("single-POS") and those having greater numbers of POSs within ("multiple-POS"). While the former can generally be typified by independent businesses, small regional chains, small business, small professional organizations and the like, the later can be typified by larger chain enterprises and the like.

A primitive multiple-POS business could ostensibly require a separate phone line for each POS. However, it is more customary for the multiple-POS businesses to instead use a single telephone line to handle the multiple-POS transactions. For example, various parties have developed systems for transmitting multiple-POS transactions over a single telephone line, such as that described by U.S. Pat. No. 5,500,890 to Rogge et al., in which a dial-up

asynchronous communication protocol allows multiple threaded transactions and interleaved file transfers over a single phone line.

Not uncommonly, multiple-POS businesses enjoy transactional cost-savings over single-POS businesses because they are frequently able to develop and support an infrastructure of fixed-function in-store-processors ("ISP") that are connected to the various POSs. The ISPs, in turn, are then commonly connected to an enterprise server ("home office" or "ES") that serves multiple enterprise locations. The ISPs frequently connect to the home office through a first set of privately leased phone lines that are primarily dedicated to this singular purpose. Similarly, the ES is commonly connected to a plurality of financial service providers through a second set of privately leased phone lines that are also primarily dedicated to this singular purpose. These privately leased phone networks are all too often the unique province of multiple-POS businesses. These private networks enable rapid financial transaction consummation—and consequently, higher throughput and profit—because the phone lines allow active, full-time communication with the financial service providers.

Multiple-POS businesses justify the cost of building their private networks on the faster transaction times that result at the POS. Heretofore, rarely—if ever—have single-POS businesses been able to afford this luxury. Heretofore, rarely—if ever—have faster transactions and the ability to amortize over multiple-POS systems been available to the single-POS businesses. Rather, single-POS businesses have traditionally been forced to settle for incomplete and more costly payment solutions that are not well integrated with the rest of their enterprises. For example, some single-POS businesses have been forced to accept only

cash payments, thereby having to forego the profits that might otherwise accrue for check and data card consumers.

What is needed, therefore, is a cost-effective POS solution that will enable faster transactions for single-POS businesses.

BRIEF SUMMARY OF THE INVENTION

Briefly and summarily, the current invention presents a system and method for consummating a financial transaction at a POS based on a secure electronic communication over an active, full-time public network such as the Internet. In a preferred embodiment, the invention comprises at least one POS, at least one network appliance, at least one primary server, and at least one financial service provider, the network appliance, primary server, and financial service provider being in electronic communication over an active, full-time public network, whereby a financial transaction is consummated at the POS based on the electronic communications over the public network.

The foregoing and other objects, advantages, and aspects of the present invention will become apparent from the following description. In the description, reference is made to the accompanying drawings which form a part hereof, and in which there is shown, by way of illustration, a preferred embodiment of the present invention. Such embodiment does not represent the full scope of the invention, however, and reference must also be made to the claims herein for properly interpreting the scope of the invention.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

Fig. 1 depicts a schematic diagram of single-POS and multiple-POS businesses in a

prior art network configuration;

Fig. 2 depicts a schematic diagram of a plurality of single-POS businesses in a network configuration in which a preferred embodiment of the present invention can be carried out;

Fig. 3 depicts a system block diagram of a preferred embodiment of the present invention;

Figs. 4 A-D depict a decision chart for POS application logic;

Fig. 5 depicts a hardware configuration for single-POS and multiple-POS configurations;

Fig. 6 depicts a preferred embodiment of time-synchronization;

Fig. 7 depicts a preferred embodiment of the server architecture;

Fig. 8 depicts a preferred embodiment of the mutual authentication protocol;

Fig. 9-A depicts a preferred embodiment of a dynamic-to-fixed network address mapping;

Fig. 9-B depicts a prior art typical embodiment of a private network configuration;

Fig. 10 depicts a data-flow diagram; and

Figs. 11 A-C depict a preferred embodiment of the major components of hardware and software.

DETAILED DESCRIPTION OF THE INVENTION

While the present invention relates to a system and method for consummating a

financial transaction at a POS based on secure electronic communications over an active, full time public network, it further relates to networking, monitoring, collecting data, selling goods and services, controlling interactive advertising, and controlling and effectuating commerce at a POS. In addition, this invention also relates to physical and virtual public networking of POS terminals and hardware, server-based public network controls, and public network security as it relates to a POS. Accordingly, before turning to an explanation of a preferred embodiment, a brief description of contextual terminology is in order.

A "data card" refers to a credit card, debit card, SmartCard, electronic purchase card, secure electronic transaction ("SET") card, cyber wallet (i.e., the expansion of the credit card concept into a concept involving multiple cards with multiple issuers in a unified package), or other financial service provider account cards. Such data cards typically have a magnetic recording or other electrical conducting region associated with the card that carries the users account number, expiration date, name of the issuing financial service provider, and other information, as well as a visible indication of an account number and other information typically in an area of embossed characters.

A "business" generally refers to any institution or enterprise tendering goods or services in exchange for a monetary payment from a consumer or a promise of an exchange of monetary payment from a consumer.

A "financial transaction" refers to an exchange of monetary payment or a promise of an exchange of monetary payment, typically between a consumer and business. It includes payment transactions involving data cards, traditional check writing, electronically converted

checks, automated clearing house ("ACH") transactions, electronic benefit transfer ("EBT") transactions, and other types of transactions as well. This term may also refer to broader types of transactions such as the exchange of information between a consumer and health care provider, or between a consumer and business with a loyalty or other reward program.

A "financial service provider" refers to an institution that processes financial transactions, such as a bank or credit card transaction processing company. The term may also refer to an independent third party institution that is not otherwise related to the financial service provider, such as a collection agency. It may further include both authorization processors and bank settlement processors (so called "front end" and "back end" processors, respectively), although it is recognized that such services are commonly provided at different times, in different ways (i.e., real-time processing or batch mode processing), and by different entities. For the purposes of this description, both types of processors are subsumed hereunder.

"Consummation" refers to whether or not a financial transaction has been approved or denied by a financial service provider, and correspondingly completing the transaction to transfer or not transfer funds from the consumer to the financial service provider as appropriate.

"Full-time" is more than part-time and refers to electronic communication that can occur essentially at any time of the day on any day of the year, so called "24/7" communication capabilities.

"Part-time" is less than full-time and refers to an electronic connection or

communication that can occur when the business is open or otherwise accepting and processing financial transactions.

"Active" refers to an electronic connection or communication that is ready for transmission without having to require some event to occur as a precondition, such as a dial-up event initiating a phone call.

"Passive" refers to an electronic connection or communication that is ready for transmission only after some event occurs as a precondition, such as a dial-up event initiating a phone call.

"Secure" refers to an electronic connection or communication that is encrypted or otherwise electronically protected to maintain data integrity.

A "private network" refers to an inherently secure network in which only a designated business and financial service provider communicate.

A "public network" refers to an inherently insecure network in which any business and financial service provider may communicate.

The "Internet" refers to a type of public network comprising a set of globally interconnected computers through which multiple users can access data and programs from around the world. It connects a plurality of server computers to a plurality of client computers and permits a wide variety of communication and informational retrieval mechanisms, including electronic mail ("e-mail"), file transfer protocol ("FTP"), USENET, the world-wide web ("web"), and others.

"Server" refer to a computer that hosts other documents and files for storage and

retrieval thereof on command from a client computer. Such a server may also provide program execution, such as providing data translation for forwarding to other servers and clients. Well-known in the art, servers and host computers can communicate with a public network such as the Internet by providing or hosting an Internet website. An Internet website is provided by creating a document containing Hypertext Markup Language ("HTML") that defines a plurality of web pages. An HTML document suitable for posting on the Internet typically contains what is referred to as "content" and "mark-up." The content refers to the information that describes the actual text of the Web page, and the mark-up refers to the information that describes the behavioral characteristics of the page, such as how the content is to be displayed by a browser or how other information can be accessed through the site.

"Client" refers to a computer that supplies requests to server computers for various documents and then displays the retrieved documents. Well-known in the art, one computer frequently functions both as client and server.

"Point-of-sale" ("POS") refers to an area, space, or environment in which a financial transaction is consummated. It may be comprised of a number of POS terminals.

A "terminal" or "POS terminal" refers generally to the hardware at the POS that enables the financial transaction to be consummated. It may include either or both a commercially available and proprietary cash register, data card reader, display device, keyboard, check processor, receipt printer, personal identification number (PIN) keypad, and other financial transaction processors.

A "Network Appliance" refers generally to a client that allows access to a Public

Network such as the Internet.

Referring now to Fig. 1, a typical business environment 10 is illustrated in which a prior art POS processing system is depicted. More specifically, a plurality of single-POS businesses 12a, 12b, ... (hereinafter referred to as "12") establish electronic communication with a plurality of financial service providers 14a, 14b, 14c . . . (hereinafter referred to as "14") through a dial-up phone connection 16a, 16b . . . (hereinafter referred to as "16"). For simplicity, only two single-POS businesses 12 and three financial service providers 14 are depicted, although any number of each may be provided. The dial-up phone connection 16 of the single-POS businesses 12 is passive and part-time, whereby the single-POS businesses 12 dial- up the financial service providers 14 as needed. For example, if a first customer presents a data card for monetary payment, the appropriate data card financial service provider 14 is called upon to consummate the financial transaction. If another customer presents a check for monetary payment, the appropriate check financial service provider 14 is called upon to consummate the financial transaction. Before the different financial transactions can be consummated, the single-POS businesses 12 must separately initiate electronic communication with each of the different financial service providers 14, each occurring separately over the dial-up phone connection 16. This dial-up phone connection 16 has traditionally resulted in significant shortcomings, including extending the elapsed time required to consummate the financial transaction in order to allow for the dial-up event initiating the phone call.

Multiple-POS businesses 18a, 18b . . . (hereinafter referred to as "18"), on the other

hand, of which two are representatively depicted in Fig. 1, establish electronic communication with the plurality of financial service providers 14 through private networks 20, 22 of leased phone lines. These private networks 20, 22 of leased phone lines are active and full-time, whereby the multiple-POS businesses 18 are continuously connected to the financial service providers 14. For example, a separate phone line is typically dedicated to each financial service provider 14 for rapid communication between the multiple-POS business 18 and the financial service providers 14. While it is also possible for single-POS businesses 12 to maintain private network connections 20-22 with each of the financial service providers 14, this is typically not cost justifiable.

In the figure, each multi-POS business 18 typically includes a plurality of POSs 24, 26, 28 of which three are representatively depicted for each multi-POS business 18. Each POS 24, 26, 28 typically maintains electronic communication with an ISP 30 that process individual requests from each of the POSs 24, 26, 28. The ISP 30 maintains electronic communication with an enterprise server that is shared by the various multiple-POS businesses 18. The electronic communication between the ISP 30 and enterprise server 32 is established through the first private network 20 of leased phone lines. Similarly, the electronic communication between the enterprise server 32 and financial service providers 14 is established through the second private network 22 of leased phone lines.

Referring now to Fig. 2, a public network environment 34 is illustrated in which a preferred embodiment of the present invention can be carried out. More specifically, one or more of the plurality of single-POS businesses 12 establish electronic communication with

one or more of the plurality of financial service providers 14 through a public network 36. For simplicity, only two single-POS businesses 12 and three financial service providers 14 are depicted, although any number of each may be provided. The public network 36 comprises an active, full-time network connection.

In a preferred embodiment, one or more network appliances 38 are used to interface between one or more of the single-POS businesses 12 and the public network 36. Accordingly, the network appliance 38 is capable of electronic communication with the POS 12 by known techniques, such as RS 232 serial interface. Similarly, the network appliance 38 is also capable of electronic communication with the public network 36 by known techniques, such as, for example, a high-speed T1 line, ADSL, cable, wireless, and other communication techniques known in the art.

At least one full-time primary server 40 is also capable of electronic communication with the public network 36, again by known techniques, as are the plurality of financial service providers 14. More specifically, a preferred primary server 40 comprises a central processing unit 42 ("CPU") and an internal memory device 44 such as random access memory ("RAM"). The internal memory device 44 preferably contains therein a resident multi-tasking operating system 46 such as Linux or another suitable multi-tasking operating system known to those in the art, a network server program 48, and also preferably an application programming interface 50 that provides extensions to enable application developers to extend or customize the core functionality thereof through software programs including plug-ins, CGI programs, servlets, and the like.

In the Internet paradigm, the present invention is preferably implemented using a computer program that is operative at a web server such as the primary server 40, which operates a so called "web-site" by known techniques. A flow diagram for such program is attached as Figure 3. An advantage of this embodiment is that all hardware for implementing the invention can be obtained commercially off the shelf. Although the invention will be described in the context of a single primary server 40, one of ordinary skill in the art will appreciate that the described functionality may be implemented across multiple primary servers 40. Moreover, the web site may be mirrored at additional ancillary servers 52 in electronic communication with the public network 36, and, if desired, one or more management ancillary servers 52 or other computer resources or the primary server 40 may be used to facilitate various billing, accounting and administrative functions as a "back end" to the underlying site.

The network server program 48 of the primary server 40 is preferably stored in the internal memory device 44 and executed upon initialization of the primary server 40. It preferably includes appropriate display routines for generating a set of display screens that together comprise the user interface for the site, as will be displayed at the POS 12 via the network appliance 38. To that regard, and as noted above, the preferred embodiment of the invention is preferably implemented within at least one primary server 40. Thus, the invention does not require any modifications to conventional POS 12 hardware or software. Furthermore, by housing the software applications on the primary server 40, the single-POS businesses 12 need not afford the cost of the equipment or software or staff to implement the

system functionality that is being described and had previously been reserved for the multi-POS businesses 14.

Although not intended to be limiting, the above-described functionality is preferably implemented as standalone native code or, alternatively, as a Java servelet. Generalizing, the above-described functionality is implemented in software executable in the CPU 42, namely, as a set of instructions (i.e., program code) in a code module that is resident in memory of the primary server 40. Unless and until required by the primary server 44, the set of instructions may be stored in computer memory, for example, in a hard disk drive, or in a removable memory such as an optical disk (for eventual use in a CD-ROM) or floppy disk (for eventual use in a floppy disk drive), or downloaded via the Internet or another computer network.

In addition, although the various methods described are conveniently implemented in a general purpose primary server 40 selectively activated or reconfigured by software, one of ordinary skill in the art would also recognize that such methods may be carried out in hardware, firmware, or in a more specialized apparatus constructed to perform the required method steps.

Further, as used herein, a "client" such as the internet appliance 38 should be broadly construed to mean any computer or component thereof directly or indirectly connected or connectable in any known or later-developed manner to the public network 36. Similarly, the term "server" should also be broadly construed to mean a computer, computer platform, an adjunct to a computer or platform, or any component thereof, that can either store data or execute programs locally on behalf of a client. Of course, the client is broadly construed to

mean the one who requests or receives files or programs, and the server is the entity that supplies the files or programs that are capable of being downloaded across the public network 36.

Referring back to Fig. 2, the network appliance 38 is a client that, in the Internet paradigm, includes a suite of Internet tools including a network browser 53, such as Netscape Navigator or Microsoft Internet Explorer, that has a Java Virtual Machine (JVM) and support for application plug-ins or helper applications. The network browser 53 allows access to the servers of the public network 36 to obtain certain services. For example, these services can include one-to-one e-mail, one-to-many messaging ("bulletin board"), on-line chat, file transfer and network browsing. Various known Internet protocols are used for these services. For example, browsing is effected using the known Hypertext Transfer Protocol ("HTTP"), which provides users access to multimedia files using the Hypertext Markup Language ("HTML"). The collection of servers and clients comprise the World Wide Web, which is the Internet's primary multimedia information retrieval system.

As known, the network path to the primary server 40 is identified by a so-called Uniform Resource Locator ("URL") having a special syntax for defining a network connection. Use of an HTML-compatible browser (e.g., Netscape Navigator or Microsoft Internet Explorer) at a client machine such as the network appliance 38 involves specification of a link via the URL. In response, the network appliance 38 makes a request to the primary server 40 identified in the link and, in return, receives a document or other object formatted according to the HTML. The collection of documents comprising the network service

program 48 that is supported by the primary server 40 comprises the web site of the present invention.

Resultant from the electronic communication of the network appliance 38 and primary server 40 and financial service providers 14 with the active, full-time public network 36, an encrypted virtual private network ("VPN") 68 is established between the single-POS businesses 12 and the financial service providers 14. Preferably, both the single-POS businesses 12 and the financial service providers 14 connect to the primary server 40 using a mutual authentication protocol ("MAP") with dual digital certificates to establish the secure VPN 68 between them. This allows the electronic communication to avoid compromise, whereby a financial transaction is consummated at the single-POS business 12 based on the secure electronic communications over the public network 36. Significantly, because the public network 36 is active at all times, dial-up protocols are not required prior to the single-POS businesses 12 consummation of financial transactions.

As described, the network appliance 38 is preferably designed to take advantage of high-speed public network connection capabilities. It preferably comprises a combination of RAM devices including dynamic RAM, or some other type of dynamic storage media, and flash RAM, or some other type of persistent storage that does not lose its contents when power is removed. Preferably, a portion of the code stored thereon remains resident in the flash RAM or its equivalent, sufficient to re-establish communication with the primary server 40 or download the latest version of application code in the event items have become corrupted or subsequent versions become available.

In a preferred embodiment, all application programming can be in an appropriate application programming language, such as Java. In a preferred embodiment, it further comprises a customer activated terminal ("CAT") 54, magnetic ink character recognition ("MICR") check device 56, and a multi-purpose printer 58, to which it preferably interfaces using the object oriented JPOS (Java POS) convention, as practiced by those skilled in the art.

As compared to a computer, the network appliance 38 is typically more limited in processing power and memory storage capacity. Nevertheless, it includes all the hardware, software, memory, and other computing components necessary to implement consummation of financial transactions at a POS. Accordingly, the primary functionality is disposed in the network appliance 38 as opposed to one of the POS terminals 54-58. For example, the hardware and software that is sufficient to support a small number of "preload" initial prompts resides in the POS terminals 54-58, with the more sophisticated functionality being directed from the network appliance 38.

More specifically, a representative network appliance 38 comprises a CPU 60 and an internal memory device 62 such as RAM. The internal memory device 62 preferably contains therein a resident multi-tasking operating system 64 such as Linux or another suitable multi-tasking operating system known to those in the art, the network firewall 66, the VPN 68, the integrated browser 70, other integrated clients 72, and other POS applications 74.

When using any public network 36, it is exceedingly difficult, if not all together impossible, to prevent others from observing the traffic placed upon it. Therefore, secure use of the public network 36 is accomplished by employing additional security measures to ensure

reliable service. Accordingly, each network appliance 38 is preferably equipped with network firewall capabilities, including disabling remote logon capability, rejecting packets arriving from the public network 36 that were not requested, and requiring a digital certificate authorization sequence upon initialization, thereby ensuring that only authorized users are utilizing the network appliance 38 to access the single-POS 12. The firewall capabilities allow the network appliance 38 to securely initiate requests for information such as e-mail, advertising, coupons, or other promotional or management data from the primary or ancillary servers 40,52. Furthermore, secondary authentication factors may also be included, such as the presence of an affixed token, SmartCard, magnetic card swipe, PIN entry, network controller MAC, address verification, device serial number, or any other parameter that may be compared to a database of known values or derived with cryptographic techniques.

The network appliance 50 also preferably utilizes sufficient boot-ROM ("read only memory") to extend the normal diagnostic routines found in most PC BIOS's in order to diagnose the attached POS terminal devices 54-58. The boot-ROM capability should include enough operating system kernel functionality to be able to establish an initial connection to the public network 36. The boot-ROM capability may determine whether the version of software resident in the persistent storage of the network appliance 38 is consistent with the current version supported by the primary server 40. For example, if the resident software is either corrupted or below current revision levels, the network appliance 38 can automatically re-load all current operating system and applications software from the primary server 40. This technique also allows the network appliance 38 to support new features automatically

downloaded from the primary server 40. Other techniques for automatically configuring a network appliance from a remote server are also known, as described, for example, in PCT Application WO 99/56447 to Giordano et al. (multiple revisions let you load different features depending on what consumer pays for; check revision level to see if it's current, and if it is not, re-load; compare stored hash to a computed hash to see if they are different...)

In a preferred embodiment, the network appliance 38 may also support additional POS terminal devices 54-58 that are capable of capturing a signature for credit card transactions. These signatures are preferably stored in the memory of the primary server 48 in a vector format, and can be viewed as needed for charge repudiation purposes via the network browser 52. Such retrieval preferably reproduces the format of the original receipt including all transactional data in addition to the captured signature. In addition to storing the captured signature, the vectorized representation can be converted to a specific bit-map image and displayed on the printed receipt from the multi-purpose printer 44, which preferably has the ability to print bit-mapped graphics. Other devices and techniques for capturing and verifying hand-written signatures electronically at a POS are also known, such as those described in U.S. Pat. No. 5,195,133 to Kapp et al., U.S. Pat. No. 5,479,530 to Nair et al., and U.S. Pat No. 5,892,824 to Beatson et al.

Also in a preferred embodiment, captured information may also be used to initiate financial transactions for verifying or guaranteeing checks, or to support check truncation or electronic check conversion ("ECC") from the POS by initiating electronic funds transfer ("EFT"). In addition, an image-scanning POS terminal device may be incorporated as well,

allowing imaging of the check, and return of the cancelled check back to the writer at the POS. Likewise, numerous other check writing and verification devices and techniques at an MICR check device 56 are known, such as those described in U.S. Pat. No. 5,448,471 to Deato et al. and U.S. Pat. No. 5,484,988 to Hills et al.

Also, optical scan features of an the MICR check device could also be used to read either MICR formed characters printed with magnetic or regular ink, or traditionally bar coded information. This raw data could be interpreted and converted into useable character strings with either appliance-based or embedded character recognition applications for encrypted transmission to the primary server 40 or for further processing by applications and ancillary servers 40 requiring the information.

The internet appliance 38 may also support electronic check conversion without requiring a scanning terminal at the POS. Rather than require a merchant-as-custodian or third-party-as-custodian model for the initial check, the present system allows the business to collect a voided and signed check from a new user. These voided checks can be subsequently delivered to primary server 40 for storage on a retrievable database. The image of the face of the check including the account holder identification information, the printed routing and transmit numbers, plus the MICR code line can be scanned and retained on this retrievable database. In addition, a signature can be obtained from the CAT and stored on a separately retrievable database.

Thus, a consumer wishing to use electronically converted checks can then present a blank check at the POS, whereby the MICR information is captured using a standard MICR

reader. The account number is transmitted to the primary server 40 and compared to those on file. If present, a transmission of the corresponding image is initiated back to the requesting POS business 12, 18. The combination of the database information and use of the signature capture and display capabilities of certain terminal devices 54-58 may then be used to present an imaged check on a terminal 54-58 at the POS and capture a signature on the imaged check as opposed to on the paper document. The customer may also include a check sequence number if desired and not otherwise included in the MICR data. The currently captured signature can be compared to the one on file using a neural network or other pattern matching technique prior to approving the transaction.

Also in a preferred embodiment, the network appliance 50 may support additional POS terminal devices 54-58 that are capable of displaying information to customers and detecting customer initiated responses to queries through the CAT 40. This capability can enable network advertising from the ancillary servers 52 or other types of promotional content, including registration in customer loyalty programs, issuance of pre-paid gift cards, and acceptance of conditional terms or offers. Accordingly, in addition to printing receipts, server coupons may also be printed on the multi-purpose printer 58 at the POS.

In addition, the network appliance 38 can be configured to support cash register functionality. Such an implementation could include a locking cash drawer that is activated by a connection to the network appliance 38, and may also include a separate bar-code scanner that is likewise controlled by the network appliance 38. The user interface for entering transactions can be incorporated into an application or applet accessed through an

interface at the network browser 53. The applet is invoked by directing the network browser 53 to a URL network address for the particular location or business. The application or applet can support authentication of the user prior to accepting transactions by techniques known in the art. Sales may be initiated through a hot-linked clerk interface form either by entering Uniform Product Codes (UPC), Shipping Container Codes (SCC) or Stock Keeping Unit (SKU) codes manually, or scanning them, and noting the quantity of each item. This information can be transmitted to the primary server 40 for each completed item, where the applet retrieves the associated price information, and sends back the total to a POS terminal device 54-58. The display of the CAT 54 may be used to present itemized charges to the customer during the transaction. At the completion of the transaction and the computation of the grand total, the clerk may identify the payment type on the clerk form, or the customer may select it from the CAT 54. If the transaction is non-cash, the applet initiates appropriate action to the network appliance 38 payment application to obtain customer data card or check information in order to authorize the transaction, obtain a signature or PIN, print a receipt, or open the cash drawer as needed.

Representative hardware that can be used to implement a preferred embodiment of the invention includes devices such as the following: eN-Touch 1000 customer activated terminal ("CAT") from IVI/Checkmate of Roswell, Georgia; eN-Scribe 612 printer available from IVI/Checkmate of Roswell, Georgia; eN-Check 3000 check reader/clerk keyboard/display available from IVI/Checkmate of Roswell, Georgia; the network appliance such as the Capio II available from Boundless Technologies of Hauppauge, New York. Representative

hardware that can be used to implement a preferred embodiment of the invention includes software packages such as eN-Concert Enterprise of Roswell, Georgia.

CLAIMS

What is claimed is

1. A system for consummating a financial transaction at a point-of-sale based on secure electronic communications over an active, full-time public network, comprising:

at least one point-of-sale;

at least one network appliance coupled for electronic communication with the point-of-sale;

at least one primary server coupled for electronic communication with the network appliance over an active, full-time public network; and

at least one financial service provider coupled for electronic communication with the primary server over the active, full-time public network;

whereby a financial transaction is consummated at the point-of-sale based on the electronic communications over the active, full-time public network.

2. The system of claim 1 wherein the network appliance utilizes a multi-tasking operating system.

3. The system of claim 2 wherein the network appliance includes a network firewall.

4. The system of claim 3 wherein the network appliance invokes a mutual authentication protocol involving a plurality of factors.

5. The system of claim 4 wherein the mutual authentication protocol launches a virtual private network over the active, full-time public network.

6. The system of claim 5 wherein the point-of-sale includes means for consummating a check transaction.

7. The system of claim 6 wherein the point-of-sale includes means for electronic check conversion.

8. The system of claim 5 wherein the point-of-sale includes means for consummating a data card transaction.

9. The system of claim 5 wherein the point-of-sale includes means for displaying information pertaining to the financial transaction.

10. The system of claim 5 wherein the point-of-sale includes means for printing information pertaining to the financial transaction.

11. The system of claim 5 wherein the point-of-sale includes means for obtaining a signature associated with the financial transaction.

12. The system of claim 11 further including means for archiving the signature obtained at the point-of-sale.

13. The system of claim 12 further including means for retrieving the archived signature obtained at the point-of-sale.

14. The system of claim 13 further including means for displaying the archived signature obtained at the point-of-sale.

15. The system of claim 14 further including means for combining the archived signature with information pertaining to the financial transaction to generate a receipt of the financial transaction.

16. The system of claim 15 further including means for printing a receipt of the financial transaction.

17. The system of claim 5 wherein the network appliance is automatically configured upon initialization in accordance with information stored in the primary server and

in the network appliance.

18. The system of claim 17 wherein the network appliance configuration incorporates information to be printed on a receipt at the point-of-sale.

19. The system of claim 17 wherein the network appliance configuration includes mapping a dynamic network address into a fixed network address that is expected by the primary server.

20. The system of claim 17 wherein the network appliance configuration includes setting either or both a date and a time in the communication at the network appliance.

21. The system of claim 17 wherein the network appliance configuration includes establishing the functionality of the network appliance.

22. The system of claim 21 wherein establishing the functionality of the network appliance includes downloading modules to accomplish a revision update.

23. The system of claim 21 wherein establishing the functionality of the network appliance includes correcting a corrupted software configuration through downloading an uncorrupted module.

24. The system of claim 21 wherein establishing the functionality of the network appliance includes adding a new feature.

25. The system of claim 21 wherein establishing the functionality of the network appliance includes configuring the network appliance to function as means for delivering application service provider capabilities embodied in the primary server.

26. The system of claim 21 wherein establishing the functionality of the network appliance includes configuring the network appliance to function as means for delivering application service provider capabilities embodied in an ancillary server.

27. A method for consummating a financial transaction at a point-of-sale based on secure electronic communications over an active, full-time public network, comprising the steps of:

providing at least one point-of-sale;

providing at least one network appliance coupled for electronic communication with the point-of-sale;

providing at least one primary server that is capable of electronic communication with the network appliance over an active, full-time public network; and

providing at least one financial service provider that is capable of electronic communication with the primary server over the active, full-time public network;

whereby a financial transaction is consummated at the point-of-sale based on the electronic communications over the active, full-time public network.

28. The method of claim 27 wherein the network appliance utilizes a multi-tasking operating system.

29. The method of claim 28 wherein the network appliance includes a network firewall.

30. The method of claim 29 wherein the network appliance invokes a mutual authentication protocol involving a plurality of factors.

31. The method of claim 30 wherein the mutual authentication protocol launches a virtual private network over the active, full-time public network.

32. The method of claim 31 wherein the point-of-sale includes means for consummating a check transaction.

33. The method of claim 32 wherein the point-of-sale includes means for electronic check conversion.

34. The method of claim 31 wherein the point-of-sale includes means for consummating a data card transaction.

35. The method of claim 31 wherein the point-of-sale includes means for displaying information pertaining to the financial transaction.

36. The method of claim 31 wherein the point-of-sale includes means for printing information pertaining to the financial transaction.

37. The method of claim 31 wherein the point-of-sale includes means for obtaining a signature associated with the financial transaction.

38. The method of claim 37 further including means for archiving the signature obtained at the point-of-sale.

39. The method of claim 38 further including means for retrieving the archived signature obtained at the point-of-sale.

40. The method of claim 39 further including means for displaying the archived signature obtained at the point-of-sale.

41. The method of claim 40 further including means for combining the archived signature with information pertaining to the financial transaction to generate a receipt of the financial transaction.

42. The method of claim 41 further including means for printing a receipt of the financial transaction.

43. The method of claim 31 wherein the network appliance is automatically configured upon initialization in accordance with information stored in the primary server and in the network appliance.

44. The method of claim 43 wherein the network appliance configuration incorporates information to be printed on a receipt at the point-of-sale.

45. The method of claim 43 wherein the network appliance configuration includes mapping a dynamic network address into a fixed network address that is expected by the primary server.

46. The method of claim 43 wherein the network appliance configuration includes setting a date and a time at the network appliance from the primary server to ensure the integrity of the financial transaction to be consummated.

47. The method of claim 43 wherein the network appliance configuration includes establishing the functionality of the network appliance.

48. The method of claim 47 wherein establishing the functionality of the network appliance includes downloading modules to accomplish a revision update.

49. The method of claim 47 wherein establishing the functionality of the network appliance includes correcting a corrupted software configuration through downloading an uncorrupted module.

50. The method of claim 47 wherein establishing the functionality of the network appliance includes adding a new feature.

51. The method of claim 47 wherein establishing the functionality of the network appliance includes configuring the network appliance to function as means for delivering application service provider capabilities embodied in the primary server.

52. The method of claim 47 wherein establishing the functionality of the network appliance includes configuring the network appliance to function as means for delivering application service provider capabilities embodied in an ancillary server.

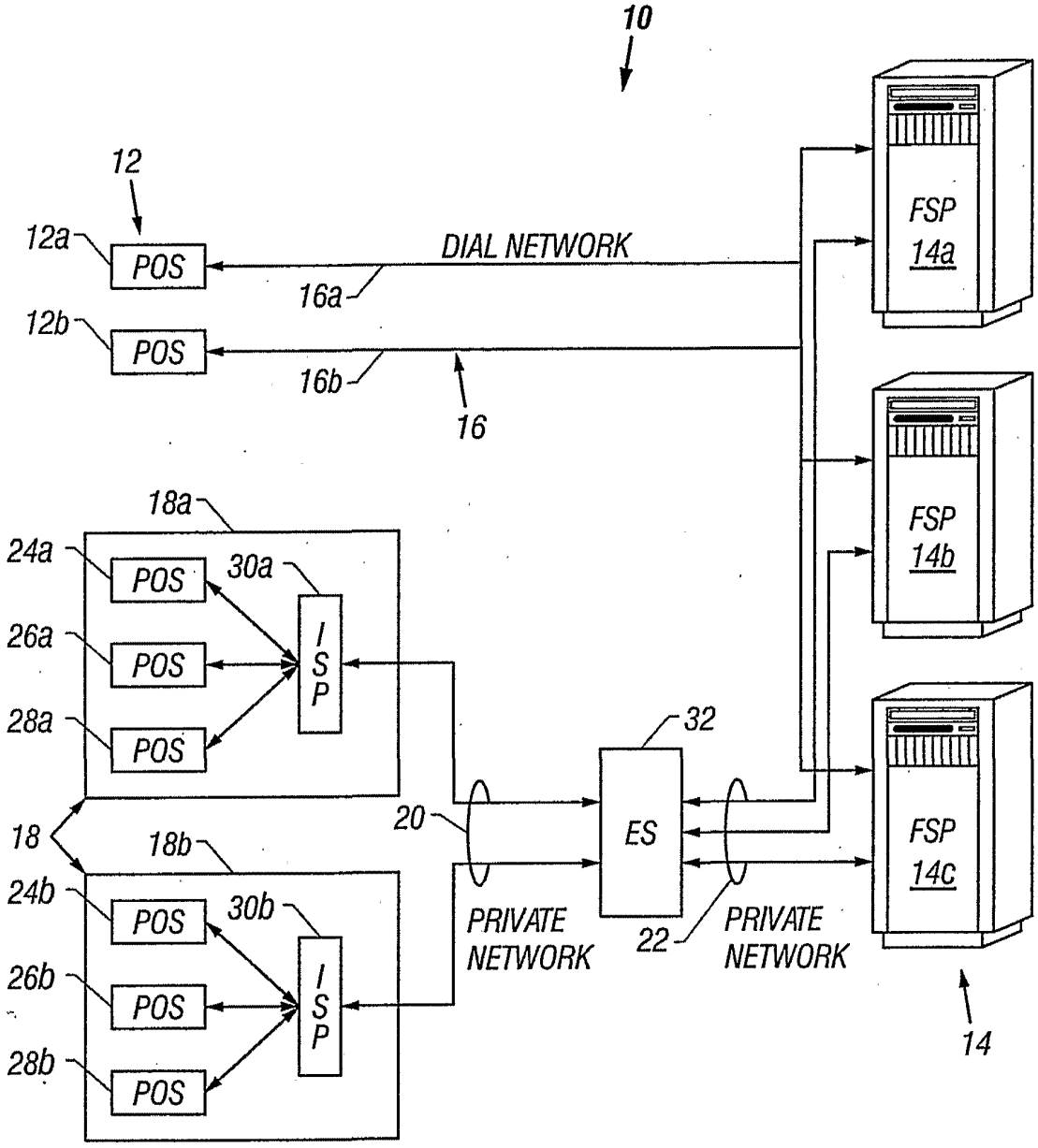


FIG. 1
(Prior Art)

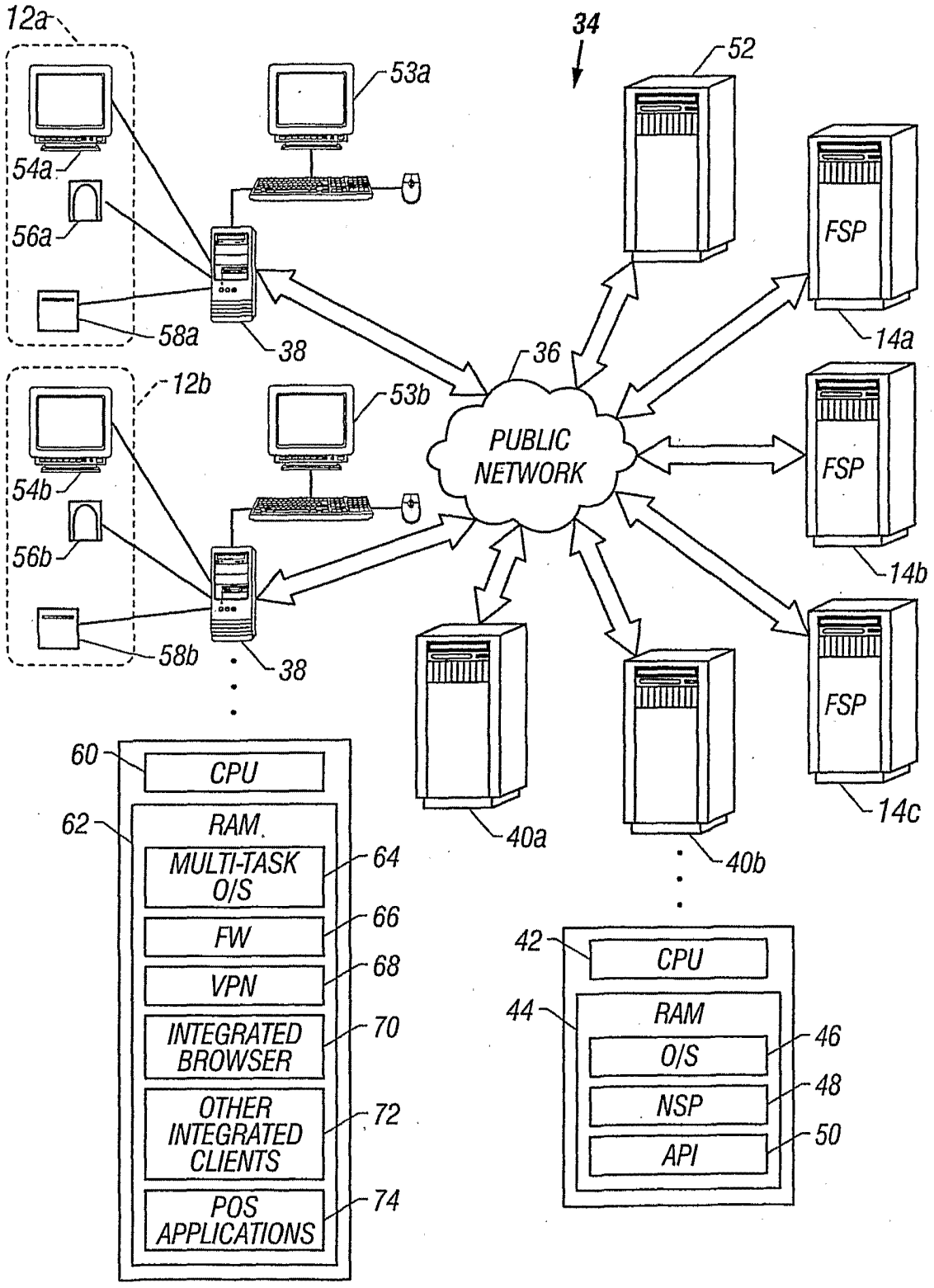

12a
34
52
53a
54a
56a
58a
38
36
FSP
14a
12b
53b
PUBLIC NETWORK
54b
56b
58b
38
FSP
14b
FSP
14c
40a
40b
60
CPU
62
RAM
MULTI-TASK O/S
64
FW
66
VPN
68
INTEGRATED BROWSER
70
OTHER INTEGRATED CLIENTS
72
POS APPLICATIONS
74
42
CPU
44
RAM
O/S
46
NSP
48
API
50

FIG. 2

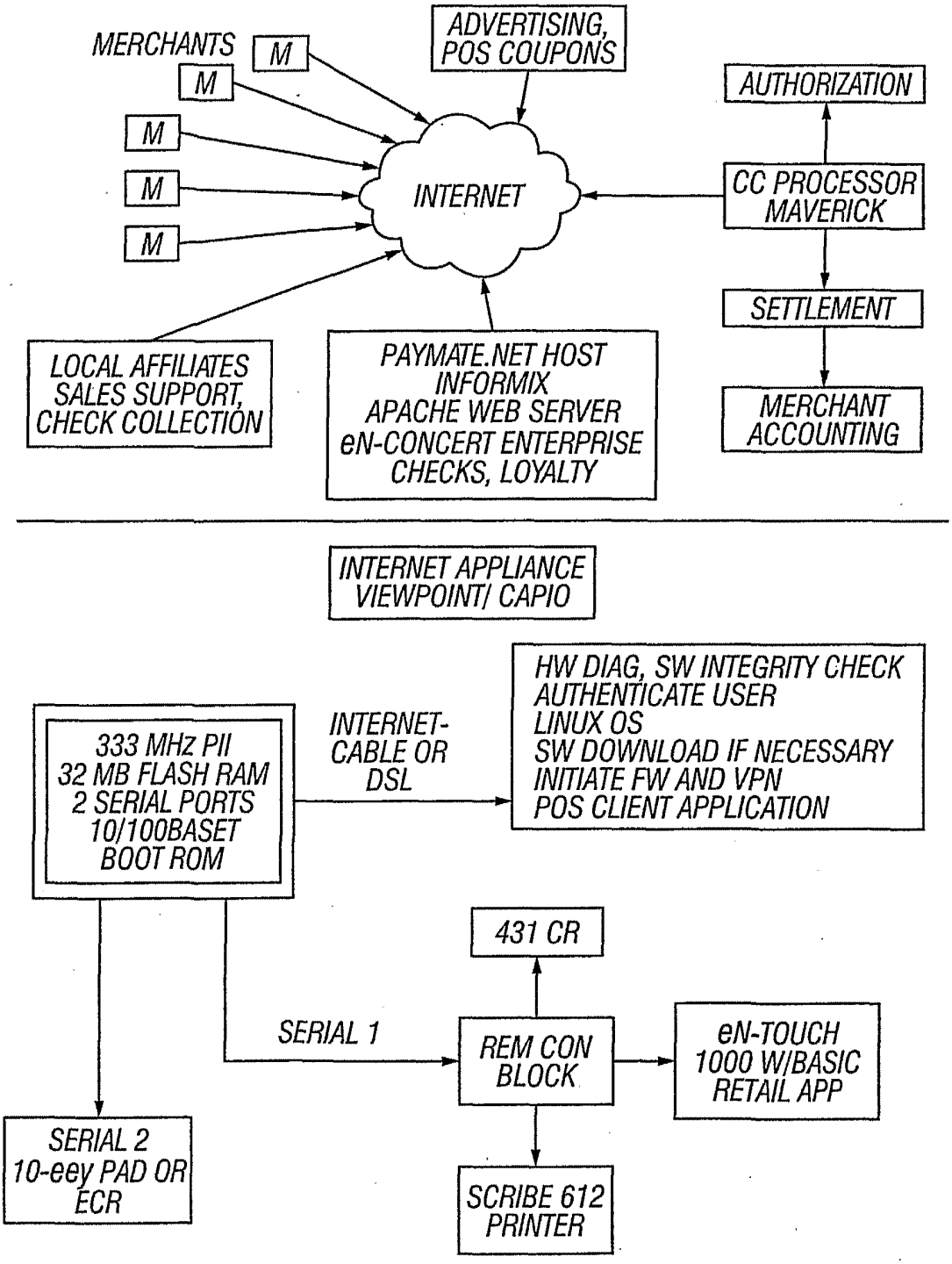

MERCHANTS
M
M
M
M
M
ADVERTISING, POS COUPONS
INTERNET
AUTHORIZATION
CC PROCESSOR MAVERICK
SETTLEMENT
MERCHANT ACCOUNTING
LOCAL AFFILIATES SALES SUPPORT, CHECK COLLECTION
PAYMATE.NET HOST INFORMIX APACHE WEB SERVER eN-CONCERT ENTERPRISE CHECKS, LOYALTY
INTERNET APPLIANCE VIEWPOINT/ CAPIO
333 MHz PII 32 MB FLASH RAM 2 SERIAL PORTS 10/100BASET BOOT ROM
INTERNET- CABLE OR DSL
HW DIAG, SW INTEGRITY CHECK AUTHENTICATE USER LINUX OS SW DOWNLOAD IF NECESSARY INITIATE FW AND VPN POS CLIENT APPLICATION
431 CR
SERIAL 1
REM CON BLOCK
eN-TOUCH 1000 W/BASIC RETAIL APP
SERIAL 2 10-eey PAD OR ECR
SCRIBE 612 PRINTER

FIG. 3

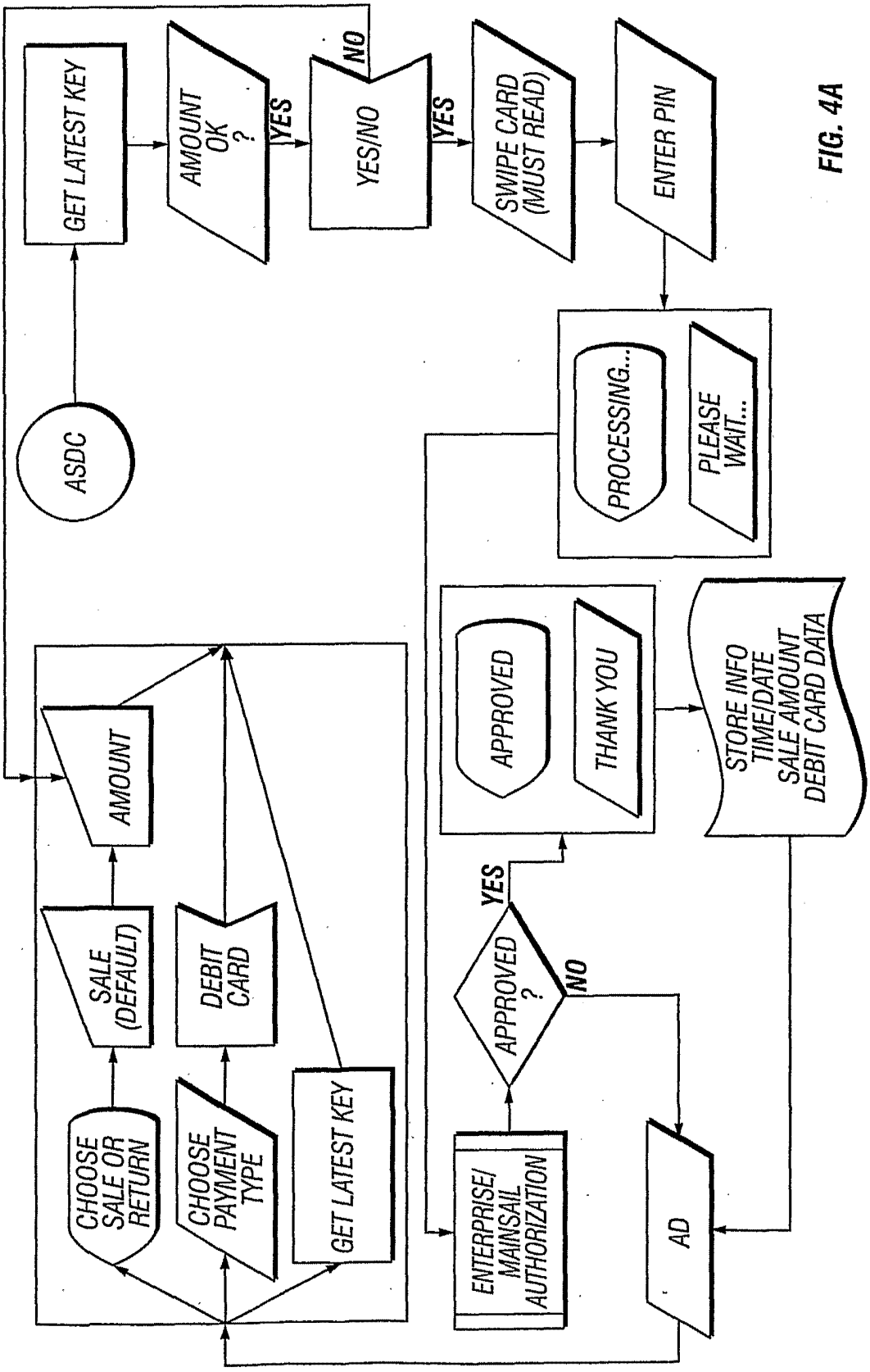

ASDC
GET LATEST KEY
AMOUNT OK ?
YES
NO
YES/NO
YES
SWIPE CARD (MUST READ)
ENTER PIN
PROCESSING...
PLEASE WAIT...
APPROVED
THANK YOU
STORE INFO TIME/DATE SALE AMOUNT DEBIT CARD DATA
AMOUNT
SALE (DEFAULT)
DEBIT CARD
CHOOSE SALE OR RETURN
CHOOSE PAYMENT TYPE
GET LATEST KEY
YES
APPROVED ?
NO
ENTERPRISE/ MAINSAIL AUTHORIZATION
AD

FIG. 4A

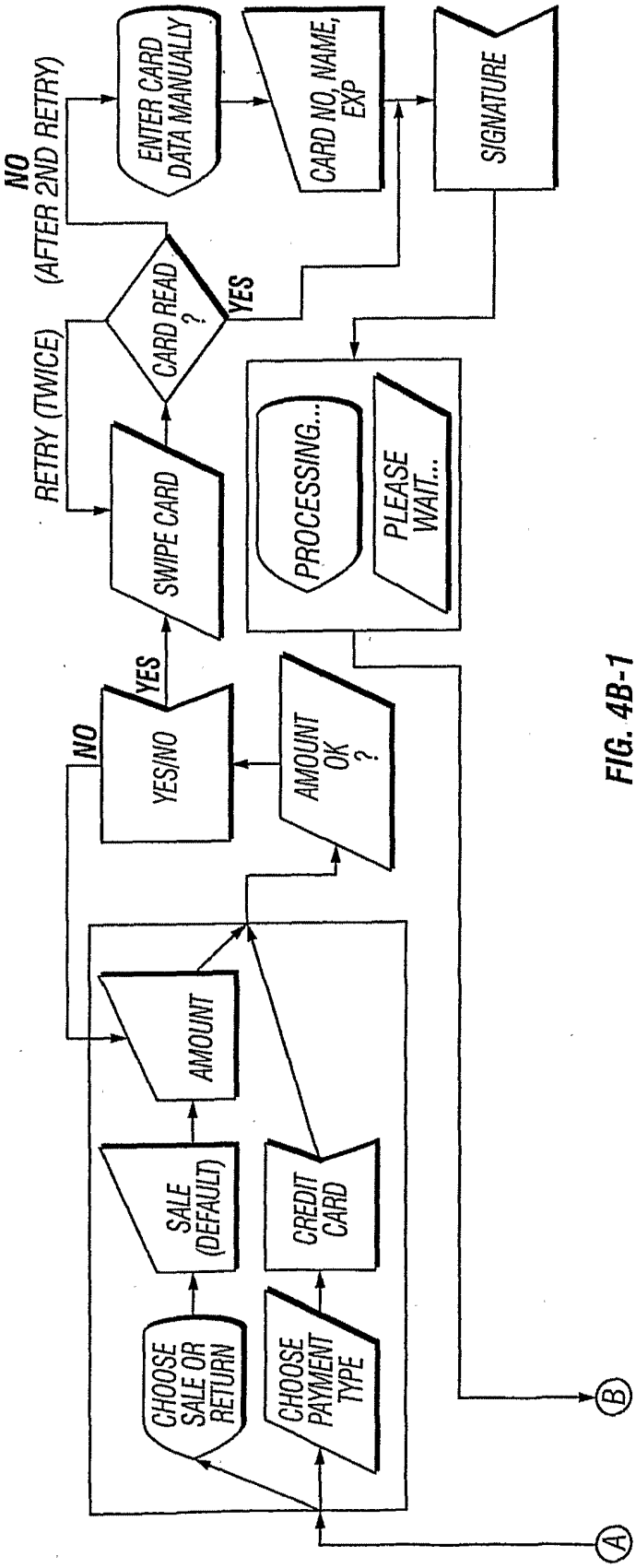

CHOOSE SALE OR RETURN
CHOOSE PAYMENT TYPE
SALE (DEFAULT)
CREDIT CARD
AMOUNT
AMOUNT OK ?
YES/NO
NO
YES
SWIPE CARD
RETRY (TWICE)
CARD READ ?
NO (AFTER 2ND RETRY)
YES
ENTER CARD DATA MANUALLY
CARD NO, NAME, EXP
SIGNATURE
PROCESSING...
PLEASE WAIT...
A
B

FIG. 4B-1

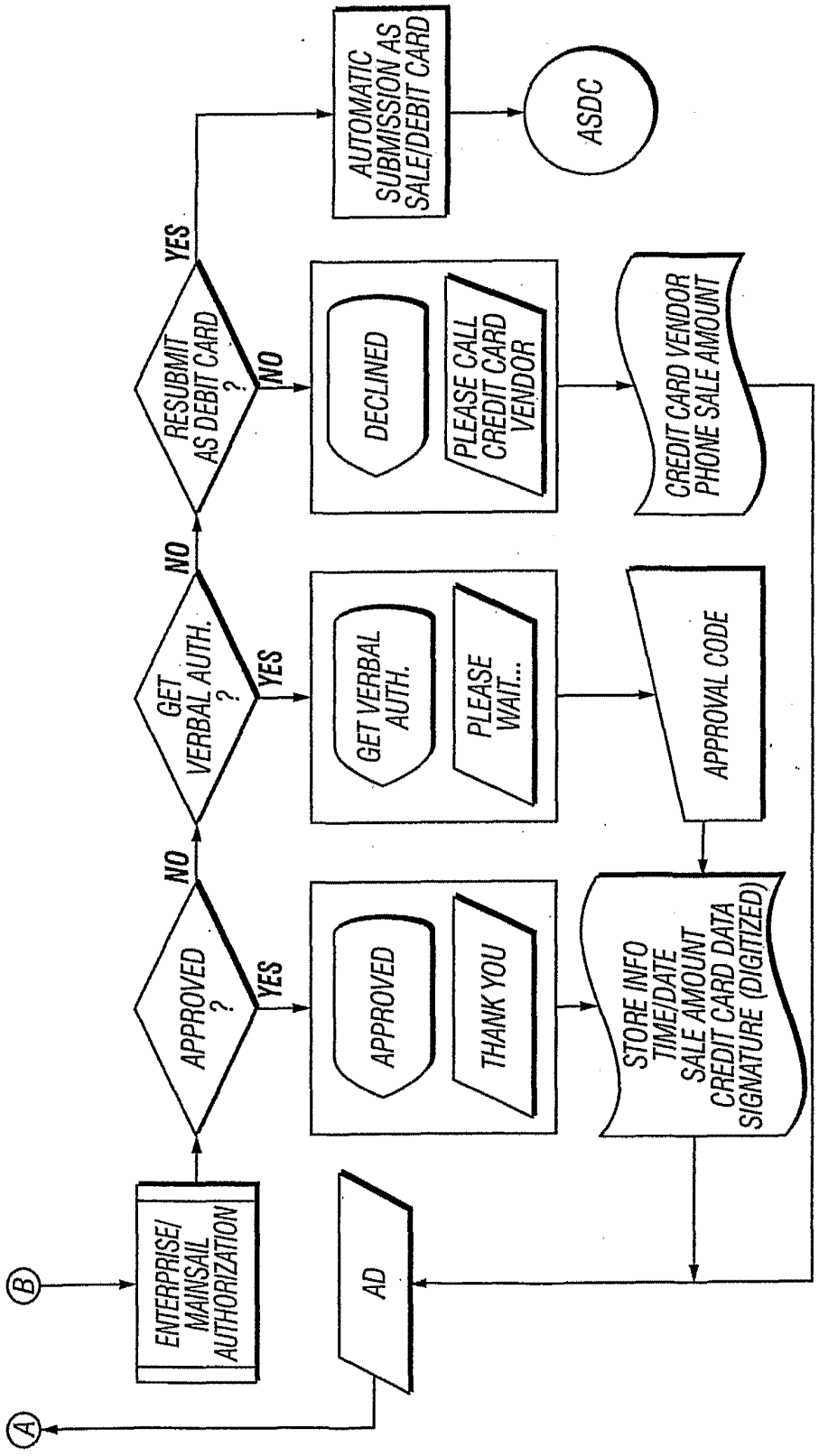

B
A
ENTERPRISE/ MAINSAIL AUTHORIZATION
AD
APPROVED ?
YES
NO
APPROVED
THANK YOU
GET VERBAL AUTH. ?
YES
NO
GET VERBAL AUTH.
PLEASE WAIT...
RESUBMIT AS DEBIT CARD ?
YES
NO
DECLINED
PLEASE CALL CREDIT CARD VENDOR
AUTOMATIC SUBMISSION AS SALE/DEBIT CARD
ASDC
APPROVAL CODE
CREDIT CARD VENDOR PHONE SALE AMOUNT
STORE INFO TIME/DATE SALE AMOUNT CREDIT CARD DATA SIGNATURE (DIGITIZED)

FIG. 4B-2

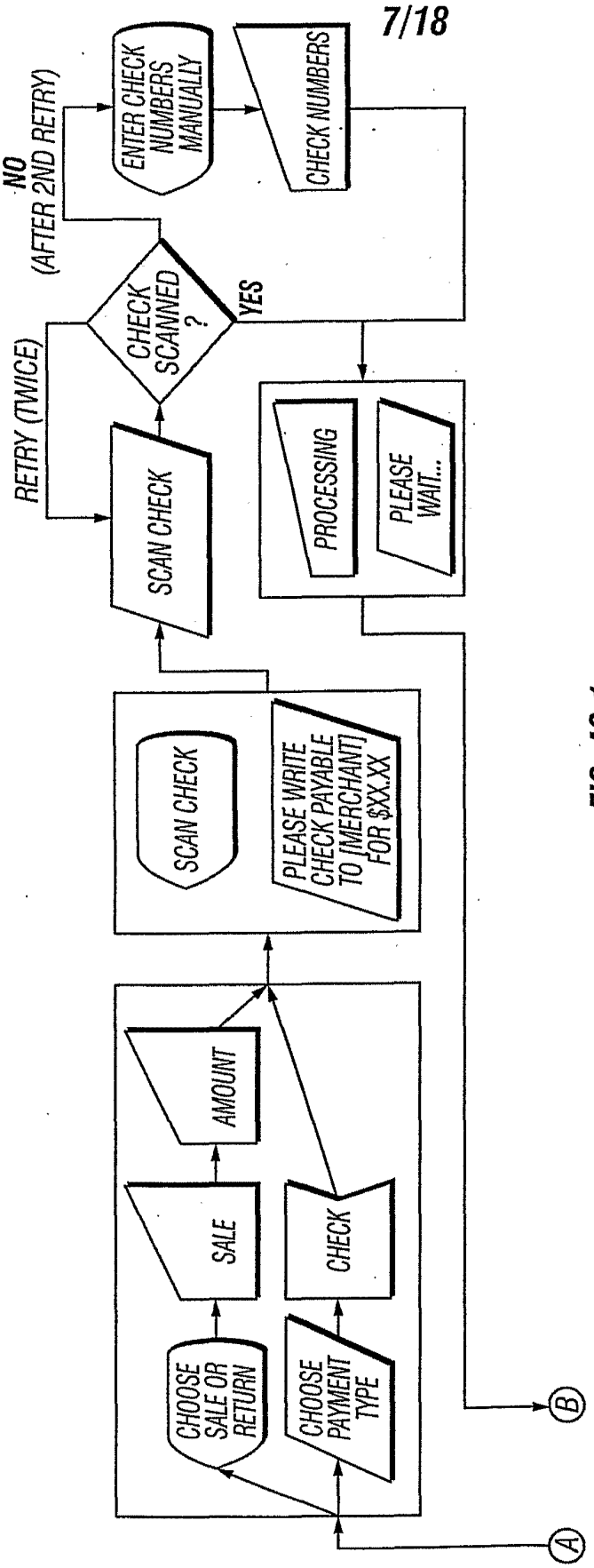

CHOOSE SALE OR RETURN
CHOOSE PAYMENT TYPE
SALE
CHECK
AMOUNT
SCAN CHECK
PLEASE WRITE CHECK PAYABLE TO [MERCHANT] FOR $XX.XX
SCAN CHECK
PROCESSING
PLEASE WAIT...
CHECK SCANNED ?
YES
NO (AFTER 2ND RETRY)
RETRY (TWICE)
ENTER CHECK NUMBERS MANUALLY
CHECK NUMBERS
A
B

FIG. 4C-1

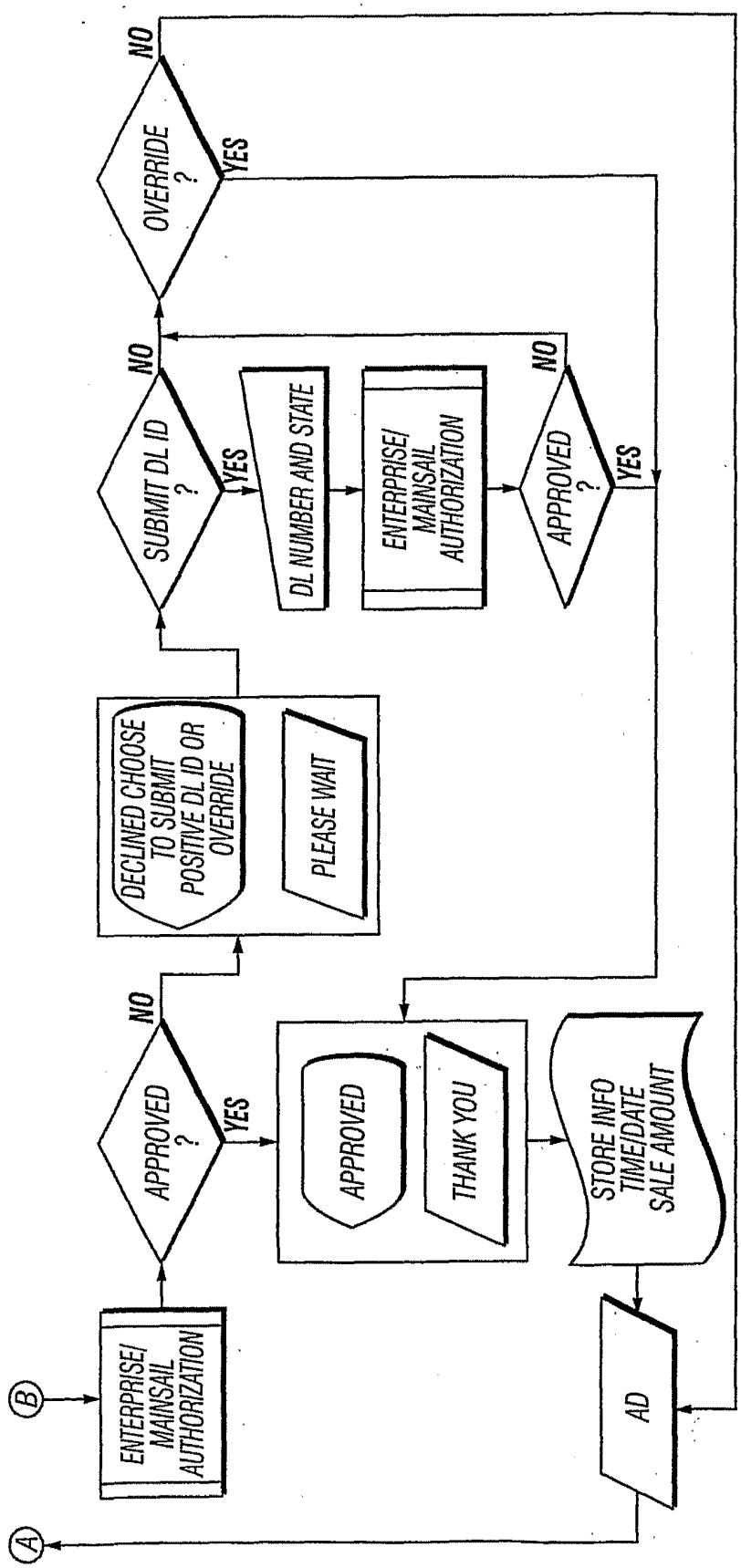

B
ENTERPRISE/ MAINSAIL AUTHORIZATION
APPROVED ?
NO
YES
DECLINED CHOOSE TO SUBMIT POSITIVE DL ID OR OVERRIDE
PLEASE WAIT
SUBMIT DL ID ?
NO
YES
DL NUMBER AND STATE
ENTERPRISE/ MAINSAIL AUTHORIZATION
APPROVED ?
NO
YES
OVERRIDE ?
NO
YES
APPROVED
THANK YOU
STORE INFO TIME/DATE SALE AMOUNT
AD
A

FIG. 4C-2

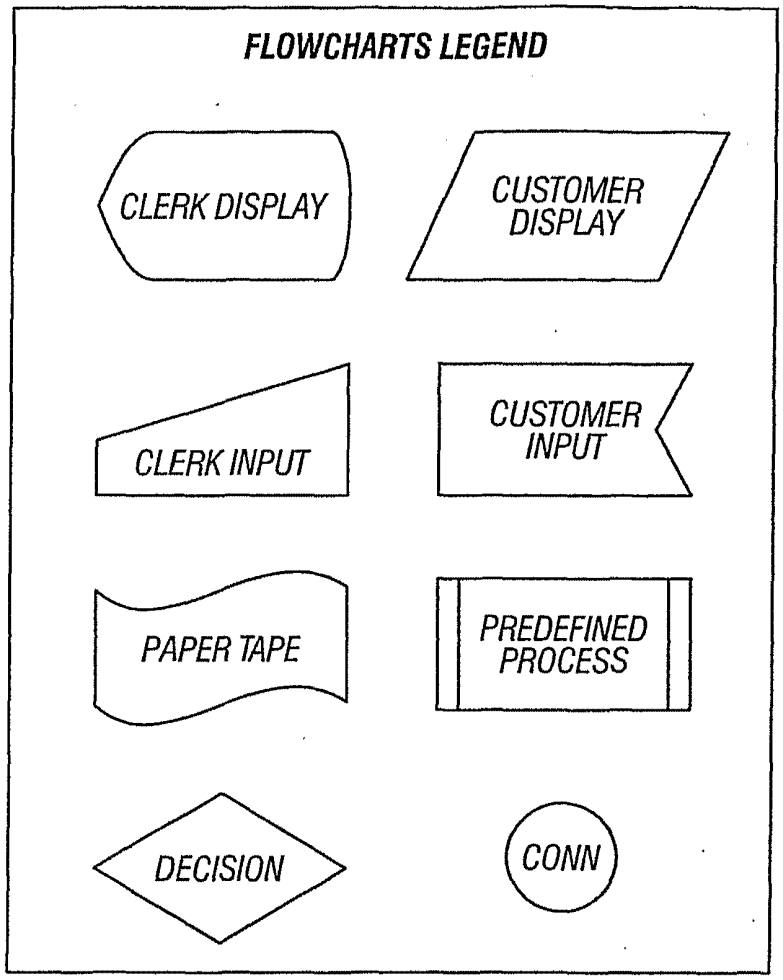

FLOWCHARTS LEGEND
CLERK DISPLAY
CUSTOMER DISPLAY
CLERK INPUT
CUSTOMER INPUT
PAPER TAPE
PREDEFINED PROCESS
DECISION
CONN

FIG. 4D

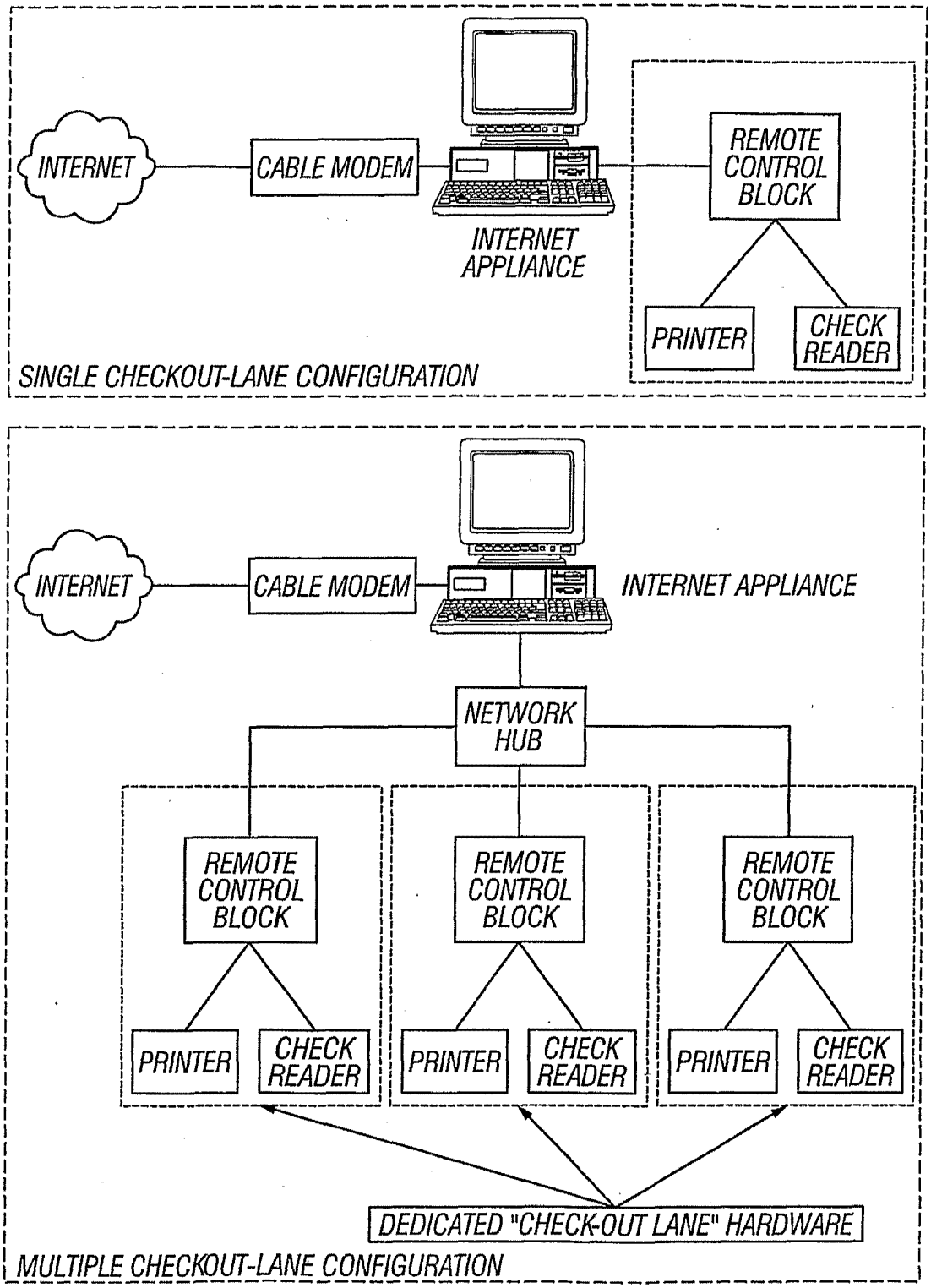

INTERNET
CABLE MODEM
INTERNET APPLIANCE
REMOTE CONTROL BLOCK
PRINTER
CHECK READER
SINGLE CHECKOUT-LANE CONFIGURATION
INTERNET
CABLE MODEM
INTERNET APPLIANCE
NETWORK HUB
REMOTE CONTROL BLOCK
REMOTE CONTROL BLOCK
REMOTE CONTROL BLOCK
PRINTER
CHECK READER
PRINTER
CHECK READER
PRINTER
CHECK READER
DEDICATED "CHECK-OUT LANE" HARDWARE
MULTIPLE CHECKOUT-LANE CONFIGURATION

FIG. 5

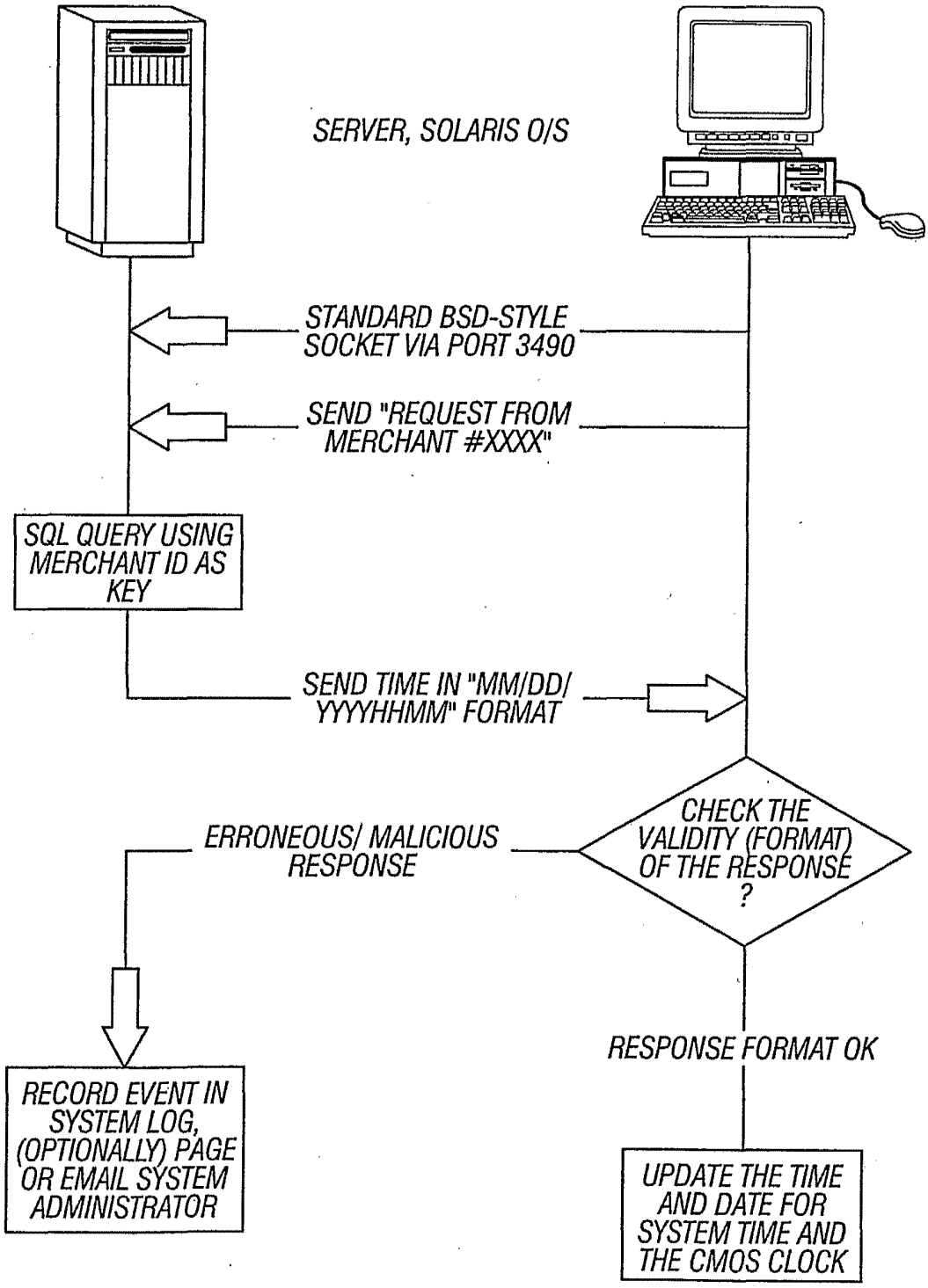

SERVER, SOLARIS O/S
STANDARD BSD-STYLE SOCKET VIA PORT 3490
SEND "REQUEST FROM MERCHANT #XXXX"
SQL QUERY USING MERCHANT ID AS KEY
SEND TIME IN "MM/DD/ YYYYHHMM" FORMAT
CHECK THE VALIDITY (FORMAT) OF THE RESPONSE ?
ERRONEOUS/ MALICIOUS RESPONSE
RESPONSE FORMAT OK
RECORD EVENT IN SYSTEM LOG, (OPTIONALLY) PAGE OR EMAIL SYSTEM ADMINISTRATOR
UPDATE THE TIME AND DATE FOR SYSTEM TIME AND THE CMOS CLOCK

FIG. 6

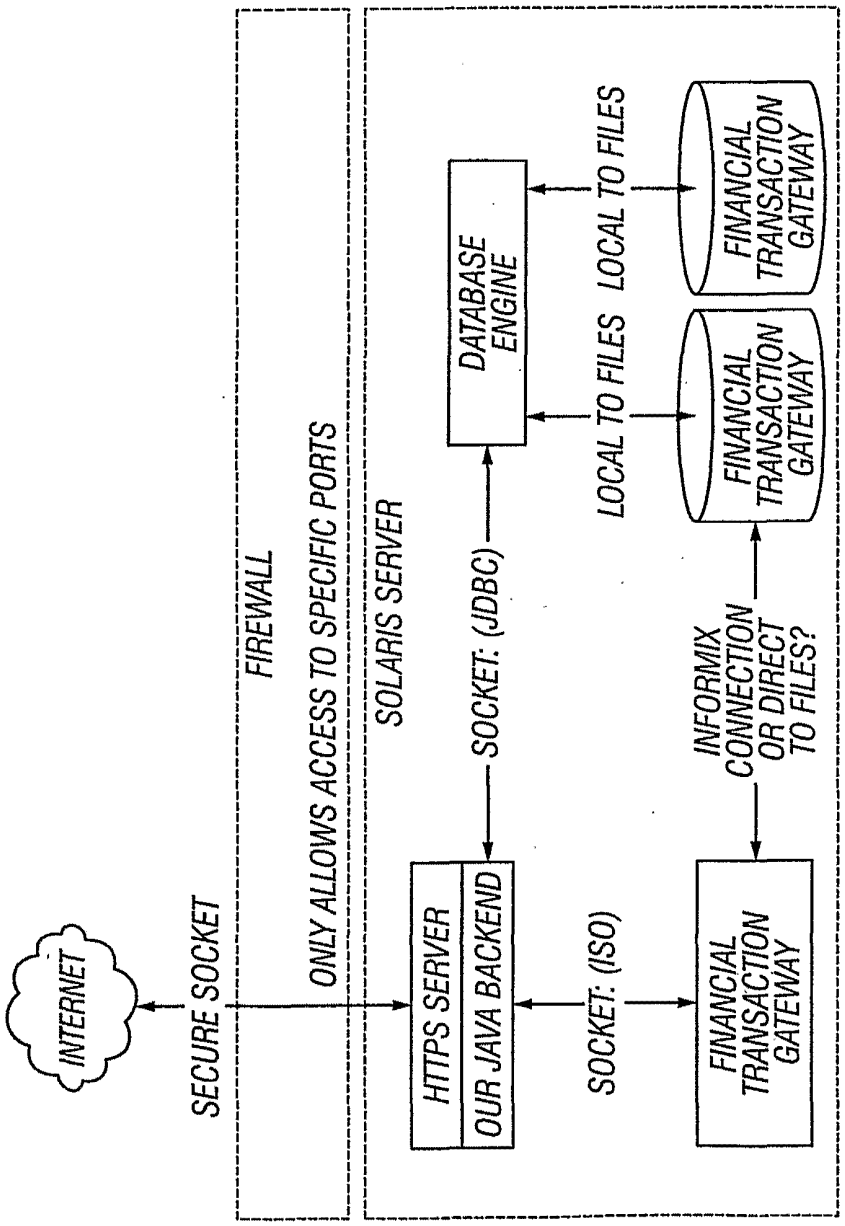

INTERNET
SECURE SOCKET
FIREWALL
ONLY ALLOWS ACCESS TO SPECIFIC PORTS
SOLARIS SERVER
HTTPS SERVER
OUR JAVA BACKEND
SOCKET: (JDBC)
DATABASE ENGINE
LOCAL TO FILES
FINANCIAL TRANSACTION GATEWAY
SOCKET: (ISO)
FINANCIAL TRANSACTION GATEWAY
INFORMIX CONNECTION OR DIRECT TO FILES?
LOCAL TO FILES
FINANCIAL TRANSACTION GATEWAY

FIG. 7

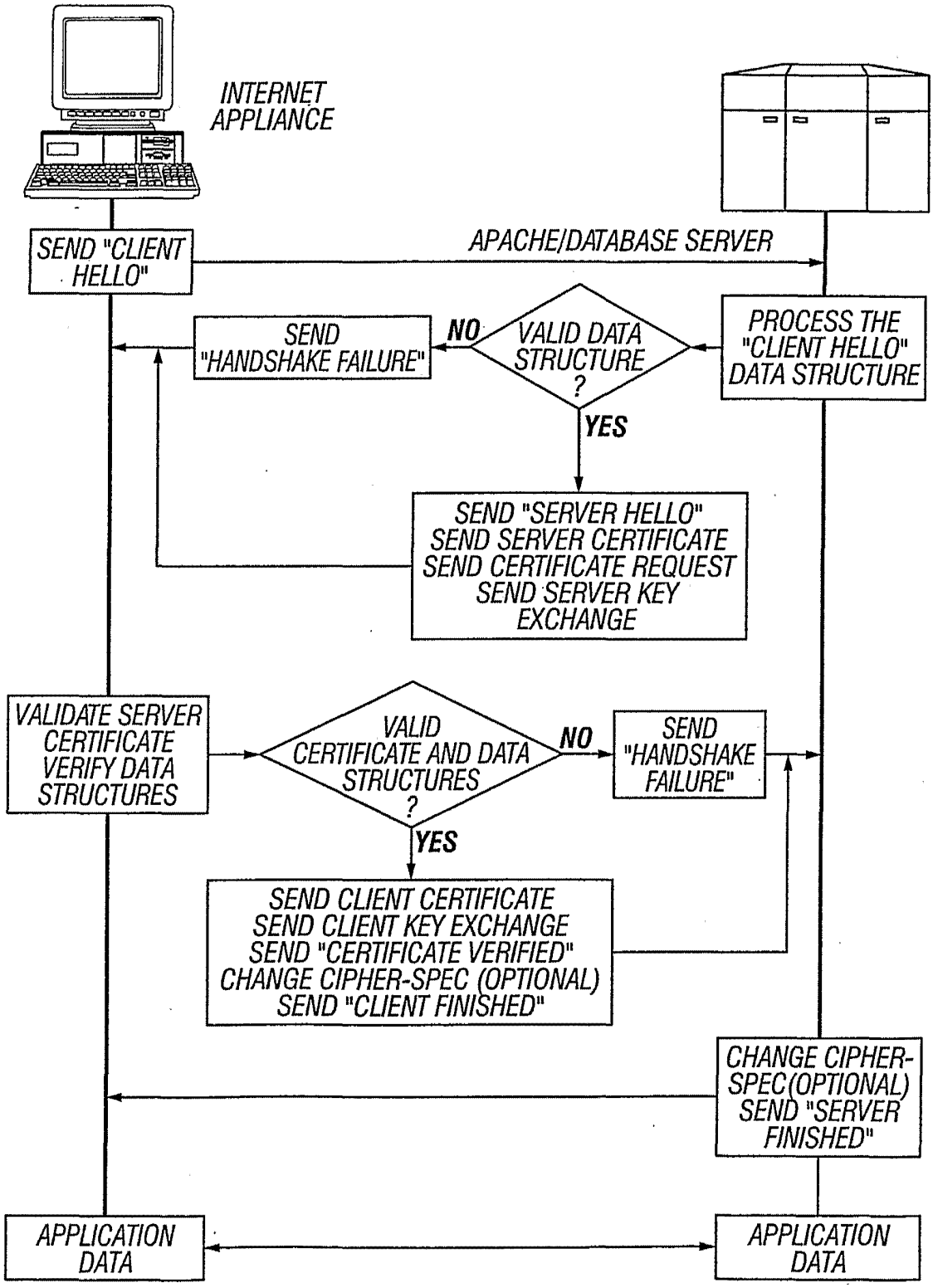

INTERNET APPLIANCE
APACHE/DATABASE SERVER
SEND "CLIENT HELLO"
PROCESS THE "CLIENT HELLO" DATA STRUCTURE
VALID DATA STRUCTURE ?
NO
SEND "HANDSHAKE FAILURE"
YES
SEND "SERVER HELLO"
SEND SERVER CERTIFICATE
SEND CERTIFICATE REQUEST
SEND SERVER KEY EXCHANGE
VALIDATE SERVER CERTIFICATE
VERIFY DATA STRUCTURES
VALID CERTIFICATE AND DATA STRUCTURES ?
NO
SEND "HANDSHAKE FAILURE"
YES
SEND CLIENT CERTIFICATE
SEND CLIENT KEY EXCHANGE
SEND "CERTIFICATE VERIFIED"
CHANGE CIPHER-SPEC (OPTIONAL)
SEND "CLIENT FINISHED"
CHANGE CIPHER-SPEC(OPTIONAL)
SEND "SERVER FINISHED"
APPLICATION DATA
APPLICATION DATA

FIG. 8

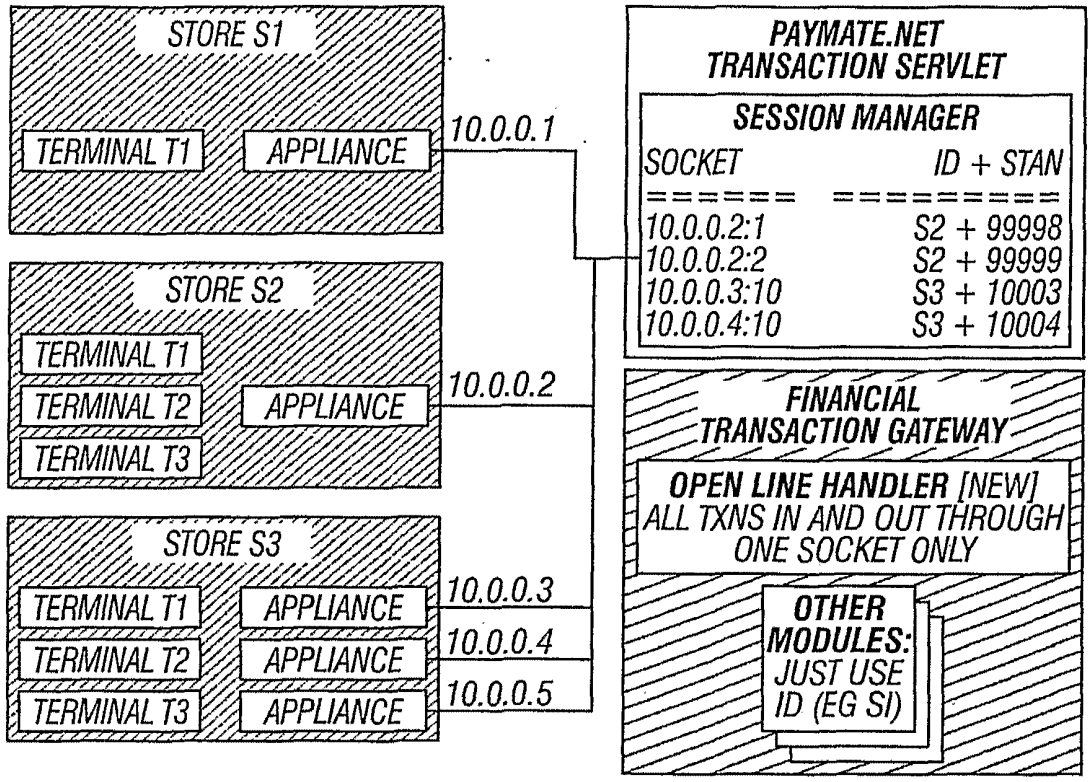


FIG. 9A

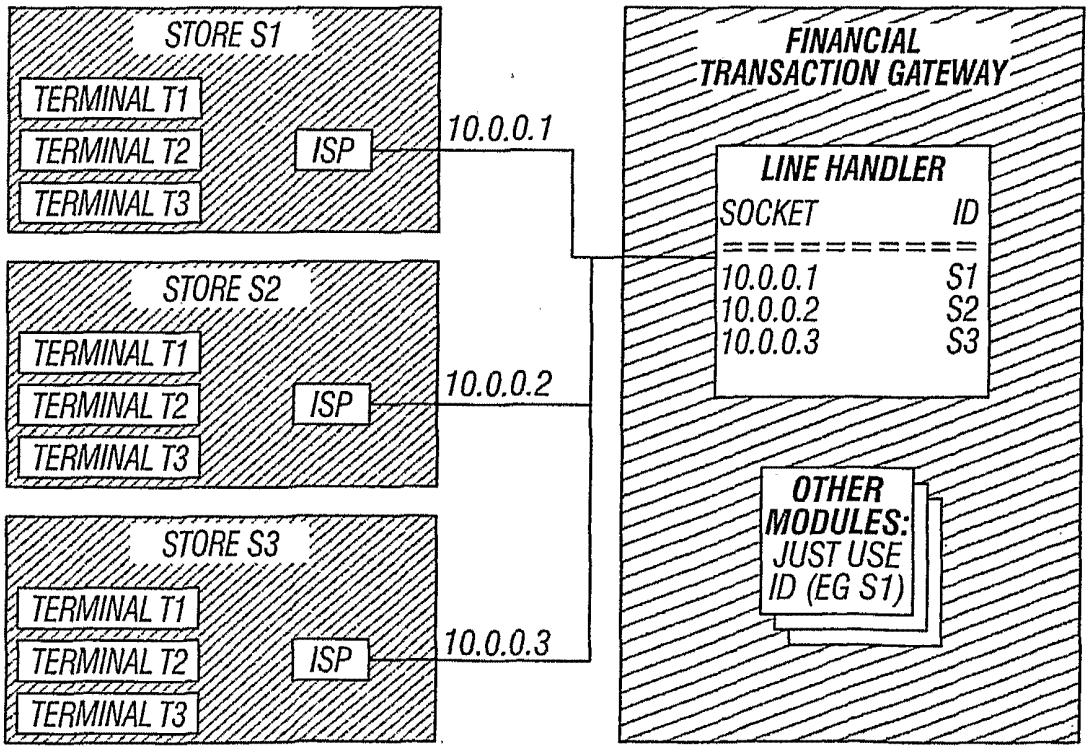


FIG. 9B
(Prior Art)

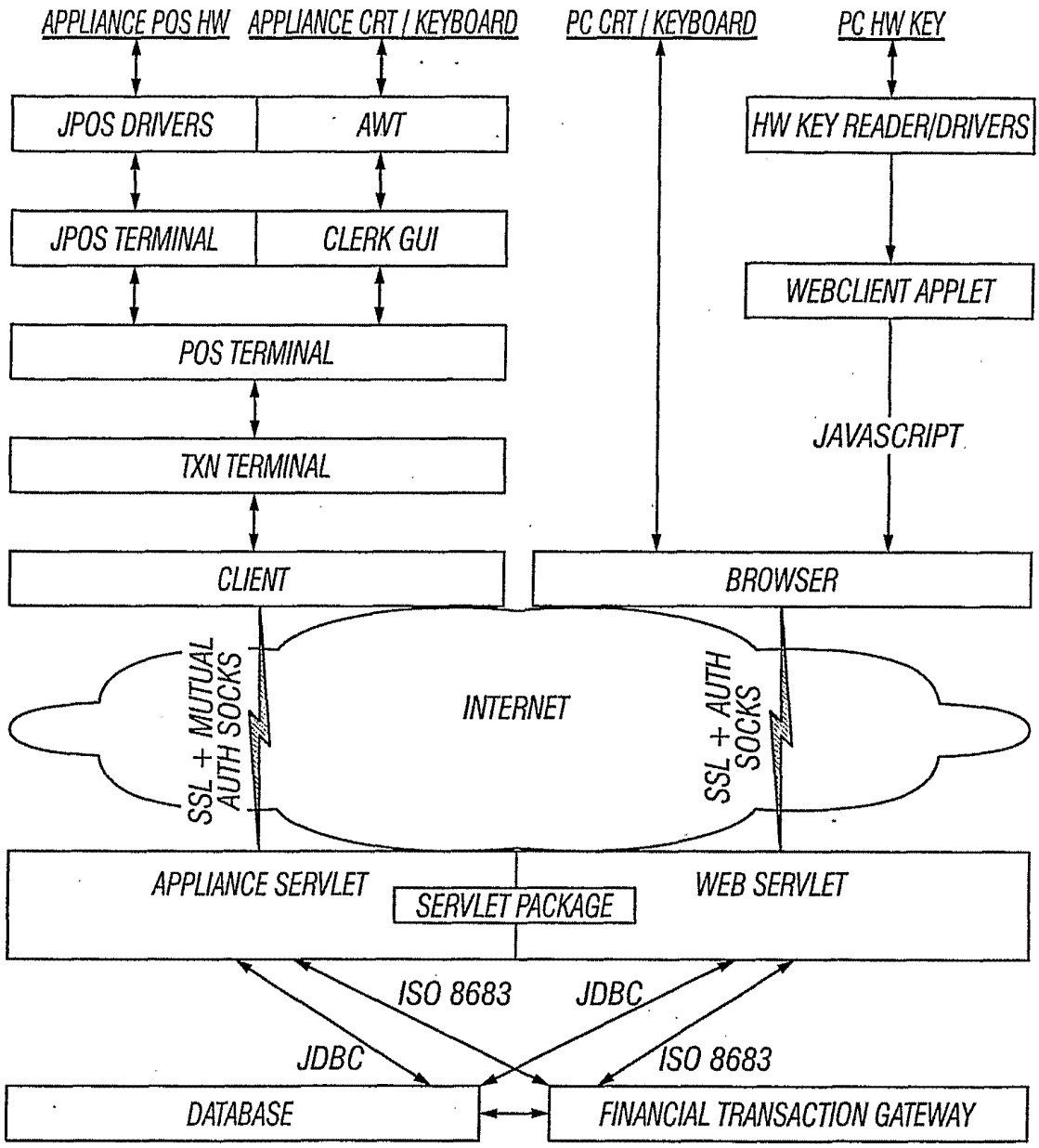

APPLIANCE POS HW
APPLIANCE CRT / KEYBOARD
PC CRT / KEYBOARD
PC HW KEY
JPOS DRIVERS
AWT
HW KEY READER/DRIVERS
JPOS TERMINAL
CLERK GUI
WEBCLIENT APPLET
POS TERMINAL
JAVASCRIPT
TXN TERMINAL
CLIENT
BROWSER
SSL + MUTUAL AUTH SOCKS
INTERNET
SSL + AUTH SOCKS
APPLIANCE SERVLET
SERVLET PACKAGE
WEB SERVLET
ISO 8683
JDBC
JDBC
ISO 8683
DATABASE
FINANCIAL TRANSACTION GATEWAY

FIG. 10

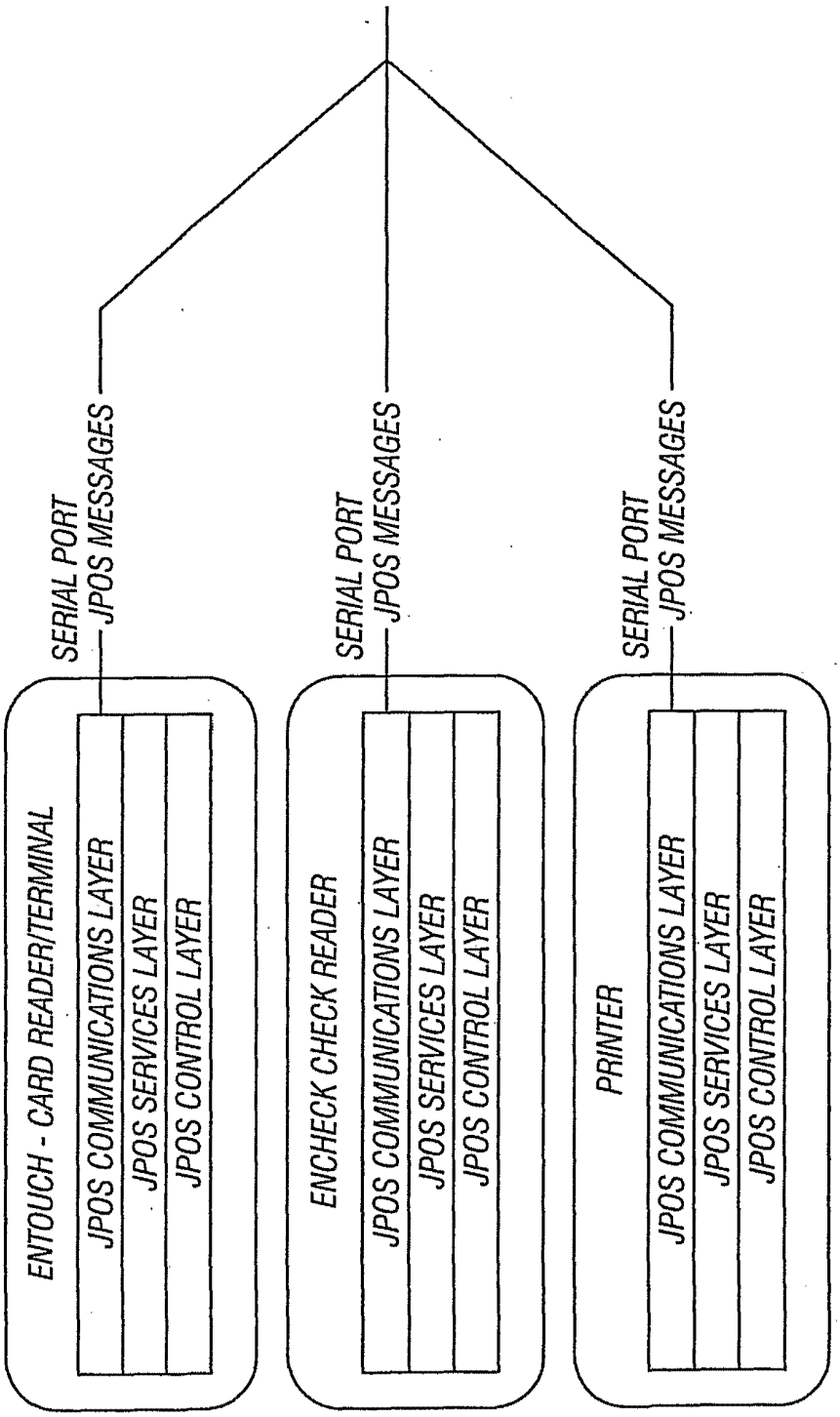

ENTOUCH - CARD READER/TERMINAL
JPOS COMMUNICATIONS LAYER
JPOS SERVICES LAYER
JPOS CONTROL LAYER
SERIAL PORT
JPOS MESSAGES
ENCHECK CHECK READER
JPOS COMMUNICATIONS LAYER
JPOS SERVICES LAYER
JPOS CONTROL LAYER
SERIAL PORT
JPOS MESSAGES
PRINTER
JPOS COMMUNICATIONS LAYER
JPOS SERVICES LAYER
JPOS CONTROL LAYER
SERIAL PORT
JPOS MESSAGES

FIG. 11A

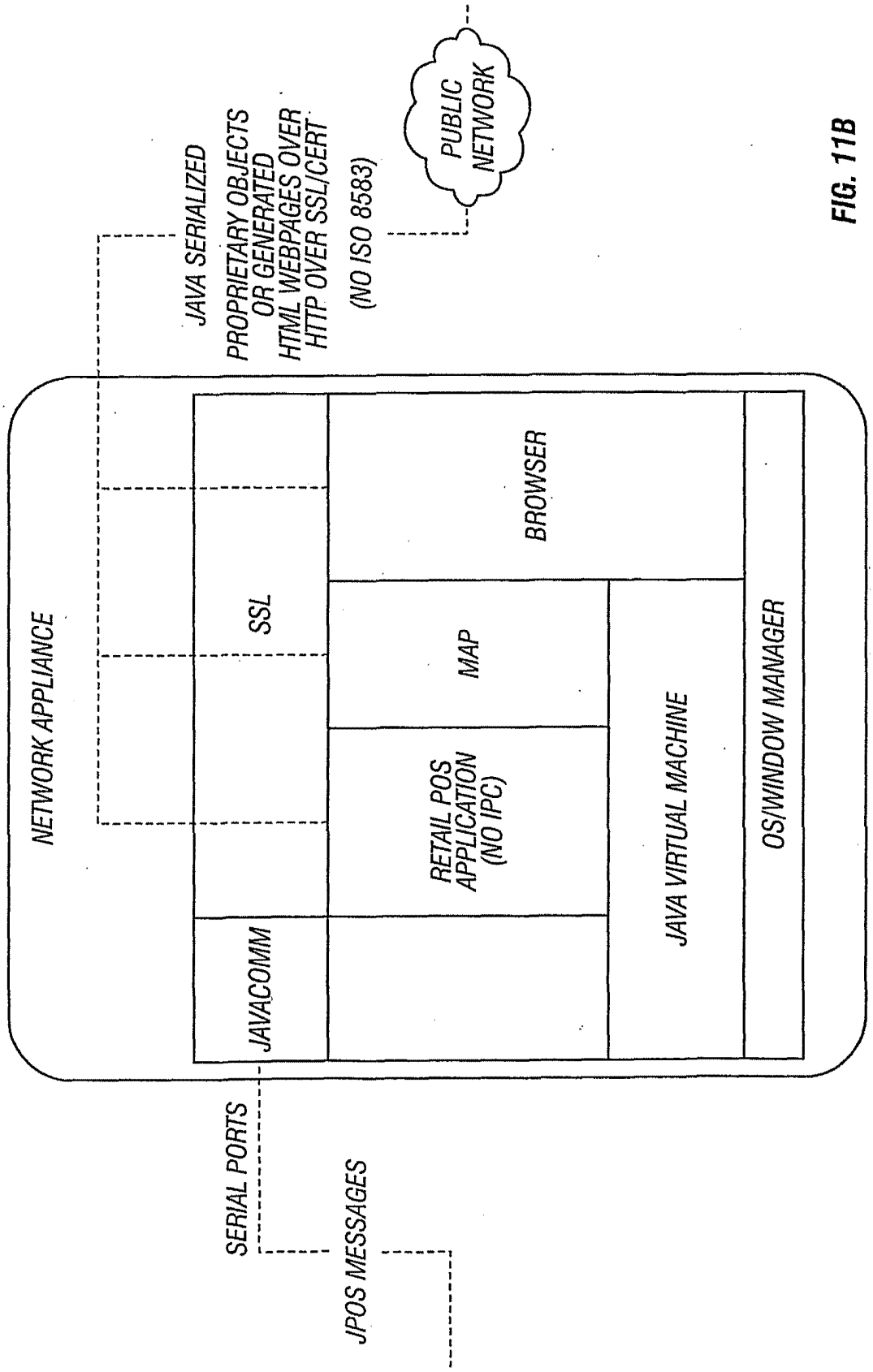

NETWORK APPLIANCE
JAVACOMM
SSL
RETAIL POS APPLICATION (NO IPC)
MAP
BROWSER
JAVA VIRTUAL MACHINE
OS/WINDOW MANAGER
SERIAL PORTS
JPOS MESSAGES
JAVA SERIALIZED PROPRIETARY OBJECTS OR GENERATED HTML WEBPAGES OVER HTTP OVER SSL/CERT
(NO ISO 8583)
PUBLIC NETWORK

FIG. 11B

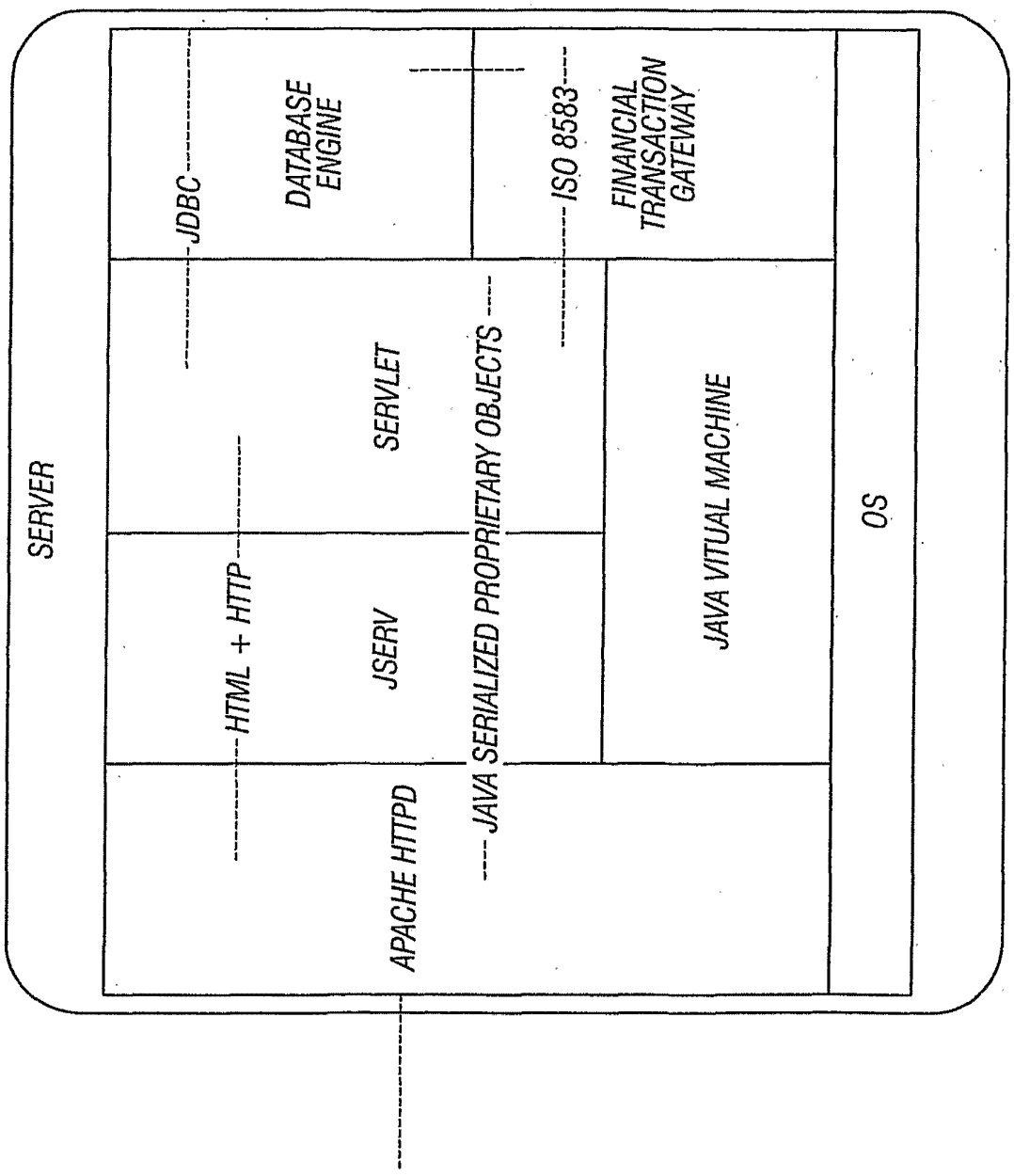

SERVER
JDBC
DATABASE ENGINE
ISO 8583
FINANCIAL TRANSACTION GATEWAY
HTML + HTTP
SERVLET
JAVA SERIALIZED PROPRIETARY OBJECTS
JSERV
JAVA VITUAL MACHINE
APACHE HTTPD
OS

FIG. 11C