Exhibit 5
Part 3
To Third Declaration of
Joseph N. Hosteny

US005910988A

United States Patent [19]

Ballard

[11] **Patent Number: 5,910,988**

[45] **Date of Patent: Jun. 8, 1999**

[54] **REMOTE IMAGE CAPTURE WITH CENTRALIZED PROCESSING AND STORAGE**

[75] Inventor: **Claudio R. Ballard**, Lloyd Harbor, N.Y.

[73] Assignee: **CSP Holdings, Inc.**, Lloyd Harbor, N.Y.

[21] Appl. No.: **08/917,761**

[22] Filed: **Aug. 27, 1997**

[51] **Int. Cl.**[6] **H04L 9/00**

[52] **U.S. Cl.** **380/24**

[58] **Field of Search** 380/25, 24

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,201,978	5/1980	Nally	340/146.3
4,264,808	4/1981	Owens et al.	235/379
4,326,258	4/1982	de la Guardia	364/515
4,417,136	11/1983	Rushby et al.	235/379
4,457,015	6/1984	Nally et al.	382/45
4,500,750	2/1985	Elander et al.	380/26
4,523,330	6/1985	Cain	382/7
4,555,617	11/1985	Brooks et al.	235/379
4,578,530	3/1986	Zeidler	380/26
4,602,936	7/1986	Green et al.	382/140
4,680,803	7/1987	Dilella	382/9
4,694,147	9/1987	Amemiya et al.	235/379
4,747,058	5/1988	Ho	364/478
4,750,201	6/1988	Hodgson et al.	379/144
4,843,220	6/1989	Haun	235/380
4,888,812	12/1989	Dinan et al.	382/7
4,912,762	3/1990	Lee et al.	380/24
4,926,325	5/1990	Benton et al.	364/408
4,960,981	10/1990	Benton et al.	235/379
5,091,968	2/1992	Higgins et al.	382/30
5,122,950	6/1992	Benton et al.	364/408
5,144,115	9/1992	Yoshida	235/379
5,159,548	10/1992	Caslavka	364/408
5,173,594	12/1992	McClure	235/380
5,175,682	12/1992	Higashiyama et al.	364/408
5,187,750	2/1993	Behera	382/7
5,204,811	4/1993	Bednar et al.	364/406
5,220,501	6/1993	Lawlor et al.	364/408
5,237,158	8/1993	Kern et al.	235/379
5,274,567	12/1993	Kallin et al.	364/478
5,283,829	2/1994	Anderson	380/24
5,321,238	6/1994	Kamata et al.	235/379
5,321,751	6/1994	Ray et al.	380/23
5,345,090	9/1994	Hludzinski	250/566
5,434,928	7/1995	Wagner et al.	382/187
5,436,970	7/1995	Ray et al.	380/23
5,444,794	8/1995	Uhland, Sr.	382/137
5,457,747	10/1995	Drexler et al.	380/24
5,479,510	12/1995	Olsen et al.	380/24
5,506,691	4/1996	Bednar et al.	358/402
5,544,043	8/1996	Miki et al.	364/406

(List continued on next page.)

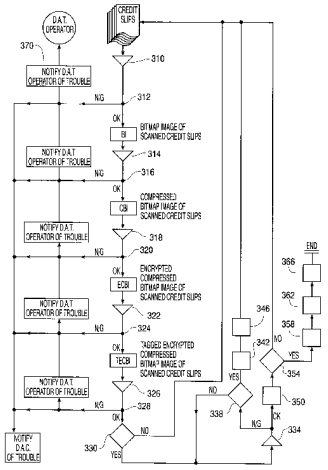
Primary Examiner—Salvatore Cangialosi

Attorney, Agent, or Firm—McGuire, Woods, Battle & Boothe LLP

[57] **ABSTRACT**

A system for remote data acquisition and centralized processing and storage is disclosed called the DataTreasury™ System. The DataTreasury™ System provides comprehensive support for the processing of documents and electronic data associated with different applications including sale, business, banking and general consumer transactions. The system retrieves transaction data at one or more remote Locations, encrypts the data, transmits the encrypted data to a central location, transforms the data to a usable form, performs identification verification using signature data and biometric data, generates informative reports from the data and transmits the informative reports to the remote location (s). The DataTreasury™ System has many advantageous features which work together to provide high performance, security, reliability, fault tolerance and low cost. First, the network architecture facilitates secure communication between the remote location(s) and the central processing facility. A dynamic address assignment algorithm performs load balancing among the system's servers for faster performance and higher utilization. Finally, a partitioning scheme improves the error correction process.

50 Claims, 10 Drawing Sheets



U.S. PATENT DOCUMENTS

5,590,038	12/1996	Pitroda	395/241
5,602,933	2/1997	Blackwell et al.	382/116
5,604,640	2/1997	Zipf et al.	359/803
5,613,001	3/1997	Bakhoum	380/4
5,647,017	7/1997	Smithies et al.	382/119
5,657,389	8/1997	Houvener	380/23
5,657,396	8/1997	Rudolph et al.	382/190
5,673,333	9/1997	Johnston	382/137
5,751,842	5/1998	Riach et al.	382/137
5,754,673	5/1998	Brooks et al.	382/112
5,781,654	7/1998	Carney	382/137
5,784,503	7/1998	Bleecker, III et al.	382/306
5,787,403	7/1998	Randle	705/43

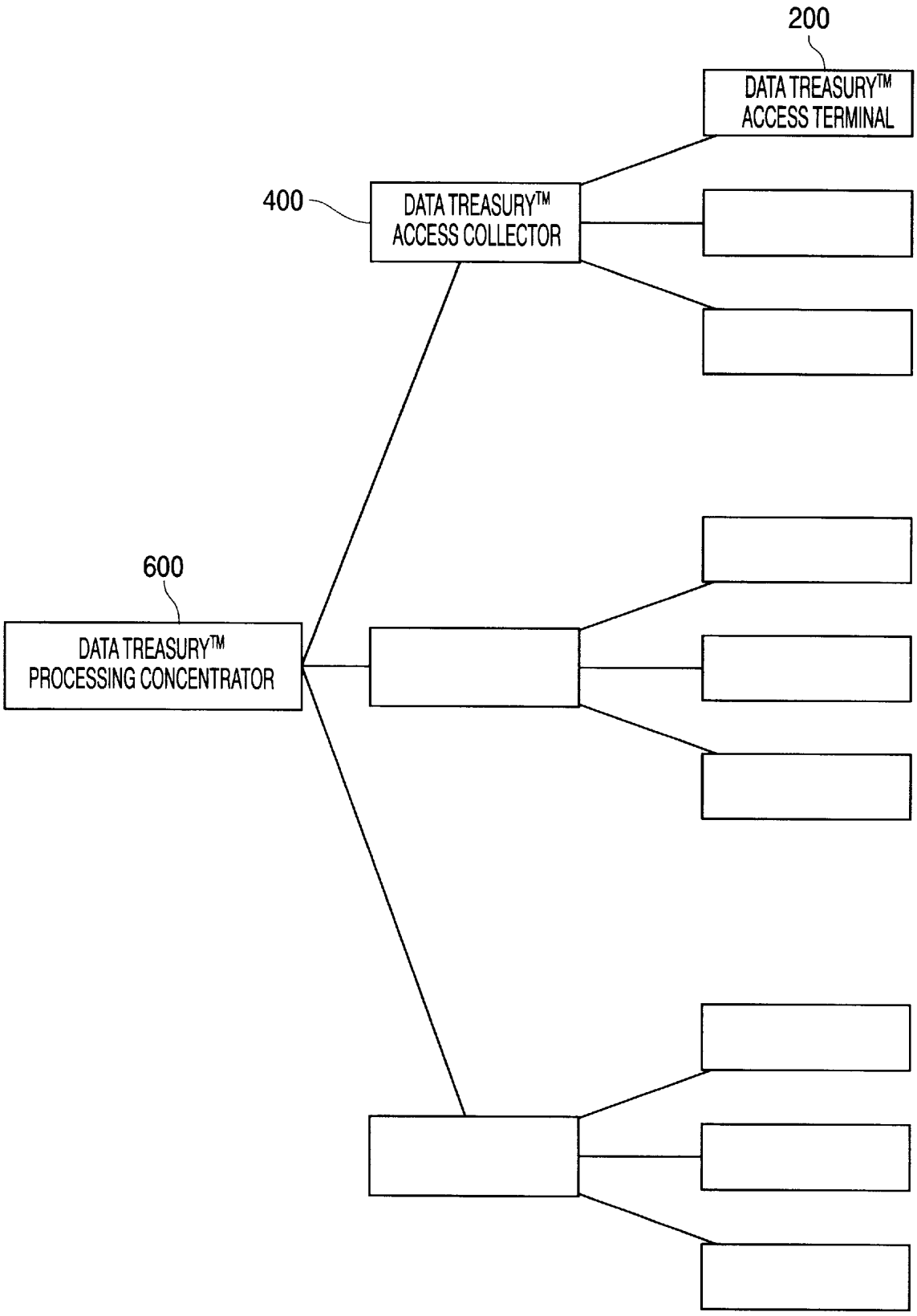

200
DATA TREASURY™ ACCESS TERMINAL
400
DATA TREASURY™ ACCESS COLLECTOR
600
DATA TREASURY™ PROCESSING CONCENTRATOR

FIG. 1

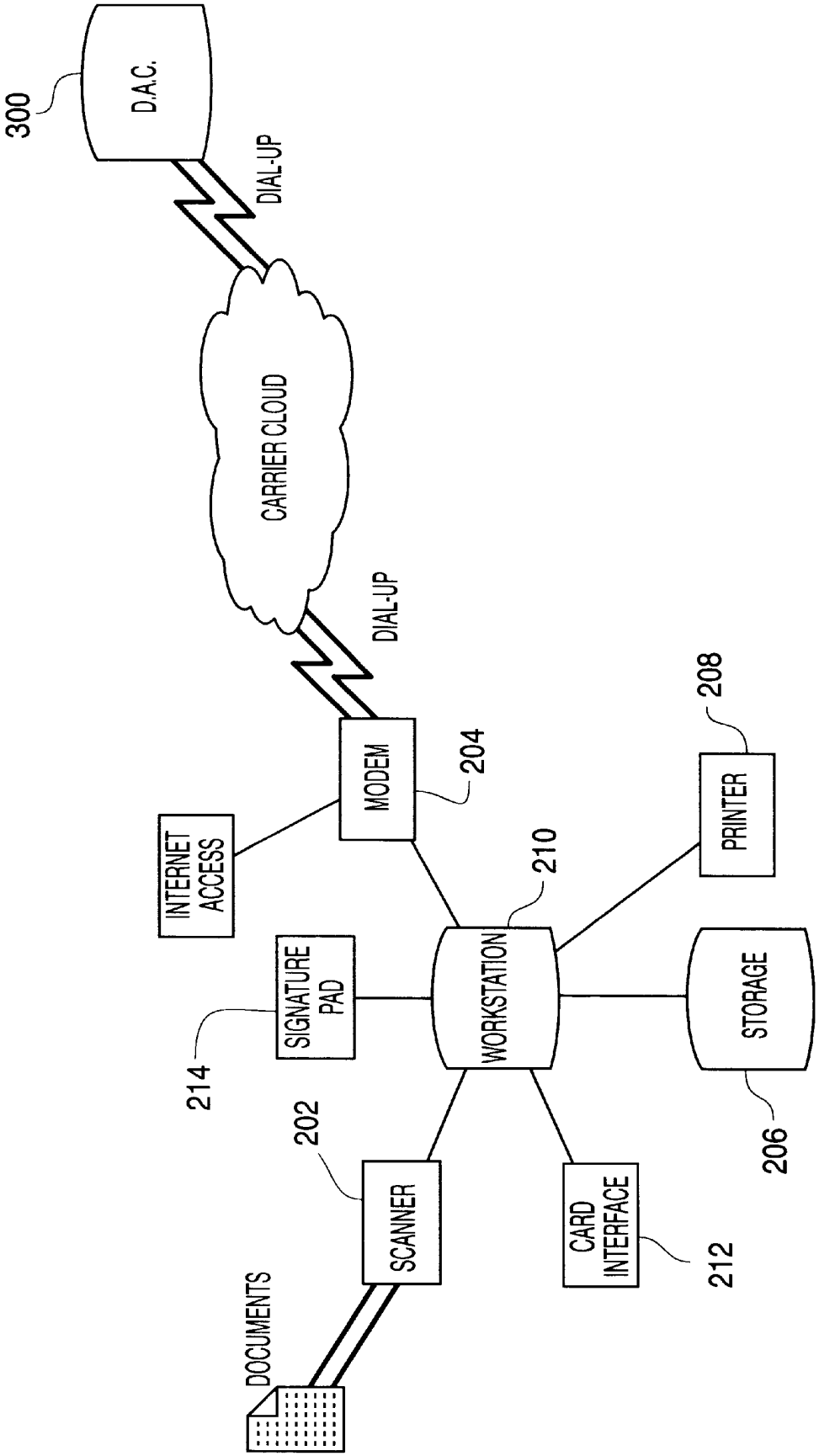

300
D.A.C.
DIAL-UP
CARRIER CLOUD
DIAL-UP
MODEM
204
INTERNET ACCESS
208
PRINTER
210
WORKSTATION
SIGNATURE PAD
214
STORAGE
206
202
SCANNER
CARD INTERFACE
212
DOCUMENTS

FIG. 2

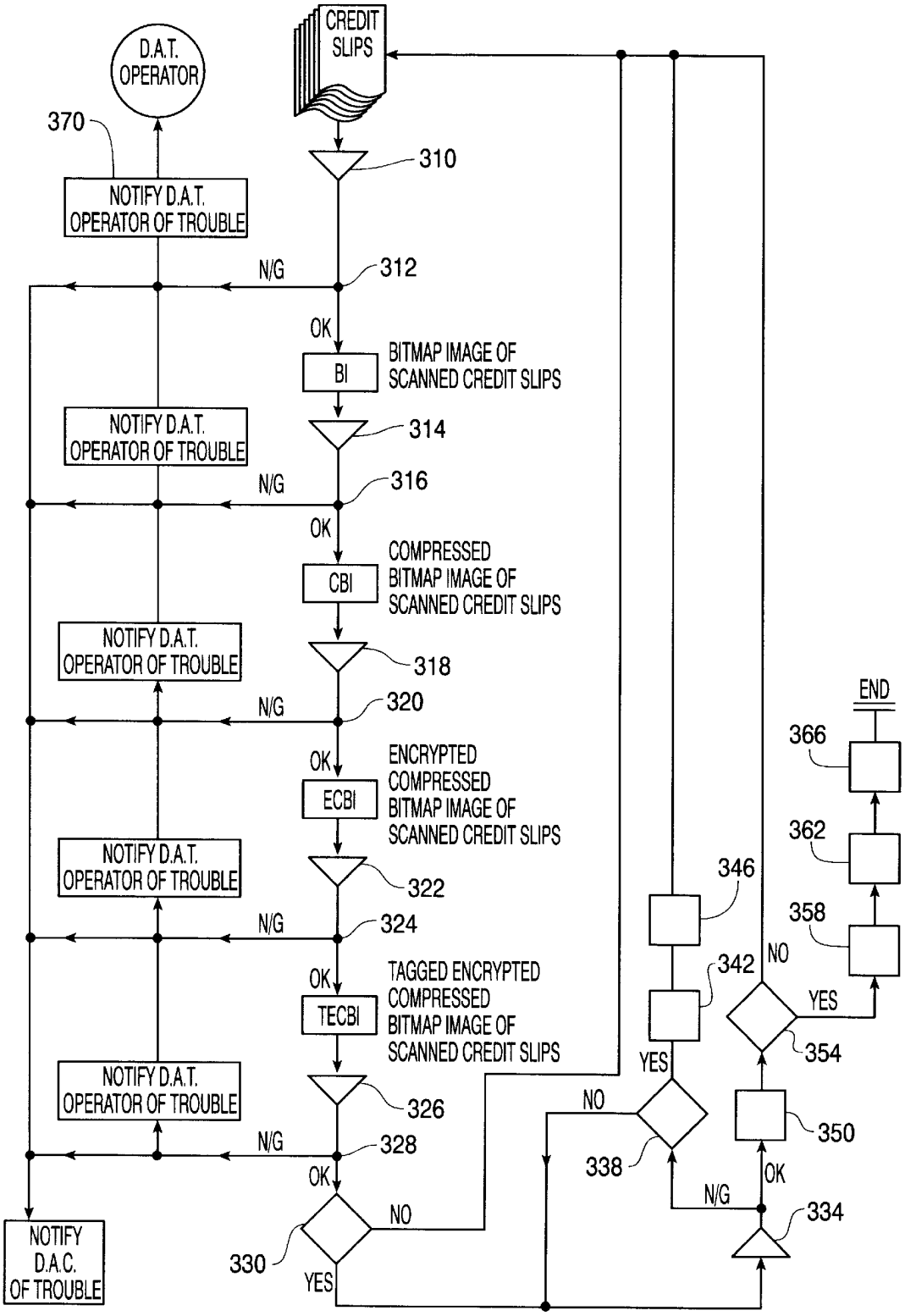

CREDIT SLIPS
D.A.T. OPERATOR
370
310
NOTIFY D.A.T. OPERATOR OF TROUBLE
N/G
312
OK
BI
BITMAP IMAGE OF SCANNED CREDIT SLIPS
NOTIFY D.A.T. OPERATOR OF TROUBLE
314
N/G
316
OK
CBI
COMPRESSED BITMAP IMAGE OF SCANNED CREDIT SLIPS
NOTIFY D.A.T. OPERATOR OF TROUBLE
318
N/G
320
OK
ECBI
ENCRYPTED COMPRESSED BITMAP IMAGE OF SCANNED CREDIT SLIPS
NOTIFY D.A.T. OPERATOR OF TROUBLE
322
N/G
324
OK
TECBI
TAGGED ENCRYPTED COMPRESSED BITMAP IMAGE OF SCANNED CREDIT SLIPS
NOTIFY D.A.T. OPERATOR OF TROUBLE
326
N/G
328
OK
NO
330
YES
NOTIFY D.A.C. OF TROUBLE
346
342
NO
YES
354
YES
NO
338
350
OK
N/G
334
END
366
362
358

FIG. 3A

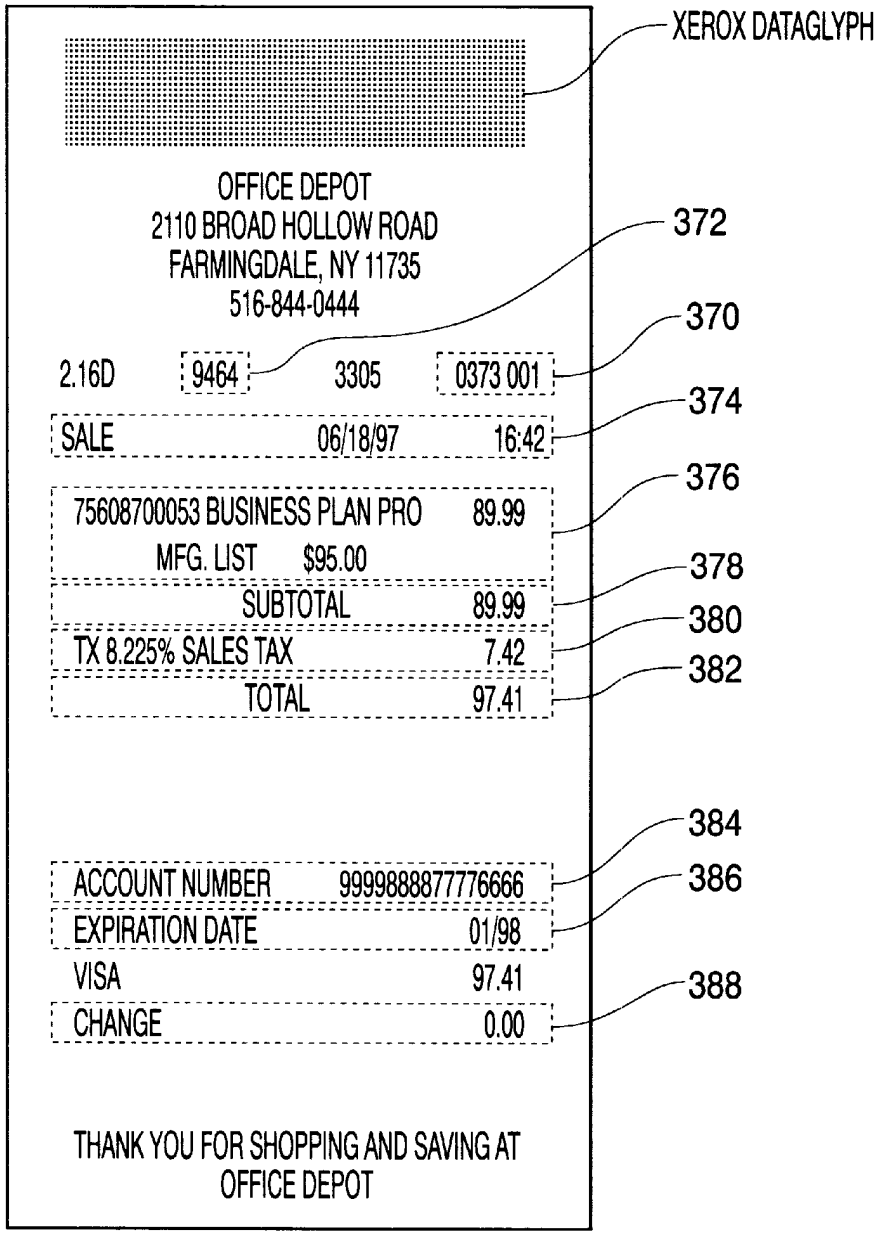

XEROX DATAGLYPH
OFFICE DEPOT
2110 BROAD HOLLOW ROAD
FARMINGDALE, NY 11735
516-844-0444
372
370
2.16D
9464
3305
0373 001
374
SALE
06/18/97
16:42
376
75608700053 BUSINESS PLAN PRO
89.99
MFG. LIST $95.00
378
SUBTOTAL
89.99
380
TX 8.225% SALES TAX
7.42
382
TOTAL
97.41
384
ACCOUNT NUMBER
9999888877776666
386
EXPIRATION DATE
01/98
VISA
97.41
388
CHANGE
0.00
THANK YOU FOR SHOPPING AND SAVING AT
OFFICE DEPOT

FIG. 3B

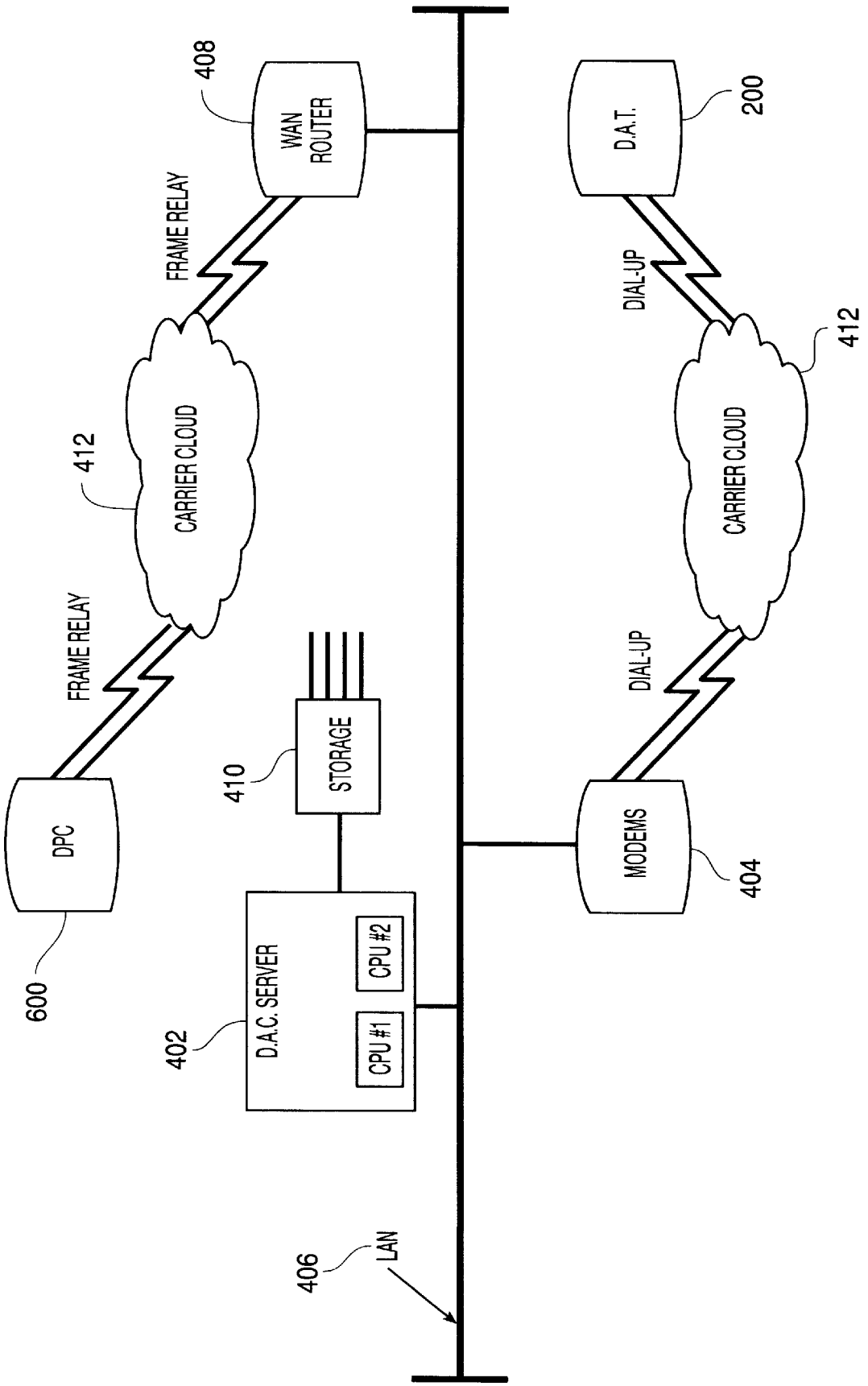

408
WAN ROUTER
FRAME RELAY
412
CARRIER CLOUD
FRAME RELAY
DPC
600
410
STORAGE
402
D.A.C. SERVER
CPU #2
CPU #1
406
LAN
200
D.A.T.
DIAL-UP
412
CARRIER CLOUD
DIAL-UP
MODEMS
404

FIG. 4

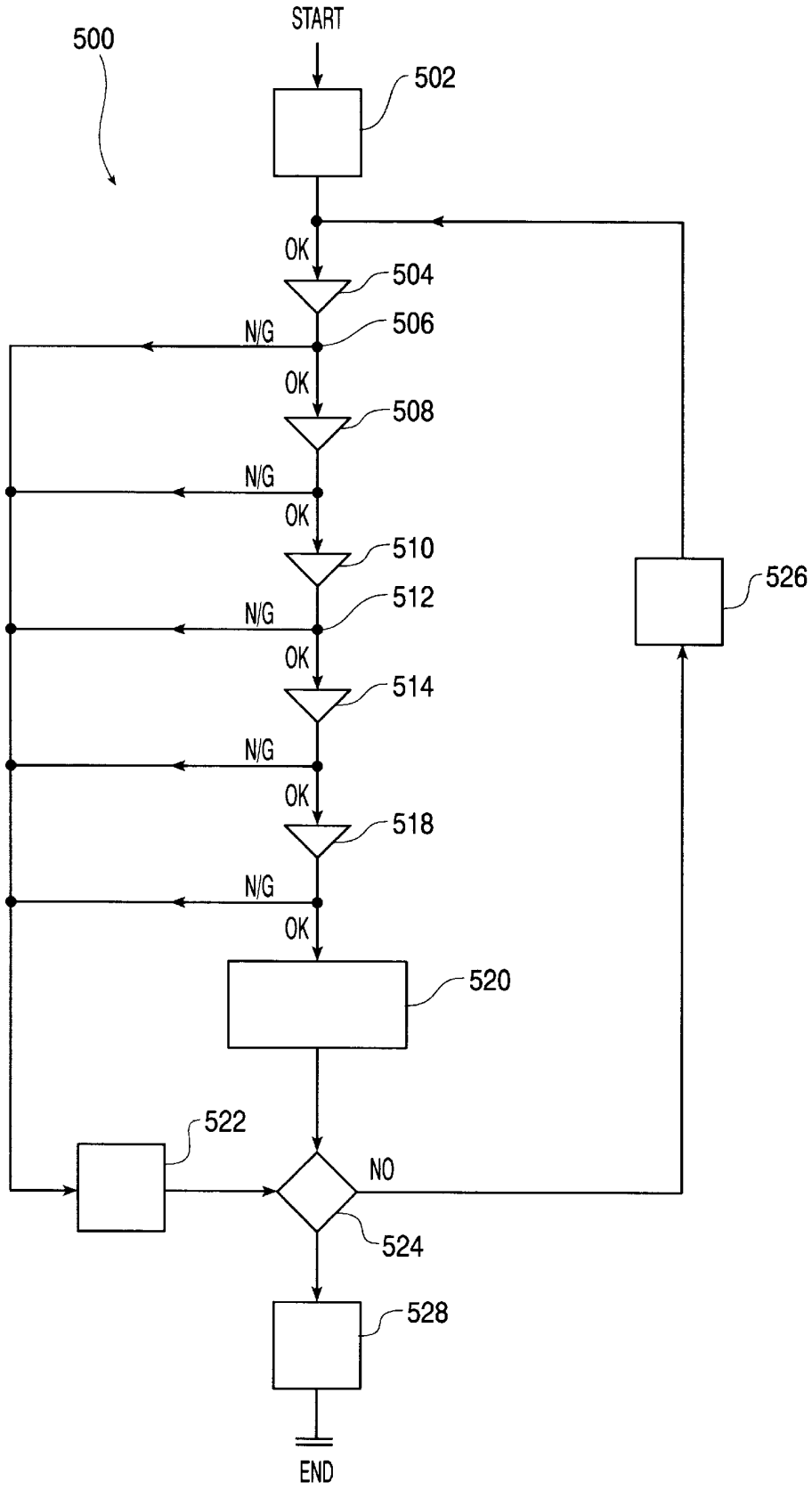

500
START
502
OK
504
N/G
506
OK
508
N/G
OK
510
N/G
512
OK
514
N/G
OK
518
N/G
OK
520
522
NO
524
526
528
END

FIG. 5

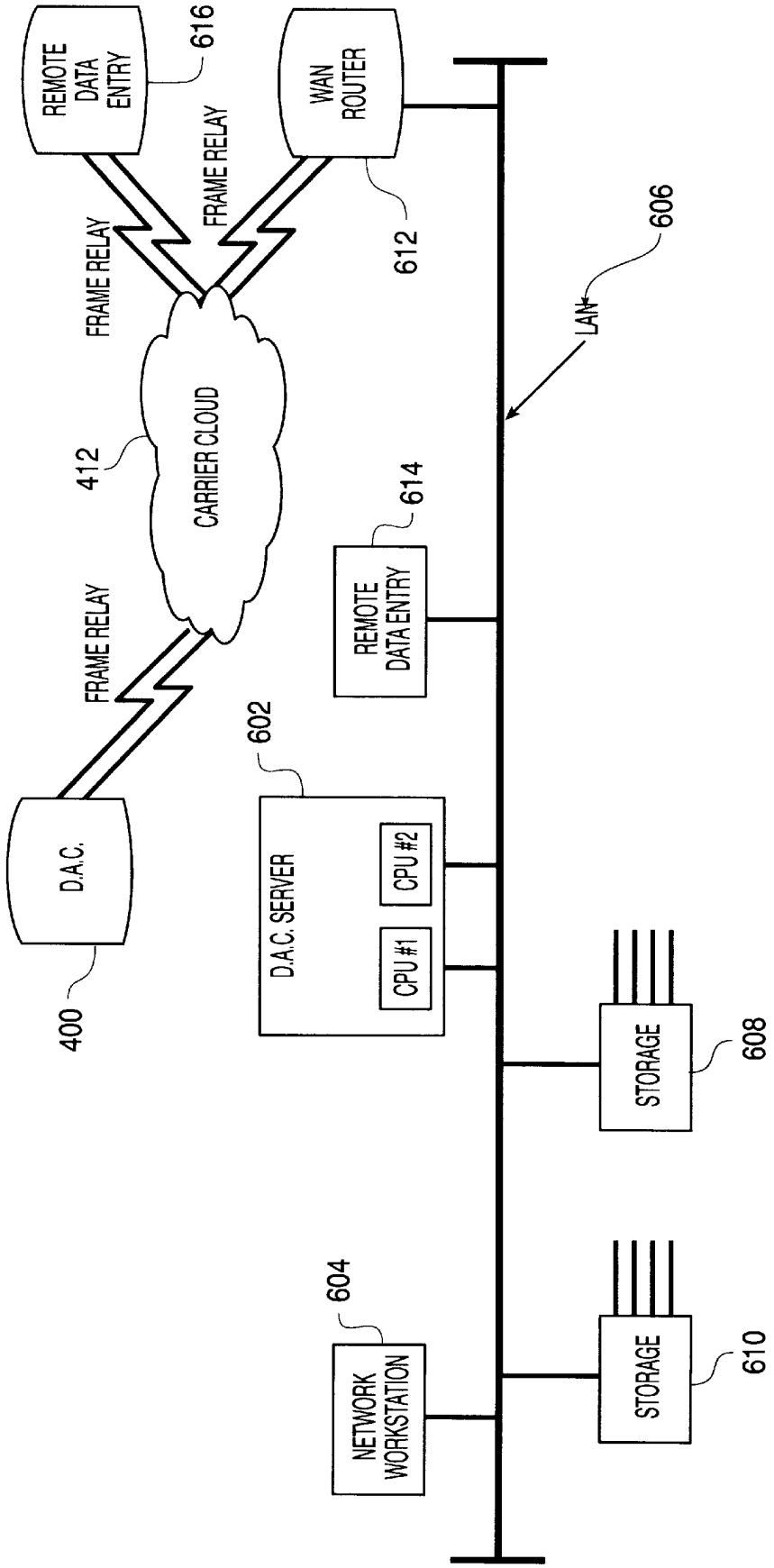

REMOTE DATA ENTRY
616
WAN ROUTER
FRAME RELAY
FRAME RELAY
612
606
LAN
412
CARRIER CLOUD
614
REMOTE DATA ENTRY
FRAME RELAY
602
D.A.C.
D.A.C. SERVER
CPU #2
CPU #1
400
STORAGE
608
604
NETWORK WORKSTATION
STORAGE
610

FIG. 6

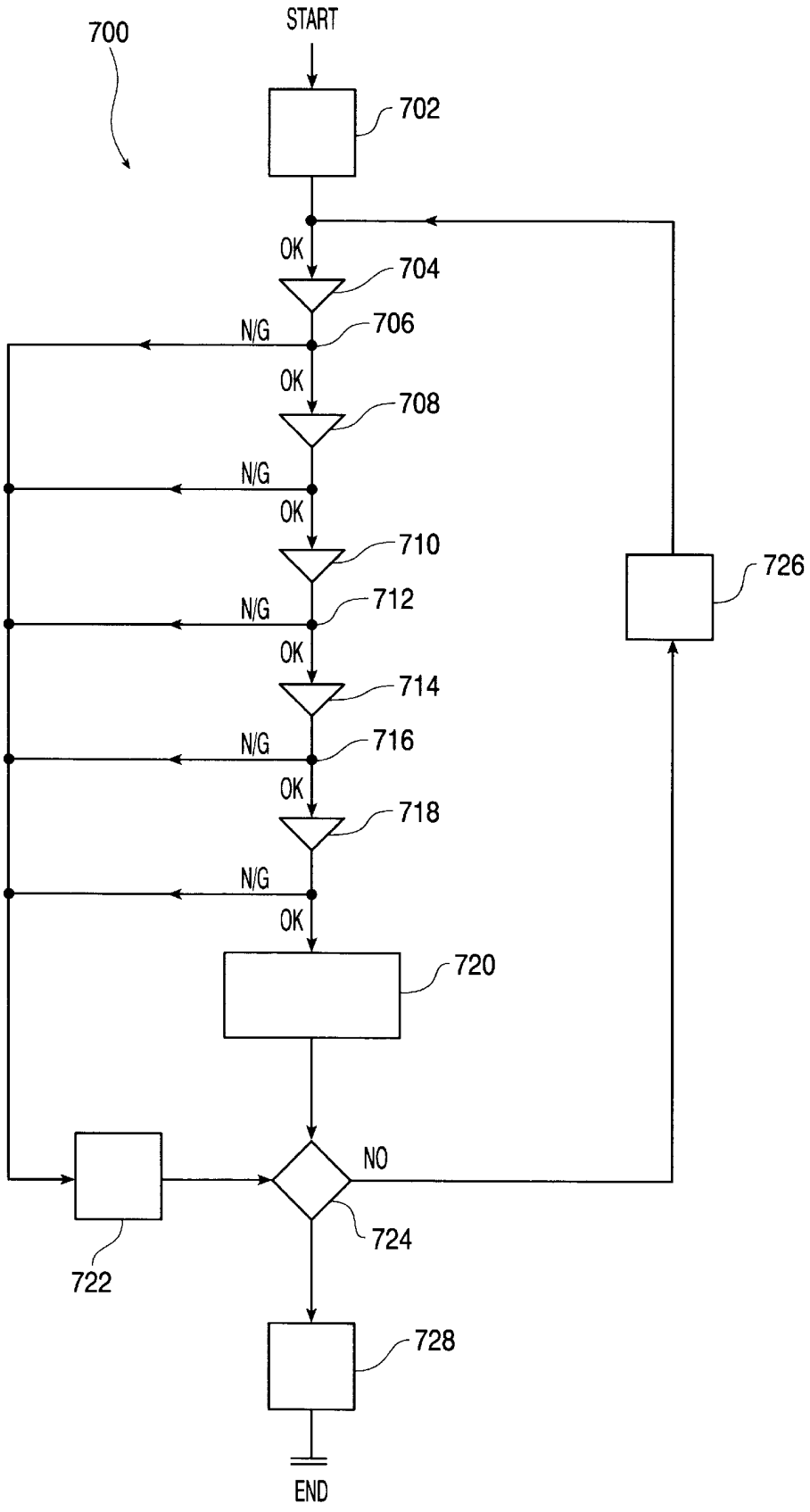

700
START
702
OK
704
N/G
706
OK
708
N/G
OK
710
N/G
712
OK
714
N/G
716
OK
718
N/G
OK
720
726
NO
724
722
728
END

FIG. 7

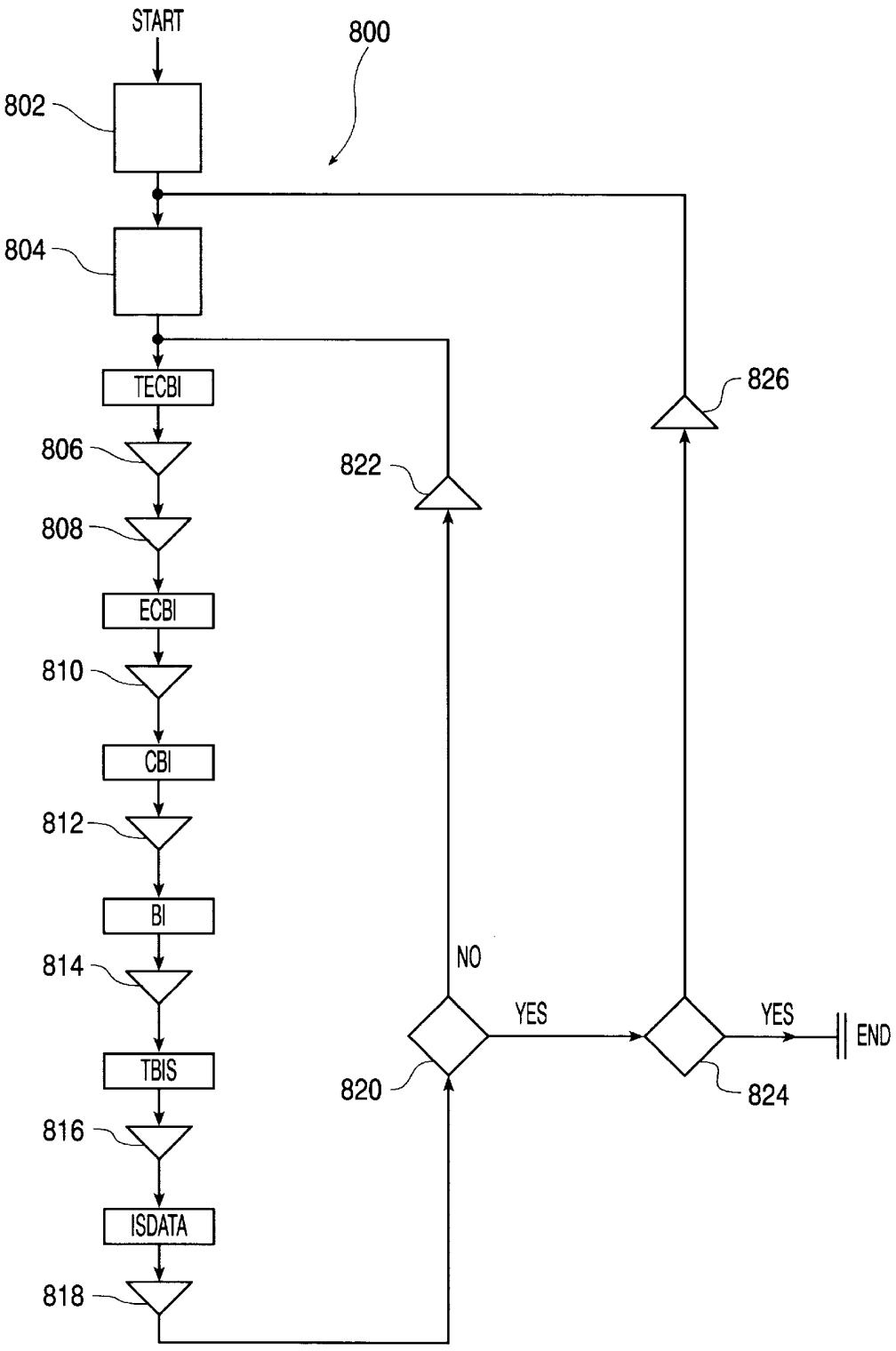

START
800
802
804
TECBI
806
808
ECBI
810
CBI
812
BI
814
TBIS
816
ISDATA
818
822
826
NO
YES
YES
END
820
824

FIG. 8

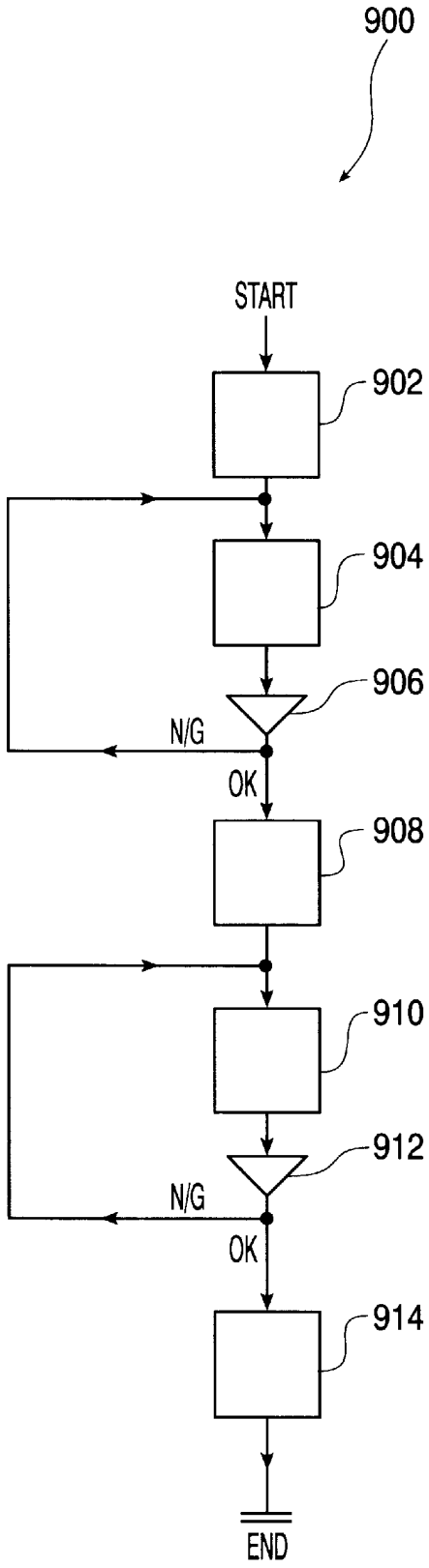


FIG. 9

REMOTE IMAGE CAPTURE WITH CENTRALIZED PROCESSING AND STORAGE

FIELD OF THE INVENTION

This invention relates generally to the automated processing of documents and electronic data from different applications including sale, business, banking and general consumer transactions. More particularly, it pertains to an automated system to retrieve transaction data at remote locations, to encrypt the data, to transmit the encrypted data to a central location, to transform the data to a usable form, to generate informative reports from the data and to transmit the informative reports to the remote locations.

BACKGROUND

This invention involves the processing of documents and electronic data which are generated, for example, from sale, business and banking transactions including credit card transactions, smart card transactions, automated teller machine (ATM) transactions, consumer purchases, business forms, W2 forms, birth certificates, deeds and insurance documents.

The enormous number of paper and electronic records generated from documents and electronic data from sale, business and banking transactions contain valuable information. First, these paper and electronic records contain information which can be used to verify the accuracy of the records maintained by consumers, merchants and bankers. For example, customers use paper receipts of sale and banking transactions to verify the information on the periodic statements which they receive from their bank or credit card institution. Merchants use paper receipts to record sale transactions for management of customer complaints. Taxpayers use paper receipts to record tax deductible contributions for use in their tax return preparation. Employees use paper receipts to record business expenses for preparation of business expense forms.

Paper and electronic records also contain information which can be used for market analysis. For example, manufacturers and retailers can determine consumer preferences in different regions as well as trends in consumer preferences from the information contained in paper and electronic records.

However, the maintenance and processing of paper and electronic records presents difficult challenges. First, paper receipts and documents could easily be lost, misplaced, stolen, damaged or destroyed. Further, the information contained in these paper and electronic records cannot be easily processed because it is scattered among individual records. For example, the market trend information contained in a group of sales records retained by merchants cannot easily be determined since this information is scattered among the individual records. Likewise, the tax information contained in a group of paper receipts of sales transactions retained by consumers cannot easily be processed.

Previous approaches have been proposed to meet the challenges associated with the maintenance and processing of paper and electronic records. For example, data archive service companies store the information from paper receipts and documents acquired from their customers on microfilm or compact disc read only memory (CD-ROM) at a central facility. Customers typically deliver the paper receipts and documents to the central facility. For sensitive documents which cannot leave the customer site, some data archive service companies perform data acquisition and transfer to

magnetic tapes at the customer site and deliver the tapes to the central facility.

The approach offered by these data archive service companies have disadvantages. First, the approach is costly and has poor performance because it requires an expensive, time consuming physical transportation of paper receipts or magnetic tapes from the customer site to the central facility. Further, the approach is not reliable as information can be lost or damaged during physical transportation. The approach also has limited capability as it does not process electronic records along with the paper receipts within a single system.

Other approaches have focused on the elimination of paper receipts and documents. U.S. Pat. No. 5,590,038 discloses a universal electronic transaction card (UET card) or smart card which stores transaction information on a memory embedded on the card as a substitute for a paper receipt. Similarly, U.S. Pat. No. 5,479,510 discloses a method of electronically transmitting and storing purchaser information at the time of purchase which is read at a later time to ensure that the purchased goods or services are delivered to the correct person.

While these approaches avoid the problems associated with paper receipts, they have other disadvantages. First, these approaches do not offer independent verification of the accuracy of the records maintained by consumers, merchants and bankers with a third party recipient of the transaction data. For example, if a UET card is lost, stolen, damaged or deliberately altered by an unscrupulous holder after recording sale or banking transactions, these approaches would not be able to verify the remaining records which are maintained by the other parties to the transactions.

Next, these approaches do not have the ability to process both paper and electronic records of transactions within a single, comprehensive system. Accordingly, they do not address the task of processing the enormous number of paper receipts which have been generated from sales and banking transactions. The absence of the ability to process both paper and electronic records of these approaches is a significant limitation as paper receipts and documents will continue to be generated for the foreseeable future because of concerns over the reliability and security of electronic transactions and the familiarity of consumers and merchants with paper receipts.

These approaches also have a security deficiency as they do not offer signature verification which is typically used on credit card purchases to avoid theft and fraud. For example, a thief could misappropriate money from a UET card holder after obtaining by force, manipulation or theft the user's personal identification number (PIN). Similarly, it is not uncommon for criminals to acquire credit cards in victims' names and make unlawful charges after obtaining the victim's social security number. This becomes a greater concern as that type of personal information becomes available, e.g., on the internet. Also, the signature verification performed manually by merchants for credit card purchases frequently misses forged signatures.

Even if smart cards or UET cards had the ability to store signature and other biometric data within the card for verification, the system would still have disadvantages. First, the stored biometric data on the card could be altered by a card thief to defeat the security measure. Similarly, the biometric data could be corrupted if the card is damaged. Finally, the security measure would be costly at it would require an expensive biometric comparison feature either on each card or on equipment at each merchant site.

Additional biometric verification systems including signature verification systems have been proposed to address the security problem. For example, U.S. Pat. No. 5,657,393 discloses a method and apparatus for verification of handwritten signatures involving the extraction and comparison of signature characteristics including the length and angle of select component lines. In addition, U.S. Pat. No. 5,602,933 discloses a method and apparatus for the verification of remotely acquired data with corresponding data stored at a central facility.

However, none of these verification systems offer general support for transaction initiation, remote paper and electronic data acquisition, data encryption, data communication, data archival, data retrieval, data mining, manipulation and analytic services. Accordingly, there is a need for a single system which offers comprehensive support for the tasks involved in the automated processing of documents, biometric and electronic data from sale, business, banking and general consumer transactions. Further, there is a need for a single comprehensive system having the reliability, performance, fault tolerance, capacity, cost and security to satisfy the requirements of the retail, business, banking and general consumer industries.

SUMMARY OF THE INVENTION

The invention provides an automated, reliable, high performance, fault tolerant, and low cost system with maximal security and availability to process electronic and paper transactions, and has been named the DataTreasury™ System.

It is an object of the present invention to provide a system for central management, storage and verification of remotely captured electronic and paper transactions from credit cards, smart cards, debit cards, documents and receipts involving sales, business, banking and general purpose consumer applications comprising:

- at least one remote data access subsystem for capturing and sending electronic and paper transaction data;
- at least one data collecting subsystem for collecting and sending the electronic and paper transaction data comprising a first data management subsystem for managing the collecting and sending of the transaction data;
- at least one central data processing subsystem for processing, sending and storing the electronic and paper transaction data comprising a second data management subsystem for managing the processing, sending and storing of the transaction data; and
- at least one communication network for the transmission of the transaction data within and between said at least one data access subsystem and said at least one data processing subsystem.

The DataTreasury™ System processes paper and/or electronic receipts such as credit card receipts, Automated Teller Machine (ATM) receipts, business expense receipts and sales receipts and automatically generates reports such as credit card statements, bank statements, tax reports for tax return preparation, market analyses, and the like.

It is a further object of the DataTreasury™ System to retrieve both paper and electronic transactions at remote locations.

It is a further object of the DataTreasury™ System to employ a scanner and a data entry terminal at a customer site to retrieve data from paper transactions and to enable additions or modifications to the scanned information respectively.

It is a further object of the DataTreasury™ System to provide an input device for retrieving transaction data from the memory of smart cards for independent verification of the records maintained by consumers, merchants and bankers to prevent the loss of data from the loss, theft, damage or deliberate alteration of the smart card.

It is a further object of the DataTreasury™ System to retrieve and process transaction data from DataTreasury™ System anonymous smart cards which are identified by an account number and password. Since DataTreasury™ System anonymous smart card transactions can be identified without the customer's name, a customer can add money to the DataTreasury™ System anonymous smart card and make expenditures with the card with the same degree of privacy as cash acquisitions and expenditures.

It is a further object of the DataTreasury™ System to retrieve customer billing data from employee time documents and to generate customer billing statements from the billing data.

It is a further object of the DataTreasury™ System to initiate electronic transactions including transactions on the internet and to provide identification verification by capturing and comparing signature and biometric data.

It is a further object of the DataTreasury™ System of the invention to process electronic and paper transactions with a tiered architecture comprised of DataTreasury™ System Access Terminals (DATs), DataTreasury™ System Access Collectors (DACS) and DataTreasury™ System Processing Concentrators (DPCs).

BRIEF DESCRIPTION OF THE DRAWINGS

These and other objects and features of the invention will be more clearly understood from the following detailed description along with the accompanying drawing figures, wherein:

FIG. **1** is a block diagram showing the three major operational elements of the invention: the DataTreasury™ System Access Terminal (DAT), the DataTreasury™ System Access Collector (DAC) and the DataTreasury™ System Processing Concentrator (DPC);

FIG. **2** is a block diagram of the DAT architecture;

FIG. **3***a* is a flow chart describing image capture by a DAT;

FIG. **3***b* displays a sample paper receipt which is processed by the DAT;

FIG. **4** is a block diagram of the DAC architecture;

FIG. **5** is a flow chart describing the polling of the DATs by a DAC;

FIG. **6** is a block diagram of the DPC architecture;

FIG. **7** is a flow chart describing the polling of the DACs by the DPC;

FIG. **8** is a flow chart describing the data processing performed by the DPC; and

FIG. **9** is a flow chart describing the data retrieval performed by the DPC.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

FIG. **1** shows the architecture of the DataTreasury™ System **100**. The DataTreasury™ System **100** has three operational elements: the DataTreasury™ System Access Terminal (DAT) **200** (the remote data access subsystem), the DataTreasury™ System Access Collector (DAC) **400** (the intermediate data collecting subsystem), and the DataTreasury™ System Processing Concentrator (DPC) **600** (the central data processing subsystem).

The DataTreasury™ System **100** architecture consists of three tiers. At the bottom tier, the DATs **200** retrieve data from the customer sites. At the next tier, the DACs **400** poll the DATs **200** to receive data which accumulates in the DATs **200**. At the top tier, the DPCs **600** poll the DACs **400** to receive data which accumulates in the DACs **400**. The DPCs **600** store the customer's data in a central location, generate informative reports from the data and transmit the informative reports to the customers at remote locations.

In the preferred embodiment, the DataTreasury™ System **100** complies with the Price Waterhouse SAS70 industry standard. Specifically, the DataTreasury™ System **100** meets the software development standard, the system deployment standard and the reliability standard specified by Price Waterhouse SAS70. By adhering to the Price Waterhouse SAS70 standard, the DataTreasury™ System **100** provides the security, availability and reliability required by mission critical financial applications of banks and stock brokerage companies.

As is known to persons of ordinary skill in the art, the DataTreasury™ System **100** could also use other software development standard, other system deployment standards and other reliability standards as long as adherence to these alternative standards provides the security, availability and reliability required by mission critical financial applications.

FIG. **2** shows a block diagram of the DAT **200** architecture. DATs **200** are located at customer sites. The DataTreasury™ System **100** customers include merchants, consumers and bankers. The DATs **200** act as the customer contact point to the suite of services provided by the DataTreasury™ System **100**. In the preferred embodiment, the DAT **200** is custom designed around a general purpose thin client Network Computer (NC) which runs SUN Microsystem's JAVA/OS operating system. The custom designed DAT **200** comprises a DAT scanner **202**, a DAT modem **204**, DAT digital storage **206**, a DAT controller **210** (workstation), a DAT card interface **212**, an optional DAT printer **208** and a signature pad **214**.

As is known to persons of ordinary skill in the art, the DAT **200** could also be custom designed around a general purpose network computer running other operating systems as long as the chosen operating system provides support for multiprocessing, memory management and dynamic linking required by the DataTreasury™ System **100**.

The DAT scanner **202** scans a paper receipt and generates a digital bitmap image representation called a Bitmap Image (BI) of the receipt. In the preferred embodiment, the DAT scanner **202** has the ability to support a full range of image resolution values which are commonly measured in Dots Per Inch (DPI). Next, the DAT scanner **202** has the ability to perform full duplex imaging. With full duplex imaging, a scanner simultaneous captures both the front and back of a paper document. The DAT scanner **202** can also support gray scale and full color imaging at any bit per pixel depth value. The DAT scanner **202** also supports the capture of handwritten signatures for identity verification.

In addition to scanning images and text, the DAT scanner **202** also scans DataGlyph™ elements, available from Xerox Corporation. As is known to persons of ordinary skill in the art, the Xerox DataGlyph™ Technology represents digital information with machine readable data which is encoded into many, tiny, individual glyph elements. Each glyph element consists of a 45 degree diagonal line which could be as short as 1/100th of an inch depending on the resolution of the scanning and printing devices. Each glyph element represents a binary 0 or 1 depending on whether it slopes downward to the left or the right respectively. Accordingly, DataGlyph™ elements can represent character strings as ASCII or EBCIDIC binary representations. Further, encryption methods, as known to persons of ordinary skill in the art encrypt the data represented by the DataGlyph™ Technology.

The use of glyph technology in the DataTreasury™ System **100** improves the accuracy, cost and performance of the system. Xerox DataGlyph™ Technology includes error correction codes which can be referenced to correct scanning errors or to correct damage to the document caused by ink spills or ordinary wear. DataGlyph™ Technology also leads to decreased system cost since the system will require less manual intervention for data entry and correction because of the improved accuracy associated with DataGlyph™ elements. Since DataGlyph™ elements represent a large amount of information in a small amount of space, the DAT scanner **100** will require a small amount of time to input a large amount of information.

The DAT card interface **212** and the DAT signature pad **214** along with the internet and telephone access through the DAT modem **204** enable the DataTreasury™ System **100** customer to initiate secure sale and banking transactions via the internet or telephone with the DAT **200** using a variety of cards including debit cards, smart cards and credit cards. After selecting a purchase or a banking transaction through a standard internet interface, the DataTreasury™ System **100** customer inserts or swipes the debit card, smart card or credit card into the DAT card interface **212**.

The DAT card interface **212** retrieves the identification information from the card for subsequent transmission to the destination of the internet transaction. Further, the DAT scanner **202** could capture a hand written signature from a document or the DAT signature pad **214** could capture an electronic signature written on it with a special pen. Similarly, these security featurs allow a credit card recipient to activate the card with a DAT **200** located at a merchant site. The security features would detect unauthorized use of debit cards, credit cards and smart cards resulting from their unlawful interception. Accordingly, the DataTreasury™ System's **100** security features offer a more secure alternative for internet and telephone transactions than the typical methods which only require transmission of a card account number and expiration date.

As is known to persons of ordinary skill in the art, the DATs **200** could also include additional devices for capturing other biometric data for additional security. These devices include facial scans, fingerprints, voice prints, iris scans, retina scans and hand geometry.

In addition to initiating sale and banking transactions, the DAT card interface **212** also reads sale and banking transactions initiated elsewhere from the memory of smart cards to enable subsequent storage and processing by the DataTreasury™ System. If a smart card is lost, stolen, damaged or deliberately altered by an unscrupulous holder after the DAT card interface **212** reads its transaction data, the DataTreasury™ System **100** can reproduce the transaction data for the customer. Accordingly, the DAT card interface **212** provides support for independent verification of the records maintained by consumers, merchants and bankers to prevent the loss of data from the loss, theft, damage or deliberate alteration of the smart card.

The DAT card interface **212** also supports the initiation and retrieval of sale and banking transactions with the DataTreasury™ System anonymous smart cards. In contrast to standard debit cards and credit cards, the DataTreasury™