

UTILITY SERIAL NUMBER	08/122071	PATENT DATE	JAN 24 1996	PATENT NUMBER	
				5524073	

SERIAL NUMBER	08/122,071	FILING DATE	09/14/93	CLASS	380	SUBCLASS	24	GROUP ART UNIT	2202	EXAMINER	Cangialosi
---------------	------------	-------------	----------	-------	-----	----------	----	----------------	------	----------	------------

APPLICANTS
LEON STAMBLER, PARKLAND, FL.

CONTINUING DATA***
VERIFIED THIS APPLN IS A DIV OF 07/977,385 11/17/92 PAT 5,267,314
gnc

FOREIGN/PCT APPLICATIONS***
VERIFIED
gnc

CERTIFICATE

SEP 10 1996

ISSUE FEE IN FILE OF CORRECTION

FOREIGN FILING LICENSE GRANTED 10/20/93 ***** SMALL ENTITY *****

Foreign priority claimed 35 USC 119 conditions met	<input type="checkbox"/> yes <input checked="" type="checkbox"/> no	AS FILED	STATE OR COUNTRY	SHEETS DRWGS.	TOTAL CLAIMS	INDEP. CLAIMS	FILING FEE RECEIVED	ATTORNEY'S DOCKET NO.
Verified and Acknowledged	gnc Examiner's Initials	→	FL	15	38	13	\$947.00	60741U1

ADDRESS
PANITCH SCHWARZE JACOBS & NADEL
1601 MARKET STREET - 36TH FLOOR
PHILADELPHIA, PA 19103

TITLE
SECURE TRANSACTION SYSTEM AND METHOD UTILIZED THEREIN

U.S. DEPT. of COMM. Pat. & TM Office - PTO-436L (rev. 10-78)

PARTS OF APPLICATION
FILED SEPARATELY

NOTICE OF ALLOWANCE MAILED	Assistant Examiner	CLAIMS ALLOWED
7-28-95		Total Claims 19 Print Claim 1
ISSUE FEE		DRAWING
Amount Due 605.00	SALVATORE CANGIALOSI PRIMARY EXAMINER ART UNIT 222 Primary Examiner	Sheets Drwg. 15 Fig. Drwg. 2 Print Fig. 8A
Date Paid 10-2-95		ISSUE BATCH NUMBER 1077
Label Area		PREPARED FOR ISSUE
WARNING: The information disclosed herein may be restricted. Unauthorized disclosure may be prohibited by the United States Code Title 35, Sections 122, 181 and 368. Possession outside the U.S. Patent & Trademark Office is restricted to authorized employees and contractors only.		

Form PTO-436A
(rev. 8/92)

(FACE)

08/122071

APPROVED FOR LICENSE ☒

INITIALS **067159307**

Date
Entered
or
Counted

CONTENTS

Date
Received
or
Mailed

	1. Application <u>13</u> papers.	
	2. <u>Pre A</u>	
	3. <u>Prior Art w/ATT</u>	
	4. <u>Pre B</u>	
	5. <u>Prior Art w/ATT</u>	
	6. <u>Pre C</u>	
<u>5/27</u>	7. <u>Rejection 3 mos</u>	
	8. <u>Response</u>	
<u>10/17</u>	9. <u>Reply 3 mos</u>	
	10. <u>Prior Art w/att.</u>	
	11. <u>Argu.</u>	
<u>3/22</u>	12. <u>Final Reply 3 mos</u>	
	13. <u>Req. Ext. Time</u>	
	14. <u>Amend. Draw.</u>	
<u>7-28</u>	15. <u>Notice of Allowability</u>	
	16. <u>Notice of Allowance</u>	
<u>12/11/96</u>	17. <u>Supplemental Declaration</u>	
	18. <u>Formal Drawings (15 sheets) set</u>	
<u>3/18/96</u>	19. <u>Notice of Drawing Requirement</u>	
	20. <u>Formal Drawings (10 sheets) set 2</u>	
	21. <u>PTO Grant JUN 04 1996</u>	
	22. <u>Req. For Copy</u>	
	23.	
	24.	
	25.	
	26.	
	27.	
	28.	
	29.	
	30.	
	31.	
	32.	

(FRONT)

Date				
Final	Original	5	10	3
1	101	✓	W	✓
2	102			
3	103			
4	104			
5	105			
6	106			
7	107			
8	108			
9	109			
10	110			
11	111			
12	112			
13	113			
14	114			
15	115			
16	116			
17	117			
18	118			
19	119			
20	120			
21	121			
22	122			
23	123			
24	124			
25	125			
26	126			
27	127			
28	128			
29	129			
30	130			
31	131			
32	132			
33	133			
34	134			
35	135			
36	136			
37	137			
38	138			
39	139			
40	140			
41	141			
42	142			
43	143			
44	144			
45	145			
46	146			
47	147			
48	148			
49	149			
50	150			

INDEX OF CLAIMS

Date				
Final	Claim	5	10	3
1	151			
2	152			
3	153			
4	154			
5	155			
6	156			
7	157			
8	158			
9	159			
10	160			
11	161			
12	162			
13	163			
14	164			
15	165			
16	166			
17	167			
18	168			
19	169			
20	170			
21	171			
22	172			
23	173			
24	174			
25	175			
26	176			
27	177			
28	178			
29	179			
30	180			
31	181			
32	182			
33	183			
34	184			
35	185			
36	186			
37	187			
38	188			
39	189			
40	190			
41	191			
42	192			
43	193			
44	194			
45	195			
46	196			
47	197			
48	198			
49	199			
50	200			

SYMBOLS

- ✓ Rejected
- = Allowed
- (Through numeral) Canceled
- + Restricted
- N Non-elected
- I Interference
- A Appeal
- O Objected

SEARCHED			
Class	Sub	Date	Exmr.
384	2-15	5/94	gmr
above 384	2-15	5/94	gmr
380	2-15	10/94	gmr
above 380	2-15	10/94	gmr
above 380	2-15	9/85	gmr
above 380	2-15	9/85	gmr

SEARCH NOTES		
	Date	Exmr.

INTERFERENCE SEARCHED			
Class	Sub	Date	Exmr.
380	4-28-45	7/95	gnc

-- 4 --

T.W.
11-3-93

PATENT APPLICATION SERIAL NO. 08/122071

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE
FEE RECORD SHEET

DF11201 10/08/93 08122071 16-0235 110 201 947.00CH

PTO-1556
(5/87)

122071

- 71 -

**SECURE TRANSACTION SYSTEM
AND METHOD UTILIZED THEREIN**

Abstract of the Disclosure

A transaction system is disclosed wherein,
5 when a transaction, document or thing needs to be
authenticated, information associated with one or more
of the parties involved is coded together to produce a
joint code. This joint code is then utilized to code
information relevant to the transaction, document or
10 record, in order to produce a variable authentication
number (VAN) at the initiation of the transaction. This
VAN is thereafter associated with the transaction and is
recorded on the document or thing, along with the
original information that was coded. During subsequent
15 stages of the transaction, only parties capable of
reconstructing the joint code will be able to uncode the
VAN properly in order to re-derive the information. The
joint code serves to authenticate the parties, and the
comparison of the re-derived information against the
20 information recorded on the document serves to
authenticate the accuracy of that information.



08/122071

- 1 -

SECURE TRANSACTION SYSTEM
AND METHOD UTILIZED THEREIN

Add A' →

Field of the Invention

The present invention relates generally to
5 secure transaction systems and, more particularly,
concerns a method and apparatus for authenticating
documents, records and objects as well as the
individuals who are involved with them or responsible
for them.

10 Background of the Invention

There are many times in our daily lives when
the need arises for highly secure transactions. For
example, instruments of commerce, such as checks, stock
certificates, and bonds are subject to theft and
15 forgery. From the time a document is issued, the
information contained on it, or the name of the
recipient could be changed. Similarly, passports, pay
checks, motor vehicle registrations, diplomas, food
stamps, wager receipts, medical prescriptions, or birth
20 certificates and other official documents are subject to
forgery, fraudulent modification or use by an unintended
recipient. As a result, special forms, official stamps
and seals, and special authentication procedures have
been utilized to assure the authenticity of such
25 documents. Medical, legal and personnel records, and
all types of information in storage media are also
subject to unauthorized access. Passwords and coding of
such records have been used to thwart unauthorized
access. However, there have always been ingenious
30 individuals who have somehow managed to circumvent or
evade all such systems of security.

2

With the introduction of computers and computer communications into business transactions and document processing, a certain degree of security was gained, in that it is now possible to verify documents and transactions much more quickly, thereby avoiding many frauds which previously went unnoticed until it was too late. However, with the elimination of the human factor, verification of the identify of parties also became more difficult. A pressing need still exists for business transaction, document processing and record access systems which can assure the identity of the parties and the accuracy of the information involved in the transaction. As used herein, the term "record access systems" includes systems which access media which contains data, messages, text, FAX, audio, video, drawings, images, photo, electronic and physical mail, safe boxes, and the like. As used herein the term "business transaction system" will be intended as a generic term to describe all such transaction, document processing and record access systems, including ones not related to business use, such as passport authentication systems.

The security problems described above have been handled with some degree of success in systems involving a single party transaction where the party is present. For example, during the use of an automatic teller machine, the customer is the sole party involved and is present in person. However, until the present invention, it has not been possible to verify the identity and to secure the interests of all parties to multi-party transactions and, in particular, absent parties to a transaction.

3

Summary of the Invention

Briefly, the present invention is directed to a transaction, document processing, or record access system which avoids the shortcomings of known systems of this type. In accordance with an embodiment of the present invention, when a transaction, document or thing needs to be authenticated, information associated with at least one of the parties involved (e.g., an originator and/or a recipient) is coded to produce a joint code. This joint code is then utilized to code information relevant to the transaction, document or record, in order to produce a variable authentication number (VAN) or code at the initiation of the transaction. This VAN is thereafter associated with the transaction and is recorded on the document or thing, along with the original information that was coded. During subsequent stages of the transaction, only parties capable of reconstructing the joint code will be able to uncode the VAN properly in order to re-derive the information. Thus, the joint code serves to authenticate the parties, and the comparison of the re-derived information against the information recorded on the document serves to authenticate the accuracy of that information. Alternatively, the information could be authenticated by regenerating a VAN from the recorded information and comparing the regenerated VAN with the recorded VAN.

In accordance with an embodiment of the present invention, at the time of enrolling as a user of the system, each user selects a personal identification number (PIN), which is secret, does not exist in an uncoded form, and cannot be recovered from other information anywhere in the system. During or after enrollment, a non-secret identification code and a secret code are also stored in a user's file at the user associated computer facility. When a user participates

in a transaction, the user is required to utilize his or her PIN, which after being coded is used to derive a coded arbitrary number. Subsequently, this arbitrary code is compared to another such code which is generated from a reconstituted version of the coded PIN, in order to authenticate the user's identity. One of the embodiments creates a computer file with a secret address to authenticate a user's identity, and to secure sensitive records. The address is preferably not stored anywhere in the system, but is generated when needed from information supplied by the user. In some embodiments of the present invention, when a joint code is created as described above, one participating user (e.g., the originator) must provide his or her PIN. The other party's non-secret identification code and the PIN are utilized in creating the joint code. In other embodiments, the joint code is created from the coded PIN's of the participants.

Brief Description of the Drawings

The foregoing brief description as well as further objects, features, and advantages of the present invention will be understood more completely from the following detailed description of the presently preferred, but nonetheless illustrative, embodiments of the invention, with reference being had to the accompanying drawings, in which:

Figs. 1-5 illustrate the symbols utilized in the present application to represent conventional building blocks used to form the invention, these building blocks being respectively, a coder, an uncoder, a linker, a mixer, and a sorter;

Figs. 6-8 are functional block diagrams illustrating a check transaction system in accordance with a first embodiment of the present invention, with Fig. 6 illustrating user enrollment, Fig. 7 illustrating

how an originator generates a check, and Figs. 8A and 8B illustrating the authentication process when the check is presented to be cashed;

Figs. 9-12 are functional block diagrams illustrating a credential issuing and authentication system in accordance with a second embodiment of the present invention, with Fig. 9 illustrating the enrollment of an official, Fig. 10 illustrating the enrollment of a user, Fig. 11 illustrating the issuance of the credential, and Fig. 12 illustrating the authentication of an issued credential;

Figs. 13A-13E, when arranged as illustrated in Fig. 14, collectively represent a functional block diagram of a check transaction system similar to that of Figs. 6-8, but including the basic processing necessary to clear and pay a check electronically;

Figs. 15A-15C are functional block diagrams of a credential issuing and authentication system according to an alternate embodiment of the present invention; and

Fig. 16 is a functional block diagram of a system for authenticating a party and for authorizing access to a secret file associated with the party according to an alternate embodiment of the present invention.

Detailed Description of the Preferred Embodiments

Figs. 1-5 illustrate the functional building blocks utilized in the preferred embodiments. All of these components are conventional building blocks for computer or communication systems. Moreover, those skilled in the art will appreciate that the blocks can be realized as hardware components, or they can be realized as functional blocks in an overall computer program.

The coder illustrated in Fig. 1 and the uncoder illustrated in Fig. 2 may be any form of such device utilizing a known algorithm, such as the Data Encryption Standard (DES). A coder, as illustrated in 5 Fig. 1, has at least one data input, at which it receives clear data. It also has one or more additional inputs for receiving keys K_1 , K_2 , which are utilized to code the clear data into a form in which it could not be easily recognized or uncoded without the use of the 10 keys. A variable which is used as a key may be padded to obtain the desired security. An uncoder (Fig. 2) reverses the process of the coder. Basically, it receives the coded data and utilizes the same keys to reconstruct the clear data.

15 A linker (Fig. 3) receives a plurality of data inputs and concatenates them into a longer code word ($D_1, D_2 \dots D_N$). Similarly, a mixer (Fig. 4) receives a plurality of data inputs (D_1 , and D_2 through D_N) and mixes their digits or binary bits. A simple example of 20 a mixer would be a conventional time division multiplexer which is used to interleave plural data inputs. However, in many applications, it will be preferable to utilize a more sophisticated mixer, such as one that utilizes arithmetic and logical combinations 25 of digits or bits. A sorter (Fig. 5) reverses the process of a linker or a mixer, that is, it receives a concatenated or mixed code word and reproduces the original component words. A time division demultiplexer could serve as a sorter for a mixed signal 30 originally generated by a multiplexer.

Figs. 6, 7, 8A and 8B constitute a functional block diagram illustrating the present invention in a check transaction system. The system illustrated in Figs. 6, 7, 8A and 8B are well suited for use in 35 generating and processing employee paychecks, for example. The system involves three phases of operation.

In the first phase, illustrated in Fig. 6, a user of the system must enroll in order to be recognized by the system. Each user enrolls at his or her bank, or at another convenient location, such as a place of
5 employment, in the presence of an officer, who appropriately verifies the user's identity and obtains the typical information from him, including his taxpayer identification number (TIN) and telephone number. An account is then opened for the user and a file is
10 created for him or her in the bank's computer, and the bank assigns a person account number (PAN) to the user's account. If a bank card is issued to the user, it usually contains the PAN and a bank identification number (BIN).

15 While operating a terminal, the user is requested to select a personal identification number (PIN) and to enter that PIN into the terminal. The user complies and such entry occurs at block 10 of Fig. 6 with the typical transaction information, including the
20 user's TIN or PAN, being entered at block 11. The PIN is applied directly to an irreversible coder 12, where it is processed to produce a coded PIN (CPN). Coder 12 may be any type of conventional coding device which can process the PIN so that the coding is irreversible
25 (i.e., the PIN cannot be recovered from the CPN). At the same time, a random number generator 14 produces a random number (RN), which is applied to a mixer 16 along with the CPN. Alternately, the user may be permitted to select an arbitrary number for RN.

30 The signal produced by mixer 16 is then transmitted to the bank's computer, where it is applied to a sorter 18. It is assumed that this transmission preferably occurs over a secure line, such as one protected by a tandem coder and uncoder which can
35 utilize a joint terminal-bank key. The sorter recovers the original CPN and RN, saving RN in the user's file at

block 22. It should be noted that in saving RN, the user's file is accessed by using his TIN as an index. The received CPN is applied as the data input to a coder 20, which receives RN as its key input, producing
5 a revisable owner code (ROC) which is saved in the user's file in the same manner as RN. Various additional information is saved in the user's file, such as his personal account number (PAN), name, phone number (PHN), account balance, and other relevant information.
10 The user's TIN, PAN or PHN can be used as an index to access the user's file. CPN represents coded authentication information since it is a coded form of the PIN, and since it is used in other parts of the system to authenticate the user and the transaction.
15 The system preferably maintains RN as a secret number (although in the present embodiment the user file is not secret since it is accessed using a non-secret index) and ROC is maintained as a non-secret number. As explained in detail below, CPN is derivable from ROC and
20 RN.

Fig. 7 illustrates how the originator generates a check in accordance with the present invention. This process preferably takes place at the originator's terminal or computer. It is assumed that
25 the originator would be generating a check in the usual manner and would include on it all of the information usually found on a check, as well as the information normally recorded or imprinted on check forms, such as the recipient's name and TIN (RTIN), and the
30 originator's personal account number and bank identification number. Preferably, the terminal includes a check reader and printer which can read necessary information from the originator's check form and print information on the form, although this could
35 also be done manually by the originator. The originator and the recipient can be the same person, for example,

where a person is cashing a personal check originated by the person. In the case of multi-party checks, the check is originated by a present party (i.e., the originator) in favor of an absent party (recipient).

5 The originator enters his or her PIN at a terminal or computer. Through irreversible coder 10, the originator's PIN is converted to a coded PIN (CPNO), which is applied as the key input to coder 28. The data input to coder 28 is the recipient's TIN (RTIN), which
10 has been read from the check, or accessed from the computer memory, or entered by the originator. The data output of coder 28 is a joint key (JK), which is applied as the key input to a coder 30. Generally, the JK is generated using information associated with at least one
15 of the parties involved in the transaction (in this case, the originator and recipient). As will be shown more fully below, the joint key (or code) is used to protect and authenticate the originator and recipient. The data input to the coder 30 is the information (INFO)
20 to be authenticated (that is, information relevant to the transaction, such as check number, amount, etc.).

 The data output of the coder 30 is a variable authentication number (VAN), which codes the information to be authenticated, based upon information related to
25 the recipient and information related to the originator. Note that the VAN is alternatively generated directly from INFO and information associated with at least one of the parties, without the intermediate step of generating the JK. The VAN and at least a portion of
30 the information relevant to the transaction are written or imprinted upon the check 32, thereby becoming a permanent part of it. Alternately, the check may represent an electronic transfer of funds or some other type of electronic transaction. In this case, the VAN

KC

and at least a portion of the information relevant to the transaction are included with the electrical signals associated with the electronic transaction.

It is contemplated that in creating the VAN,
5 all information would not necessarily be coded in the same manner. For example, the amount of the check might be considered important enough so as to be recoverable completely, and it would be coded into the VAN in a manner that would permit complete recovery. Other
10 information, such as the date and check control number might be considered less important and would be coded into the VAN in such a manner as to permit detection of changes (e.g., error detection coding), but without complete recovery of the original information.

15 As noted above, other predetermined information which is known jointly by the originator and recipient, and which does not appear on the check, can also be used to derive the VAN. For example, when a check is drawn to multiple recipients, e.g., husband and
20 wife, each recipient's TIN (which does not appear on the check) may be used to derive the joint code and VAN. This makes it more difficult to fraudulently generate the VAN since the predetermined information not appearing on the check would not be generally known.

25 Figs. 8A and 8B illustrate the authentication process at a terminal when the recipient presents the originator's check to be cashed. The terminal communicates via a network of the banks involved in the transaction. Preferably, the terminal includes a device
30 which can read information directly from the check 32. Alternately, the terminal operator can manually key information into the terminal, based upon information appearing on the face of the check 32. At block 40, the recipient inserts his or her PIN, and at block 41,
35 identifies his bank and enters his TIN (RTIN) and all information required by the terminal to initiate the

transaction. An irreversible coder 42 processes the PIN to produce the coded PIN, CPNR, which is applied as the key input to a coder 44. A random number generator produces a random number (i.e., an arbitrary number) RNX
5 which is applied as the data input to coder 44. Coder 44 then produces a coded random number (i.e., a coded arbitrary number), CRNX, which is applied to mixer 48 along with RNX. The output of the mixer is, therefore, a signal which contains CRNX and RNX in a
10 converted form, so that neither number nor CPNR may readily be discerned from the signal. CRNX represents coded authentication information because it is a coded representation of CPNR, and because it is used by the system to authenticate the recipient and the
15 transaction.

The mixer signal, along with the information entered in block 41 and the information read from the check are transmitted to the computer at the recipient's bank (i.e., remote bank CPU) over preferably an
20 unsecured line (the use of an unsecured line is possible because CRNX and RNX, not CPNR, are transmitted from the mixer 48 to the sorter 62). The system first authenticates the identify of the check holder at the recipient's bank. Next, the information on the check,
25 as well as the originator and recipient, are authenticated at the originator's bank.

At the recipient's bank, the output of mixer 48 is received in a sorter 62, which separates CRNX and RNX, with CRNX being applied to a comparison
30 block 64 and RNX being applied as the data input to a coder 66. Based upon the recipient's TIN, RTIN, his bank's computer is able to access his file at block 68 and to extract his ROC (a non-secret number) and RN (a secret number), ROCR and RNR therefrom. ROCR and RNR
35 are applied as the data and key inputs, respectively, to an uncoder 70, which generates the recipient's CPN,

12

CPNR, which is applied as the key input to coder 66. Coder 66, therefore, reproduces the recipient's coded random number, CRNX (in the same manner as coder 44), which is applied as the second input to comparison
5 block 64. It should be appreciated that the CPNR output of uncoder 70 is the true CPNR derived from the bank's records. Accordingly, the CRNX produced by coder 66 is the true CRNX. Therefore, should the comparison at
10 block 64 fail, the authentication of the recipient has failed and it is presumed that recipient is not the party presenting the check. The transaction is therefore aborted. On the other hand, if the recipient's identity is authenticated, the transaction can proceed. The recipient's bank then communicates
15 with the originator's bank, conveying all the information about the transaction and requesting authorization to pay (block 71).

As shown in Fig. 8B, at the originator's bank, using OTIN (or the originator's PAN) as an index, the
20 originator's ROC and random number, RNO, are extracted from the originator's file at block 50. ROC is applied as the data input to an uncoder 52, and RNO is applied as the key input to uncoder 52. Uncoder 52 therefore reverses the operation performed by coder 20 (Fig. 6)
25 when the originator enrolled, producing the originator's CPN, CPNO. CPNO is then applied as the key input to a coder 56, which receives the recipient's TIN, RTIN, as the data input.

In accordance with the embodiment just
30 described, it is contemplated that security considerations may warrant revising the ROC from time to time independent of any transaction. Toward this end, CPN could be reconstituted from the current ROC and RN as in block 52. Next, a new RN is used with CPN to
35 generate a revised ROC, making use of a coder in the same manner as coder 20 of Fig. 6. The user's new RN

and ROC are stored and accessed, and CPN need only be reproduced at the bank where the user maintains an account.

In the same manner as coder 28 of Fig. 7, coder 56 therefore produces the joint key JK. JK is applied as the key input to an uncoder 58, which receives the VAN from check 32 as its data input. Uncoder 58 therefore reverses the coding operation performed by coder 30 of Fig. 7. If the information on the check has been unmodified, the coder 58 should therefore reproduce the information INFO from the check which was sought to be authenticated. In block 60, a comparison is made between the output of uncoder 58 and the information appearing on the check. Failure of this comparison is an indication that the check may have been modified after being issued, and the originator's bank notifies the recipient's bank that the check will not be honored. Alternatively, the joint key JK from the coder 56 can be used to code the information (INFO) from the check to generate a new VAN, which can then be compared with the VAN from the check to authenticate the check.

Should the comparison be favorable, this is an indication that the check is authentic and unmodified, and the originator's bank accesses the originator's account (block 61) to determine if the account is in order and has sufficient funds or credit to pay the check. The date of the check is determined to be acceptable. If the check control number does not appear in the originator's file as a previously cashed check, then the current check control number is saved to prevent fraudulent check reuse. The originator's bank generates a redeemed or redemption VAN (RVAN) in coder 54, using its bank key and the original VAN. RVAN is saved in the originator's file (block 55) and is recorded on the check (block 57). The originator's

account is then debited. The originator's bank then authorizes the recipient's bank to pay the check. On the other hand, if originator's bank finds any irregularity in the check or in the originator's
5 account, it will notify the recipient's bank that the check is dishonored.

The RVAN (and other RVAN's from other transactions) can be accessed from originators' files by banks and other financial institutions involved with
10 processing checks to determine the status of checks. Thus, by creating and storing the RVANs in the originators' files, fraudulent reuse of checks is avoided.

At block 72 (Fig. 8A), the recipient's bank
15 receives the originator's bank's instructions. It will then notify the recipient if the check has been dishonored. If the check has been honored, the recipient's account may be credited as in a deposit. Alternately, the recipient can receive payment
20 immediately if he is at an appropriate terminal, such as an automatic teller machine.

Essentially, the check has cleared automatically, on-line, without further check handling or processing.

25 In a transaction where the user cashes his own personal check, the originator and recipient are one and the same. A VAN is created from a joint code which combines information associated with the user, such as the user's identification number (TIN or PAN) and the
30 user's CPN, which is generated directly from a PIN entered by the user. When the VAN is authenticated, the joint code is derived by combining the user's identification number (TIN or PAN), and the user's true CPN, which is generated from the RN and ROC retrieved
35 from the user's file, with the TIN (or PAN) serving as a file index.

15

As noted above, in Fig. 8A it is possible to use an unsecured link between the mixer 48 and the sorter 62 because CRNX and RNX, not CPNR, are transmitted from the mixer 48 to the sorter 62.

5 However, a security problem still exists in using an unsecured line between the mixer 48 and the sorter 62 because the signal can be recorded and then played back later to attempt to fraudulently authenticate a fraudulent transaction. In an alternate embodiment of
10 the present invention, an anti-duplication variable authentication number (ADVAN) is generated at the recipient's terminal by coding at least a transmission date and time with the CPNR by a coder (not shown). The ADVAN is then mixed with the CRNX and the RNX by the
15 mixer 48 and sent to the remote bank CPU over the unsecured line to the sorter 62. At the remote bank CPU, the CPNR which is generated by the uncoder 70 is used to uncode the ADVAN to regenerate the transmission date and time. The signal received over the unsecured
20 line is then authenticated by comparing the regenerated transmission date and time to a reception date and time (that is, the date and time at which the signal was received at the remote bank CPU). In this manner, the recipient and transaction are further authenticated.

25 According to another embodiment of the present invention, RNX is generated at both the recipient terminal and the remote bank CPU. To generate the RNX at the remote bank CPU, a random number generator is located at the remote bank CPU, wherein the random
30 number generator at the remote bank CPU is similar to and synchronized with the random number generator 46 located at the recipient's terminal. Instead of transferring the RNX and the CRNX, only the CRNX is transferred over the unsecured line from the recipient's
35 terminal to the remote bank CPU. At the remote bank CPU, the CPNR generated by the uncoder 70 is coded by

16

- 16 -

the coder 66 with the RNK generated at the remote bank CPU to generate the CRNX. The generated CRNX is then compared by the comparator 64 with the CRNX transferred from the recipient's terminal to the remote bank CPU to
5 authenticate the recipient and the signal received over the unsecured line. In this manner, the recipient and transaction are further authenticated.

According to another embodiment of the present invention, CRNX is never generated. Instead, the CPNR
10 generated by the irreversible coder 42 is sent to the remote bank CPU over a secured line, rather than over an unsecured line. The CPNR generated by the uncoder 70 is then compared by a comparator (not shown) with the CPNR sent from the recipient's terminal to the remote bank
15 CPU to authenticate the recipient. In this alternate embodiment, the random number generator 46, coder 44, mixer 48, sorter 62, and coder 66 are not required, although a secure line is required.

Figs. 9-12 constitute a functional block
20 diagram illustrating the present invention in a credential issuing and authentication system. The system involves the same three phases of operation as the check transaction system of Figs. 6, 7, 8A and 8B. However, all users are enrolled by an authorized
25 official who must be enrolled first. Accordingly, there are two enrollment processes which are somewhat different. The first one is enrollment of the official, and the second one is enrollment of a user prior to or at the time of issuing his credentials. It is
30 contemplated that this system would be useful for all types of credentials and records; for example, motor vehicle registrations, social security cards, passports, birth certificates and all types of identification cards or personal storage media. This system would also be
35 useful in protecting against unauthorized access to all types of records, as previously indicated.

17

Fig. 9 illustrates enrollment of the official. This can be accomplished at a terminal or computer which is in communication with a remote computer over a link which is assumed to be secure. The remote computer may, for example, be the central computer at the agency issuing the credential. At the remote computer, number generator 100 generates a random number which, at block 102, is compared to a current list of all assigned personal keys. If the random number does not correspond to an assigned personal key, then the random number is assigned as the personal key, PKO, of the official being enrolled. Alternatively, PKO can be selected at random, from a list of unused PKO's, and the list of available PKO's would thereby be diminished. In yet another alternative, PKO could be accessed from a counter, such as a pseudorandom or an ordinary sequential counter the output of which may be coded with a secret key. The size, or length, of PKO can be such as to provide a full size memory address or an offset or an index extension, to limit or enlarge the memory space wherein concealed files are stored. PKO is then transmitted over the secure link to the enrollment terminal.

At the terminal, the official enters his PIN and name and various other information required by the system. The name can be numerically coded by using a telephone type key pad. The PIN is applied to an irreversible coder 104, which produces his coded PIN CPNO. CPNO is applied as the key input to a coder 106, which receives PKO as the data input. The data output of coder 106 is the official's coded personal key, CPKO, which is applied as an input to mixer 107. The official's name code and TIN, OTIN, are also applied as inputs to mixer 107. CPKO represents a coded address since it is a coded representation of PKO.

The output of mixer 107 is transmitted back to the remote computer over the secure link. At the remote computer, sorter 109 separates the received signal into its component parts: CPKO, the official's name code, and OTIN. At block 108, CPKO and the official's name code are then saved (i.e., written) into File No. 1 assigned to the official with the official's TIN, OTIN, serving as a File No. 1 index. It is assumed that during the official's enrollment various other information will be provided by the official over the secure line and may be stored in his File No. 1. It should be noted that OTIN is not secret and, therefore, the location of File No. 1 and the contents of File No. 1 (including CPKO) are not secret.


At block 112, PKO is used as an index for File No. 2, which is also allocated to the enrolling official. The location of File No. 2 (and thus, the contents of File No. 2) is concealed, since PKO is secret and not stored anywhere in the system. The information or records which are stored in File No. 2 can be coded or uncoded. The memory space wherein concealed files are stored may be previously filled (or pre-loaded) with dummy or false information to make the contents and locations of authentic allocated files undistinguishable from the dummy files. The concealed File No. 2 can also be used to store the ROC and RN (or store only RN, since only RN is secret -- ROC could be stored in a non-secret file, such as Official's File No. 1), as previously described in Figs. 6, 7, 8A and 8B, to reconstitute a user's coded PIN, CPN. The concealed File No. 2 can also be used to store other secret information (not shown) associated with the official. An official's coded number, CNO, is generated at the output of coder 110, and is saved in File No. 2 at block 112. The key input to coder 110 is CPKO and the data input to coder 110 is PKO or an arbitrary

predetermined number (APN). CNO represents coded authentication information because it is a coded representation of CPKO, and because it is used by the system to authenticate the official.

5 At coder 110, CPKO and PKO can be interchanged as the key and data inputs. However, the arrangement selected must then be used consistently in each phase of the operation of the system.

10 Those skilled in the art will appreciate that the present embodiment offers an additional level of security in that, not only is secret information unavailable to a person who does not know the related PK and PIN, but that person is even unable to determine the location of the file containing the information, and is
15 unable to uncode the information contained therein.

 Fig. 10 illustrates user enrollment. The user is enrolled by a previously enrolled official, who verifies the user's identity, based on acceptable documentation. Before the user can be enrolled, the
20 official's identity and authority are preferably authenticated. The official operates the terminal, where he enters his PIN, and his TIN, OTIN, and the name code used during his enrollment, which was stored in his "File 1". OTIN is transmitted to the remote computer,
25 where it is used as an index to access CPKO from the official's File No. 1, and CPKO is returned to the terminal. The official's PIN is applied to the irreversible coder 104, which produces CPNO. CPNO is applied as the key input to an uncoder 114, which
30 receives CPKO as a data input over the secure link from the remote computer. It will be appreciated that uncoder 114 simply reverses the process of coder 106 of Fig. 9, therefore producing PKO. PKO is applied to a mixer 118, the other input to which is the official's
35 name code. The output of mixer 118 is then transmitted to the remote computer.



At the remote computer, the signal transmitted from mixer 118 is received in a sorter 124, which separates out PKO, and the name code. The extracted PKO is utilized as an index to address the official's "File 2" whereby CNO is read. The CNO read from File No. 2 is compared against the CNO generated by coder 120, which has as its data input PKO which is extracted by sorter 124 and as its key input is CPKO read from "File 1". Should this comparison fail, the identity of the official is not authenticated and the enrollment of the user is aborted. Assuming that the comparison is successful, comparator 130 is then enabled. At block 130, the name code which is extracted from sorter 124 is compared against the name code read from the official's "File 1" (using OTIN as index). Should this comparison fail, the enrollment of the user is aborted. Should the comparison be successful, the official has been fully authenticated and the user's enrollment may proceed.

At the remote computer, number generator 100 generates a unique random number, which is assigned to the user as a personal address key, PKU. Alternately, PKU can be generated from a counter as previously described. As discussed below, PKU represents a predetermined secret address of a File No. 2 associated with the user. PKU is transmitted over the secure link to the enrollment terminal, where it is applied to the data input of coder 113.

The user operates the terminal and selects a PIN which he enters along with his TIN, UTIN. The user's PIN is applied to the irreversible coder 104, which produces the user's coded PIN, CPNU. CPNU is applied as a key input to coders 113 and 115. The output of coder 113 is the user's coded personal key, CPKU (which represents a coded address of the user's File No. 2), which is applied as a data input to

coder 115. The output of coder 115 is the user's coded number, CNU, which is applied to the input of mixer 116. The user's TIN, UTIN and CPKU are also applied as inputs to mixer 116. The output of mixer 116 is transmitted
5 back to the remote computer over the secure link. CNU represents coded authentication information because it is a coded representation of CPKU, and because it is used by the system to authenticate the user.

At the remote computer, sorter 119 separates
10 the received signal into its component parts: CPKU, CNU and UTIN. At block 108, CPKU and CNU are saved (i.e., written) into File No. 1 assigned to the user, with the user's TIN, UTIN serving as a File No. 1 index. It should be noted that CPKU and CNU may be recorded on the
15 user's credential when they are generated at the terminal. It should also be noted that UTIN is not secret, and therefore, the location and contents of the user's File No. 1 are not secret. It should further be noted that the official's CNO is stored in the
20 official's secret File No. 2 (Fig. 9) while the user's CNU is stored in the user's non-secret File No. 1 (Fig. 10A), even though both CNO and CNU are used to authenticate the official and the user, respectively. These two different ways for storing CNO and CNU (as
25 shown in Figs. 9 and 10A) illustrate two embodiments of the present invention.

The user's PK, PKU (or an arbitrary predetermined number APN), is applied as the data input to a coder 132, which receives the official's CPKU as a
30 key input. Coder 132 produces a joint key, JKU, which it will be appreciated, is determined by information related to the user and information related to the official. Using PKU as an address, the joint key is written into the user's "File 2" at block 112', and
35 using PKO and UTIN as address indices, the joint key JKU is written into the official's "File 2" at block 134

22

(Fig. 10B). These writes are enabled as a result of the success of the comparison occurring at block 130. Accordingly, the user's "File 2" will contain a joint key, and the official's "File 2" will contain a joint
5 key for each user the official enrolls. Since the user's file 2 is addressed by PKU (which is secret), the location and contents of the user's file 2 are secret. At coder 132, when the joint key JKU is generated, CPK and PK can be interchanged as key and data inputs, or as
10 to user and official inputs. However, the arrangement selected must then be used consistently.

Fig. 11 illustrates issuance of the credential. This is shown separate from the user enrollment process of Fig. 10. However, in many
15 instances, it would occur at the same time. In the preferred embodiment, this process is shown as occurring at the agency's computer, although it may be performed by the official from a terminal where he may communicate with the computer. It is assumed that the official has
20 a credential printer or recorder which contains credential forms on which information is printed or recorded to produce the actual credential. However, it is also possible to create the credential by inserting information manually or on a typewriter, provided the
25 necessary information derived by the system can be entered. The official enters the usual information (INFO) normally contained on a particular credential 145. The user's TIN may also be recorded on the credential. Alternately, the user's CPKU and CNU
30 may be recorded on the credential, after being extracted from the user's File No. 1, with UTIN serving as a file index. If CPKU and CNU are recorded on the credential, they may be erased from the user's File No. 1. Alternatively, only CNU may be recorded on the
35 credential, with CPKU remaining in File No. 1, or vice versa.

23

The issuing process continues with the official entering his PIN, which is applied to an irreversible coder 140 to produce his CPNO, which is applied as a key input to an uncoder 142. At block 144, the official's TIN, OTIN is utilized as an index to access the official's "File 1", so that CPKO may be read therefrom and applied as the input to uncoder 142. Uncoder 142 therefore performs the same process as uncoder 114 of Fig. 10 to produce PKO. At block 146, PKO and UTIN are utilized as address indices to access the official's "File 2" and JKU is read therefrom. The information INFO on the credential is applied as the data input to a coder 152 and JKU is applied as the key input, whereby coder 152 codes the INFO to produce a VAN, which is recorded on the credential. After recording the VAN on the credential, the joint key, JKU, may be erased from the official's File 2, where it was stored (or held in escrow or in trust), until the credential was issued. Alternately, the authentic JKU may be replaced with a false or dummy JK for security purposes. This completes the issuance of the credential 145. It should be noted that the joint key JKU stored in the official's File No. 2 can only be used in a transaction if a party exists with knowledge of the official's PIN, since this PIN is required to access the official's File No. 2 (at block 146). Thus, a person who does not have knowledge of the official's PIN (such as an unscrupulous person trying to issue a fraudulent credential) cannot legitimately issue a credential.

The VAN which is generated from information (INFO) recorded on the credential, or from information which is otherwise stored by the system, can include (coded) personal descriptive details to further identify the user (in addition to the user's PIN and TIN) in order to limit the use of the credential to the sole individual to whom it was issued (or sold). Thus, items

such as bank cards, tickets, green cards, food stamps, ballots, travel checks, FAX messages, etc., can be protected and used solely by the individuals to whom they were issued. Also, the use of the credential may
5 be enlarged to include a group, such as a family, by coding such information into the VAN.

Fig. 12 illustrates the authentication of an issued credential. This is preferably performed at a terminal provided for that purpose. The terminal
10 includes a reading device for the credential 145 and an input device, such as a keypad for the user. The information could, however, be read from the credential and keyed in by hand. The terminal communicates with the remote processor via a preferably secure link.

15 As part of the credential authentication process, the identity of the user is authenticated. This requires that the user enter certain information at the terminal, including a PIN and user's TIN, UTIN, which is transmitted to the remote computer, which
20 returns CPKU and CNU (box 178) via a secure data link. Alternatively, CPKU and CNU could have been recorded on the credential (or on some other item in the possession of the user, such as a card having a magnetic stripe for storing data) and inputted directly into the terminal.
25 The PIN is applied to the irreversible coder 170 which produces CPNU. CPNU is applied as the key input to coder 172 and uncoder 174. Coder 172 receives CPKU as a data input. It should be noted that coder 172 performs in the same manner as coder 115, which produced CNU at
30 its output during the user's enrollment. The output of coder 172 is applied as an input to the comparator at block 182, which also has as an input the CNU extracted from the user's File No. 1 (or inputted from the user's credential).

75

Should this comparison fail, the identity of the user is not authenticated, and the credential authentication is aborted. Assuming the comparison is successful, the user is identified, and the credential authentication, with access to the hidden File No. 2, 5 ensues. The favorable output from comparator 182 enables uncoder 174. The data input to uncoder 174 is the user's CPKU. The key input to uncoder 174 is the user's CPNU, as already explained. It will be 10 appreciated that uncoder 174 simply reverses the process of coder 113 of Fig. 10, therefore producing PKU. PKU is applied to a mixer 176 which also receives the VAN and INFO of the credential. The output of mixer 176 is then transmitted to the remote computer over the secure 15 link.

At the remote computer, UTIN is utilized as an index to access the user's "File 1" at block 178. This permits reading of CPKU and CNU from the file, whereby CPKU and CNU were transmitted back to the user's 20 terminal. At the remote computer, the signal transmitted from mixer 176 is received in sorter 180, which separates out PKU, VAN and INFO. The extracted PKU is utilized to address the user's "File No. 2" at block 184 whereby JKU is read. It will be appreciated 25 that the user's File No. 2 has been accessed by an authorized user without reference to, or use of, information stored in the file. The VAN extracted from sorter 180 is applied as a data input to an uncoder 162, which receives the joint key JKU extracted from the 30 user's "File 2" at block 184. It will be appreciated that uncoder 162 therefore reverses the process performed by coder 152 of Fig. 11. Assuming the VAN on the credential is the same one as originally recorded, uncoder 162 will have produced the recovered INFO which 35 should be the same as the actual INFO recorded on the credential.

26

At block 169, the INFO from the credential is compared to the INFO recovered from uncoder 162. Should the comparison fail, this is an indication that INFO on the credential has been modified, and the credential is indicated as not being authentic. Should the comparison be successful, this is an indication that INFO is accurate, and the authenticity of the credential is confirmed. Alternatively, the credential information from the credential is coded using the JKU from the user's File No. 2 to generate a new VAN, which is compared with the VAN from the credential to authenticate the credential.

In order to enhance the security of this system, it would be desirable to make unassigned areas of memory indistinguishable from those utilized to store information for the "File 1" and "File 2" information. This is accomplished by pre-storing pseudo-information in unused memory allocated as hidden memory space. This pseudo-information constitutes random information arranged in the same format as actual files. This prevents an intruder from searching memory for structures that look like actual information files and using the uncovered information to work backwards to breach security.

Figs. 13A-13E, when arranged as shown in Fig. 14, constitute a functional block diagram illustrating further aspects of the check transaction system of Figs. 6, 7, 8A and 8B. Specifically, these figures illustrate a three-party check transaction, with each of the participants and the fidelity of the information on the check being authenticated, the check being automatically cleared, and the funds of the participants being immediately credited or debited, all of these processes being performed on-line. The participating parties in this transaction are the check originator, whose account is to be debited; the check

77

recipient to whom the check is drawn; and the check redeemer, who is cashing the check for the recipient or accepting it in payment for goods or services, and whose account is to be credited. In addition, the banks for
5 each of these participants will also be participating in the transaction, and the messages generated by these banks will be authenticated. It is assumed that any individual or bank participating in the system will have enrolled as illustrated in Fig. 6. In addition, it is
10 assumed that a check used in the system is generated in the manner illustrated in Fig. 7.

Referring first to Fig. 13A, the recipient of the originator's check has presented the check to the redeemer (block 200). The recipient and the redeemer
15 are at a terminal which includes appropriate input means 202. Preferably, the input means includes a check reader and a keypad for each of them. However, in the absence of a check reader, it is also possible to key in information from the face of the check. The check is
20 examined to determine if it contains a redemption VAN from a previous transaction. The presence of a redemption VAN is an indication that the check was used previously, and it will not be honored. If a redemption VAN is not present, then the transaction can proceed.
25 It is assumed that the redeemer's bank identification number (RDBIN), and TIN are stored in the terminal, otherwise the redeemer keys in his bank's name and TIN, and the recipient keys in his TIN, PIN and bank's name. A bank directory is addressed at block 203 to produce
30 the recipient bank's identification number (RCPBIN). The recipient's PIN is applied to an irreversible coder 42, which produces his CPNR. Irreversible coder 42, coder 44, random number generator 46, and mixer 48 are the same components illustrated in Fig. 8A
35 and cooperate in the same manner to produce RNX, CRNX, in a mixed form at the output of mixer 48.

24

- 28 -

The terminal has available to it the redeemer's bank key (RDBK), which is applied to the key input of a coder 204, the data input to which is the terminal ID (TID), which is generated by the terminal.

5 Coder 204 then produces a joint terminal bank key (JTBK), which is applied as the key input to a coder 206, the data input to which is the output of mixer 48. The mixer output is therefore coded with a joint key JTBK which has been generated on the basis of

10 information related to the redeemer's bank identity and the terminal identity.

The output of coder 206 and the information from input means 202, and the recipient's TIN, RCPTIN, and the recipient's bank ID number, RCPBIN, are then

15 transmitted to the computer at the redeemer's bank. At the redeemer's bank (Fig. 13B), all of the received information is placed in temporary storage (block 208).

The redeemer's TIN, RDTIN, (originally stored in the terminal, or keyed in by the redeemer), is then

20 utilized as an index to access his account file, at block 210.

The check control number (CCN) of the present check is then compared to the CCN's stored in the redeemer's file during previous transactions (block

25 212), and the transaction is terminated if the present CCN matches that of a previously processed check. If the CCN of the present check is not a duplicate, processing continues.

RDBIN, and RCPBIN are utilized as indices to

30 access a bank key table (block 213), which produces the redeemer's bank key RDBK, and the recipient's bank key RCBK, which are applied as the data and key inputs, respectively, to a coder 214. The coder 214 then produces a joint bank key JBK, which is derived from

35 information related to the identity of the redeemer's bank and the identity of the recipient's bank.

26

The terminal identification (TID) is input to a coder 216, which has as a key input RDBK. In the same manner as coder 204, coder 216 therefore produces JTBK, which is applied as a key input to an uncoder 218. The
5 data input to uncoder 218 is the information in temporary storage 208 which was originally received from coder 206. Coder 218 therefore reverses the process performed by coder 206, yielding the output of mixer 48, which is applied as a data input to a coder 220. The
10 key input to coder 220 is JBK, so that the output of mixer 48 is now coded with the joint bank key JBK. The output of coder 220 is then transmitted in a message to the recipient's bank, along with RCPTIN, RDBIN, and RCPBIN.

15 At the recipient's bank, the received information is saved in temporary storage 230. RCPBIN and RDBIN are then applied to a bank key table (block 232), to yield RCBK and RDBK, which are applied as the key and data inputs, respectively, to a
20 coder 234. In the same manner as coder 214, coder 234 therefore yields the joint bank key JBK, which is applied as a key input to uncoder 236. The data input to this uncoder 236 is the coded combination of RNX and CRNX produced by coder 220. Uncoder 236 therefore
25 reverses the process of coder 220, yielding the mixture of RNX and CRNX as an output. This mixture is applied as an input to a sorter 238, to recover RNX and CRNX.

The recipient's TIN, RCPTIN, is utilized as an index to access the recipient's file at block 240 and
30 read therefrom the random number, RNR, and his ROC, which are applied as the key and data inputs, respectively, to an uncoder 242. In the same manner as uncoder 70 of Fig. 8A, uncoder 242 therefore derives the true CPNR, which is applied as a key input to a
35 coder 244, which receives RNX as a data input. The data output of coder 244 is therefore the true CRNX.

At block 246, this true CRNX is compared to the CRNX derived from sorter 238. If this comparison is favorable, the recipient's identity is confirmed, and processing may proceed. Otherwise, processing is terminated, with the originator's check being dishonored, because the recipient has not been properly authenticated. The recipient's bank then transmits a message to the redeemer's bank, informing it whether or not the recipient has been authenticated. If the recipient has not been authenticated, the redeemer's terminal is notified, and processing will terminate.

Assuming that the recipient has been authenticated, the recipient's bank message includes various information which is temporarily stored by the redeemer's bank (block 250 of Fig. 13C). At block 252, the originator's bank identification number ORBIN, which was read from the check, and the redeemer's bank identification number RDBIN are applied as indices to a bank key table to recover bank keys for these banks, OBK and RDBK, respectively. These keys are applied to a coder 254 to produce a joint bank key JBK', which is therefore dependent upon information related to the originator's bank and the information related to the redeemer's bank. JBK' is applied to the key input of a coder 256, which receives the original VAN, OVAN, (from the check) as a data input. The output of coder 256 is a redeemer's bank RDEVAN, which is transmitted to the originator's bank, along with various transaction information and the information from the check. RDEVAN serves to authenticate the communication between the banks.

At the originator's bank, the received information is temporarily stored at block 258. ORBIN and RDBIN are then utilized to reference a bank key table at block 260, whereby OBK and RDBK are extracted in the same manner as in block 252. The joint key JBK'

31

is then generated by means of a coder 262 in the same manner as coder 254. JBK' is then applied as the key input to an uncoder 264, which receives RDBVAN as a data input. This uncoder 264 therefore reverses the process
5 performed by coder 256 and produces an extracted OVAN, which is applied to a comparator 266 (as shown in Fig. 13D).

The originator's personal account number ORGPAN which originally appeared on the check is
10 utilized as an index to access the originator's account file at block 268 of Fig. 13C. This provides access to various information about the originator's account including the balance and a list of prior check control numbers (CCN's), and in addition, provides access to his
15 revisable owner code ROCO and random number RNO, which are applied as the data and key inputs to an uncoder, to produce the originator's coded pin CPNO. CPNO is then applied as the key input to a coder 272 (Fig. 13D) which receives the recipient's TIN, RCPTIN, as a data input.
20 The output of coder 272 is the joint key JK, which is applied as the key input to a coder 274, which receives the check information as a data input. It will be appreciated that coders 272 and 274 regenerate the original VAN, OVAN, from the check in the same manner as
25 coders 28 and 30 of Fig. 7. This regenerated VAN is then compared to the extracted VAN at block 266. If this comparison fails, it is an indication that the check information may have been tampered with and the originator's bank informs the redeemer's bank that the
30 check will be dishonored. On the other hand, if the comparison succeeds, the process continues.

The originator's bank then performs a series of computations, including determining whether the CCN of the check is proper (i.e., has not been used before)
35 and whether the originator has a sufficient balance in his account (or credit) to cover the check, and whether

the date of the check is acceptable. In the case of any defects, the check will be dishonored and the process will terminate. Assuming that everything is in order, modification of the originator's account is approved,
5 and a record of the check created at block 271, with the new information being added to temporary storage at block 273. Coders 275 and 276 are then utilized to encode the original VAN, OVAN, into an originator's bank VAN OBVAN. Various information about the transaction,
10 and authorization to credit the redeemer's account are then transmitted is a message to the redeemer's bank.

At the redeemer's bank, all of the received information is stored in temporary storage at block 278. At block 280, coder 282 and uncoder 284, steps are
15 performed to extract OVAN from OBVAN in a manner which is similar to that which was done in block 260, coder 262 and uncoder 264. This extracted OVAN is then applied to a comparator 286 of Fig. 13E, which receives as an additional input the stored OVAN from the check
20 presented by the recipient. If this comparison fails, the process has not been authenticated, and the originator's bank will be notified. On the other hand, if the comparison succeeds, this is an indication that full authentication of the entire process and all
25 parties has occurred and that the message received from the originator's bank is authentic.

Processing then continues by accessing the redeemer's account at block 288, computing a new balance at block 290 and updating the redeemer's account. The
30 redeemer's bank then transmits a message back to the originator's bank, informing it that the redeemer's account has been credited. This information is saved at the originator's bank in temporary storage at block 291. The originator's bank then accesses the originator's
35 account file using his personal account number ORGPAN as

33

an index, and updates his account with the information that was placed in temporary storage at block 273 (Fig. 13D).

5 The redeemer's bank also communicates with the terminal at which the check was presented (block 294 of Fig. 13D), and informs it that the transaction has been satisfactorily completed and that the recipient may receive payment in the form of cash, goods or services (block 296). The terminal prints the redemption VAN
10 (RDBVAN) on the check.

Although various embodiments of the present invention have been described herein as useful for particular types of transactions, those skilled in the art will appreciate that they actually have universal
15 utility. For example, the last embodiment (depicted in Figs. 13A-13E) was described as useful in a check transaction system, but it will be appreciated that it would also be useful in a bill payment system as well as a paperless/cashless system (as further described
20 below).

Figs. 15A, 15B and 15C are functional block diagrams of a credential issuing and authentication system according to an alternate embodiment of the present invention, wherein the alternate embodiment
25 includes many of the features of the embodiments depicted in Figs. 6-8 and Figs. 9-12. For example, the alternate embodiment of Figs. 15A-15C include steps for enrolling an official, enrolling a user, issuing a credential, and authenticating the credential. Fig. 15A
30 illustrates user enrollment, Fig. 15B illustrates issuance of a credential, and Fig. 15C illustrates the authentication of an issued credential. In the alternate embodiment of Figs. 15A-15C, enrollment of the official is the same as shown in Fig. 9 and, therefore,
35 shall not be discussed further.

34

Referring to Fig. 15A, a user is enrolled by a previously enrolled official who verifies the user's identity, based on acceptable documentation. Before the user can be enrolled, the official's identity and
5 authority must be authenticated. The official operates a terminal, where he enters his PIN and his TIN, OTIN, and the name code used during his enrollment, which was stored in his File No. 1. OTIN is transmitted to the remote computer, where it is used as an index or address
10 to access the official's File No. 1 and retrieve CPKO (block 1546). CPKO is returned to the terminal.

The official's PIN is applied to irreversible coder 1530, which produces CPNO. CPNO is applied as the key input to an uncoder 1532, which receives CPKO as a
15 data input from the remote computer, and which uncodes CPKO to generate PKO. CPKO is also applied as a key input to a coder 1534, which receives PKO as an input. The coder 1534 codes PKO using CPKO as the key input to generate a coded number for the official (CNO), which
20 represents coded authentication information. Another coder 1538 codes the official's name code using CNO as a key input to generate a coded name code. A mixer 1536 mixes the coded name code, PKO, and CNO and transmits the mixed signal to the sorter 1540 at the remote
25 computer over preferably a secure link.

At the remote computer, the signal transmitted from mixer 1536 is received by the sorter 1540, which separates out PKO, CNO, and the coded name code. PKO is applied as an index (or address) to access the
30 official's File No. 2 and to thereby retrieve CNO, which was previously stored in the official's File No. 2 during the enrollment of the official (see Fig. 9). The CNO transmitted from the terminal and the CNO retrieved from File No. 2 are then compared in a comparator 1542.
35 If the comparison fails, the identify of the official is not authenticated and the enrollment of the user is

35

- 35 -

aborted. Assuming that the comparison is successful, the comparator 1542 is enabled and sends a signal to an uncoder 1544. The uncoder 1544 then uncodes the coded name code using the CNO retrieved from the official's
5 File No. 2 to regenerate the name code. The name code is also accessed from File No. 1 and then compared at 1550. If the comparison fails, the identify of the official is not authenticated and the enrollment of the user is aborted. Assuming that the comparison is
10 successful, the comparator 1550 sends an authentication signal ("okay to enroll user") and user enrollment begins. It should be noted that the "okay to enroll user" signal is applied as a write enabled to the official's File No. 2 at 1552 to save a joint key JKU
15 therein (described below).

At the remote computer, number generator 1516 generates a unique random number (as discussed above), which is assigned to the user as a secret predetermined address or key, PKU. PKU is transmitted over a secured
20 link to the enrollment terminal, where it is applied to the data input of a coder 1504.

The user operates a terminal and selects a PIN which he enters along with his TIN, UTIN. The user's PIN is applied to irreversible coder 1502 which produces
25 the user's coded PIN, CPNU. CPNU is applied as a key input to coder 1504. The output of the coder 1504 is the user's coded predetermined address or key, CPKU. CPKU may be stored in a user record (at block 1510). A mixer 1506 mixes CPNU and CPKU and transmits the mixed
30 signal to the remote CPU.

At the remote computer, sorter 1512 separates the received signal into its component parts CPKU and CPN. At the remote computer, a random number RN is generated (as discussed above) and applied as a key
35 input to coder 1518. The coder 1518 also receives CPN as an input and thereby generates a revisable owner code

36

(ROC). ROC is stored in the user's File No. 1 (at block 1520), wherein the user's File No. 1 is accessed (or addressed) using UTIN. CPKU is also stored in the user's File No. 1 (at block 1520).

5 PKU is applied as an index or address to the user's File No. 2 in order to store RN (at block 1522). PKU is secret in the system and, therefore, the location and contents of the user's File No. 2 (including RN) is secret. Additional information may be coded in a
10 coder 1524 using CPKU as a key input to generate coded information which is also stored in the user's File No. 2. The information which is coded using CPKU in the coder 1524 may include the secret information RN.

 PKU is applied as an input to coder 1528,
15 which also receives CPKO as a key input. The coder 1528 generates a user joint key (JKU) which is stored in the user's File No. 2. JKU is also stored in the official's File No. 2 (at block 1552).

 It should be noted that the storage and
20 handling of RN and ROC in the embodiment shown in Fig. 15A is different from the storage and handling of RN and ROC shown in Fig. 6. In Fig. 6, the file in which RN and ROC are stored is generally non-secret because it is indexed (or addressed) by generally non-
25 secret user information (such as the user's TIN). However, in the embodiment shown in Fig. 15A, the non-secret ROC is stored in the user's File No. 1, which is non-secret, and the secret RN is stored in the user's File No. 2, which is secret (since it is accessed or
30 addressed using the secret PKU). Therefore, the embodiment of 15A includes an additional level of security and protection over the embodiment shown in Fig. 6.

 Fig. 15B illustrates issuance of a credential
35 according to the alternate embodiment of the present invention. The issuance of credential in the alternate

37

embodiment is essentially the same as the issuance of credentials in the previous embodiment shown in Fig. 11. Note, however, that it is possible to record the ROC retrieved from the user File No. 1 on the
5 credential 1564 since the ROC is public (although the ROC could also have been recorded on the credential in the previous embodiment).

Fig. 15C illustrates the authentication of an issued credential. This is preferably performed at a
10 terminal provided for that purpose. The terminal includes a reading device for the credential 1564 and an input device, such as a keypad, for the user. The information from the credential 1564 could, however, be keyed in by hand. The terminal communicates with the
15 remote processor via a preferably secured link. As part of the credential authentication process, the identity of the user is authenticated. Specifically, the user enters his PIN which is applied as an input to irreversible coder 1570, which generates a coded PIN
20 (CPNU). The user also enters his TIN (UTIN), which is used to access the user File No. 1 (at block 1588) and retrieve CPKU, which is transmitted from the remote CPU to the terminal. CPKU is applied as an input to coder 1574, which also receives CPNU as a key input.
25 The coder 1574 generates a coded number CNU, which represents coded authentication information. CPKU is also applied as an input to uncoder 1572, which also receives CPNU as a key input. The uncoder 1572 uncodes CPKU to regenerate PKU. Both CNU and PKU are mixed by
30 mixer 1576 and sent to the sorter 1578 at the remote CPU.

At the remote CPU, the sorter 1578 separates the signal into its component parts PKU and CNU. PKU is applied as an index into the user's File No. 2 in order
35 to retrieve the secret information RN. UTIN is applied as an index to the user's File No. 1 to retrieve the

non-secret revisable owner code (ROC). ROC is applied as an input to uncoder 1584, and the secret information RN is applied as a key input to uncoder 1584. The uncoder 1584 thereby uncodes ROC using RN in order to
5 regenerate CPNU as RCPN, which is applied as a key input at coder 1582. CPKU, which is read from the credential 1564, is applied as an input to coder 1582. The coder 1582 codes CPKU using RCPN as a key input in order to generate a coded number CNU. The generated
10 coded number CNU is compared at the comparator 1580 to the coded number CNU received from the terminal. If the comparison fails, authentication of the user aborts. However, if the comparison is successful, the user is authenticated and the process continues by
15 authenticating the credential 1564.

The credential 1564 is authenticated by reading the official's ID number OTIN from the credential and using OTIN as an index in order to access the official's File No. 1 and read CPKO (block 1599).
20 CPKO is applied as an input to coder 1598 which also receives PKU as a key input. The coder 1598 codes CPKO using PKU in order to regenerate the user joint key JKU. JKU is also read from the user's File No. 2 using PKU as an index and then applied to a comparator 1596. The
25 comparator 1596 compares the JKU which was retrieved from the user's File No. 2 and the JKU which was generated by the coder 1598. If the comparison fails, then authentication of the credential aborts. However, if the comparison is successful, the comparator 1596 is
30 enabled and sends an okay signal to a comparator 1594.

The JKU retrieved from the user's File No. 2 at 1586 is applied to an uncoder 1592, which also receives as an input the VAN which was read from the credential 1564. The uncoder 1592 uncodes the VAN in
35 order to regenerate INFO. The regenerated INFO is applied as an input to the comparator 1594, which also

39

receives the INFO read from the credential 1564. The comparator 1594 compares the regenerated INFO and the INFO from the credential and if the comparison is successful, the credential is authenticated. Otherwise, the credential is not authenticated.

As noted above, in Fig.15C, the transmission link between the mixer 1576 and the sorter 1578 is preferably secured since using an unsecured link would present a potential security problem. For example, the signal from the mixer 1576 could be recorded and then transmitted to the sorter 1578 at a later date in order to attempt to fraudulently authenticate a user and a credential. In accordance with an alternate embodiment of the present invention, an anti-duplication variable authentication number (ADVAN) is generated at the terminal by coding at least a transmission date and a time with the CPNU. The ADVAN is then mixed with the CNU and the PKU at the mixer 1576 and sent to the sorter 1578 at the remote CPU over an unsecured link. At the remote CPU, the received ADVAN is uncoded using the derived RCPN to regenerate the transmission date and the time. The regenerated transmission date and time are then compared to a reception date and time (that is, the date and time at which the signal was received at the sorter 1578) and if the comparison is successful, the information transmitted over the transmission medium between the mixer 1576 and the sorter 1578 is authenticated. In this manner, the user and credential are further authenticated.

Alternatively, a semi-random number (not shown) is generated at the terminal using a counter or other random number generator (not shown). The semi-random number is coded using the CPNU to generate a coded semi-random number. The coded semi-random number is then transmitted along with CNU and PKU to the remote CPU over an unsecured medium. At the remote CPU, the

47

coded semi-random number is uncoded using RCPN to regenerate the semi-random number. A second semi-random number is then generated at the remote CPU using another counter or random number generator (not shown) which is
5 generally synchronized with the counter (not shown) at the terminal. The communication medium between the mixer 1576 and the sorter 1578 is then authenticated by comparing at the remote CPU the regenerated semi-random number to the second semi-random number which was
10 generated at the remote CPU. If the comparison is successful, then the information transmitted over the communication medium between the mixer 1576 and the sorter 1578 is authenticated. In this manner, the user and credential are further authenticated.

15 As described above, the predetermined secret address PKU is coded to generate the coded secret address CPKU. According to an alternate embodiment, PKU comprises one or more components which are combinable to form the predetermined secret address PKU. In this
20 alternative embodiment, only one of the components of the PKU is transmitted from the remote CPU to the terminal. The coder 1504 (Fig. 15A) codes this one component of the PKU to generate CPKU. Therefore, in this alternate embodiment, CPKU represents a coded
25 portion of the PKU. Then, to access the user's File No. 2, the CPKU is uncoded as described above to regenerate the portion of the PKU. This PKU portion is combined with the other portions of the PKU to regenerate the PKU, which is then used to access the
30 user's File No. 2. The other portions of the PKU may be stored throughout the system, such as in the operating system, in the executive program, in files, etc.

Fig. 16 is a functional block diagram of a system for authenticating the identity of a party and
35 for authorizing access to a party's hidden (or secret) file according to an alternate embodiment of the present

41

invention. The party's hidden file (such as hidden memory file 1622) may contain coded or uncoded secret information. In the embodiment of Fig. 16, the party is in possession of a portable storage media, such as a
5 card 1602 having a magnetic stripe for recording information thereon. The card 1602 is issued by an agency, or a bank, during enrollment of the party. Information recorded on the card 1602 includes the party's revisable owner code (ROC), a coded address
10 (CPK) of the hidden file 1622, an agency identification number (AID or Agency ID), and a transaction sequence number (TSN). The party's ROC is generated as described above (see Fig. 6). The coded address CPK of the hidden memory file 1622 may either represent the entire address
15 of the hidden memory file 1622 or only a portion of the address of the hidden memory file 1622, as described above.

The party to be authenticated enters a personal identification number (PIN) at a terminal. The
20 PIN is input to an irreversible coder 1606 to produce a coded personal identification number (CPN). The information recorded on the party's card 1602 is read from the card 1602 using an appropriate reader (not shown). The CPK read from the card 1602 is applied as
25 an input to an uncoder 1612, which also receives the CPN as a key input. The uncoder 1612 uncodes CPK using CPN as a key input to generate PK, which represents either the total address of the hidden memory file 1622 or a portion of the address of the hidden memory file 1622
30 (as noted above).

The transaction sequence number (TSN) read from the card 1602 is input to a mixer 1608 and then to a coder 1610. The coder 1610 also receives the CPN as a key input. The coder 1610 codes the TSN using the CPN
35 as a key input to generate an anti-duplication VAN (ADVAN). The ADVAN, PK, ROC, and AID are input to a

42

mixer 1614 and the resulting mixed signal is sent to the remote CPU over a preferably unsecured communication link.

5 The user's hidden memory file 1622 is part of
a memory which is used to store such files at the remote CPU. The sorter 1616 separates the received mixed signal into its component parts ROC, PK, AID, and ADVAN. Where the PK generated by the uncoder 1612 is only a portion of the address to the hidden memory file 1622,
10 the AID is used as an index to a memory table 1618 to retrieve other address components for the hidden memory file 1622. Thus, the address components in the memory table 1618 applicable in any given transaction depends on the particular AID. The PK is combined with the
15 other address components at a combiner 1620 to thereby form the composite address of the hidden memory file 1622. The AID could also identify a predetermined procedure for combining the applicable address components. The composite address is used to access the
20 hidden memory file 1622 to retrieve a secret random number RN (which is generated according to the method described above with respect to Fig. 6). RN is input as a key to a coder 1624. The coder 1624 also receives the ROC from the sorter 1616 and thereby generates CPN.

25 A transaction sequence number (TSN) is also retrieved from the hidden memory file 1622 and is input to a coder 1632. The coder 1632 also receives CPN as a key input and thereby generates an ADVAN. The ADVAN generated by the coder 1632 is compared with the ADVAN
30 output from the sorter 1616 at a comparator 1630. If a favorable comparison is obtained, then coder 1628 is enabled. If the comparison is not favorable, then the user is not authenticated and does not gain access to the memory file 1622.

43

Coder 1628 receives PK as an input and CPN as a key and thereby generates CPK. The CPK generated by the coder 1628 is received by an uncoder 1626 as a key input. The uncoder 1626 also receives as input coded
5 information which is retrieved from the hidden memory file 1622. The uncoder 1626 uncodes the coded information from the hidden memory file 1622 using the CPK as a key input to thereby produce clear information. The clear information is then provided to the
10 authenticated user.

As a result of the favorable comparison of the ADVANs at the comparator 1630, a new (or revised) transaction sequence number (TSN) is generated and stored in the hidden memory file 1622. Also, a
15 coder 1634 is enabled. The coder 1634 receives the CPN as an input and also receives a revised RN as a key input. The output of coder 1634 is a new ROC, which is combined with the new TSN in mixer 1635. The mixer 1635 output is sent back to the terminal where the
20 sorter 1604 separates the new TSN and ROC, which are then recorded on the user's card (in order to prepare for the next transaction by the user). Note also that a new CPK may be generated as well by revising a memory address component, such as the address displacement. In
25 this event, the new CPK would also be returned to the terminal to be recorded on the user's card.

It should be noted that an unsecured communication link between the mixer 1614 and the sorter 1616 is utilized if the hidden memory file 1622
30 is remote from the location where the party's PIN is entered (that is, the terminal). It should also be noted that the transaction sequence number (TSN), in conjunction with the ADVAN, serves to protect the authenticity of the transaction and the user's card
35 against fraudulent duplication of the transaction

44

information (that is, by recording the output of the mixer 1614 and retransmitting it later to the sorter 1616).

5 A number of additional applications for the present invention will now be described.

The invention could be utilized in a pay telephone system in which calls could be made without the use of money. The call originator uses a telephone in the usual way to enter the telephone number of the party to be called (i.e., to the call recipient). The call originator also enters his own telephone number and PIN. The system then authenticates the identity of the originator as described above (by using, for example, the embodiment depicted in Figs. 6-8 or in Figs. 9-12).
10 In the first embodiment (i.e., Figs. 6, 7, 8A and 8B), the originator's PIN is coded, and used to derive an arbitrary number, which is subsequently compared to another such number which is generated from a reconstituted version of the coded PIN. The
15 reconstituted coded PIN is formed from an RN and ROC which are accessed from the originator's account file, with the originator's telephone number serving as a file index. If the comparison is unfavorable, the call is aborted; otherwise, call processing continues.

25 In the second embodiment, the originator's telephone number is used as an index to file no. 1 to access an originator's CPKO and true CNO. The originator's coded PIN, CPNO, is then combined with the originator's CPKO to generate a CNO (as in Fig. 12).
30 The originator's identify is then authenticated by comparing the true CNO with the derived CNO. If the comparison is unfavorable, the call is aborted; otherwise, processing continues. The originator can use a machine readable card, or the like which has CPKO and
35 CNO previously recorded thereon. In this event, access to file no. 1 is unnecessary.

45

In either embodiment, if the identity comparison is favorable, then the originator's credit balance is extracted from the originator's file to determine whether the call should be allowed. If the
5 credit balance is favorable, then the telephone connection is extended to the call recipient, and the recipient's telephone is rung.

At the end of the call, the originator's credit balance is diminished by the cost of the call,
10 and the new balance is computed and rewritten to the originator's file. The originator may then be advised of the cost of the call. When the recipient's telephone rings and the call is answered, the system can require that the identity of the person answering the phone be
15 authenticated, as in a person to person call. In this event, the recipient is asked to enter a PIN, and the recipient's identity is authenticated using either of the two embodiments mentioned above.

Alternatively, a first joint code could be
20 generated when the call is initiated, e.g., from the originator's CPN, and the recipient's reconstituted CPN. When the call is answered, the recipient enters his PIN, which is converted to a CPN and combined with the originator's reconstituted CPN to form a second joint
25 code. A comparison then ensues between the first and second joint codes.

Another application of the invention is a system which uses a bill as the means of (or vehicle for) payment. The bill contains the usual payment
30 information, and a VAN is also recorded on the bill when the bill is generated. The VAN is derived from the payment information (INFO) and identification information associated with the originator of the bill (e.g., similar to the bank identification line of
35 information which appears at the bottom of an originator's check) or the originator's TIN and BIN.

46

The bill may also contain the recipient's TIN and BIN. Preferably, the above information is coded in a standard format, at a fixed location on the bill itself. The bill is then used in an appropriate document reader to
5 provide the transaction payment information to the system. The party paying the bill (i.e., the payor) enters his PIN and the payor is then authenticated using the PIN. Also, the VAN is authenticated (using one of the methods described above). If the payor and the VAN
10 are authentic, the bill is paid. A redemption VAN is generated (using information associated with the payee party) and printed on the bill, when it has been paid.

Alternatively, the payor could simply key in the information from the face of the bill. When the
15 transaction is completed, a redemption VAN is displayed to the payor, which he records on the bill (or the VAN could be automatically recorded on the bill).

In accordance with a further application of the embodiments of this invention, a medical
20 prescription form which has been originated and issued by a doctor to a patient (a recipient), can be authenticated to permit dispensing of the designated medicine, or drug, in a processing jurisdiction, along with automated payment. Automated payment may include a
25 third party such as an insurance provider. This system is particularly useful for a patient who is in desperate need of medicine, and is in a remote or strange environment, where the prescription cannot be easily authenticated, or an available pharmacy cannot be found.

30 The prescription form contains identification information associated with the doctor and the patient, and the usual information which appears on a prescription, such as the type of medicine, strength, quantity, application, date, refills, generic, and a
35 control number. The prescription form also contains a VAN, which is the result of coding the medical and

47

identification information. Preferably, the information and the VAN are recorded on the prescription form so that it is readable by an individual, and it also includes coded symbols or characters representing the
5 same information in machine readable form.

When the prescription form is utilized by the recipient to obtain the medicine from a processing entity (such as a drug store), the information on the form is read automatically by a terminal of the system,
10 or it is entered via a keyboard. The recipient also enters his PIN, and the system authenticates the prescription form, the doctor, and the recipient in accordance with the embodiments described previously. An indication of the cost of the prescribed medicine,
15 and the method of payment is provided to the recipient. The recipient may elect to pay by using one of the methods described herein.

Note that the processing entity may also include a centralized clearinghouse in communication
20 with dispensing outlets (i.e., drug stores) for authenticating prescriptions. An RVAN may be generated from the VAN and information associated with the processing entity, and then associated with the transaction, to thereby document the processing entity's
25 involvement in the transaction.

If a patient attempts to use a prescription in a state where the originating physician is not licensed, such as out of state, the original prescription may not be usable. In this situation, a directory system of
30 predetermined licensed "correspondent" physicians may be established, and a correspondent physician can automatically authorize the prescription of an originating physician (on-line), after the original prescription is authenticated.

48

The invention also finds utility in a
paperless/cashless transaction system, in which "funds
transfer" transactions, such as purchases, occur without
the use of money, or checks. In this system, the
5 payment originator uses a payment recipient's terminal
which stores information to identify the precise
location of the recipient's account. Alternatively, an
originator PIN, information identifying an originator
account and a recipient account, and funds transfer
10 information (INFO) which includes a payment amount are
entered directly into a terminal of this system by the
payment originator. The system initially generates a
VAN, (OVAN), by using the payment information (INFO) in
conjunction with the identification information
15 associated with the payment originator and payment
recipient. The payment originator is authenticated
using the originator PIN using a method described above.
The system then approves or disapproves the payment
based upon an authentication of the VAN, and the "joint"
20 identification information associated with the
participants, and the availability of funds, or credit.
Such transactions are carried on entirely
electronically, the participant's bank accounts are
credited and debited automatically, allowing commercial
25 transactions to be completed "instantaneously". An RVAN
may be generated using the INFO and printed on a receipt
which is dispensed to the originator.

Although preferred embodiments of the
invention have been disclosed for illustrative purposes,
30 those skilled in the art will appreciate that many
additions, modifications, and substitutions are possible
without departing from the scope or spirit of the
invention as defined in the accompanying claims.

46

CLAIMS

1. In a system comprising a storage means addressable using a predetermined address and party information associated with a party and stored in the storage means, the party information comprising first coded authentication information previously generated by using a personal identification number (PIN) associated with the party, a method for authenticating the party comprising the steps of:
- 10 receiving a PIN from the party to be authenticated;
- addressing the storage means using the predetermined address to locate the party information and to retrieve the first coded authentication
- 15 information;
- generating second coded authentication information using the received PIN;
- comparing at least part of the retrieved first coded authentication information to at least part
- 20 of the generated second coded authentication information; and
- authenticating the party if said at least part of the retrieved first coded authentication information corresponds to said at least part of the
- 25 generated second coded authentication information.
2. The method of claim 1, wherein the predetermined address comprises non-secret information associated with the party, such that the location of the storage means and the first coded authentication
- 30 information stored in the storage means are non-secret.
3. The method of claim 1, wherein the first coded authentication information is extracted from a storage means which is in the possession of the party.

4. The method of claim 1, wherein the location of the storage means is secret, and wherein the step of addressing the storage means comprises the steps of:

- 5 accessing a second storage means using a second predetermined address to locate and to retrieve a coded address previously stored in the second storage means, the coded address having been previously generated by coding the first predetermined address of
10 the first storage means using the PIN;
 uncoding the coded address using the received PIN to generate the first predetermined address; and
 accessing the first storage means using
15 the generated first predetermined address to retrieve the first coded authentication information.

5. The method of claim 4, wherein the first storage means is a part of a memory and wherein, prior to use of the memory, pseudo information is stored in
20 the memory, thereby making unused portions of the memory indistinguishable from the first storage means.

6. The method of claim 4, wherein the party information also comprises secret information associated with the party.

25 7. In a transaction system, a method for authenticating a transaction and at least one party to the transaction comprising the steps of:

- coding information relevant to a transaction with information associated with at least
30 one party to generate a variable authentication number (VAN), wherein the information associated with said at least one party comprises coded authentication information derivable from a predetermined secret code and a predetermined non-secret code, and wherein the
35 coded authentication information was previously

generated by coding a personal identification number (PIN), the PIN being unrecoverable within the transaction system;

5 associating the VAN with the transaction;
deriving the coded authentication
information using the predetermined secret and non-secret codes; and
10 authenticating the VAN associated with the transaction using the derived coded authentication information.

Sub D1
8. The method of claim 7, wherein the information relevant to the transaction comprises at least one information group which is coded so as to enable detection of a change in its content or
15 structure.

9. The method of claim 7, wherein the transaction involves an electrical signal, the VAN being included in the electrical signal together with at least a portion of the information relevant to the
20 transaction.

10. The method of claim 7, wherein the transaction includes originating an instrument and wherein the step of associating the VAN with the transaction comprises the step of recording the VAN and
25 at least a portion of the information relevant to the transaction on the instrument.

11. The method of claim 10, wherein the information relevant to the transaction comprises a combination of predetermined information recorded on the
30 instrument and predetermined information not recorded on the instrument, such that prevention of fraudulent regeneration of the VAN is enhanced.

12. The method of claim 7, wherein the step of authenticating the VAN comprises the steps of:
35 uncoding the VAN using at least the derived coded authentication information;

comparing the uncoded VAN to the
information relevant to the transaction; and
authenticating the VAN and the
transaction associated with the VAN if the uncoded VAN
5 corresponds to the information relevant to the
transaction.

13. The method of claim 7, wherein the step
of authenticating the VAN comprises the steps of:
coding the information relevant to the
10 transaction using at least the derived coded
authentication information to generate a second VAN;
comparing the first VAN associated with
the transaction to the second VAN; and
authenticating the first VAN and the
15 transaction associated with the first VAN if the first
VAN corresponds to the second VAN.

14. The method of claim 7, wherein the
transaction comprises originating and processing a
medical prescription form and said at least one party
20 comprises an originating physician and a patient
presenting the medical prescription form for processing
in a processing jurisdiction, the coded authentication
information being associated with the originating
physician and with the patient, and wherein the step of
25 associating the VAN with the transaction comprises the
step of recording the VAN on the medical prescription
form.

15. The method of claim 14, further
comprising the steps of:
30 authenticating the patient; and
dispensing medicine as indicated on the
medical prescription form to the patient if the VAN and
the patient are authenticated.

16. The method of claim 15, wherein the VAN is authenticated by a processing entity associated with the processing jurisdiction, further comprising the steps of:

- 5 if the originating physician is not licensed to practice in the processing jurisdiction, then obtaining authorization for processing the medical prescription form in the processing jurisdiction from a correspondent physician licensed in the processing
- 10 jurisdiction;
- generating a redemption VAN from the VAN and information associated with the processing entity; and
- associating the redemption VAN with the
- 15 medical prescription form, such that the processing entity is accountable for the processing of the medical prescription form.

- SUBA² 17. In a multi-party transaction system, a method for authenticating a transaction and parties to
- 20 the transaction comprising the steps of:
- coding information relevant to a transaction with at least information associated with at least two parties to generate a variable authentication number (VAN); and
- 25 associating the VAN with the transaction.

18. The method of claim 17, wherein at least one of the parties is present, and wherein at least one of the parties is absent.

- SUBA³ 19. The method of claim 17, wherein the
- 30 coding step comprises the steps of:
- coding the information associated with said at least two parties to generate a joint code; and
- coding the information relevant to the transaction with the joint code to generate the VAN.

20. In a system wherein a party has a personal identification number from which first coded authentication information is generated, the first coded authentication information being derivable from a
5 predetermined secret number and a predetermined non-secret number which have been previously stored in a storage means, a method for authenticating the party comprising the steps of:
- 10 receiving at a first site a personal identification number from the party;
 - generating second coded authentication information by using the received personal identification number;
 - 15 transmitting at least the second coded authentication information from the first site to a second site;
 - retrieving at the second site the secret and non-secret numbers from the storage means;
 - generating at the second site third coded
20 authentication information by using the retrieved secret and non-secret numbers;
 - comparing at the second site the second coded authentication information and the third coded authentication information; and
25 authenticating the party if the second coded authentication information corresponds to the third coded authentication information.
21. The method of claim 20, wherein the transmitting step comprises the step of transmitting the
30 second coded authentication information from the first site to the second site over a secured communication medium, and wherein the step of generating the third coded authentication information comprises the step of deriving the first coded authentication information from
35 the retrieved secret and non-secret numbers.

22. The method of claim 20, wherein the step of generating the second coded authentication information comprises the steps of coding the received personal identification number to generate a coded
5 personal identification number and coding an arbitrary number using the coded personal identification number to generate a first coded arbitrary number.

23. The method of claim 22, further comprising the step of generating at the first site an
10 anti-duplication variable authentication number (ADVAN) by coding at least a transmission date and time with the first coded authentication information, wherein the transmitting step comprises the step of transmitting the ADVAN, the first coded arbitrary number and the
15 arbitrary number from the first site to the second site over an unsecured communication medium.

24. The method of claim 23, further comprising the steps of:
deriving at the second site the first
20 coded authentication information from the retrieved secret and non-secret numbers;
uncoding the ADVAN at the second site using the derived first coded authentication information to regenerate the transmission date and time; and
25 further authenticating the party if the regenerated transmission date and time correspond to a reception date and time.

25. The method of claim 22, wherein the arbitrary number is generated at both the first site and
30 the second site, and wherein the transmitting step comprises the step of transmitting the first coded arbitrary number from the first site to the second site over an unsecured communication medium.

26. The method of claim 25, wherein the step
35 of generating the third coded authentication information comprises the steps of deriving the first coded

authentication information from the retrieved secret and non-secret numbers and coding the arbitrary number generated at the second site using the derived first coded authentication information to generate a second
5 coded arbitrary number.

27. The method of claim 26, wherein the comparing step comprises the step of comparing at the second site the first coded arbitrary number transmitted from the first site to the second site and the second
10 coded arbitrary number, and wherein the authentication step comprises the step of authenticating the party if the first coded arbitrary number corresponds to the second coded arbitrary number.

28. In a transaction system, a method for
15 enrolling a party, wherein the party is authenticated during at least one stage of a subsequent transaction, the method comprising the steps of:

receiving a personal identification
number (PIN) from the party;
20 coding the PIN to produce a coded PIN
(CPN);

coding the CPN using a predetermined
arbitrary number to produce a revisable owner code
(ROC); and
25 storing the predetermined arbitrary
number and the ROC in a storage means at a location associated with the party, wherein the CPN is derivable from the predetermined arbitrary number and the ROC.

29. The method of claim 28, further
30 comprising the step of modifying the predetermined arbitrary number and the ROC such that the CPN remains derivable from the revised arbitrary number and the revised ROC, thereby further preventing unauthorized derivation of the CPN.

- 50.6A⁴ → 30. In a transaction system wherein a party has a first personal identification number (PIN) and an official has a second PIN, a method for enrolling the party comprising the steps of:
- 5 coding information associated with the party with information associated with the official to generate a joint code, the joint code being subsequently associable with a transaction; and
- 10 storing the joint code in a first storage means, the first storage means being accessible only to a party with knowledge of the first PIN, such that if no party exists with knowledge of the first PIN, the joint code cannot be accessed from the first storage means and, therefore, cannot be associated with a transaction.
- 15 31. The method of claim 30, further comprising the steps of:
- coding information relevant to the transaction with the joint code to generate a variable authentication number (VAN);
- 20 recording the VAN on a credential associated with the transaction; and
- issuing the credential.
32. The method of claim 30, further comprising the steps of:
- 25 storing the joint code in a second storage means, the second storage means being accessible only to a party having knowledge of the second PIN;
- receiving the second PIN from the official;
- 30 using the received second PIN to access the second storage means and to retrieve the joint code;
- coding information relevant to the transaction with the joint code to generate a variable authentication number (VAN);

recording the VAN on a credential
associated with the transaction; and

issuing the credential, wherein a party
without knowledge of the second PIN cannot access the
5 second storage means or the joint code stored therein
and, therefore, cannot legitimately issue the
credential.

SUB A5
33. In a multi-party transaction system, a
method for processing transactions comprising the steps
10 of:

coding information relevant to a
transaction with information associated with at least
one party to generate a variable authentication number
(VAN);

15 associating the VAN with the transaction;
determining whether a recipient party and
the transaction are authentic; and
if the recipient party and the
transaction are authentic, then authorizing the
20 transaction.

Sub D2
34. The method of claim 33, further comprising
the steps of:

coding information associated with at
least one party with the VAN to generate a redemption
25 VAN (RVAN);

associating the RVAN with the
transaction, such that the transaction cannot be
fraudulently presented for further redemption; and
storing the RVAN in a storage means
30 associated with at least one party, such that the
transaction is cleared in a substantially instantaneous
manner.

35. The method of claim 34, wherein the
transaction involves an electrical signal, the RVAN
35 being included in the electrical signal.

36. A method for enrolling and authenticating a party, comprising the steps of:
- receiving a personal identification number (PIN) from the party;
 - 5 generating coded authentication information using the received PIN;
 - generating first and second numbers such that the coded authentication information is derivable from the first and second numbers, the first number
 - 10 being secret and the second number being non-secret;
 - storing information comprising the secret number in a first storage means addressable using a predetermined secret address;
 - generating a coded secret address using
 - 15 at least part of the predetermined secret address and the received PIN; and
 - storing the coded secret address and the non-secret number in a second storage means addressable using a predetermined non-secret address.
- 20 37. The method of claim 36, wherein the step of storing the information comprising the secret number in the first storage means comprises the steps of:
- coding the information comprising the secret number using non-secret information associated
 - 25 with the party to generate coded information; and
 - storing the coded information in the first storage means.
38. The method of claim 37, wherein the non-secret information associated with the party is the
- 30 coded secret address.
39. The method of claim 36, further comprising the steps of:
- receiving a second PIN from a party to be authenticated;

generating at a first site second coded authentication information using the received second PIN;

5 addressing the second storage means using the predetermined non-secret address to locate and retrieve the coded secret address and the non-secret number;

10 generating at the first site a first coded number using the second coded authentication information and the coded secret address;

 generating the predetermined secret address using at least the received second PIN and the retrieved coded secret address;

15 transmitting at least the first coded number and the predetermined secret address from the first site to a second site;

 addressing the first storage means using the generated predetermined secret address to locate and retrieve the secret number;

20 deriving at the second site the first coded authentication information using the retrieved non-secret number and the retrieved secret number;

 generating at the second site a second coded number using the derived first coded authentication information and the coded secret address;

25 and

 authenticating the party to be authenticated if the first coded number corresponds to the second coded number.

30 40. The method of claim 39, further comprising the step of generating at the first site an anti-duplication variable authentication number (ADVAN) by coding at least a transmission date and time with the second coded authentication information, the

35 transmitting step comprising the step of transmitting

the first coded number, the predetermined secret address, and the ADVAN from the first site to the second site via an unsecured communication medium.

41. The method of claim 40, further comprising
5 the steps of:

uncoding the ADVAN at the second site using the derived first coded authentication information to regenerate the transmission date and time; and

further authenticating the party to be
10 authenticated if the regenerated transmission date and time correspond to a reception date and time.

42. The method of claim 39, wherein a first semi-random number is generated at the first site using a first counter, and further comprising the step of
15 coding the first semi-random number to generate a coded first semi-random number, and wherein the transmitting step comprises transmitting the first coded number, the predetermined secret address, and the coded first semi-random number from the first site to the second site via
20 an unsecured communication medium.

43. The method of claim 42, further comprising the steps of:

uncoding the coded first semi-random number at the second site to regenerate the first semi-
25 random number;

generating at the second site a second semi-random number using a second counter which is generally synchronized with the first counter; and

further authenticating the party to be
30 authenticated if the regenerated first semi-random number corresponds to the second semi-random number.

44. The method of claim 39, wherein the predetermined secret address comprises one or more components combinable to form the predetermined secret
35 address, the step of generating the coded secret address

comprising the step of coding one of the components of the predetermined secret address using the received first PIN to generate the coded secret address.

45. The method of claim 44 wherein the step of generating the predetermined secret address comprises the steps of:

uncoding the retrieved coded secret address using the received second PIN to generate said one of the components of the predetermined secret address; and

generating the predetermined secret address by combining the generated said one of the components with the other components of the predetermined secret address.

46. A method for automatically and instantaneously transferring funds from an account associated with an originator party to an account associated with a recipient party, the method comprising the steps of:

receiving from the originator party a personal identification number (PIN) associated with the originator party, information identifying the originator party account and the recipient party account, and information comprising a payment amount and specifying a funds transfer;

generating a variable authentication number (VAN) using the originator party PIN, the recipient party account identifying information, and the fund transfer information;

determining whether the originator party is authentic by using the PIN;

determining whether the funds transfer is authentic by using the VAN;

if the originator party and the funds transfer are authentic, then transferring authenticated funds to the recipient party account from the originator party account;

- 5 generating a redemption variable authentication number (RVAN) using at least the funds transfer information; and
- associating the RVAN with the fund transfer, such that the funds transfer is substantiated
- 10 by the RVAN.

Sub 73 47. The method of claim 46, wherein the step of associating the RVAN with the funds transfer comprises the step of recording the RVAN on a receipt, the receipt being dispensed to the originator party.

SUB A 15 48. A method for processing an invoice comprising the steps of:

- generating a variable authentication number (VAN) using at least information associated with an invoice, the information associated with the invoice
- 20 including information identifying a payee party account and payment information comprising a payment amount;
- recording the VAN and the information associated with the invoice on the invoice;
- receiving the VAN and a personal
- 25 identification number (PIN) from a payor party;
- determining whether the payor party and the VAN are authentic by using the information associated with the invoice and the received PIN;
- receiving the payee party account
- 30 identifying information and the payment information from the invoice; and
- if the payor party and the VAN are authentic, then crediting the payment amount to the payee party account from funds associated with the payor
- 35 party.

Sub-
D4

49. The method of claim 48, further comprising the steps of:

generating a redemption VAN (RVAN) by coding the VAN with at least information associated with
5 the payee party; and
associating the RVAN with the invoice such that payment of the invoice is substantiated by the RVAN.

50. The method of claim 49, wherein the step
10 of receiving the VAN comprises the steps of:

receiving the invoice from the payor party; and
reading the VAN from the received invoice.

51. A method for authenticating a party and for authorizing access to a storage means associated with the party, the storage means being addressable using a secret predetermined address, the method comprising the steps of:

20 receiving a personal identification number (PIN) from a party to be authenticated;
generating coded authentication information using the PIN, the coded authentication information being derivable from a secret number
25 previously stored in the storage means and a non-secret number previously stored in a storage medium in possession of the party;

retrieving from the storage medium at least a coded address and the non-secret number, the
30 coded address having been previously generated by coding at least a portion of the secret predetermined address using the coded authentication information;

generating said at least a portion of the secret predetermined address by uncoding the coded
35 address using the coded authentication information;

transmitting at least the generated said
at least a portion of the secret predetermined address
and the retrieved non-secret number from a first site to
a second site over a communication link;

5 generating at the second site the secret
predetermined address using the transmitted said at
least a portion of the secret predetermined address;
 addressing the storage means using the
generated secret predetermined address to retrieve the
10 secret number;

 deriving the coded authentication
information using the retrieved secret number and the
transmitted non-secret number; and

 authenticating the party and authorizing
15 further access to the storage means by using at least
the derived coded authentication information.

52. The method of claim 51, further
comprising the steps of:

 retrieving from the storage medium a
20 first transaction sequence number (TSN) previously
stored therein;

 generating a first anti-duplication
variable authentication number (ADVAN) by coding the
first TSN with the coded authentication information;

25 transmitting the first ADVAN from the
first site to the second site over the communication
link;

 addressing the storage means using the
generated secret predetermined address to retrieve a
30 second TSN previously stored therein;

 generating a second ADVAN by coding the
second TSN with the derived coded authentication
information; and

 authenticating the party and authorizing
35 further access to the storage means if the second ADVAN
corresponds to the first ADVAN;

wherein the first and second TSNs are modified after each transaction, such that fraudulent receipt and use of messages over the communication link and fraudulent duplication of the storage medium are prevented.

53. The method of claim 51, further comprising the steps of retrieving agency identification information from the storage medium and transmitting the agency identification information from the first site to the second site over the communication link, wherein the step of generating at the second site the secret predetermined address comprises the steps of using the agency identification information to retrieve other portions of the secret predetermined address and combining the transmitted said at least a portion of the secret predetermined address with the other portions to form the secret predetermined address.

54. The method of claim 51, further comprising the step of revising the TSN, the secret number, and/or the coded address.

55. The method of claim 51, wherein the communication link is unsecured.

~~56. A multi-party transaction system for authenticating a transaction and parties to the transaction comprising:~~

~~means for coding information relevant to a transaction with at least information associated with at least two parties to generate a variable authentication number (VAN); and~~

~~means for associating the VAN with the transaction.~~

57. A transaction system for enrolling a party wherein the enrolled party is authenticated during at least one stage of a subsequent transaction, the system comprising:

means for receiving a personal identification number (PIN) from the party;

means for coding the PIN to produce a coded PIN (CPN);

5 means for coding the CPN using a predetermined arbitrary number to produce a revisable owner code (ROC); and

means for storing the predetermined arbitrary number and the ROC in a storage means at a
10 location associated with the party, wherein the CPN is derivable from the predetermined arbitrary number and the ROC.

58. A transaction system for enrolling a party, wherein the party has a first personal
15 identification number (PIN) and an official has a second PIN, the system comprising:

means for coding information associated with the party with information associated with the official to generate a joint code, the joint code being
20 subsequently associable with a transaction;

a storage means being accessible only to a party with knowledge of the first PIN; and

means for storing the joint code in the storage means, such that if no party exists with
25 knowledge of the first PIN, the joint code cannot be accessed from the storage means and, therefore, cannot be associated with a transaction.

59. A multi-party transaction system for processing transactions comprising:

SOBAP
30 means for coding information relevant to a transaction with information associated with at least one party to generate a variable authentication number (VAN);

means for associating the VAN with the
35 transaction;

means for determining whether a recipient party and the transaction are authentic; and

means for authorizing redemption of the transaction if the recipient party and the transaction are authentic.

60. A system for authenticating a party comprising:

means for receiving a personal identification number (PIN) from the party;

means for generating coded authentication information using the received PIN;

means for generating first and second numbers such that the coded authentication information is derivable from the first and second numbers, the first number being secret and the second number being non-secret;

means for storing the secret number in a first storage means addressable using a predetermined secret address;

means for generating a coded secret address using at least a part of the predetermined secret address and the received PIN; and

means for storing the coded secret address and the non-secret number in a second storage means addressable using a predetermined non-secret address.

61. The system of claim 60, wherein the second storage means is a storage medium in the possession of the party.

62. In a system comprising a storage means addressable using a secret predetermined address and a first coded number previously stored in the storage means and derivable from the secret predetermined address and a coded address generated by coding the secret predetermined address with first coded

authentication information associated with a party to be authenticated, a method for authenticating the party comprising the steps of:

- receiving a PIN from the party to be
- 5 authenticated;
- generating second coded authentication information using the received PIN;
- deriving the secret predetermined address by uncoding the coded address using the second coded
- 10 authentication information;
- generating a second coded number by coding the derived secret predetermined address with the coded address;
- using the derived secret predetermined
- 15 address to access the storage means and retrieve the first coded number; and
- authenticating the party if the retrieved first coded number corresponds to the generated second coded number.

20 ~~50B-110~~ 63. In a system comprising a credential and party information associated with a party and recorded on the credential, the party information comprising first coded authentication information previously generated by using a personal identification number

- 25 (PIN) associated with the party, a method for authenticating the party comprising the steps of:
- receiving a PIN from the party to be authenticated;
- retrieving the first coded authentication
- 30 information from the credential;
- generating second coded authentication information using the received PIN;
- comparing at least part of the retrieved first coded authentication information to at least part
- 35 of the generated second coded authentication information; and

- 70 -

authenticating the party if said at least
part of the retrieved first coded authentication
information corresponds to said at least part of the
generated second coded authentication information.

Add A" 06
~~Add B~~
~~Add C~~

Attorney Docket No. 6074-1

DECLARATION AND POWER OF ATTORNEY
(Original Application)

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled
SECURE TRANSACTION SYSTEM AND METHOD UTILIZED THEREIN

the specification of which (check one)

☒ [X] is attached hereto.

☐ [] was filed on _____
as Application Serial No. _____

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to herein.

I acknowledge the duty to disclose information which is material to patentability in accordance with Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119, of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

FOREIGN PRIORITY APPLICATION(S)

<u>N/A</u>			<u>Priority</u>
<u>(Number)</u>	<u>(Country)</u>	<u>(Day/month/ year filed)</u>	<u>Claimed</u>
			[] Yes [] No
<u>(Number)</u>	<u>(Country)</u>	<u>(Day/month/ year filed)</u>	<u>Priority</u>
			<u>Claimed</u>
			[] Yes [] No

And I hereby appoint Ronald L. Panitch, Registration No. 22,825; William W. Schwarze, Registration No. 25,918; Alan S. Nadel, Registration No. 27,363; Leslie L. Kasten, Jr., Registration No. 28,959; Joel S. Goldhammer, Registration No. 22,130; Wallace D. Newcomb, Registration No. 14,823; John Jamieson, Jr., Registration No. 29,546; Martin G. Belisario, Registration No. 32,886; Kirk Baumeister, Registration No. 33,833; Michele L. Simons, Registration No. 34,962, a Patent Agent; and Michael Q. Lee, Registration No. 35,239, a Patent Agent; as my attorneys or agents with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith.

Address all correspondence to **PANITCH SCHWARZE JACOBS & NADEL**, 1601 Market Street, 36th Floor, Philadelphia, Pennsylvania 19103. Please direct all communications and telephone calls to Michael Q. Lee at 215-567-2020.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both,

under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of sole or first inventor 100 Leon Stambler
Inventor's Signature Leon Stambler
Date 11/16/92
Residence Parkland Fh JS 11/16/92
Park Land, Florida
Citizenship U.S.A.
Post Office Address 7803 Boulder Lane
Parkland
Park Land, Florida 33067 JS 11/16/92

Full name of second joint inventor, if any _____
Inventor's Signature _____
Date _____
Residence _____
Citizenship _____
Post Office Address _____

Full name of third joint inventor, if any _____
Inventor's Signature _____
Date _____
Residence _____
Citizenship _____
Post Office Address _____

"Express Mail" Mailing Label No. ³ TB 255321187 US

380
25
Copyright

FIG. 1

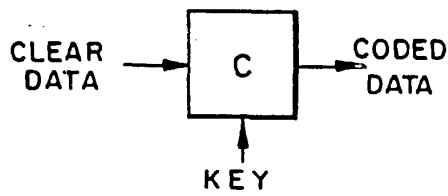


FIG. 2

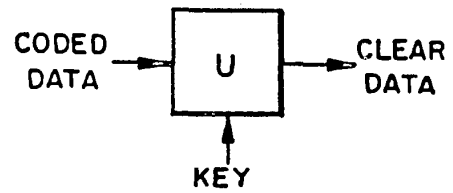


FIG. 3

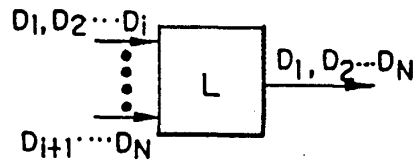


FIG. 4

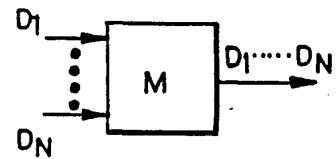


FIG. 5

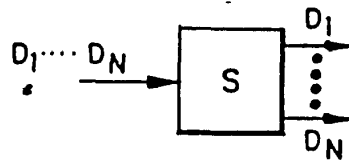
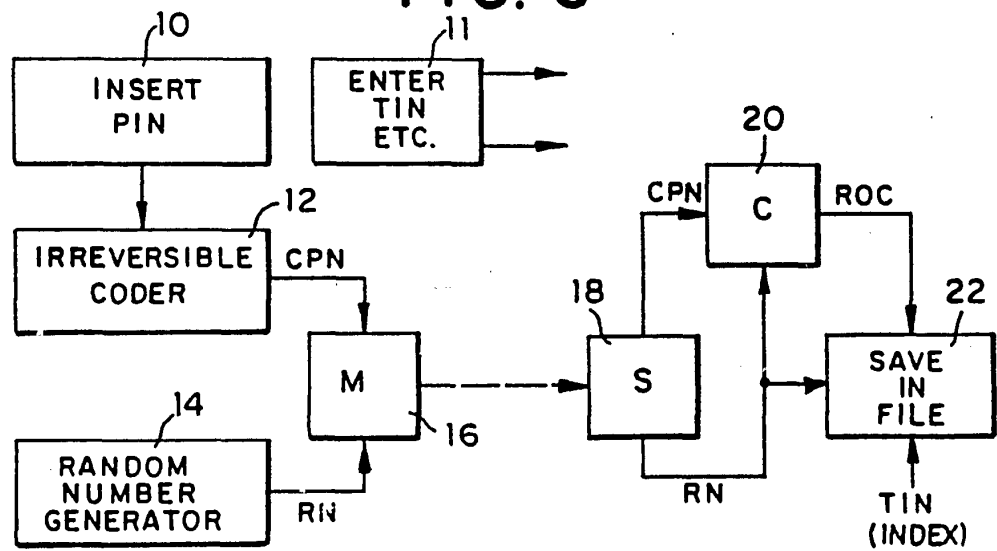
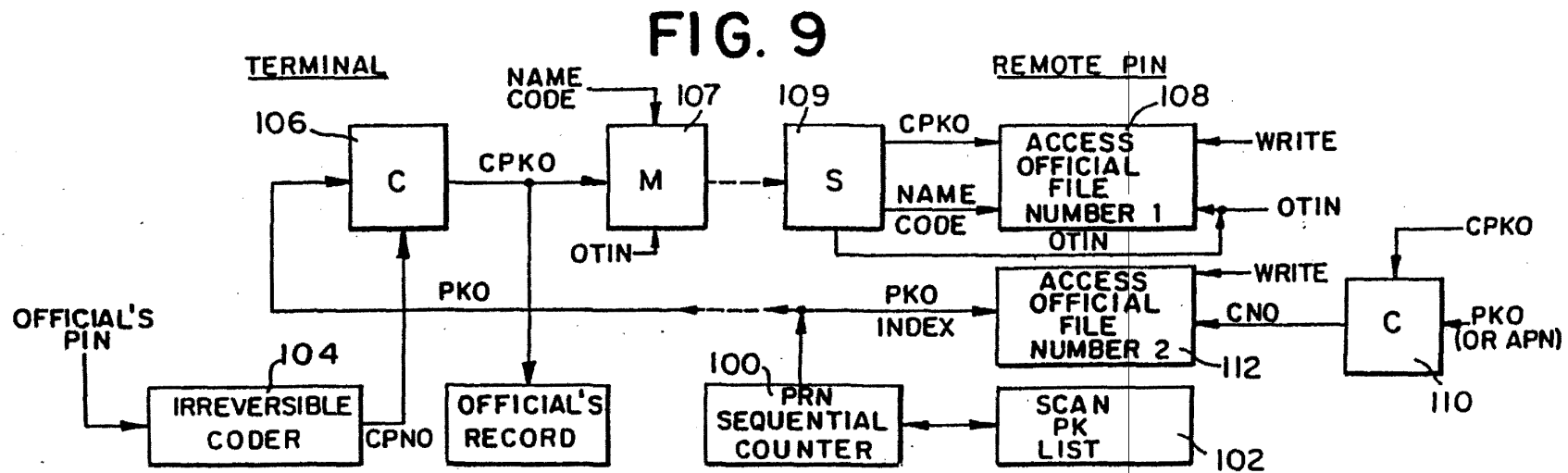
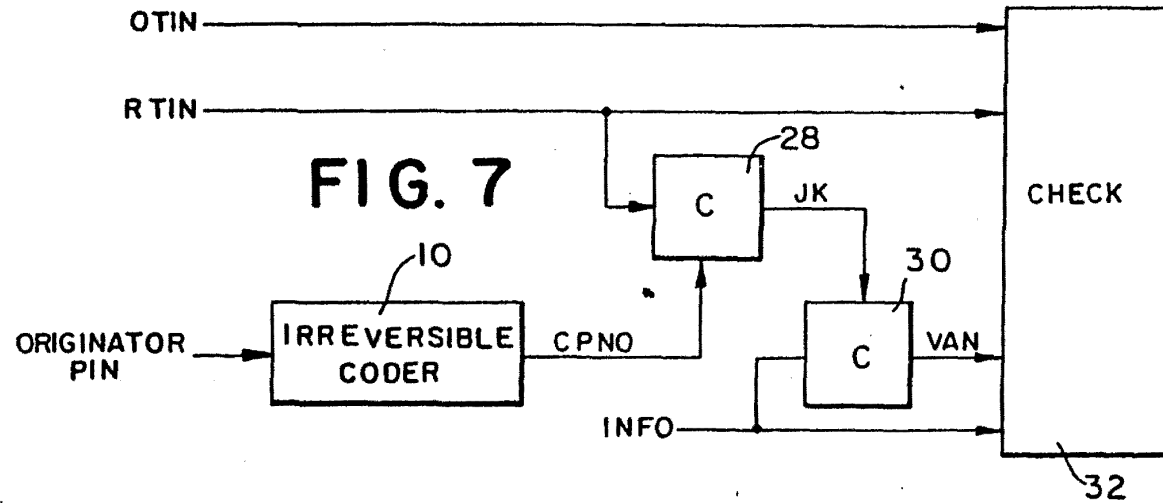
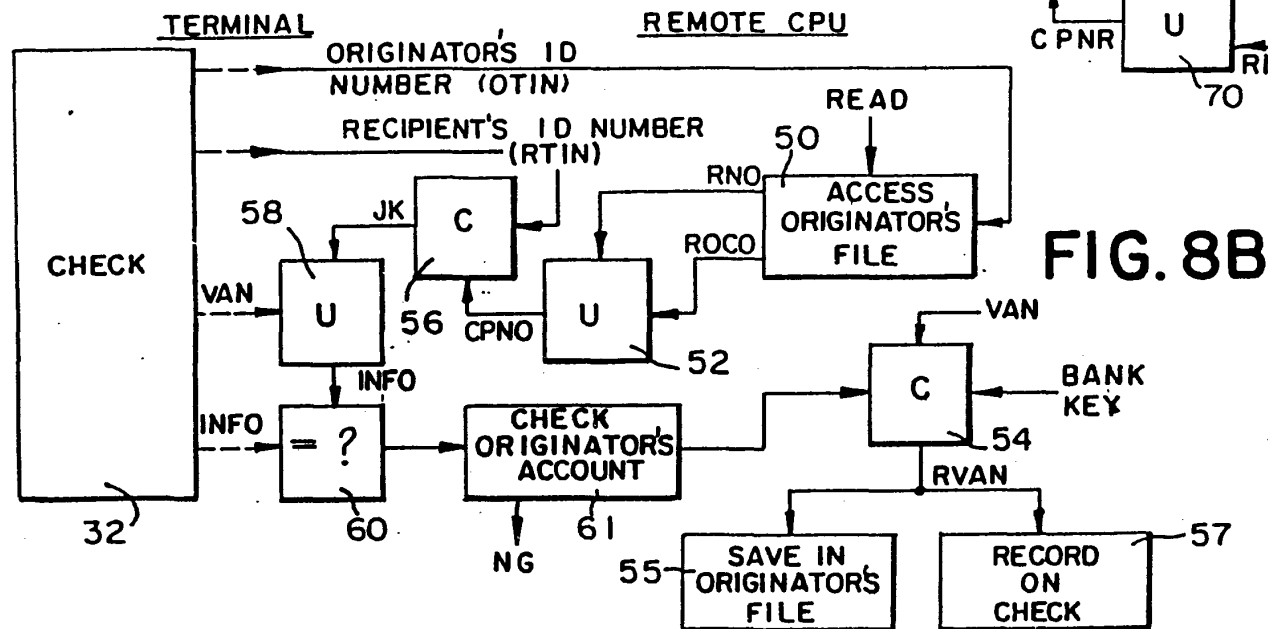
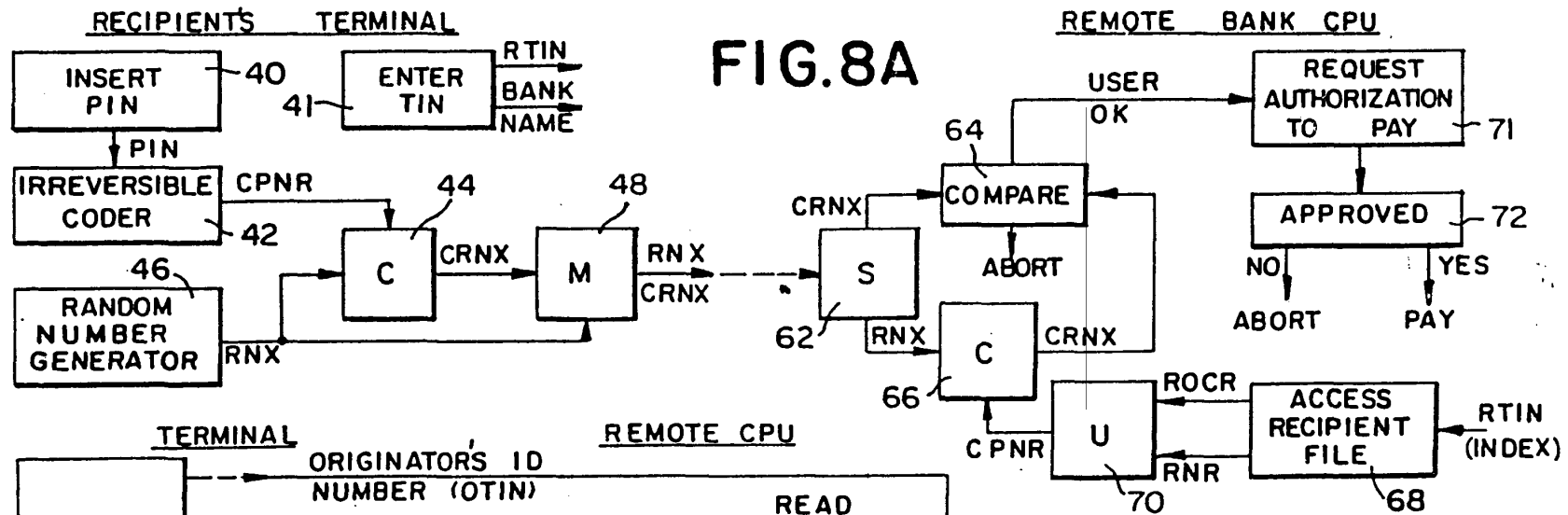


FIG. 6





08/122071



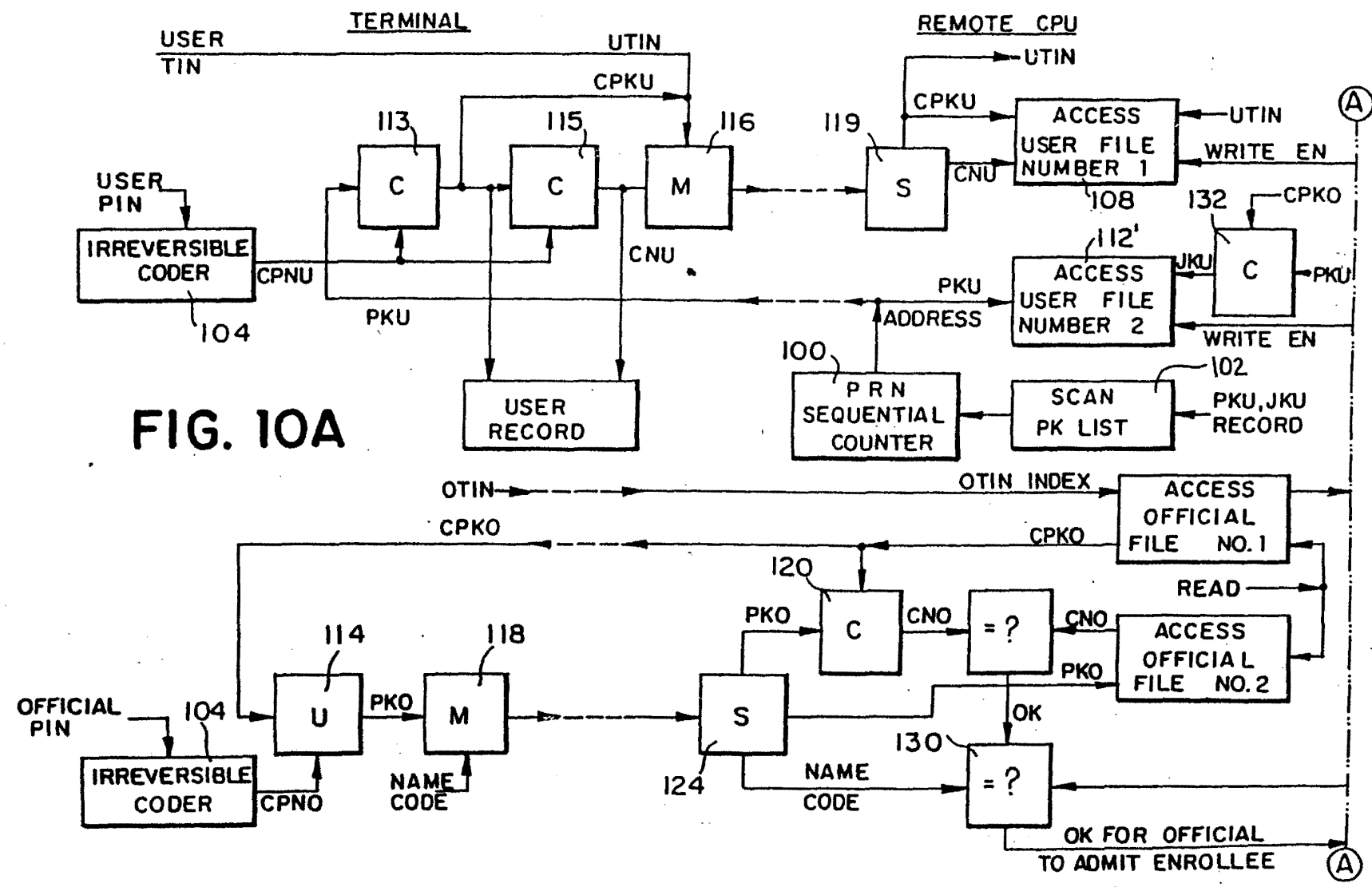


FIG. 10B

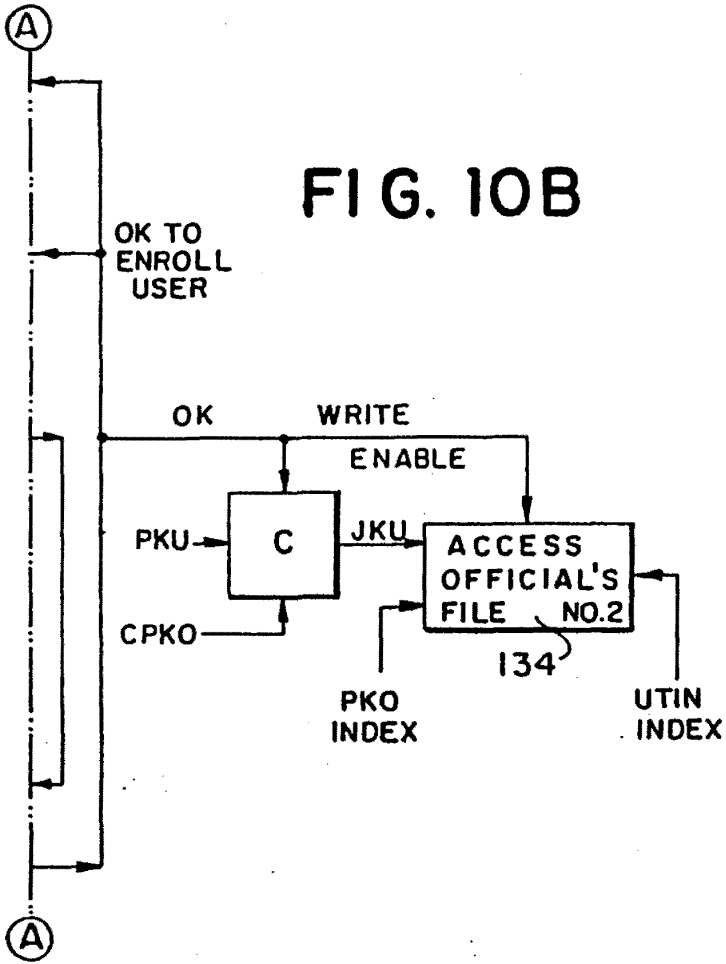
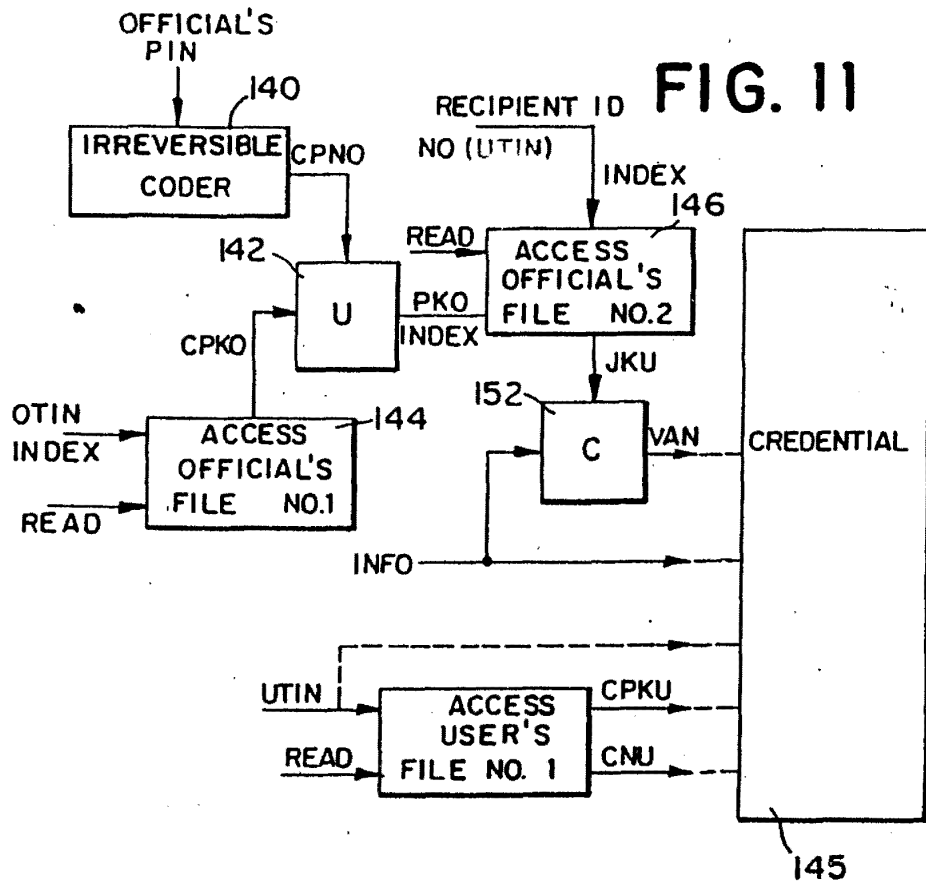
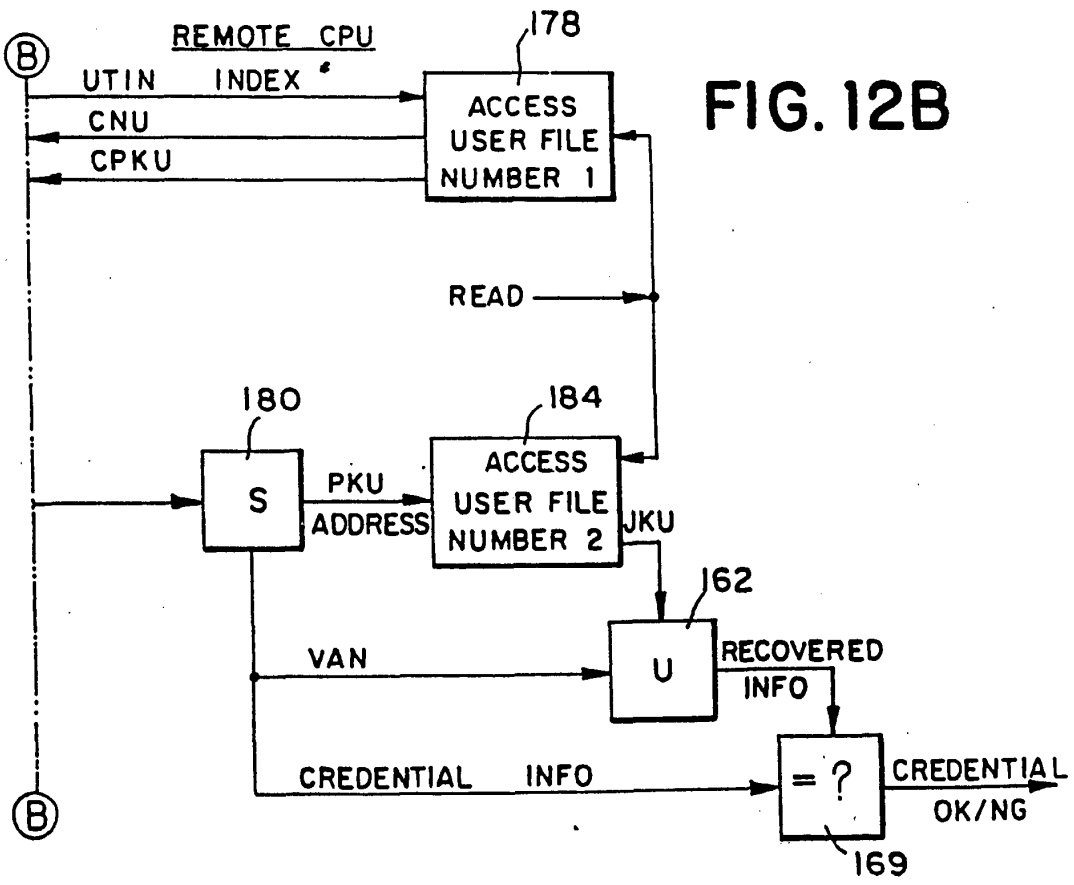
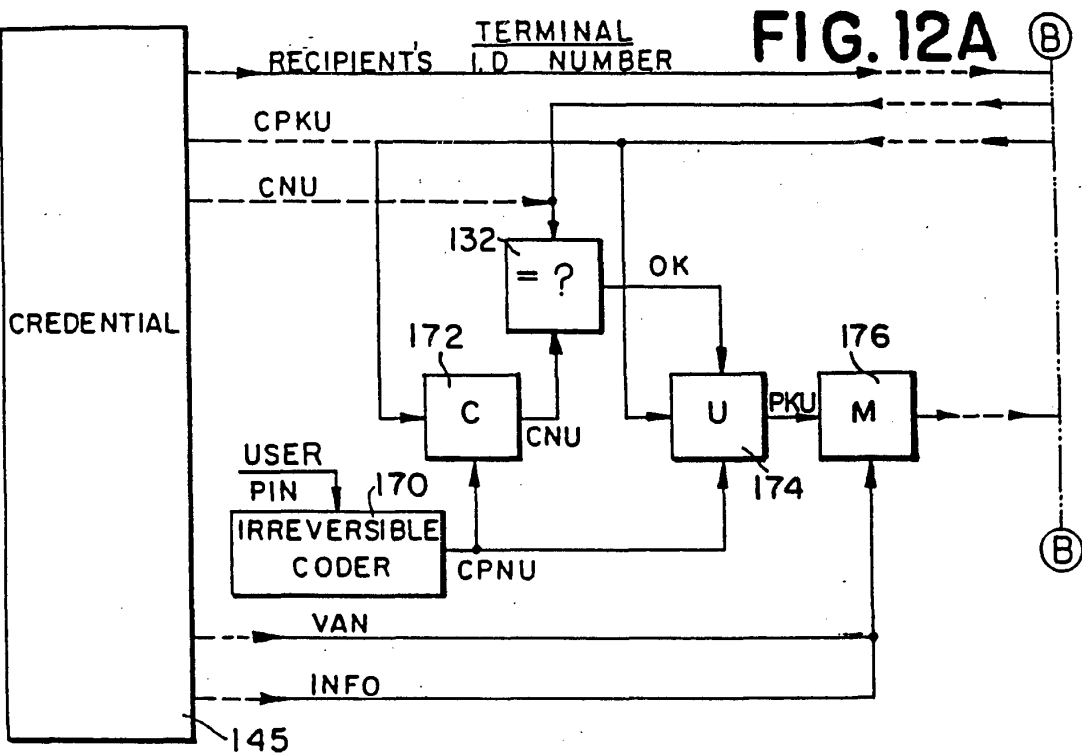


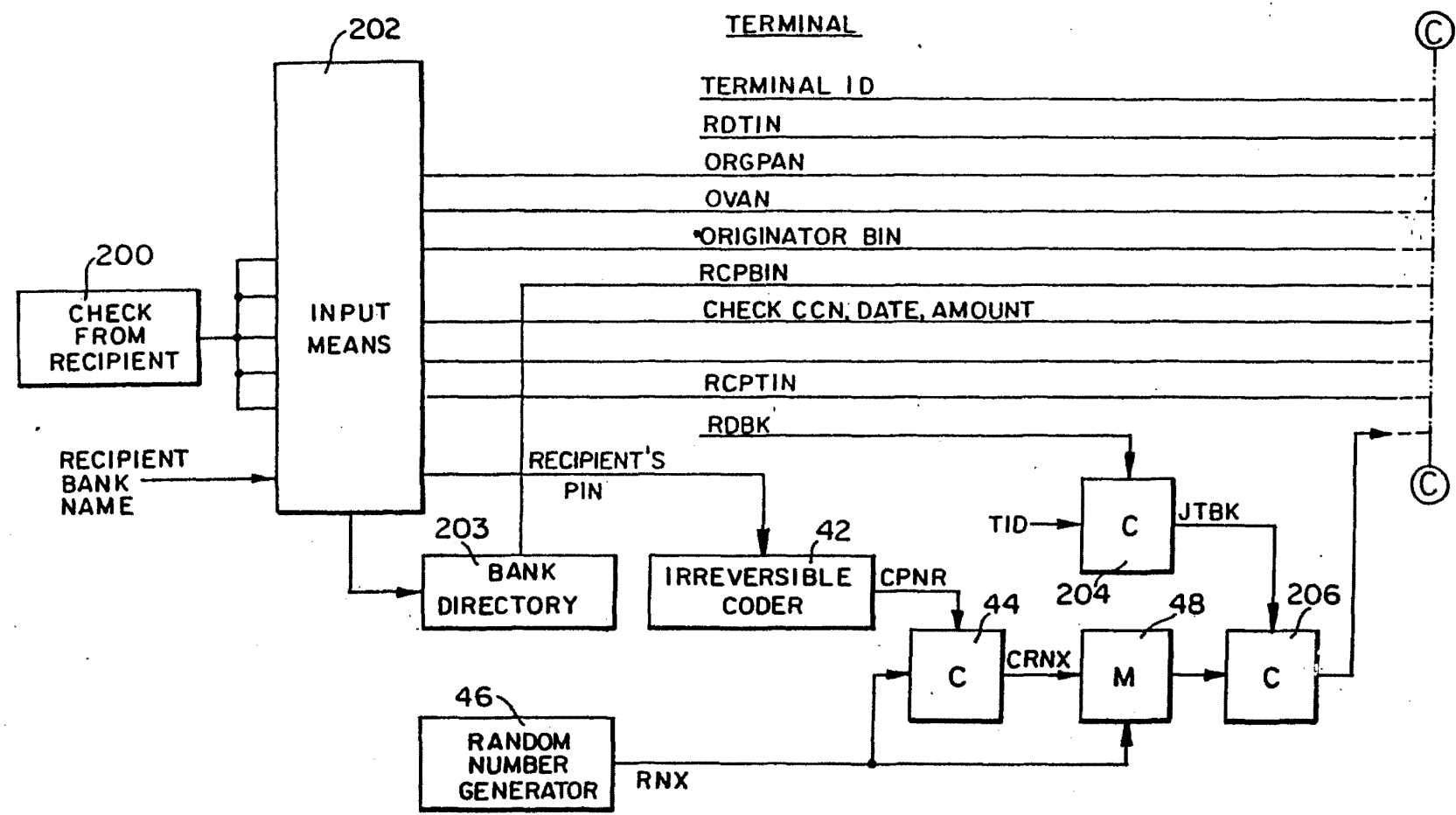
FIG. 11



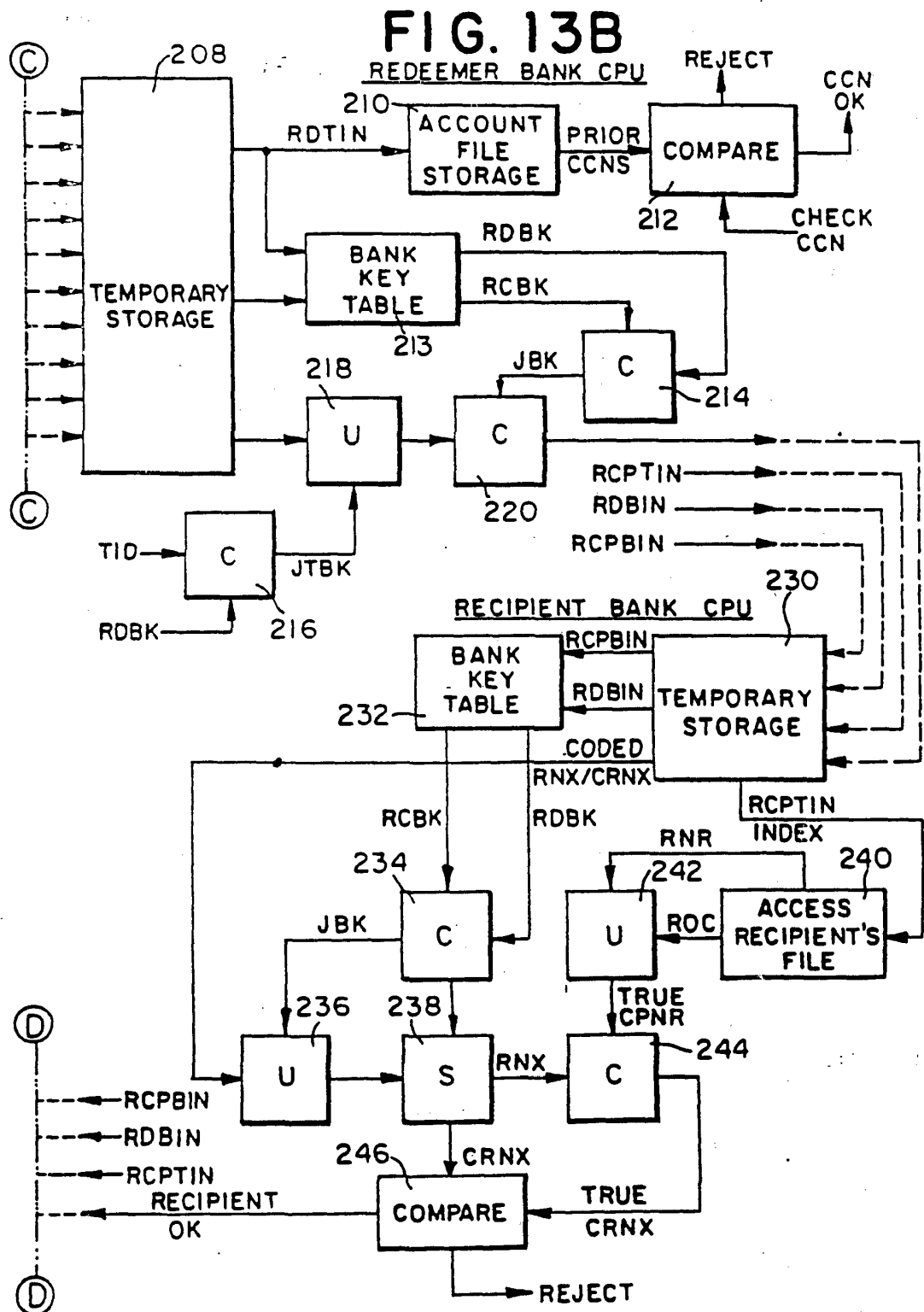


AS ORIGINALLY FILED

FIG. 13A



08/122071



REDEEMER BANK

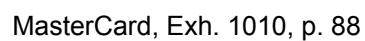


FIG. 13D

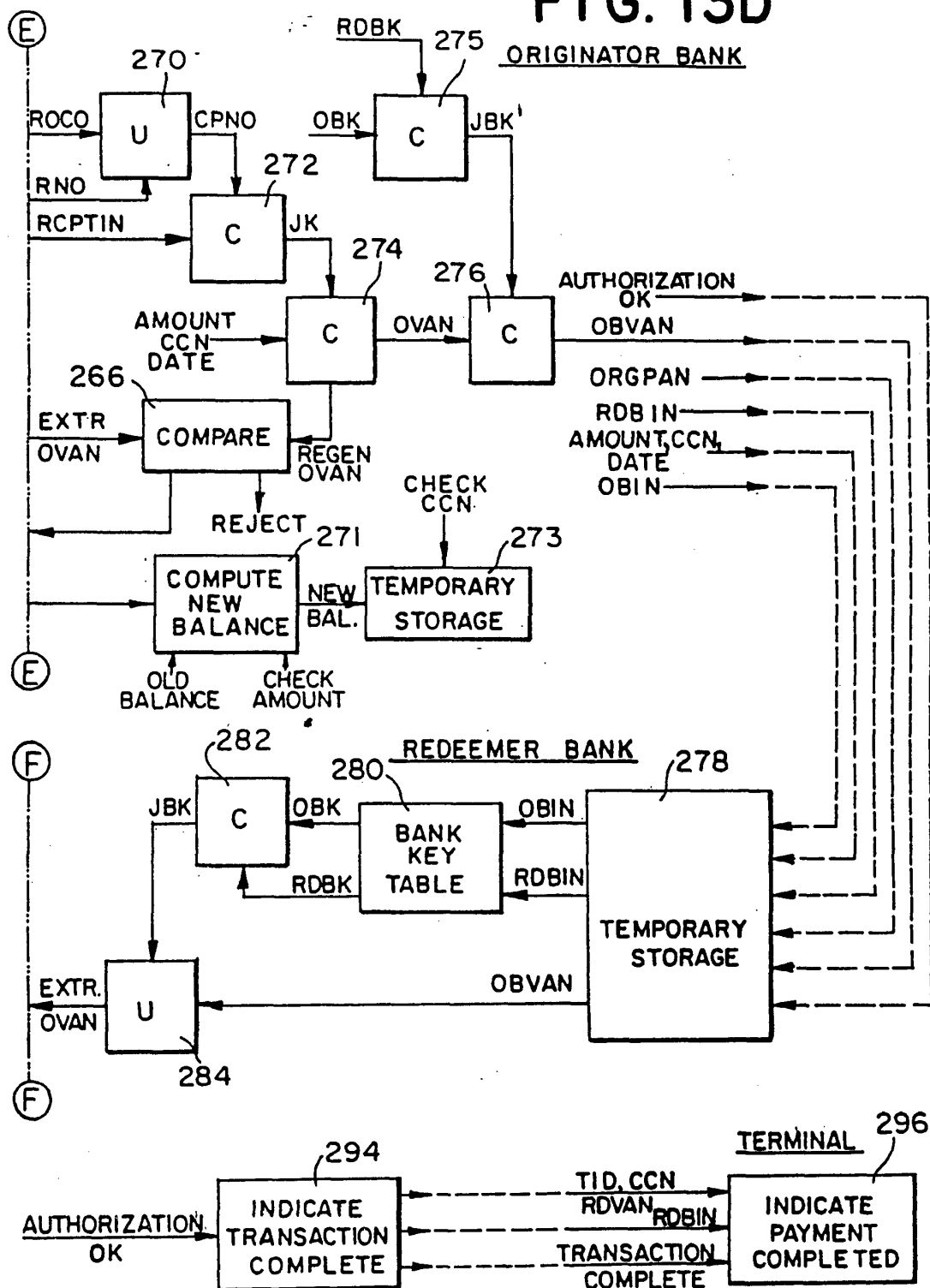


FIG. 13E

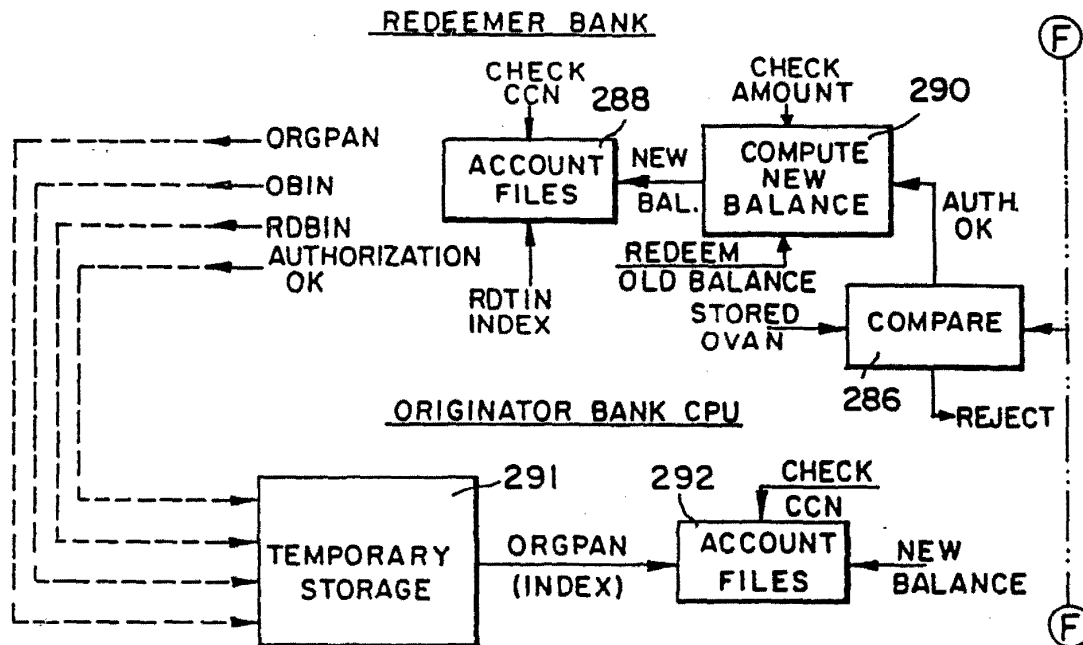
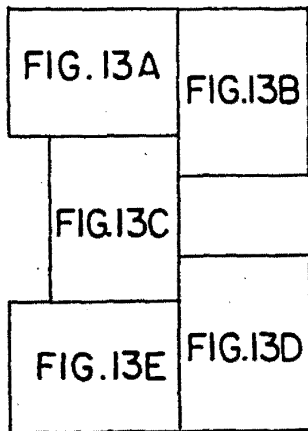
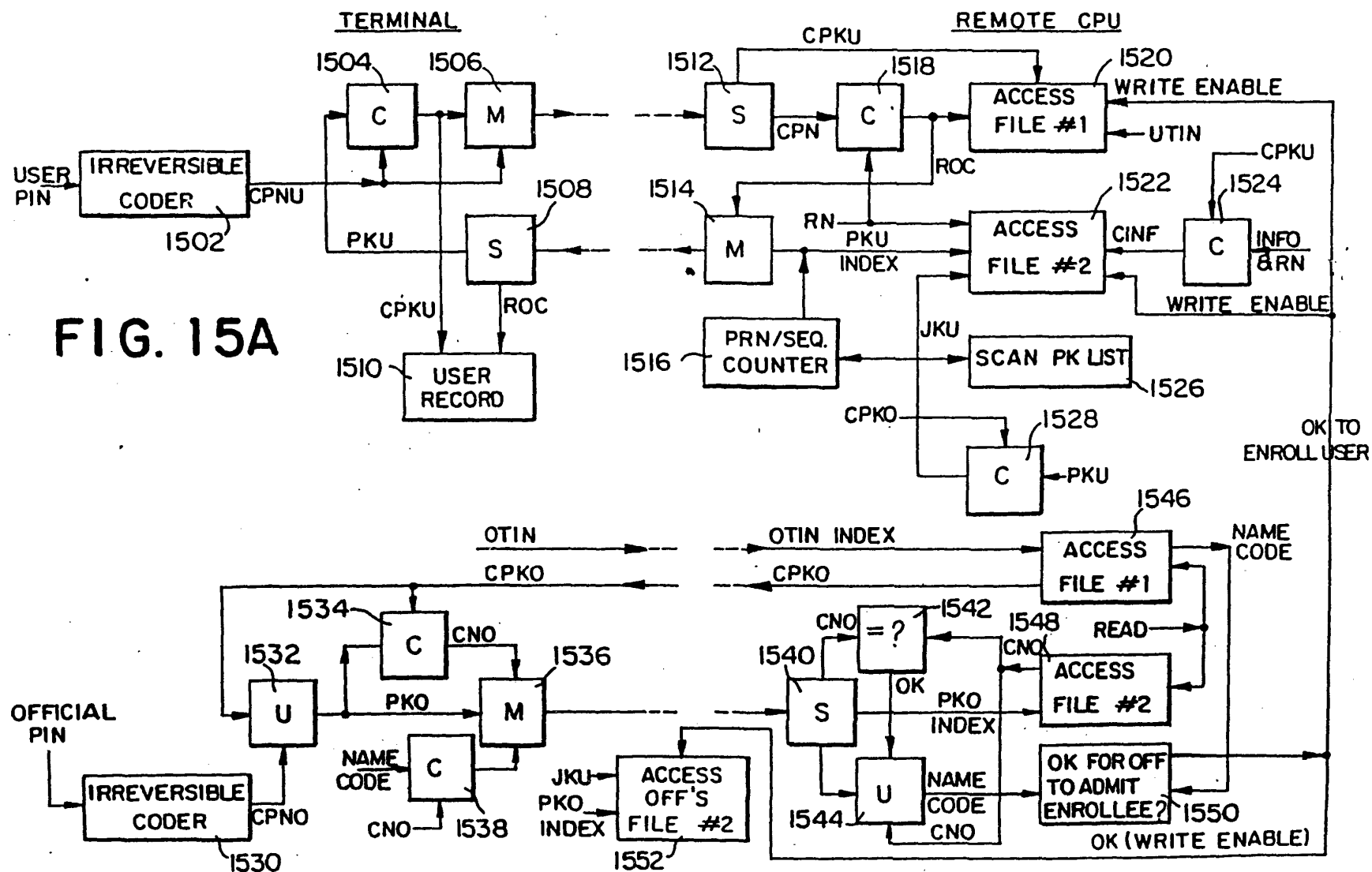


FIG. 14



NOT A DRAWING
IS ORIGINALLY FILED



08/122071

08/122071

CREDENTIAL ISSUE PROCESSING AGENCY TERMINAL/COMPUTER

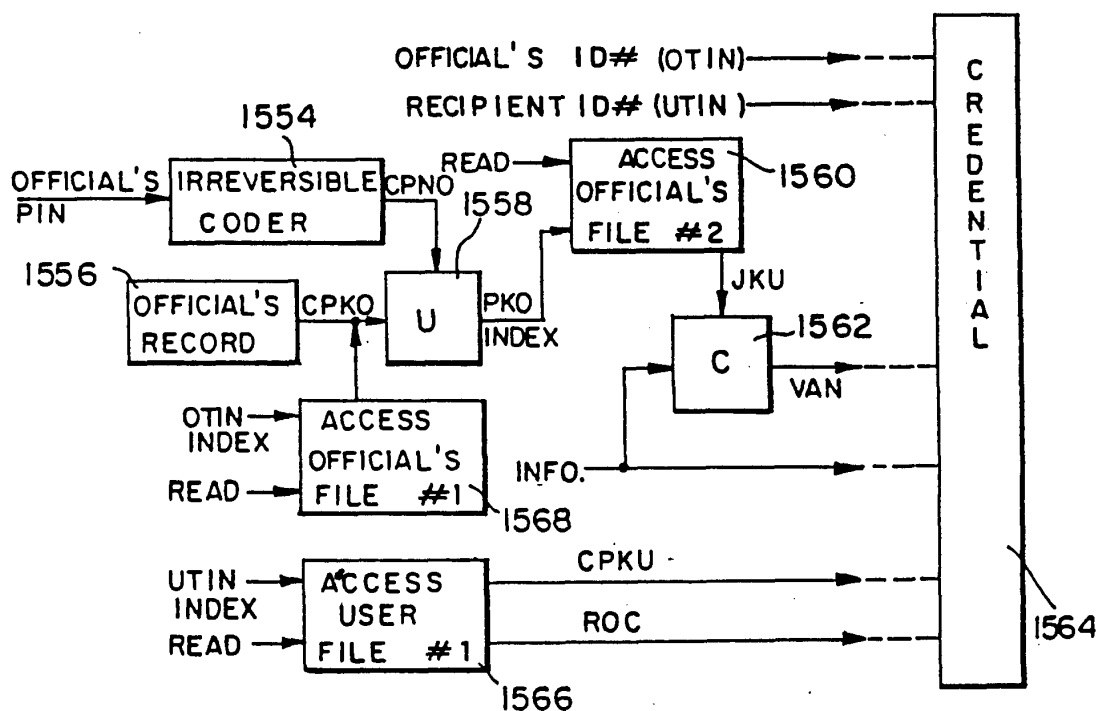


FIG. 15 B

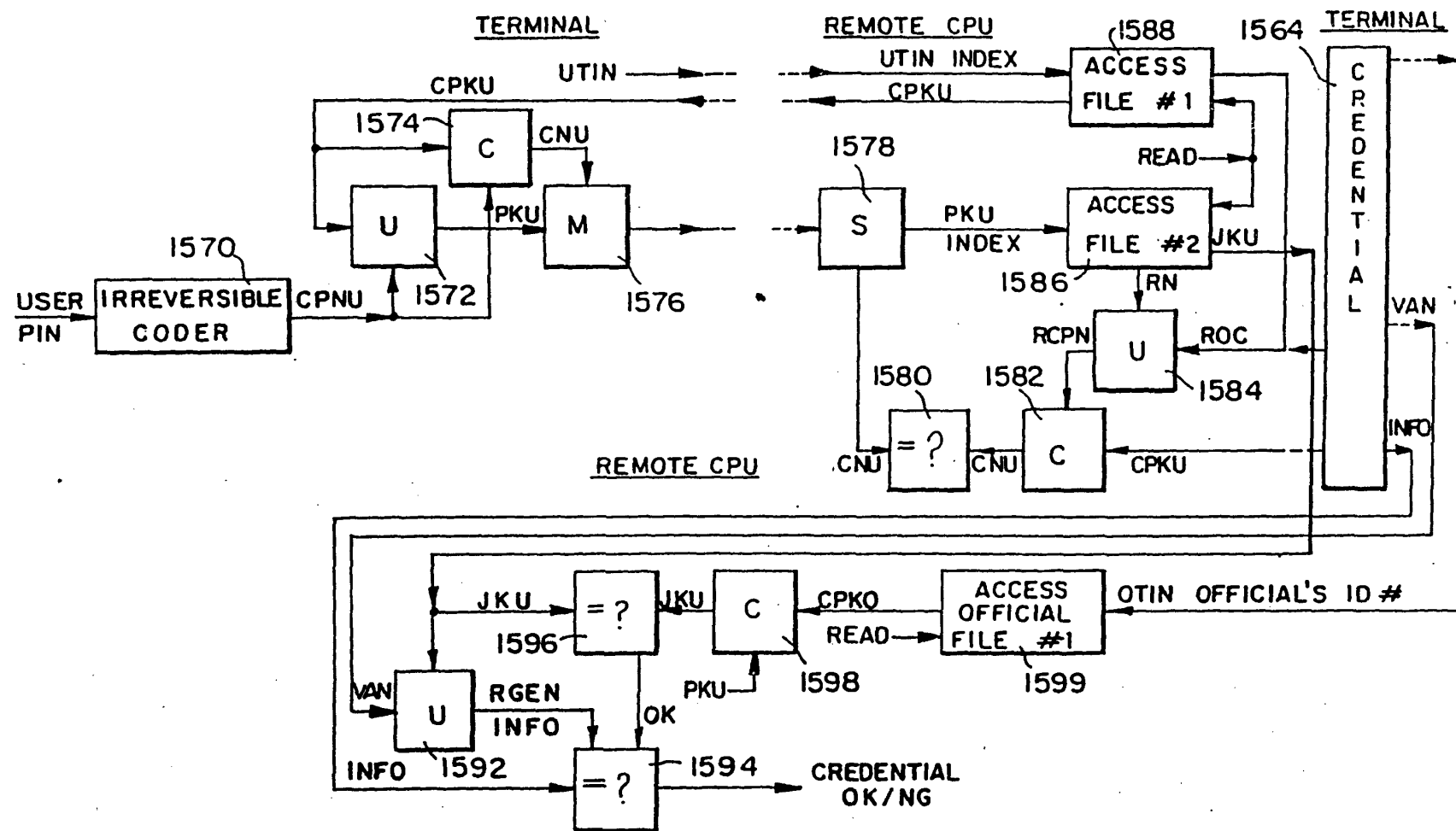
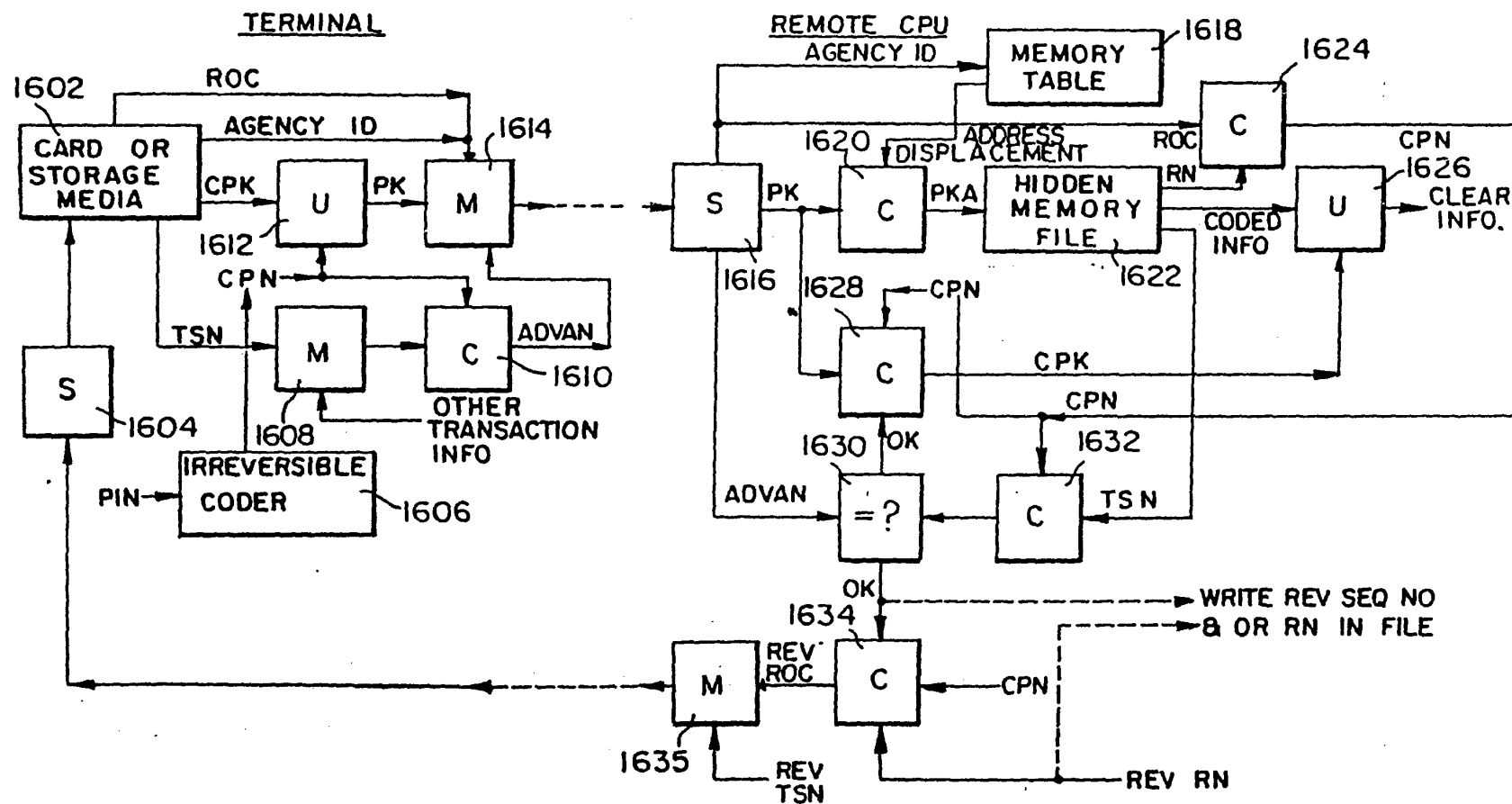


FIG. 15C





08/122071

A/CIP

Express Mail Mailing Label"
Number TB255321187 US
Date of Deposit September 14, 1993

I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Commissioner of Patents and Trademarks, Washington, D.C. 20231

Name: LOUISA DRAIN

Signed: Louisa Drain

PATENT
Attorney Docket No. 6074-1U1
BOX PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

The Commissioner of Patents and Trademarks
Washington, D.C. 20231

Sir:

This is a request under 37 C.F.R. §1.60 for filing a

☐ Continuation application (Group Art Unit _____)

☒ Divisional application. Anticipated classification
Class_____, Subclass_____,

of pending prior application Serial No. 07/977,385 filed on
November 17, 1992 of Leon Stambler for SECURE TRANSACTION SYSTEM
AND METHOD UTILIZED THEREIN

The filing fee is calculated below:

			SMALL ENTITY		OR	LARGE ENTITY	
CLAIMS	NO. FILED	NO. EXTRA	BASIC FEE	\$355		BASIC FEE	\$710
TOTAL	59-20=	39	x11=	\$429	OR	x22=	\$
INDEPENDENT	17- 3=	14	x37=	\$518	OR	x74=	\$
MULTIPLE DEPENDENT CLAIMS PRESENT			x115=	\$	OR	+230=	\$
			TOTAL	\$947	OR TOTAL	\$	

- ☒ Enclosed is a copy of the prior application including drawings (if any) as originally filed. I hereby verify that the attached papers are a true copy of the prior application identified above as originally filed.
- ☐ Enclosed is a copy of the properly executed late-filed Declaration and Power of Attorney in the prior application. I hereby verify that the attached paper is a true copy of the executed Declaration and Power of Attorney as filed in the prior application.
- ☐ Enclosed is a copy of the prior application including drawings (if any) as originally filed. The attached papers are believed to be a true copy of the prior application identified above as originally filed. This statement is based upon information and belief, since the prior application was originally filed by applicant's prior attorney, to whom the original Power of Attorney was given and who provided a copy of the prior application to applicant's present attorneys.
- ☒ A Verified Statement Claiming Small Entity Status:
- ☒ was filed with the original application, and such status is still proper and desired (37 C.F.R. §1.28(a)).
- ☐ is enclosed herewith.
- ☒ The Commissioner is hereby authorized to charge any of the following fees which may be required, or credit any overpayment, to Account No. 16-0235. Two additional copies of this request are enclosed.
- ☒ The above calculated filing fee \$ 947.00.
- ☒ Any additional fees required under 37 C.F.R. §1.16 or §1.17.
- ☒ If the filing of any paper during the prosecution of this application requires an extension of time in order for the paper to be timely filed, applicant(s) hereby petition(s) for the appropriate extension of time pursuant to 37 C.F.R. §1.136(a).
- ☐ Applicant(s) hereby claim the right of foreign priority under 35 U.S.C. §119 based on the following application(s), the priority of which was claimed in the prior application:
- | Country: | Application No.: | Filing Date: |
|----------|------------------|--------------|
| _____ | _____ | _____ |
| _____ | _____ | _____ |
| _____ | _____ | _____ |
- ☐ A certified copy of the priority document(s) is of record in the prior application or application S.N. _____, filed _____.
- ☐ Cancel claims _____

- ☐ Amend the specification by inserting before the first line the sentence: --This is a ☐ continuation ☐ division of application Serial No. _____, filed _____.--
- ☒ A preliminary amendment is enclosed.
- ☐ New formal drawings are enclosed.
- ☐ The prior application is assigned to _____
-
- ☐ The assignment of the prior application applies to this application.
- ☒ The power of attorney in the present application is to the attorneys and agents in the firm of Panitch Schwarze Jacobs & Nadel as listed in:
- ☐ A new Declaration and Power of Attorney is enclosed.
- ☒ The power appears in the prior application, as filed.
- ☐ Since the power does not appear in the prior application, as filed, a copy of the power in the prior application is enclosed.
- ☐ Revocation and Appointment of Attorney is enclosed.
- ☒ Address all future communications to the undersigned attorney at:
- PANITCH SCHWARZE JACOBS & NADEL**
1601 Market Street - 36th Floor
Philadelphia, PA 19103
- ☐ A Petition for Extension of Time
- ☐ to _____ has been filed in the prior application.
- ☐ is not needed.

Respectfully submitted,

LEON STAMBLER

Sept 14, 1993
 (Date)

By:

Leslie L. Kasten, Jr.
LESLIE L. KASTEN, JR.
 Registration No. 28,959
PANITCH SCHWARZE JACOBS & NADEL
 1601 Market Street - 36th Floor
 Philadelphia, PA 19103
 Telephone: 215-567-2020

CEB:maj
 Enclosures



08/122071

Patent

T.W. 11/3-93
PWA
paper #2

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Patent Application of : Group Art Unit 2207
Leon Stambler :
Serial No: Not yet assigned : Examiner:
Filed: Herewith : S. Cangialosi
For: SECURE TRANSACTION SYSTEM : Attorney Docket
AND METHOD UTILIZED THEREIN : No. 6074-1U1

PRELIMINARY AMENDMENT

In the above-identified divisional application of
Serial No. 07/977,385, filed herewith, please enter the following
preliminary amendment:

In the specification:

On page 1, after the title, add the sentence, --This
is a Division of application S.N. 07/977,385, filed November 17,
1992, ^{now U.S. Patent 5,267,314} ~~now allowed.~~--

In the claims:

Please cancel claims 1-6, 18, 36-45, 51-55 and 60-62.
Please amend claims 17, 19, 30, 33, 46, 48, 56, 59, and 63 as
follows:

17. (Amended) In a multi-party transaction system, a
method for authenticating a transaction and parties to the
transaction comprising the steps of:
coding information relevant to a transaction with
[at least] information associated with at least one present party

18091.1

-1-

A²
Concluded [two parties] and with information associated with at least one
absent party to generate a variable authentication number [VAN];
and
associating the VAN with the transaction.

A³
19. (Amended) The method of claim 17, wherein the
coding step comprises the steps of:
coding the information associated with said at
least one present party and said at least one absent party [two
parties] to generate a joint code; and
coding information relevant to the transaction
with the joint code to generate the VAN.

A⁴
30. (Amended) In a transaction system wherein a party
has a first personal identification number (PIN) and an official
as a second PIN, a method for enrolling the party to thereby
enable the party to participate in a subsequent transaction
comprising the steps of:
coding information associated with the party with
information associated with the official to generate a joint
code, the joint code being subsequently associable with a
transaction; and
storing the joint code in a first storage means,
the first storage means being accessible only to a party [with
knowledge of] who can input the first PIN, such that if no party
exists [with a knowledge of] who can input the first PIN, the
joint code cannot be accessed from the storage means and,

~~therefore, cannot be associated with the transaction.~~

33. (Amended) In a multi-party transaction system, a method for processing transactions comprising the steps of:

coding information relevant to a transaction with information associated with at least one party to generate a variable authentication number (VAN);

associating the VAN with the transaction;

receiving a personal identification number (PIN) from a recipient party;

determining whether [a] the recipient party [and the transaction are] is authentic by using the received recipient PIN; [and]

determining whether the transaction is authentic;

and

if the recipient party and the transaction are authentic, then authorizing the transaction.

46. (Amended) A method for automatically and instantaneously transferring funds from an account associated with an originator party to an account associated with a recipient party, the method comprising the steps of:

receiving from the originator party a personal identification number (PIN) associated with the originator party, information identifying the originator party account and the recipient party account, and information comprising a payment amount and specifying a funds transfer;

generating a variable authentication number (VAN)
using the originator party PIN, the recipient party account
identifying information, and the fund transfer information;

determining whether the originator party is
authentic by using the PIN;

determining whether the funds transfer is
authentic by using the VAN;

if the originator party and the funds transfer are
authentic, then transferring authenticated funds to the recipient
party account from the originator party account;

generating after transferring the authenticated
funds to the recipient party account a redemption variable
authentication number (RVAN) using at least the funds transfer
information; and

associating the RVAN with the fund transfer, such
that the funds transfer is substantiated by the RVAN.

48. (Amended) ~~In an invoice processing system, [A] a~~
method for processing an invoice comprising the steps of:

generating a variable authentication number (VAN)
using at least information associated with an invoice, the
information associated with the invoice including information
identifying a payee party account and payment information
comprising a payment amount;

recording the VAN and the information associated
with the invoice on the invoice;

receiving the VAN and a personal identification number (PIN) from a payor party, the received PIN being unrecoverable in the system;

determining whether the payor party and the VAN are authentic by using the information associated with the invoice and the received PIN;

receiving the payee party account identifying information and the payment information from the invoice; and

if the payor party and the VAN are authentic, then crediting the payment amount to the payee party account from funds associated with the payor party.

56. (Amended) A multi-party transaction system for authenticating a transaction and parties to the transaction comprising:

means for coding information relevant to a transaction with [at least] information associated with at least one present party [two parties] and with information associated with at least one absent party to generate a variable authentication number (VAN); and

means for associating the VAN with the transaction.

59. (Amended) A multi-party transaction system for processing transactions comprising:

means for coding information relevant to a transaction with information associated with at least one party

to generate a variable authentication number (VAN);

means for associating the VAN with the transaction;

means for determining whether a recipient party and the transaction are authentic; [and]

means for authorizing redemption of the transaction if the recipient party and the transaction are authentic[.];

means for coding information associated with at least one party with the VAN to generate a redemption VAN (RVAN);

means for associating the RVAN with the transaction after the transaction has been authorized and processed such that the transaction cannot be fraudulently presented for further redemption; and

means for storing the RVAN in a storage means associated with at least one party, such that the transaction is cleared in a substantially instantaneous manner.

63. (Amended) In a system comprising a credential and party information associated with a party and recorded on the credential, the party information comprising first coded authentication information previously generated by using a personal identification number (PIN) associated with the party, a method for authenticating the party comprising the steps of:

receiving a PIN from the party to be authenticated, the PIN being unrecoverable in the system;

AKO
Conclude

retrieving the first coded authentication
information from the credential;
generating second coded authentication information
using the received PIN;
comparing at least part of the retrieved first
coded authentication information to at least part of the
generated second coded authentication information; and
authenticating the party if said at least part of
the retrieved first coded authentication information corresponds
to said at least part of the generated second coded
authentication information.

Please add new claims 64 - 84 as follows:

AK
Cont.

--64. In a multi-party transaction system, a method
for authenticating a transaction and parties to the transaction
comprising the steps of:

coding information relevant to a transaction with
information associated with a first party and information
associated with at least one other party to generate a variable
authentication number (VAN), the information associated with the
first party comprising information derivable by uncoding a
predetermined nonsecret number with a predetermined secret number
associated with the first party; and
associating the VAN with the transaction.

65. In a system comprising a storage means addressable using a predetermined address and party information associated with a party, the party information comprising a personal identification number (PIN) and first coded authentication information, the first coded authentication information comprising a first part (CPK1), and a second part (CN1), the first part previously generated by coding the PIN and the predetermined address, and the second part previously generated by coding the PIN and CPK1, and wherein CPK1 is not stored anywhere in the system and CN1 is stored in the storage means at the predetermined address, a method for authenticating the party comprising the steps of:

receiving the personal identification number (PIN) from the party to be authenticated;

generating second coded authentication information by coding the received PIN and the predetermined address, the second coded authentication information comprising a first part (CPK2);

accessing the storage means using the predetermined address to locate and retrieve CN1;

generating third coded authentication information by uncoding the retrieved CN1 with the received PIN, the third coded authentication information comprising a first part (CPK3);

comparing at least part of the generated second coded authentication information (CPK2) with at least part of the

third coded authentication information (CPK3); and
authenticating the party if the compared part of
the generated second coded authentication information (CPK2)
corresponds to the compared part of the third coded
authentication information (CPK3).

66. The method of claim 65 wherein the personal
identification number (PIN) is a coded personal identification
number (CPN).

67. In a transaction system comprising a first storage
means in possession of a first party, containing party
information, the party information comprising a predetermined
first non-secret code (ROC1), a predetermined arbitrary first
transaction number (TN1), and predetermined party information
used to form a predetermined address (PA), a second storage
means, and party information stored in the second storage means,
the second storage means party information comprising a
predetermined arbitrary first secret number (RN1), and a
predetermined second transaction number (TN2) corresponding to
the TN1, a method for authenticating the first party, the first
storage means, and transaction information comprising the steps
of:

receiving a personal identification number (PIN)
from the first party, at a first site, and generating first coded

*All
Confidential
A11
Cont*

authentication information using the received PIN;
retrieving the party information from the first
storage means, at the first site;
coding the transaction information and the TN1
with the first coded authentication information to generate a
first anti-duplication variable authentication number (ADVAN1),
at the first site;
transmitting the ADVAN1, and a portion of the
retrieved first storage means party information, said portion
comprising the ROC1 and the predetermined party information used
to form the PA, from the first site to a second site;
deriving the PA at the second site from the
received predetermined party information;
accessing the second storage means using the
derived PA to locate and retrieve RN1 and TN2;
generating second coded authentication information
using the received ROC1 and the retrieved RN1;
uncoding the ADVAN1 using the second coded
authentication information to derive the TN1 and the transaction
information;
comparing the derived TN1 to the retrieved TN2;
authenticating the first party, the first storage
means, and the transaction information if the derived TN1
corresponds to the retrieved TN2;
forming a revised third transaction number (TN3)

and a revised second secret number (RN2);

storing the TN3 and the RN2 in the second storage means at the predetermined address (PA);

generating a revised second non-secret code (ROC2) using the second coded authentication information and the RN2;

coding the TN3 with the second coded authentication information to generate a second anti-duplication variable authentication number (ADVAN2);

transmitting the ADVAN2 and the ROC2 from the second site to the first site;

uncoding the received ADVAN2 at the first site using the first coded authentication information to derive the TN3; and

storing the derived TN3 and the received ROC2 in the first storage means for use in a subsequent transaction.

68. The method of claim 67 wherein the PIN is unrecoverable within the system.

69. The method of claim 67 wherein the TN3 is coded with the second coded authentication information and TN2, to generate the ADVAN2; and

the received ADVAN2 is uncoded at the first site using the first coded authentication information and TN1, to derive the TN3.

70. The method of claim 67, further comprising the step of:

coding the predetermined address (PA) with the first coded authentication information to form a coded predetermined address (CPA) so that the PA is secret; and storing the CPA in the first storage means.

71. The method of claim 70 wherein at least a portion of the CPA is revisable.

72. The method of claim 71 wherein a first terminal transfer code (TTC1) is stored at the first site and a corresponding second terminal transfer code (TTC2) is stored at the second site, further comprising the steps of:

deriving the PA at the first site using the first coded authentication information by uncoding the CPA;

coding the derived PA with TTC1 to generate a terminal coded address (TCA);

transmitting the TCA from the first site to the second site;

uncoding the TCA at the second site using the TTC2 to derive the PA; and

accessing the second storage means using the derived PA to locate and retrieve the second storage means party information.

73. The method of claim 72 further comprising the steps of:

revising the TTC2 at the second site to form a third terminal transfer code (TTC3) for use in a subsequent transaction;

storing the TTC3 at the second site;

coding the TTC3 with the TTC2 to generate a coded transfer number (CTN);

transmitting the CTN from the second site to the first site;

uncoding the CTN at the first site using the TTC1 to derive the TTC3;

storing the uncoded TTC3 at the first site.

74. The method of claim 67 wherein the step of transmitting the ADVAN1, and a portion of the retrieved first storage means party information, said portion comprising the ROC1 and the predetermined party information used to form the PA, from the first site to the second site, further comprises transmitting at least a portion of the transaction information;

the step of comparing the derived TN1 to the retrieved TN2, further comprises the step of comparing the transaction information uncoded from the ADVAN1 using the second coded authentication information with the at least a portion of the transaction information transmitted; and

the step of authenticating additionally requires that the uncoded transaction information corresponds to the transmitted transaction information.

75. In a transaction system wherein a party has a first personal identification number (PIN1) and an official has a second personal identification number (PIN2), a method for enrolling the party and issuing the party a credential, and then authenticating the party and the credential in a subsequent transaction, the method of enrolling and issuing comprising the steps of:

coding information associated with the party with information associated with the official to generate a joint code;

storing the joint code in a first storage means, the joint code being retrievable from the first storage means only by a party who can provide the PIN1;

storing the joint code in a second storage means, the joint code being retrievable from the second storage means only by a party who can provide the PIN2;

coding information relevant to the credential with the joint code to generate a first variable authentication number (VAN1);

recording the VAN1 on the credential;

issuing the credential to the party; and

the method of authenticating the party and the credential in a subsequent transaction comprising the steps of:

receiving the PIN1 from the party to be authenticated;

accessing the first storage means with the PIN1 to locate and retrieve the joint code;

coding information relevant to the credential with the retrieved joint code to generate a second variable authentication number (VAN2);

comparing the VAN2 to the VAN1; and

authenticating the party and the credential if the VAN2 corresponds to the VAN1.

76. The method of claim 75, further comprising the steps of:

retrieving the joint code from the second storage means;

regenerating the joint code by coding information associated with the party with information associated with the official;

comparing the retrieved joint code with the regenerated joint code; and

authenticating the official if the retrieved joint code corresponds to the regenerated joint code.

77. The method of claim 75, further comprising the steps of:

retrieving the joint code from the first storage means;

retrieving the joint code from the second storage means;

comparing the retrieved joint codes; and

authenticating the official if the retrieved joint codes correspond.

78. The method of claim 75 wherein the joint code is revised or erased from the second storage means after the VAN1 is recorded on the credential.

79. The method of claim 15, further comprising the steps of:

debiting the patient's account for the patient amount of liability to pay for the medicine dispensed by an authorized dispenser having an account, the dispenser located in a processing jurisdiction;

debiting a co-payor's account for a co-payor amount of liability; and

crediting the dispenser's account by the sum of the debited amounts.

80. The method of claim 20, wherein the predetermined secret number comprises a joint code, the joint code being generated from information associated with the party and at least a second party.

81. The method of claim 30, wherein a subsequent transaction with a second party comprises the steps of:
retrieving the joint code from the first storage means;
coding the joint code with information associated with the second party to generate a multiple joint code; and
associating the multiple joint code with the transaction.

82. The method of claim 81, further comprising the steps of:
storing the joint code in a second storage means, the second storage means being accessible only to a party having the second PIN;
receiving the second PIN from the official;
using the received second PIN to access the second storage means and to retrieve the joint code;
coding information relevant to the transaction with the joint code to generate a variable authentication number (VAN);

recording the VAN on a credential associated with the transaction; and

issuing the credential, wherein a party without knowledge of the second PIN cannot access the second storage means or the joint code stored therein and, therefore, cannot legitimately issue the credential.

83. The method of claim 30, further comprising the steps of:

retrieving the joint code from the first storage means;

regenerating the joint code by coding information associated with the party with information associated with the official;

comparing the retrieved joint code with the regenerated joint code; and

authenticating the official if the retrieved joint code corresponds to the regenerated joint code.

84. The method of claim 32, further comprising the steps of:

retrieving the joint code from the first storage means;

retrieving the joint code from the second storage means;

*ALL
Concluded*

comparing the retrieved joint codes; and
authenticating the official if the retrieved joint
codes correspond.--

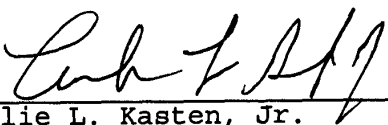
REMARKS

After the foregoing amendment, claims 7-17, 19-35, 46-50, 56-59, and 63-84 are active in the present application. Claims 1-6, 18, 36-45, 51-55, and 60-62 were cancelled. Claims 17, 19, 30, 33, 46, 48, 56, 59, and 63 have been amended, in substantially the same manner as submitted in the Response to the Office Action submitted March 18, 1993 in the parent application. New claims 64-84 are presented and are adequately supported in the specification. No new matter has been added. Consideration and allowance of this application is respectfully requested.

Respectfully submitted,

LEON STAMBLER

BY:


Leslie L. Kasten, Jr.
Registration No. 28,959
PANITCH, SCHWARZE, JACOBS & NADEL
1601 Market Street, 36th Floor
Philadelphia, PA 19103
(215) 567-2020

08/122071



"EXPRESS MAIL" Mailing Label No. TB255321187US

DATE OF DEPOSIT: September 14, 1993

I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 C.F.R. § 1.10 on the date indicated above and is addressed to the Commissioner of Patents and Trademarks, Washington, D.C. 20231.

NAME: Louisa Drain

SIGNED: Louisa Drain

PATENT
T.W. 11-3-93
Prior Art w/TT
fypu

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Patent Application of : Group Art Unit
Leon Stambler :
Serial No.: Not yet assigned : Examiner:
Filed: Herewith :
For: SECURE TRANSACTION : Attorney Docket
SYSTEM AND METHOD : No. 6074-1U1
UTILIZED THEREIN

INFORMATION DISCLOSURE STATEMENT

It is requested that the reference/s listed on the attached Information Disclosure Citation Form PTO-1449 be considered by the Patent Examiner in connection with the above-identified application and be made of record therein.

Copies of the references were previously cited and submitted in related Application Serial No. 07/977,385, filed November 17, 1992, of which the present application is a **division**.

Independent consideration and acknowledgment of the listed reference/s are respectfully requested.

Respectfully submitted,

September 14, 1993 BY: Leslie L. Kasten, Jr.
(Date)

LESLIE L. KASTEN, JR.
Registration No. 28,959
PANITCH SCHWARZE JACOBS & NADEL
1601 Market Street - 36th Floor
Philadelphia, PA 19103
Telephone: (215) 567-2020

CEB:mcg
Enclosure

3

Sheet 1 of 5

Form PTO-1449 (Modified)
(REV. 8-83)

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE

ATTORNEY DOCKET NO.:
6704-103

SERIAL NO.: 122,071

53
SEP 14 1993
PAT. & TRADEMARK OFFICE

APPLICANT:
Stamblor

FILING DATE:

GROUP ART UNIT: 2202

INFORMATION DISCLOSURE CITATION

(Use several sheets if necessary)

U.S. PATENT DOCUMENTS

EXAMINER INITIAL	DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
gc	4 9 6 5 5 6 8	10/90	Atalla et al.	380	24	
gc	5 1 6 3 0 9 8	11/92	Dahbura	380	24	
gc	4 3 0 2 8 1 0	11/81	Bouricius et al.	380	24	
gc	4 6 0 5 8 2 0	8/86	Campbell, Jr.	380	24	
gc	3 6 0 9 6 9 0	9/71	Nissman	340	149 R	
gc	3 6 1 1 2 9 3	10/71	Constable	340	149 A	
gc	3 6 5 7 5 2 1	4/72	Constable	235	61.7 B	
gc	3 8 9 2 9 4 8	7/75	Constable	340	149 R	
gbc	3 9 3 8 0 9 1	2/76	Atalla et al.	340	149 A	
gc	4 0 0 4 0 8 9	1/77	Richard et al.	178	22	
gc	4 0 1 6 4 0 5	4/77	McCune et al.	235	380	

FOREIGN PATENT DOCUMENTS

	DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION	
						YES	NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)


EXAMINER

S. Cangialosi

DATE CONSIDERED

10/94

*EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Form PTO-1449 (Modified) (REV. 8-83)		U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE		ATTORNEY DOCKET NO. 6074-1 U1		SERIAL NO.: 124071	
INFORMATION DISCLOSURE CITATION						FILING DATE: 2-20-2	
(Use several sheets if necessary)							
U.S. PATENT DOCUMENTS							
EXAMINER INITIAL	DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE	
gn	4 1 8 6 8 7 1	2/80	Anderson et al.	235	380		
gn	4 1 9 8 6 1 9	4/80	Atalla	340	149 A		
gn	4 2 0 8 5 7 5	6/80	Haltof	235	380		
gn	4 2 2 3 4 0 3	9/80	Konheim et al.	375	2		
gn	4 2 3 4 9 3 2	11/80	Gorgens	364	900		
gn	4 2 6 4 7 8 2	4/81	Konheim	178	22		
gn	4 2 6 8 7 1 5	5/81	Atalla	178	22		
gn	4 2 8 1 2 1 5	7/81	Atalla	178	22.08		
gn	4 2 8 3 5 9 9	8/81	Atalla	178	22.1		
gn	4 3 0 2 8 1 0	11/81	Bouricius et al.	364	200		
gn	4 3 0 4 9 9 0	12/81	Atalla	235	380		
FOREIGN PATENT DOCUMENTS							
	DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION	
						YES	NO
OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)							
EXAMINER	S. Camp, et al.			DATE CONSIDERED 10/94			
*EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.							

Form PTO-1449 (Modified)
(REV. 8-83)

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE

ATTORNEY DOCKET NO.
6074-1U1

APPLICANT:
Leon Stambler

FILING DATE:

MAIL ROOM
58 SEP 14 1993
PAT & TRADEMARK OFF

SERIAL NO.: 122,071

GROUP ART UNIT:

INFORMATION DISCLOSURE CITATION

(Use several sheets if necessary)

U.S. PATENT DOCUMENTS

EXAMINER INITIAL	DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
gle	4 3 1 7 9 5 7	3/82	Sendrow	178	22.08	
gre	4 3 2 8 4 1 4	5/82	Atalla	235	380	
gre	4 3 8 6 2 6 6	5/83	Chesarek	235	380	
gre	4 4 9 8 0 0 0	2/85	Decavele et al.	235	380	
gre	4 5 9 0 4 7 0	5/86	Koenig	340	825.31	
gre	4 6 0 5 8 2 0	8/86	Campbell, Jr.	178	22.09	
gre	4 6 6 5 3 9 6	5/877	Dieleman	380	23	
gre	4 6 8 6 3 5 7	8/87	Douno et al.	235	379	
gre	4 7 2 0 8 5 9	1/88	Aaro et al.	380	23	
gre	4 7 3 4 8 5 8	3/88	Schlaflly	364	408	
gre	4 7 5 5 9 4 0	7/88	Brachtl et al.	364	408	

FOREIGN PATENT DOCUMENTS

DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION
					YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER

S. Gargioli

DATE CONSIDERED

10/94

*EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.



I HEREBY CERTIFY THAT THIS CORRESPONDENCE IS BEING DEPOSITED WITH THE UNITED STATES POSTAL SERVICE AS FIRST CLASS MAIL IN AN ENVELOPE ADDRESSED TO: COMMISSIONER OF PATENTS AND TRADEMARKS, WASHINGTON, D.C. ON THE DATE INDICATED BELOW.

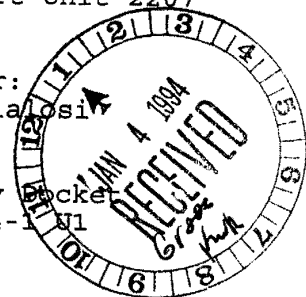
BY Maureen Blump
DATE December 6, 1993

#4
TW. 1-12-94
Pre B
2207

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Patent Application of : Group Art Unit 2207
Leon Stambler :
Serial No: 08/122,071 : Examiner:
Filed: Sept. 14, 1993 : S. Cangialosi
For: SECURE TRANSACTION SYSTEM : Attorney
AND METHOD UTILIZED THEREIN : No. 6074-1 V1



SECOND PRELIMINARY AMENDMENT

Prior to examination of the above-identified application, please enter the following preliminary amendment:

In the Claims:

Please add new claims 85 - 100 as follows:

--85. In a multi-party transaction system, a method for securing information relevant to a transaction comprising the step of:

coding the information relevant to the transaction with information associated with at least one present party, and information associated with at least one absent party.

86. The method of claim 85 wherein the coded information relevant to the transaction is uncoded with information associated with at least one present party and with information associated with at least one absent party to recover

P 11117 12/27/93 08122071

16-0235 110 203

176.00CH

P 11117 12/27/93 08122071

16-0235 110 202

185.00CH

the relevant transaction information.

87. The method of claim 85 wherein the information relevant to the transaction comprises coded information.

88. The method of claim 85 wherein the information relevant to the transaction comprises noncoded information.

89. In a multi-party transaction system, a method for securing information relevant to a transaction comprising the steps of:

coding information associated with at least two parties to generate a joint code; and

coding the information relevant to the transaction with the joint code.

90. The method of claim 89 wherein the coded information relevant to the transaction is uncoded with the joint code.

91. The method of claim 89 wherein the information associated with the at least two parties used to generate the joint code comprises information associated with at least one present party and information associated with at least one absent party.

92. The method of claim 89 wherein the information relevant to the transaction comprises coded information.

93. The method of claim 89 wherein the information relevant to the transaction comprises noncoded information.

94. In a transaction system, a method for securing information relevant to a transaction comprising the steps of:

generating a joint code by coding information accessed from one or more data storage means with information associated with at least one party to the transaction; and

coding the information relevant to the transaction with the joint code.

95. The method of claim 94 wherein the coded information relevant to the transaction is uncoded with the joint code.

96. The method of claim 94 wherein the information relevant to the transaction comprises coded information.

97. The method of claim 94 wherein the information relevant to the transaction comprises noncoded information.

98. A method for coding clear information comprising the steps of:

coding a first information group with a second information group to generate a third information group; and coding the clear information with the third information group.

99. The method of claim 98 wherein the coded information can be uncoded with the third information group.

100. In a system comprising a computer program partially executable on a computer, a subset of the computer program being locked, the program being fully executable using a predetermined key, the key in possession of a first party and the computer program in possession of a second party, a method of making the computer program fully executable comprising the steps

of *B1*
included

the first party receiving information associated with the second party from the second party;

the first party coding the predetermined key with the information associated with the second party to generate a coded key;

the first party giving the coded key to the second party;

the second party entering the coded key and the information associated with the second party at a prompt from the computer program, whereby the computer program decodes the coded key with the information associated with the second party to generate the predetermined key and unlocks the locked subset of the computer program with the generated predetermined key so that the computer program is fully executable by the second party.--

REMARKS

After the foregoing amendment, claims 7-17, 19-35, 46-50, 56-59, and 63-100 are active in the present application. New claims 85-100 are presented and are adequately supported in the specification. Claims 85-93 are supported at page 28, lines 29-36; page 29, lines 15-22; page 30, lines 12-22, and 32-36; page 36, lines 1-4; page 31, lines 20-25; page 32, lines 14-17; and in FIGs. 13B, 13C, and 13D at blocks 214, 234, 254, 262, 272, and 282. New claims 94-97 are supported at page 28, lines 1-8 for Fig. 13A, block 204; page 29, lines 1-7; and Fig. 13B, block 216.

New claim 98 is supported at page 43, lines 1-14 for Fig. 16, blocks 1626 and 1628; page 35, lines 25-30; page 36, lines 9-13 for Fig. 15A, blocks 1504 and 1524. New claims 99-100 are supported at page 25, lines 6-32 for Fig. 12A, block 174; and Fig. 12B, blocks 162 and 184.

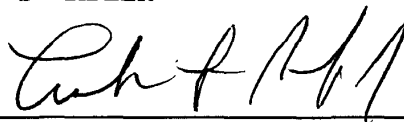
Accordingly, no new matter has been added. Consideration and allowance of this application, including new claims 85-100, is respectfully requested.

Respectfully submitted,

LEON STAMBLER

DATE: December 6, 1993

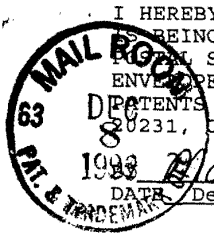
BY:



LESLIE L. KASTEN, JR.
Registration No. 28,959
PANITCH, SCHWARZE, JACOBS & NADEL
1601 Market Street, 36th Floor
Philadelphia, PA 19103
(215) 567-2020

LLK/CEB

#4



I HEREBY CERTIFY THAT THIS CORRESPONDENCE
BEING DEPOSITED WITH THE UNITED STATES
POSTAL SERVICE AS FIRST CLASS MAIL IN AN
ENVELOPE ADDRESSED TO: COMMISSIONER OF
PATENTS AND TRADEMARKS, WASHINGTON, D.C.
20231, ON THE DATE INDICATED BELOW.

1993 Lauren Stumpo
DATE December 6, 1993

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Patent Application of : Group Art Unit 207
Leon Stambler :
Serial No: 08/122,071 : Examiner:
Filed: Sept. 14, 1993 : S. Cangialosi
For: SECURE TRANSACTION SYSTEM : Attorney Docket
AND METHOD UTILIZED THEREIN : No. 6074-1 U1



AMENDMENT COVER SHEET

Transmitted herewith is an Amendment in the above identified application.

- ☒ A verified statement to establish small entity status under 37 CFR 1.9 and 1.27 is
- ☒ already on file;
- ☐ enclosed.
- ☐ No additional fee is required.
- ☒ An Information Disclosure Statement with one copy of each of the cited patents is also attached.

The fee has been calculated as shown below:

					SMALL ENTITY		LARGE ENTITY	
	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NO. PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE	ADDIT. FEE	RATE	ADDIT. FEE
TOTAL	75	(-)	59	= 16	x11=	\$ 176	x22=	\$
INDEP.	22	(-)	17	= 5	x37=	\$ 185	x74=	\$
1ST PRESENT. OF MULTIPLE DEP. CLAIMS					x15=	\$ 0	+230=	\$
					TOTAL \$ 361		TOTAL \$	

[] The applicant(s) hereby petition(s) for any extension of time which may be required in connection with the filing of the enclosed paper(s). (**Petition and Fee for _____ month(s) extension is enclosed.**)

[X] The Commissioner is hereby authorized to charge payment of the following fees associated with this communication or credit any overpayment to Deposit Account No. 16-0235. Two copies of this sheet are attached for accounting purposes.

[X] The above calculated additional claim fees \$361.00.

[X] Any additional fees under 37 CFR 1.16 or 1.17.

Respectfully submitted,

LEON STAMBLER

DATE: December 6, 1993

BY: 

LESLIE L. KASTEN, JR.
Registration No. 28,959
PANITCH, SCHWARZE, JACOBS & NADEL
1601 Market Street, 36th Floor
Philadelphia, PA 19103
(215) 567-2020

LLK/CEB:djw
Enclosures

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to Commissioner of Patents and Trademarks, Washington, D.C., 20231 on the date indicated below.

BY: December 6, 1993
DATE: Maureen Stump

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Patent Application of : Group Art Unit 2207
Leon Stambler :
Serial No.: 08/122,071 : Examiner:
Filed: September 14, 1993 : S. Cangialosi
For: SECURE TRANSACTION : Attorney Docket
SYSTEM AND METHOD : No. 6074-1U1
UTILIZED THEREIN

INFORMATION DISCLOSURE STATEMENT

It is requested that the reference listed on the attached Information Disclosure Citation Form PTO-1449 be considered by the Patent Examiner in connection with the above-identified application and be made of record therein.

Independent consideration and acknowledgment of the listed reference is respectfully requested.

Respectfully submitted,

Dec 6 1993 By: Leslie L. Kasten, Jr.
(Date)
LESLIE L. KASTEN, JR.
Registration No. 28,959
PANITCH SCHWARZE JACOBS & NADEL
1601 Market Street - 36th Floor
Philadelphia, PA 19103
Telephone: (215) 567-2020

LLK:CEB
Enclosure

63 DEC 8 1993



22X CAN-IA/OSI

#6

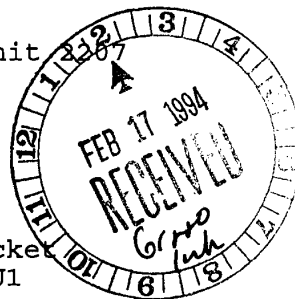
I HEREBY CERTIFY THAT THIS CORRESPONDENCE IS BEING DEPOSITED WITH THE UNITED STATES POSTAL SERVICE AS FIRST CLASS MAIL IN AN ENVELOPE ADDRESSED TO: COMMISSIONER OF PATENTS AND TRADEMARKS, WASHINGTON, D.C. 20513, ON THE DATE INDICATED BELOW.

BY *Roman J. Hoff*
DATE 2/8/94

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re: Patent Application of : Group Art Unit
Leon Stambler :
Serial No.: 08/122,071 : Examiner:
Filed: September 14, 1993 :
For: SECURE TRANSACTION SYSTEM : Attorney Docket
AND METHOD UTILIZED THEREIN : No. 6074-1 U1



AMENDMENT COVER SHEET

Transmitted herewith is an Amendment in the above identified application.

☒ A verified statement to establish small entity status under 37 CFR 1.9 and 1.27 is

☒ already on file;

☐ enclosed.

☐ No additional fee is required.

☒ An Information Disclosure Statement with one copy of each of the cited patents is also attached.

The fee has been calculated as shown below:

					SMALL ENTITY		LARGE ENTITY	
	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NO. PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE	ADDIT. FEE	RATE	ADDIT. FEE
TOTAL	81	(-)	75	= 6	x11=	\$ 66	x22=	\$
INDEP.	22	(-)	22	= 0	x37=	\$ 0	x74=	\$
1ST PRESENT. OF MULTIPLE DEP. CLAIMS					115=	\$ 0	+230=	\$
					TOTAL	\$ 66	TOTAL	\$

[X] The applicant(s) hereby petition(s) for any extension of time which may be required in connection with the filing of the enclosed paper(s). (Petition and Fee for _____ month(s) extension is enclosed.)

[X] The Commissioner is hereby authorized to charge payment of the following fees associated with this communication or credit any overpayment to Deposit Account No. 16-0235. Two copies of this sheet are attached for accounting purposes.

[X] The above calculated additional claim fees \$66.00

[X] Any additional fees under 37 CFR 1.16 or 1.17.

Respectfully submitted,

LEON STAMBLER

Feb 8, 1994
(Date)

By:

Leslie L. Kasten, Jr.
LESLIE L. KASTEN, JR.
Registration No. 28.959
PANITCH SCHWARZE JACOBS & NADEL
1601 Market Street - 36th Floor
Philadelphia, PA 19103
Telephone: (215) 567-2020

LLK/CEB:djw
Enclosures

cc: David S. Shrager, Esq.



2207

#69

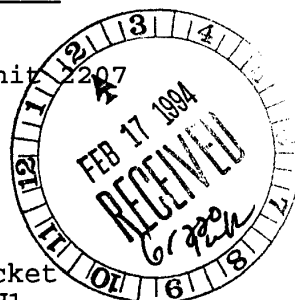
I HEREBY CERTIFY THAT THIS CORRESPONDENCE
BEING DEPOSITED WITH THE UNITED STATES
POSTAL SERVICE AS FIRST CLASS MAIL IN AN
ENVELOPE ADDRESSED TO: COMMISSIONER OF
PATENTS AND TRADEMARKS, WASHINGTON, D.C.
20231, ON THE DATE INDICATED BELOW.

BY Donna J. Hall
DATE 2/8/94

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re: Patent Application of : Group Art Unit 2207
Leon Stambler :
Serial No.: 08/122,071 : Examiner:
Filed: September 14, 1993 :
For: SECURE TRANSACTION SYSTEM : Attorney Docket
AND METHOD UTILIZED THEREIN : No. 6074-1 U1



THIRD PRELIMINARY AMENDMENT - C 46-94

Prior to examination of the above-identified application,
please enter the following preliminary amendment:

In the Claims:

Please add new claims 101-106 as follows:

--101. The method of claim 100 wherein the predetermined
key is stored in the partially executable computer program prior to
possession of said program by the second party, further comprising the
steps of:

comparing the decoded coded key with the
previously stored predetermined key; and
unlocking the locked subset of the computer
program in accordance with the results of said comparison step.

102. The method of claim 101 further comprising the steps
of:

revising the predetermined key stored within said
program each time said program is executed;

revising the coded predetermined key each time said program is executed;

storing the revised predetermined key at a location within said executed program; and

storing the revised coded key at a location external to said executed program, so that execution of said executed program renders a copy of said program not fully executable due to the revision of said coded key and said predetermined key.

103. The method of claim 102 further comprising the step of storing more than one coded predetermined key at a location external to said program, wherein each coded predetermined key is associated with a particular copy of said program, said particular copy containing a corresponding predetermined key at a location in said particular program copy, so that more than one copy of said program is executable.

104. The method of claim 102 wherein the revised predetermined key is stored at a hidden location within said program, said hidden location being accessible by a secret predetermined address.

105. The method of claim 102 wherein said revised predetermined key is stored at said location external to said executed program and said revised coded key is stored at said location within said executed program.

106. The method of claim 100 wherein the computer program regenerates the predetermined key from the coded key using the information associated with the second party, and the predetermined key is stored in the partially executable computer program prior to

~~1/2~~
possession of said program by the second party, further comprising the steps of:

comparing the regenerated predetermined key with the previously stored predetermined key; and

unlocking the locked subset of the computer program in accordance with the results of said comparison step.--

REMARKS

After the foregoing amendment, claims 7-17, 19-35, 46-59, and 63-106 are active in the present application. New claims 101-106 are presented and are adequately supported in the specification. No new matter has been added.

New claims 101-106 are supported in the specification at Fig. 16 and the corresponding text.

Consideration and allowance of this application, including new claims 101-106 is respectfully requested.

Respectfully submitted,

LEON STAMBLER

Feb 8, 1994
(Date)

By:

Leslie L. Kasten, Jr.
LESLIE L. KASTEN, JR.
Registration No. 28,959
PANITCH SCHWARZE JACOBS & NADEL
1601 Market Street - 36th Floor
Philadelphia, PA 19103
Telephone: (215) 567-2020

LLK/CEB:djw
Enclosure



UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office

Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

SERIAL NUMBER	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
---------------	-------------	----------------------	---------------------

08/122,071 09/14/93 STAMBLER

L. 60741U1

EXAMINER
CANGIALOSI, S

ART UNIT PAPER NUMBER

2202

DATE MAILED: 05/31/94

This is a communication from the examiner in charge of your application.
COMMISSIONER OF PATENTS AND TRADEMARKS

☒ This application has been examined ☐ Responsive to communication filed on _____ ☐ This action is made final.

A shortened statutory period for response to this action is set to expire 3 month(s), _____ days from the date of this letter.
Failure to respond within the period for response will cause the application to become abandoned. 35 U.S.C. 133

Part I THE FOLLOWING ATTACHMENT(S) ARE PART OF THIS ACTION:

- | | |
|---|---|
| 1. <input checked="" type="checkbox"/> Notice of References Cited by Examiner, PTO-892. | 2. <input type="checkbox"/> Notice of Draftsman's Patent Drawing Review, PTO-948. |
| 3. <input checked="" type="checkbox"/> Notice of Art Cited by Applicant, PTO-1449. | 4. <input type="checkbox"/> Notice of Informal Patent Application, PTO-152. |
| 5. <input type="checkbox"/> Information on How to Effect Drawing Changes, PTO-1474. | 6. <input type="checkbox"/> _____ |

Part II SUMMARY OF ACTION

1. ☒ Claims 7-17, 19-35, 46-50, 56-59, 63-106 are pending in the application.
Of the above, claims _____ are withdrawn from consideration.
2. ☐ Claims _____ have been cancelled.
3. ☐ Claims _____ are allowed.
4. ☒ Claims 7-17, 19-35, 46-50, 56-59, 63-106 are rejected.
5. ☐ Claims _____ are objected to.
6. ☐ Claims _____ are subject to restriction or election requirement.
7. ☒ This application has been filed with informal drawings under 37 C.F.R. 1.85 which are acceptable for examination purposes.
8. ☐ Formal drawings are required in response to this Office action.
9. ☐ The corrected or substitute drawings have been received on _____. Under 37 C.F.R. 1.84 these drawings are ☐ acceptable; ☐ not acceptable (see explanation or Notice of Draftsman's Patent Drawing Review, PTO-948).
10. ☐ The proposed additional or substitute sheet(s) of drawings, filed on _____, has (have) been ☐ approved by the examiner; ☐ disapproved by the examiner (see explanation).
11. ☐ The proposed drawing correction, filed _____, has been ☐ approved; ☐ disapproved (see explanation).
12. ☐ Acknowledgement is made of the claim for priority under 35 U.S.C. 119. The certified copy has ☐ been received ☐ not been received ☐ been filed in parent application, serial no. _____; filed on _____.
13. ☐ Since this application appears to be in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under Ex parte Quayle, 1935 C.D. 11; 453 O.G. 213.
14. ☐ Other

EXAMINER'S ACTION

PTOL-326 (Rev. 2/83)

08/120,071
Art Unit 222


- 2 -

Claims 7-17,19-35,46-50,56-59,63-106 are rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Taken as a whole the claims recite an undue multiplicity of claims by virtue of the unreasonable number of claims presented would tend to obfuscate and confuse the claimed invention. Because the examiner believes in his judgement that twenty-five claims are sufficient to properly define applicants' invention, applicants are required to select certain claims, not to exceed twenty-five for examination on the merits< See M.P.E.P. 706.03(I).

It is further noted that it would appear that a multiplicity of inventions are also be involved and the the applicants are requested to group their selection accordingly to read on a single invention. The applicants should group the claims according to distinct inventions which may be restricted in a subsequent action.

Any inquiry concerning this communication should be directed to Salvatore Cangialosi at telephone number (703) 308-0482.


SALVATORE CANGIALOSI
PRIMARY EXAMINER
ART UNIT 222

TO SEPARATE, HOLD TOP AND BOTTOM EDGES, SNAP-APART AND DISCARD CARBON

FORM PTO-892 (REV. 2-92)		U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE		SERIAL NO. <i>122,071</i>		GROUP/ART UNIT <i>220</i>		ATTACHMENT TO PAPER NUMBER <i>7</i>						
NOTICE OF REFERENCES CITED				APPLICANT(S) <i>Stamblor</i>										
U.S. PATENT DOCUMENTS														
*		DOCUMENT NO.						DATE	NAME	CLASS	SUB-CLASS	FILING DATE IF APPROPRIATE		
	A	<i>5</i>	<i>2</i>	<i>6</i>	<i>7</i>	<i>3</i>	<i>1</i>	<i>4</i>	<i>11/30/93</i>	<i>Stamblor</i>	<i>380</i>	<i>25</i>		
	B													
	C													
	D													
	E													
	F													
	G													
	H													
	I													
	J													
	K													
FOREIGN PATENT DOCUMENTS														
*		DOCUMENT NO.						DATE	COUNTRY	NAME	CLASS	SUB-CLASS	PERTINENT SHTS. DWG.	PP. SPEC.
	L													
	M													
	N													
	O													
	P													
	Q													
OTHER REFERENCES (Including Author, Title, Date, Pertinent Pages, Etc.)														
	R													
	S													
	T													
	U													
EXAMINER <i>S. Congirolasi</i>								DATE <i>5/94</i>						
* A copy of this reference is not being furnished with this office action. (See Manual of Patent Examining Procedure, section 707.05 (a).)														

8122071

NOTICE OF DRAFTSPERSON'S PATENT DRAWING REVIEW

PTO Draftpersons review all originally filed drawings regardless of whether they are designated as formal or informal. Additionally, patent Examiners will review the drawings for compliance with the regulations. Direct telephone inquiries concerning this review to the Drawing Review Branch, 703-305-8404.

The drawings filed (insert date) 9/14/93, are
 A. ☒ not objected to by the Draftsperson under 37 CFR 1.84 or 1.152.
 B. ☒ objected to by the Draftsperson under 37 CFR 1.84 or 1.152 as indicated below. The Examiner will require submission of new, corrected drawings when necessary. Corrected drawings must be submitted according to the instructions on the back of this Notice.

1. DRAWINGS. 37 CFR 1.84(a): Acceptable categories of drawings:

Black ink. Color.

☐ Not black solid lines. Fig(s) _____☐ Color drawings are not acceptable until petition is granted.

2. PHOTOGRAPHS. 37 CFR 1.84(b)

☐ Photographs are not acceptable until petition is granted.

3. GRAPHIC FORMS. 37 CFR 1.84 (d)

☐ Chemical or mathematical formula not labeled as separate figure. Fig(s) _____☐ Group of waveforms not presented as a single figure, using common vertical axis with time extending along horizontal axis. Fig(s) _____☐ Individuals waveform not identified with a separate letter designation adjacent to the vertical axis. Fig(s) _____

4. TYPE OF PAPER. 37 CFR 1.84(e)

☐ Paper not flexible, strong, white, smooth, nonshiny, and durable. Sheet(s) _____☐ Erasures, alterations, overwritings, interlineations, cracks, creases, and folds not allowed. Sheet(s) _____

5. SIZE OF PAPER. 37 CFR 1.84(f): Acceptable paper sizes:

21.6 cm. by 35.6 cm. (8 1/2 by 14 inches)

21.6 cm. by 33.1 cm. (8 1/2 by 13 inches)

21.6 cm. by 27.9 cm. (8 1/2 by 11 inches)

21.0 cm. by 29.7 cm. (DIN size A4)

☐ All drawing sheets not the same size. Sheet(s) _____☐ Drawing sheet not an acceptable size. Sheet(s) _____

6. MARGINS. 37 CFR 1.84(g): Acceptable margins:

Paper size

21.6 cm. X 35.6 cm. (8 1/2 X 14 inches)	21.6 cm. X 33.1 cm. (8 1/2 X 13 inches)	21 cm. X 27.9 cm. (8 1/2 X 11 inches)	21 cm. X 29.7 cm. (DIN Size A4)
T 5.1 cm. (2")	2.5 cm. (1")	2.5 cm. (1")	2.5 cm.
L .64 cm. (1/4")	.64 cm. (1/4")	.64 cm. (1/4")	2.5 cm.
R .64 cm. (1/4")	.64 cm. (1/4")	.64 cm. (1/4")	1.5 cm.
B .64 cm. (1/4")	.64 cm. (1/4")	.64 cm. (1/4")	1.0 cm.

Margins do not conform to chart above.

Sheet(s) _____

☐ Top (T) ☐ Left (L) ☐ Right (R) ☐ Bottom (B)

7. VIEWS. 37 CFR 1.84(h)

REMINDER: Specification may require revision to correspond to drawing changes.

☐ All views not grouped together. Fig(s) _____☐ Views connected by projection lines. Fig(s) _____☐ Views contain center lines. Fig(s) _____

Partial views. 37 CFR 1.84(h)(2)

☐ Separate sheets not linked edge to edge.

Fig(s) _____

☐ View and enlarged view not labeled separately.

Fig(s) _____

☐ Long view relationship between different parts not clear and unambiguous. 37 CFR 1.84(h)(2)(ii)

Fig(s) _____

Sectional views. 37 CFR 1.84(h)(3)

☐ Hatching not indicated for sectional portions of an object.

Fig(s) _____

☐ Hatching of regularly spaced oblique parallel lines not spaced sufficiently. Fig(s) _____☐ Hatching not at substantial angle to surrounding axes or principal lines. Fig(s) _____☐ Cross section not drawn same as view with parts in cross section with regularly spaced parallel oblique strokes.

Fig(s) _____

☐ Hatching of juxtaposed different elements not angled in a different way. Fig(s) _____

Alternate position. 37 CFR 1.84(h)(4)

☐ A separate view required for alternate position.

Fig(s) _____

Modified forms. 37 CFR 1.84(h)(5)

☐ Modified forms of construction must be shown in separate views. Fig(s) _____

8. ARRANGEMENT OF VIEWS. 37 CFR 1.84(i)

☐ View placed upon another view or within outline of another. Fig(s) _____☒ Words do not appear in a horizontal, left-to-right fashion when page is either upright or turned so that the top becomes the right side, except for graphs. Fig(s) 150

9. SCALE. 37 CFR 1.84(k)

☐ Scale not large enough to show mechanism without crowding when drawing is reduced in size to two-thirds in reproduction.

Fig(s) _____

☐ Indication such as "actual size" or "scale 1/2" not permitted.

Fig(s) _____

☐ Elements of same view not in proportion to each other.

Fig(s) _____

10. CHARACTER OF LINES, NUMBERS, & LETTERS. 37 CFR 1.84(l)

☐ Lines, numbers & letters not uniformly thick and well defined, clean, durable, and black (except for color drawings).

Fig(s) _____

11. SHADING. 37 CFR 1.84(m)

☐ Shading used for other than shape of spherical, cylindrical, and conical elements of an object, or for flat parts.

Fig(s) _____

☐ Solid black shading areas not permitted. Fig(s) _____

12. NUMBERS, LETTERS, & REFERENCE CHARACTERS. 37 CFR 1.84(p)

☐ Numbers and reference characters not plain and legible. 37 CFR 1.84(p)(1) Fig(s) _____☐ Numbers and reference characters used in conjunction with brackets, inverted commas, or enclosed within outlines. 37 CFR 1.84(p)(1) Fig(s) _____☐ Numbers and reference characters not oriented in same direction as the view. 37 CFR 1.84(p)(1) Fig(s) _____☐ English alphabet not used. 37 CFR 1.84(p)(2)

Fig(s) _____

☐ Numbers, letters, and reference characters do not measure at least .32 cm. (1/8 inch) in height. 37 CFR(p)(3)

Fig(s) _____

13. LEAD LINES. 37 CFR 1.84(q)

☐ Lead lines cross each other. Fig(s) _____☐ Lead lines missing. Fig(s) _____☐ Lead lines not as short as possible. Fig(s) _____

14. NUMBERING OF SHEETS OF DRAWINGS. 37 CFR 1.84(t)

☐ Number appears in top margin. Fig(s) _____☐ Number not larger than reference characters.

Fig(s) _____

☐ Sheets not numbered consecutively, and in Arabic numerals, beginning with number 1. Sheet(s) _____

15. NUMBER OF VIEWS. 37 CFR 1.84(u)

☐ Views not numbered consecutively, and in Arabic numerals, beginning with number 1. Fig(s) _____☐ View numbers not preceded by the abbreviation Fig.

Fig(s) _____

☐ Single view contains a view number and the abbreviation Fig.☐ Numbers not larger than reference characters.

Fig(s) _____

16. CORRECTIONS. 37 CFR 1.84(w)

☐ Corrections not durable and permanent. Fig(s) _____

17. DESIGN DRAWING. 37 CFR 1.152

☐ Surface shading shown not appropriate. Fig(s) _____☐ Solid black shading not used for color contrast.

Fig(s) _____

ATTACHMENT TO PAPER NO. Fig 11, 13 B, 134, 134, 134, 134DATE 10/22/93



HEREBY CERTIFY THAT THIS CORRESPONDENCE
IS BEING DEPOSITED WITH THE UNITED STATES
POSTAL SERVICE AS FIRST CLASS MAIL IN AN
ENVELOPE ADDRESSED TO: COMMISSIONER OF
PATENTS AND TRADEMARKS, WASHINGTON, D.C.
20231, ON THE DATE INDICATED BELOW.

BY: [Signature]
DATE: July 22, 1994

EP2202
#1/Depos
RECEIVED
JUL 29 1994
GROUP 2200
8/2/94

PATENT
Box Non-Fee Amendment

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re:	Patent Application of	: Group Art Unit 2202
	Leon Stambler	:
		:
Serial No.:	08/122,071	: Examiner: S.
		: Cangialosi
Filed:	September 14, 1993	:
		:
For:	SECURE TRANSACTION SYSTEM	: Attorney Docket
	AND METHOD UTILIZED THEREIN	: No. 6074-1 U1

RESPONSE

The following election and remarks are submitted in response to the Office Action mailed May 31, 1994 (Paper No. 7) in connection with the above-identified application, and are being submitted within the three-month shortened statutory period for a response.

Applicant selects, without prejudice, to prosecute claims 7-17, 19, 33-35, 46-50, 56, 59, 64 and 79 and to withdraw from consideration claims 20-32, 57, 58, 63, 65-78 and 80-106 subject to the filing of a divisional application.

REMARKS

Claims 7-17, 19, 33-35, 46-50, 56, 59, 64 and 79 are pending in the application. Claims 20-32, 57, 58, 63, 65-78 and 80-106 have been withdrawn.

Claims 7-17, 19-35, 46-50, 56-59 and 63-106 were rejected under 35 U.S.C. § 112, second paragraph for indefiniteness. The Office Action alleges that as a whole the claims recite an undue multiplicity of claims. Applicant respectively traverses the rejection.

Claims 20-32, 57-58, 63, 65-78 and 86-106 have been withdrawn, leaving claims 7-17, 19, 33-35, 46-50, 56, 59, 63 and 79 pending. As requested by the Examiner, Applicant has grouped and selected less than 25 claims for examination on the merits. The pending claims are all directed to a transaction system and a method for authenticating a transaction using a variable authentication number.

The Office Action further alleges that a multiplicity of inventions appear to be involved. The Examiner has requested the claims be grouped according to distinct inventions. Applicant proposes the following groupings:

<u>Group I</u>	claims 7-17, 19, 33-35, 46-50, 56, 59, 64, 79	Class 380/24 Transaction system and method of authenticating a transaction using a variable authentication number;
<u>Group II</u>	claims 20-27, 63, 75-78	Class 340/825.34 Authentication system;
<u>Group III</u>	claims 28-32, 57-58, 81-84	Class 340/825.31 Method and apparatus of enrolling;
<u>Group IV</u>	claims 65-73	Class 340/825.15 Method and apparatus of enrolling with storage means;
<u>Group V</u>	claims 85-93	Class 380/23 Method and apparatus for enrolling with user authentication;

- 2 -

Group VI claims 94-106

Class 38/45

Method and apparatus for enrolling
with multiple keys.

Applicant respectfully asserts that all of claims 7-17,
19, 33-35, 46-50, 56, 59, 64 and 79 are directed to a single
invention and that all of the claims are presently in condition
for allowance.

In view of the foregoing remarks, the present
application including claims 7-17, 19, 33-35, 46-50, 56, 59, 64
and 79 is in condition for allowance and such action is
respectfully requested.

Respectfully submitted,

LEON STAMBLER

July 22, 1994
(Date)

By: 

LESLIE L. KASTEN, JR.

Registration No. 28,959

PANITCH SCHWARZE JACOBS & NADEL, P.C.

1601 Market Street - 36th Floor

Philadelphia, PA 19103

Telephone: (215) 567-2020

Facsimile: (215) 567-2991

LLK/CEB:ac-djw



UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office

Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

SERIAL NUMBER	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
---------------	-------------	----------------------	---------------------

08/122,071 09/14/93 STAMBLER

L 60741U1

CANGIAL EXAMINER

22M2/1019

PANITCH SCHWARZE JACOBS & NADEL
1601 MARKET STREET - 36TH FLOOR
PHILADELPHIA, PA 19103

ART UNIT PAPER NUMBER

2202

DATE MAILED: 10/19/94

This is a communication from the examiner in charge of your application.
COMMISSIONER OF PATENTS AND TRADEMARKS

☐ This application has been examined ☒ Responsive to communication filed on 7/27/94 ☐ This action is made final.

A shortened statutory period for response to this action is set to expire 3 month(s), _____ days from the date of this letter.
Failure to respond within the period for response will cause the application to become abandoned. 35 U.S.C. 133

Part I THE FOLLOWING ATTACHMENT(S) ARE PART OF THIS ACTION:

- ☒ Notice of References Cited by Examiner, PTO-892.
- ☒ Notice of Draftsman's Patent Drawing Review, PTO-948.
- ☐ Notice of Art Cited by Applicant, PTO-1449.
- ☐ Notice of Informal Patent Application, PTO-152.
- ☐ Information on How to Effect Drawing Changes, PTO-1474.
- ☐

Part II SUMMARY OF ACTION

1. ☒ Claims 7-17, 19-35, 46-50, 56-59, 63, 106 are pending in the application.
Of the above, claims 20-32, 57, 58, 63, 65-78 and 90-106 are withdrawn from consideration.

2. ☐ Claims _____ have been cancelled.
3. ☐ Claims _____ are allowed.
4. ☒ Claims 7-17, 19, 33-35, 46-50, 56, 59, 64 and 79 are rejected.
5. ☐ Claims _____ are objected to.
6. ☐ Claims _____ are subject to restriction or election requirement.
7. ☐ This application has been filed with informal drawings under 37 C.F.R. 1.85 which are acceptable for examination purposes.
8. ☐ Formal drawings are required in response to this Office action.
9. ☐ The corrected or substitute drawings have been received on _____. Under 37 C.F.R. 1.84 these drawings are ☐ acceptable; ☐ not acceptable (see explanation or Notice of Draftsman's Patent Drawing Review, PTO-948).
10. ☐ The proposed additional or substitute sheet(s) of drawings, filed on _____, has (have) been ☐ approved by the examiner; ☐ disapproved by the examiner (see explanation).
11. ☐ The proposed drawing correction, filed _____, has been ☐ approved; ☐ disapproved (see explanation).
12. ☐ Acknowledgement is made of the claim for priority under 35 U.S.C. 119. The certified copy has ☐ been received ☐ not been received ☐ been filed in parent application, serial no. _____; filed on _____.
13. ☐ Since this application appears to be in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under Ex parte Quayle, 1935 C.D. 11; 453 O.G. 213.
14. ☐ Other

EXAMINER'S ACTION

PTOL-326 (Rev. 2/93)

Serial Number: 08/122,071

-2-

Art Unit: 2202

1. 35 U.S.C. § 101 reads as follows:

"Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter or any new and useful improvement thereof, may obtain a patent therefore, subject to the conditions and requirements of this title".

Claims 7-17, 19, 33-35, 46-50, 56, 59, 64, and 79 are rejected under 35 U.S.C. § 101 because the invention as claimed is directed to non-statutory subject matter.

The claims appear to be directed to the mental processes required for the use of a transaction variable. No automatic electronic signal selections are required and hence, the claims appear to be directed at the actions of individual human intervention with fund transfers and not the statutory classes of invention.

At issue is whether the claim recite an algorithm, as an abstract concept, for which patent protection is sought. The principles controlling this issue are believed to be stated in the following case law decisions, i.e. Gottschalk v. Benson, 409 U.S. 63, 175 USPQ 673 (1972); Parker v. Flook, 437 U.S. 584, 198 USPQ 193 (1978); Diamond v. Diehr, 450 U.S. 175, 209 USPQ 1 (1981); In re Freeman, 573 F.2d 1237, 197 USPQ 464 (CCPA 1978); In re Walter, 618 F.2d 758, 205 USPQ 397 (CCPA 1980); In re Abele, 214 F.2d 684, 214 USPQ 682 (CCPA 1982).

An "algorithm", in the legal sense, is limited to a procedure for solving a given mathematical problem, Diehr,

Serial Number: 08/122,071

-3-

Art Unit: 2202

Benson, supra. While a claim drawn to subject matter otherwise statutory does not become nonstatutory simply because it uses an algorithm, an algorithm does not suddenly become patentable subject matter simply by having applicant acquiesce to limiting the reach of the patent for the algorithm to particular technical use, Diehr, supra. If a mathematical algorithm is merely presented and solved by the claimed invention and is not applied in any manner to physical elements or process steps it is not saved by the preamble merely reciting a field of use of the algorithm, In re Walter, supra. If the end product of the invention is a pure number, the invention is nonstatutory regardless of any post-solution activity that makes it available for use by person or machine for other purposes, Flook, supra.

The determination of the issue is made by the application of the two-step analysis of In re Freeman, supra, as further interpreted by In re Walter, and In re Abele, supra. The claims use prose to express a mathematical formula for creating a variable. The result of this mathematical manipulation are sets of pure numbers describing that process, therefore meeting the definition of an algorithm in the Benson sense.

In the second step of the analysis, the claims are reviewed to determine whether the claims implement the algorithm in a specific manner to define structural relationships between the elements of the claims. They do not, therefore an algorithm is

Serial Number: 08/122,071

-4-

Art Unit: 2202

recited in a manner that is preempted by Freeman, Walter, and Abele.

2. The following is a quotation of 35 U.S.C. § 103 which forms the basis for all obviousness rejections set forth in this Office action:

A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Subject matter developed by another person, which qualifies as prior art only under subsection (f) or (g) of section 102 of this title, shall not preclude patentability under this section where the subject matter and the claimed invention were, at the time the invention was made, owned by the same person or subject to an obligation of assignment to the same person.

9/12
11/94
3. Claims ~~1-53~~ ^{7, 19, 33-35, 46-50, 56, 58, 64 and 79} are rejected under 35 U.S.C. § 103 as being unpatentable over Brachtl et al (Newly cited).

Brachtl et al (See Col. 5, lines 25-35 and claim 1) discloses a transaction security system using time variant authentication parameters including a transaction variable for each transaction substantially as claimed. The differences between the above and the claimed invention is the use of explicit terms "variable authentication number". It is believed that the transaction variable for each transaction is the functional equivalent of "variable authentication number". It would have been obvious to the person having ordinary skill in this art to provide a similar


Serial Number: 08/122,071

-5-

Art Unit: 2202

arrangement for Bracht1 et al because it is conventional and standard practice to employ a transaction variable for the authentication of each transaction. The deficiencies of the art with respect to the dependent claims if any deal with the conventional authentication schemes.

4.Any inquiry concerning this communication should be directed to Salvatore Cangialosi at telephone number (703) 308-0482.


SALVATORE CANGIALOSI
PRIMARY EXAMINER
ART UNIT 222

TO SEPARATE, HOLD TOP AND BOTTOM EDGES, SNAP-APART AND DISCARD CARBON

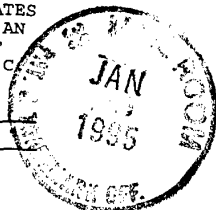
FORM PTO-892 (REV. 2-92)		U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE		SERIAL NO. <i>122,071</i>		GROUP ART UNIT <i>2202</i>		ATTACHMENT TO PAPER NUMBER <i>9</i>						
NOTICE OF REFERENCES CITED				APPLICANT(S) <i>Stumbler</i>										
U.S. PATENT DOCUMENTS														
*		DOCUMENT NO.						DATE	NAME	CLASS	SUB-CLASS	FILING DATE IF APPROPRIATE		
	A	<i>4747050</i>						<i>5/24/88</i>	<i>Bracht et al</i>	<i>380</i>	<i>24</i>			
	B													
	C													
	D													
	E													
	F													
	G													
	H													
	I													
	J													
	K													
FOREIGN PATENT DOCUMENTS														
*		DOCUMENT NO.						DATE	COUNTRY	NAME	CLASS	SUB-CLASS	PERTINENT SHTS. DWG.	PP. SPEC.
	L													
	M													
	N													
	O													
	P													
	Q													
OTHER REFERENCES (Including Author, Title, Date, Pertinent Pages, Etc.)														
	R													
	S													
	T													
	U													
EXAMINER <i>S. Campionosi</i>								DATE <i>10/94</i>						
• A copy of this reference is not being furnished with this office action. (See Manual of Patent Examining Procedure, section 707.05 (a).)														

I HEREBY CERTIFY THAT 1. CORRESPONDENCE
IS BEING DEPOSITED WITH THE UNITED STATES
POSTAL SERVICE AS FIRST CLASS MAIL IN AN
ENVELOPE ADDRESSED TO: COMMISSIONER OF
PATENTS AND TRADEMARKS, WASHINGTON, D.C.
20231, ON THE DATE INDICATED BELOW.

BY

DATE

Donna T. Watt
1/13/95



10
Prior Art
w/att.

PATENT

Coper

1-31-95

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Patent Application of : Group Art Unit 2202
Leon Stambler :
Serial No.: 08/122,071 : Examiner: S.
Filed: September 14, 1993 : Cangialosi
For: SECURE TRANSACTION : Attorney Docket
SYSTEM AND METHOD : No. 6074-1U1
UTILIZED THEREIN

Supplemental INFORMATION DISCLOSURE STATEMENT

It is requested that the enclosed reference(s) listed on the attached Information Disclosure Citation Form PTO-1449 be considered by the Patent Examiner in connection with the above-identified application and be made of record therein.

Certification Under 37 C.F.R. § 1.97(e)(2)

I hereby certify that the enclosed reference(s) were not cited in a communication from a foreign Patent Office concerning a counterpart foreign application or known to any individual designated in § 1.56(c) more than three months prior to the filing of this Statement.

Independent consideration and acknowledgment of the enclosed reference(s) are respectfully requested.

Respectfully submitted,

LEON STAMBLER

By:

Leslie L. Kasten, Jr.
LESLIE L. KASTEN, JR.
Registration No., 28,959
PANITCH SCHWARZE JACOBS & NADEL, P.C.
1601 Market Street, 36th Floor
Philadelphia, PA 19103
Telephone: (215) 567-2020
Facsimile: (215) 567-2991

LLK/CEB/cqz

Jan 13, 95
(Date)



I HEREBY CERTIFY THAT THIS CORRESPONDENCE IS BEING DEPOSITED WITH THE UNITED STATES POSTAL SERVICE AS FIRST CLASS MAIL IN AN ENVELOPE ADDRESSED TO: COMMISSIONER OF PATENTS AND TRADEMARKS, WASHINGTON, D.C. 20231, ON THE DATE INDICATED BELOW.

BY: Donna T. Work
DATE: 1/13/95

loc 11
22 MI
Argu
Coper
1-31-95

PATENT
Box Non-Fee Amendment

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re: Patent Application of : Group Art Unit: 2202 ✓
Leon Stambler :
Serial No.: 08/122,071 : Examiner: S. Cangialos
Filed: September 14, 1993 :
For: SECURE TRANSACTION SYSTEM : Attorney Docket
AND METHOD UTILIZED THEREIN : No. 6074-1 ✓

RECEIVED
JAN 30 1995
GROUP 2200

AMENDMENT

The following remarks are submitted in response to the Office Action mailed October 19, 1994 (Paper No. 6) in connection with the above-identified application, and are being submitted within the three-month shortened statutory period for a response.

REMARKS

Claims 7-17, 19, 33-35, 46-50, 56, 59, 64 and 79 are pending in the application.

Claims 7-17, 19, 33-35, 46-50, 56, 59, 64 and 79 were rejected under 35 U.S.C. § 101, as being directed nonstatutory to subject matter. The Office Action alleges that the claims appear to be directed toward the mental processes required for the use of a transaction variable and that no automatic electronic signal selections are required, and therefore, under the Freeman-Walter-Abele test, the claims fall within a judicially created exception

to the classes of statutory subject matter defined in § 101.

Applicant respectfully traverses the rejection.

The present invention is directed to a secure transaction system for authenticating documents, such as stock certificates, bonds, checks and medical prescriptions, as well as the individuals or parties who are involved with the transaction. The present invention is particularly suited to verifying the identity and securing the interests of all parties to multi-party transactions, including and especially absent parties to a transaction.

The claims recite the steps required to properly authenticate a party to a transaction. In addition, the steps recited are performed using specific devices, such as coders and uncoders, and linkers, mixers and sorters, as described on page 6, lines 1-4 and 15-30, respectively, of the specification. The steps recited in the claims are not mere mental processes or merely an algorithm, but are separate and discrete steps. In addition, the steps are applied to real world processes, such as originating an instrument (claims 10-11), processing medical prescriptions for dispensing medicine (claims 14-16 and 79), automatically transferring funds (claims 46-47), and processing invoices (claims 48-50).

For instance, claim 10 recites that the transaction includes "originating an instrument" and "recording the VAN and at least a portion of the information relevant to the transaction on the instrument"; claim 14 recites that the transaction

comprises "originating and processing a medical prescription form and a patient presenting the medical prescription form" and includes the step of "recording the VAN on the medical prescription form"; claim 15 recites the steps of "authenticating the patient" and "dispensing medicine" if the VAN and the patient are authenticated. These steps, recited in the body of the claims, respectively, are an integral part of the claims and are not mere post-solution activity.

The Patent Act defines patentable subject matter as:

...any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof...

35 U.S.C. § 101. The courts have interpreted this portion of the statute to mean that "anything under the sun that is made by man" constitutes patentable subject matter. Diamond v. Chakrabarty, 447 U.S. 303, 309 (1980). As noted by the Examiner, the courts have also created certain categories of subject matter not entitled to patent protection, namely, "laws of nature, natural phenomena, and abstract ideas". Diamond v. Diehr, 450 U.S. 175, 185 (1981). In Diehr, the Supreme Court held that certain mathematical subject matter is not, standing alone, entitled to patent protection, Id., at 186. However, the Court also stated that a "claim drawn to subject matter otherwise statutory does not become nonstatutory simply because it uses a mathematical formula". Id., at 187. Moreover, "whether the invention is called a machine or a process is inconsequential". In re Alappat, 31 U.S.P.Q.2d 1545, 1590 (Fed. Cir. 1994) (Rader, J.

concurring). Thus, a process or method claim drawn to statutory subject matter which recites an algorithm is not nonstatutory because it recites a mathematical algorithm. Rather, the claim as a whole is analyzed to determine whether the claimed subject matter as a whole is a disembodied mathematical concept. The ultimate issue has always been whether the claim as a whole is drawn to statutory subject matter. Id., at 1557.

As previously stated, the claims at issue are directed to real world processes and include separate and distinct steps for verifying and authenticating parties to and instruments in a transaction. Applicant respectfully asserts that the claims as a whole are not merely directed to mental steps or a mathematical algorithm, but are drawn to statutory subject matter. Accordingly, Applicant respectfully requests that the rejection of claims 7-17, 19, 33-35, 46-50, 56, 59, 64 and 79 under § 101 be withdrawn.

Claims 7-17, 19, 33-35, 46-50, 56, 59, 64 and 79 were rejected under 35 U.S.C. § 103, as being unpatentable over U.S. Patent No. 4,747,050 (Bracht1 et al.). The Office Action states that Bracht1 et al. disclose a transaction security system using time variant authentication parameters including a transaction variable for each transaction, and that the difference over Bracht1 et al. and the claims is semantic, i.e. the transaction variable of Bracht1 et al. is functionally equivalent to a "variable authentication number." Applicant respectfully traverses the rejection.

Bracht1 et al. is directed to a transaction security system using time variant parameters (T_{card} , T_{term} , T_{iss} , TAP1, TAP2, etc.) and time invariant parameters (KP, PAN, etc.) to generate session keys (KS). Each user of the system has an intelligent bank card on which is stored a personal account number (PAN) and a personal key (KP). The parameters T_{card} , T_{term} , and T_{iss} are generated by the user's card, an electronic funds terminal (EFT) and the card/PIN issuer's data processing center (IDPC) or bank, respectively. The user's PAN and the user's KP are stored in a read only store (ROS) in the user's card by the issuer at the time that the card and PIN are issued to the user (col. 7, lines 7-17). As long as the user continues to use the same card that was issued, the PAN and KP remain the same, i.e. time invariant, since they are accessible from the ROS.

A message authentication code (MAC) is attached to each transaction message sent and authenticates the transaction data in a received message (col. 4, lines 67-68). A MAC is generated by enciphering the message transaction data with a generated session key (KS) (col. 5, lines 1-2). In addition, apart and separate from message authentication using the MAC, Bracht1, et al. generates a transaction authentication parameter (TAP2) to validate the users' PIN.

A user originates a transaction by inserting his card into a terminal. The terminal obtains information from the card, generates a MAC and attaches the MAC to a transaction message request (M_{req}) which is sent to the IDPC. The M_{req} is

authenticated by regenerating the MAC and comparing the regenerated MAC to the MAC in the received M_{req} . If M_{req} is authentic, TAP2 is generated by the IDPC, and a response message is formed (M_{resp}) which includes TAP2 and another MAC, and sent from the IDPC to the terminal and card (col. 17, lines 18-19). The time invariant parameters (PIN, PAN and KP) or an authentication parameter (AP) is used in conjunction with the time variant parameters (T_{card} and T_{term}) to generate a first transaction authentication parameter (TAP1) (see col. 6, lines 32-33 and col. 13, lines 43-66). Note, AP is pregenerated at the IDPC using the PIN, PAN and KP. The AP is then prestored at a PAN index at the time that the PIN and card are issued (col. 13, lines 62-64 and col. 7, lines 31-33). The second transaction authentication parameter (TAP2) is generated from TAP1 and the time variant parameters T_{card} , T_{term} and T_{iss} .

Applicant respectfully asserts that the transaction variable for each transaction is not the functional equivalent of the VAN of the present invention. With reference to claims 7 and 64, a VAN is generated by coding the transaction information with information associated with at least one party (or a first party), the information comprising coded authentication information derivable from a predetermined secret code and a predetermined nonsecret code. The coded authentication information was previously generated by coding a personal identification number (PIN). Brachtel et al. generate a MAC by

coding the transaction message data with information associated with at least one party, for example, Bracht1 et al.'s user (or transaction originator) (col. 5, lines 29-31). The information associated with the user to generate session keys, which are used to code transaction message data to generate MACs, comprises user card information and the users' PIN. The card information used to generate the session keys includes the users' PAN, KP and T_{card} (see Bracht1 et al., Fig. 6). Each of these parameters is secret. KP and T_{card} are not released or exposed in clear form or enciphered form beyond the card terminal boundary. The PAN is enciphered before it is released from the card/terminal boundary or from the IDPC boundary into the public communications network. Bracht1 et al. do not disclose or teach the use of a user-associated predetermined nonsecret number which is used to generate the session key and the MAC. In contrast, in claims 7 and 64, the VAN is generated using a predetermined nonsecret number associated with the user.

In addition, Bracht1 et al. validate the users' PIN separately, i.e. with TAP2, but not with the MAC (col. 17, lines 18-24). In contrast, in claim 7, the party to the transaction is authenticated together with the transaction through the use of the VAN, since the party's PIN is used in generating the VAN.

Regarding claim 17 the transaction and parties to the transaction are authenticated using information relevant to the transaction, a present party, and an absent party. Bracht1 et

al. do not disclose or teach that the MAC may be generated using information associated with an absent party.

Regarding claim 33, the recipient in this claim is a payee (e.g. funds are transferred into the recipient's account). The recipient, as payee, needs to be identified and authenticated with a PIN before any funds are transferred to the recipient's account. For example, a transaction is originated by a payor who makes a payment for goods or services with a check. The payor originates the check as a payment instrument. The payor or the originator of the check, uses a PIN to identify himself when the check is being prepared. The payor's PIN is used as one of the elements to derive a joint key and a VAN. Thereafter, the VAN is associated with the check and the subsequent transaction. The subsequent transaction is when the recipient of the check, i.e. the payee, uses the instrument which was previously produced by the payor to have the funds designated on the instrument transferred from the payor's account into the recipient's account. In the present invention, the recipient inserts a PIN into a terminal to obtain a separate identification and PIN authentication, to prove to the system that he is the rightful payee into whose account funds are to be transferred. In Brachtl et al., the card user is portrayed as a transaction originator (i.e. a payor for goods and services). The Brachtl et al. card user who originates the transaction pays for the goods or services from funds transferred in his bank accounts, with the

use of his card and PIN. Bracht1 et al.'s recipient (payee) does not input a PIN to authenticate himself and have the payor's funds transferred into his account. Thus, a transaction in Bracht1 et al., may be accomplished without the recipient entering a PIN to authenticate himself and or his account prior to receiving funds from the payor's account. Thus, claim 33 is distinguished from Bracht1 et al., since the Bracht1 et al. transaction recipient does not enter a PIN as recited in claim 33.

Regarding claim 46, the VAN is generated using the PIN of the originator party together with the recipient party's account identifying information. Additionally, a redemption VAN (RVAN) is generated and associated with the transaction. Bracht1 et al. do not disclose, use or teach any of these elements.

Claim 48 is directed to an invoice processing system, where the VAN is generated using information associated with the invoice, including information identifying a payee party account and a payment amount. Bracht1 et al. do not identify a payee's account which is used in the derivation of the Bracht1 et al. MAC. In addition, the payor (the card user) and MAC are not authenticated using invoice payment information.

Claim 56 is directed to a system for authenticating a transaction and the parties to the transaction and includes a means for coding information associated with a present party and an absent party. Bracht1 et al. do not disclose, use or teach

that a MAC may be generated using information associated with an absent party.

Regarding claim 59, Bracht1 et al. do not teach, use or disclose means for determining whether a recipient party and transaction are authentic; means for authenticating redemption of the transaction if the recipient party and transaction are authentic; means to generate an RVAN; means to associate an RVAN with a transaction; and means to store an RVAN.

For the foregoing reasons, Applicant submits that claims 7-17, 19, 33-35, 46-50, 56, 59, 64 and 79 are patentable over Bracht1 et al. and respectfully requests that the rejection under § 103 be withdrawn.

Applicant has recently become aware of U.S. Patent No. 5,341,428 (Schatz) enclosed herewith and listed on the attached form PTO 1449. Schatz is directed to a multiple cross-check document verification system. In Schatz, a check derivation number is derived from the information on the check and from the recipient's (i.e. payee's) PIN. The check derivation number is printed on the check when it is prepared, in order to validate the check and the recipient, when the check is negotiated. There are essential differences between Schatz and the present invention. For instance, Schatz stores the recipient's PIN in the memory of the computer that produces the check. (In the present invention, the PIN is not stored in the system). The recipient's (payee's) PIN is then used to derive the check

derivation number, which is printed on the check. When the check is negotiated, Schatz validates the recipient's PIN twice; first, with a personal card (which stores an encrypted PIN) and then, with the check derivation number from the check. In the present invention, the originator's (i.e. payor's) PIN, is used to generate the VAN. This makes the payor (originator) responsible for generating the check. Since Schatz does not authenticate the payor's responsibility, a fraudulent check may be prepared by a person with knowledge of the encryption algorithm.


In view of the foregoing remarks, the present application including claims 7-17, 19, 33-35, 46-50, 56, 59, 64 and 79 is in condition for allowance and such action is respectfully requested.

Respectfully submitted,

LEON STAMBLER

Jan 13/1995
(Date)

By:


LESLIE L. KASTEN, JR.
Registration No. 28,959
PANITCH SCHWARZE JACOBS & NADEL, P.C.
1601 Market Street - 36th Floor
Philadelphia, PA 19103
Telephone: (215) 567-2020
Facsimile: (215) 567-2991

LLK/CEB/cqz



UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office

Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

SERIAL NUMBER	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
---------------	-------------	----------------------	---------------------

08/122,071 09/14/93 STAMBLER

L 60741U1
EXAMINER

CANGIALOSI, S

ART UNIT PAPER NUMBER

2202

DATE MAILED:

03/23/95

22M2/0323
PANITCH SCHWARZE JACOBS & NADEL
1601 MARKET STREET - 36TH FLOOR
PHILADELPHIA, PA 19103

This is a communication from the examiner in charge of your application.
COMMISSIONER OF PATENTS AND TRADEMARKS

☐ This application has been examined ☒ Responsive to communication filed on 1/20/95 ☒ This action is made final.

A shortened statutory period for response to this action is set to expire 3 month(s), _____ days from the date of this letter.
Failure to respond within the period for response will cause the application to become abandoned. 35 U.S.C. 133

Part I THE FOLLOWING ATTACHMENT(S) ARE PART OF THIS ACTION:

- | | |
|---|---|
| 1. <input type="checkbox"/> Notice of References Cited by Examiner, PTO-892. | 2. <input type="checkbox"/> Notice of Draftsman's Patent Drawing Review, PTO-948. |
| 3. <input checked="" type="checkbox"/> Notice of Art Cited by Applicant, PTO-1449. | 4. <input type="checkbox"/> Notice of Informal Patent Application, PTO-152. |
| 5. <input type="checkbox"/> Information on How to Effect Drawing Changes, PTO-1474. | 6. <input type="checkbox"/> _____ |

Part II SUMMARY OF ACTION

1. ☒ Claims 7-17, 19-35, 46-50, 56-59, 63-106 are pending in the application.
Of the above, claims 20-32, 57, 58, 63, 65-78, 80-106 are withdrawn from consideration.
2. ☐ Claims _____ have been cancelled.
3. ☐ Claims _____ are allowed.
4. ☒ Claims 7-17, 19, 33-35, 46-59, 56, 59, 64 and 79 are rejected.
5. ☐ Claims _____ are objected to.
6. ☐ Claims _____ are subject to restriction or election requirement.
7. ☐ This application has been filed with informal drawings under 37 C.F.R. 1.85 which are acceptable for examination purposes.
8. ☐ Formal drawings are required in response to this Office action.
9. ☐ The corrected or substitute drawings have been received on _____. Under 37 C.F.R. 1.84 these drawings are ☐ acceptable; ☐ not acceptable (see explanation or Notice of Draftsman's Patent Drawing Review, PTO-948).
10. ☐ The proposed additional or substitute sheet(s) of drawings, filed on _____, has (have) been ☐ approved by the examiner; ☐ disapproved by the examiner (see explanation).
11. ☐ The proposed drawing correction, filed _____, has been ☐ approved; ☐ disapproved (see explanation).
12. ☐ Acknowledgement is made of the claim for priority under 35 U.S.C. 119. The certified copy has ☐ been received ☐ not been received ☐ been filed in parent application, serial no. _____; filed on _____.
13. ☐ Since this application appears to be in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under Ex parte Quayle, 1935 C.D. 11; 453 O.G. 213.
14. ☐ Other

EXAMINER'S ACTION

PTOL-326 (Rev. 2/93)

Serial Number: 08/122,071

-2-

Art Unit: 2202

1. 35 U.S.C. § 101 reads as follows:

"Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter or any new and useful improvement thereof, may obtain a patent therefore, subject to the conditions and requirements of this title".

Claims 7-17, 19, 33-35, 46-50, 56, 59, 64, and 79 are rejected under 35 U.S.C. § 101 because the invention as claimed is directed to non-statutory subject matter.

The claims appear to be directed to the mental processes required for the use of a transaction variable. No automatic electronic signal selections are required and hence, the claims appear to be directed at the actions of individual human intervention with fund transfers and not the statutory classes of invention.

At issue is whether the claim recite an algorithm, as an abstract concept, for which patent protection is sought. The principles controlling this issue are believed to be stated in the following case law decisions, i.e. Gottschalk v. Benson, 409 U.S. 63, 175 USPQ 673 (1972); Parker v. Flook, 437 U.S. 584, 198 USPQ 193 (1978); Diamond v. Diehr, 450 U.S. 175, 209 USPQ 1 (1981); In re Freeman, 573 F.2d 1237, 197 USPQ 464 (CCPA 1978); In re Walter, 618 F.2d 758, 205 USPQ 397 (CCPA 1980); In re Abele, 214 F.2d 684, 214 USPQ 682 (CCPA 1982).

An "algorithm", in the legal sense, is limited to a procedure for solving a given mathematical problem, Diehr,

Serial Number: 08/122,071

-3-

Art Unit: 2202

Benson, supra. While a claim drawn to subject matter otherwise statutory does not become nonstatutory simply because it uses an algorithm, an algorithm does not suddenly become patentable subject matter simply by having applicant acquiesce to limiting the reach of the patent for the algorithm to particular technical use, Diehr, supra. If a mathematical algorithm is merely presented and solved by the claimed invention and is not applied in any manner to physical elements or process steps it is not saved by the preamble merely reciting a field of use of the algorithm, In re Walter, supra. If the end product of the invention is a pure number, the invention is nonstatutory regardless of any post-solution activity that makes it available for use by person or machine for other purposes, Flook, supra.

The determination of the issue is made by the application of the two-step analysis of In re Freeman, supra, as further interpreted by In re Walter, and In re Abele, supra. The claims use prose to express a mathematical formula for creating a variable. The result of this mathematical manipulation are sets of pure numbers describing that process, therefore meeting the definition of an algorithm in the Benson sense.

In the second step of the analysis, the claims are reviewed to determine whether the claims implement the algorithm in a specific manner to define structural relationships between the elements of the claims. They do not, therefore an algorithm is

Serial Number: 08/122,071

-4-

Art Unit: 2202

recited in a manner that is preempted by Freeman, Walter, and Abele.

2. The following is a quotation of 35 U.S.C. § 103 which forms the basis for all obviousness rejections set forth in this Office action:

A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Subject matter developed by another person, which qualifies as prior art only under subsection (f) or (g) of section 102 of this title, shall not preclude patentability under this section where the subject matter and the claimed invention were, at the time the invention was made, owned by the same person or subject to an obligation of assignment to the same person.

3. Claims 7-17, 19, 33-35, 46-50, 56, 59, 64, and 79 are rejected under 35 U.S.C. § 103 as being unpatentable over Bracht1 et al (Newly cited).

Bracht1 et al (See Col. 5, lines 25-35 and claim 1) discloses a transaction security system using time variant authentication parameters including a transaction variable for each transaction substantially as claimed. The differences between the above and the claimed invention is the use of explicit terms "variable authentication number". It is believed that the transaction variable for each transaction is the functional equivalent of "variable authentication number" It would have been obvious to

Serial Number: 08/122,071

-5-

Art Unit: 2202


the person having ordinary skill in this art to provide a similar arrangement for Brachtl et al because it is conventional and standard practice to employ a transaction variable for the authentication of each transaction. The deficiencies of the art with respect to the dependent claims if any deal with the conventional authentication schemes.

4. Applicant's arguments filed 1/20/95 have been fully considered but they are not deemed to be persuasive.

5.THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 C.F.R. § 1.136(a).

A SHORTENED STATUTORY PERIOD FOR RESPONSE TO THIS FINAL ACTION IS SET TO EXPIRE THREE MONTHS FROM THE DATE OF THIS ACTION. IN THE EVENT A FIRST RESPONSE IS FILED WITHIN TWO MONTHS OF THE MAILING DATE OF THIS FINAL ACTION AND THE ADVISORY ACTION IS NOT MAILED UNTIL AFTER THE END OF THE THREE-MONTH SHORTENED STATUTORY PERIOD, THEN THE SHORTENED STATUTORY PERIOD WILL EXPIRE ON THE DATE THE ADVISORY ACTION IS MAILED, AND ANY EXTENSION FEE PURSUANT TO 37 C.F.R. § 1.136(a) WILL BE CALCULATED FROM THE MAILING DATE OF THE ADVISORY ACTION. IN NO EVENT WILL THE STATUTORY PERIOD FOR RESPONSE EXPIRE LATER THAN SIX MONTHS FROM THE DATE OF THIS FINAL ACTION.

6.Any inquiry concerning this communication should be directed to Salvatore Cangialosi at telephone number (703) 308-0482.


SALVATORE CANGIALOSI
PRIMARY EXAMINER
ART UNIT 222



Corres. and Mail
BOX AF

I HEREBY CERTIFY THAT THIS CORRESPONDENCE IS BEING DEPOSITED WITH THE UNITED STATES POSTAL SERVICE AS FIRST CLASS MAIL IN AN ENVELOPE ADDRESSED TO: COMMISSIONER OF PATENTS AND TRADEMARKS, WASHINGTON, D.C. 20231, ON THE DATE INDICATED BELOW.

BY Ara M. Hansbury
DATE July 19, 1995

13202
Reg. Ext. Time
RECEIVED
Intd
(1) no. Cofr
JUL 26 1995
GROUP 2200
7-27-95
PATENT
BOX AF

RESPONSE UNDER 37 CFR 1.116
EXPEDITED PROCEDURE EXAMINER
GROUP ART UNIT 2202

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re:	Patent Application of Leon Stambler	: Group Art Unit: 2202
		:
Serial No.:	08/122,071	: Examiner:
		: S. Cangialosi
Filed:	September 14, 1993	:
		:
For:	SECURE TRANSACTION SYSTEM AND METHOD UTILIZED THEREIN	: Attorney Docket : No. 6074-1 U1

PETITION FOR EXTENSION OF TIME

Applicant in the above-identified application hereby petitions for a one (1) month extension of time to and including July 24, 1995 (July 23 being a Sunday) for responding to the Office Action mailed March 23, 1995. An Amendment After Final Under 37 C.F.R. § 1.116 accompanies this Petition.

Please charge the extension fee of \$55.00 and any additional fees, or credit any overpayment, to the account of Panitch Schwarze Jacobs & Nadel, Deposit Account No. 16-0235. One additional copy of this form is enclosed.

Respectfully submitted,

LEON STAMBLER

July 19, 1995 By: Leslie L. Kasten, Jr.
(Date) ✓

Registration No. 28,959
PANITCH SCHWARZE JACOBS & NADEL, P.C.
1601 Market Street - 36th Floor
Philadelphia, PA 19103-2398
Telephone: (215) 567-2020
Facsimile: (215) 567-2991

LLK:amh

T128124 07/24/95 08122071

16-0235 280 215

55.00CH



Corres. and Mail
BOX AF

I HEREBY CERTIFY THAT THIS CORRESPONDENCE IS BEING DEPOSITED WITH THE UNITED STATES POSTAL SERVICE AS FIRST CLASS MAIL IN AN ENVELOPE ADDRESSED TO: COMMISSIONER OF PATENTS AND TRADEMARKS, WASHINGTON, D.C. 20231, ON THE DATE INDICATED BELOW.

BY Ann M. Hansbury

DATE July 19, 1995

14
10/16
RECEIVED

JUL 26 1995

GROUP 2200

Copier
7-27-95
PATENT

BOX AF

RESPONSE UNDER 37 CFR 1.116
EXPEDITED PROCEDURE EXAMINER
GROUP ART UNIT 2202

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re:	Patent Application of Leon Stambler	: Group Art Unit: 2202
Serial No.:	08/122,071	: Examiner:
Filed:	September 14, 1993	: S. Cangialosi
For:	SECURE TRANSACTION SYSTEM AND METHOD UTILIZED THEREIN	: Attorney Docket No. 6074-1 U1

AMENDMENT AFTER FINAL UNDER 37 C.F.R. § 1.116

OK to enter file 7/95
This amendment is being filed in response to the final Office Action mailed March 23, 1995 (Paper No. 10) in connection with the above-identified application and is being filed within the first month after the initial due date. A Petition for a one-month extension of time is enclosed.

Please amend the above-identified application as follows:

In the Claims:

1 1 1 1 1 1 1
Please cancel claims 7, 17, 19-33, 46, 48, 50, 56-59, 63-78 and 80-106.
D

Please amend claims 8-16, 34, 35, 47, 49 and 79 as follows:

28. (Amended) The [method] system of claim [7] ~~107~~, wherein the information relevant to the transaction comprises at least one information group which is coded [so as] to enable detection of a change in [its] the content or structure of said information group.

35. (Amended) The [method] system of claim [7] ~~107~~, wherein the transaction involves an electrical signal, the VAN being included in the electrical signal together with at least a portion of the information relevant to the transaction.

410. (Amended) The [method] system of claim [7] ~~107~~, wherein the transaction includes originating an instrument and wherein the [step of] means for associating the VAN with the transaction [comprises the step of recording] records the VAN and at least a portion of the information relevant to the transaction on the instrument.

511. (Amended) The [method] system of claim ~~10~~, wherein the information relevant to the transaction comprises a combination of predetermined information recorded on the instrument and predetermined information not recorded on the instrument, such that prevention of fraudulent regeneration of the VAN is enhanced.

622. (Amended) The [method] system of claim [7] ~~107~~, wherein the [step of] means for authenticating the VAN comprises [the steps of]:

52

first means for uncoding the VAN using at least the derived encoded authentication information; and
second means for comparing the uncoded VAN to the information relevant to the transaction[;] and for
authenticating the VAN and the transaction associated with the VAN only if the uncoded VAN corresponds to the information relevant to the transaction.

7 13. (Amended) The [method] system of claim [7] ~~107~~,
wherein the [step of] means for authenticating the VAN comprises [the steps of]:

first means for coding the information relevant to the transaction using at least the derived encoded authentication information to generate a second VAN; and

second means for comparing the first VAN associated with the transaction to the second VAN[;] and for
authenticating the first VAN and the transaction associated with the first VAN only if the first VAN corresponds to the second VAN.

8 14. (Amended) The [method] system of claim [7] ~~107~~,
wherein the transaction comprises originating and processing a medical prescription form and [said at least one party comprises]
the parties comprise an originating physician and a patient presenting the medical prescription form for processing in a processing jurisdiction, the encoded authentication information being associated with the originating physician and with the patient, and wherein the [step of associating the] VAN is

53

associated with the transaction [comprises the step of] by
recording the VAN on the medical prescription form.

9¹⁵. (Amended) The [method] system of claim ~~14~~⁸,
further comprising [the steps of]:

means for authenticating the patient; and wherein
[dispensing] the medicine is dispensed as
indicated on the medical prescription form to the patient only if
the VAN and the patient are authenticated.

10¹⁶. (Amended) The [method] system of claim ~~15~~⁹,
wherein the means for authenticating the VAN is [authenticated
by] located at a processing entity associated with the processing
jurisdiction, [further comprising the steps of] and wherein:

if the originating physician is not licensed to
practice in the processing jurisdiction, [then obtaining]
authorization for processing the medical prescription form in the
processing jurisdiction is obtained from a correspondent
physician licensed in the processing jurisdiction[;] and wherein
the system further includes

means for generating a redemption VAN from the VAN and
from information associated with the processing entity; and

means for associating the redemption VAN with the
medical prescription form, such that the processing entity is
accountable for the processing of the medical prescription form.

13²⁴. (Amended) The [method] system of claim [33] ~~109~~¹²,
further comprising [the steps of]:

54

means for coding a signal representative of
information associated with at least one party with the signal
representative of the VAN to generate therefrom a signal
representative of a redemption VAN (RVAN);

means for associating the RVAN with the
transaction, such that the transaction cannot be fraudulently
presented for further redemption; and

means for storing the signal representative of the
RVAN in a storage means associated with at least one party, such
that the transaction is cleared in a substantially instantaneous
manner.

1435. (Amended) The [method] system of claim 13,
wherein the transaction involves an electrical signal, the RVAN
being included in the electrical signal.

1647. (Amended) The [method] system of claim [46] 140,
wherein the [step of] means for associating the RVAN with the
funds transfer [comprises the step of recording] records the RVAN
on a receipt, the receipt being dispensed to the originator
party.

1849. (Amended) The [method] system of claim [48] 111,
further comprising [the steps of]:

means for generating a redemption VAN (RVAN) by
encoding a signal representative of the VAN with a signal
representative of at least information associated with the payee
party; and

14
small

means for associating the RVAN with the invoice
such that payment of the invoice is substantiated by the RVAN.

1975. (Amended) The [method] system of claim 25,
further comprising [the steps of]:

5

means for debiting [the patient's account] an
account of the patient for the patient amount of liability to pay
for the medicine dispensed by an authorized dispenser having an
account, the dispenser located in a processing jurisdiction;

means for debiting a co-payor's account for a co-
payor amount of liability; and

means for crediting the dispenser's account by the
sum of the debited amounts.

Please enter new claims 107-111 as follows:

1--107. A system for authenticating a transaction and
at least one party to the transaction comprising:

206
Cont

means for receiving a first signal representative
of a personal identification number (PIN) of the at least one
party to the transaction, the PIN being unrecoverable within the
system and for generating an encrypted signal derived from the
PIN;

means for receiving the encrypted signal and a
signal representative of predetermined non-secret information and
for generating therefrom a signal representative of encoded
authentication information;

means for receiving the signal representative of
the encoded authentication information and a signal

representative of information relevant to the transaction and for generating therefrom a signal representative of a variable authentication number (VAN);

means for associating the VAN with the transaction;

means for receiving a second signal representative of the PIN and a signal representative of the predetermined non-secret information and for deriving therefrom a signal representative of the encoded authentication information; and

means for authenticating the VAN associated with the transaction using the derived encoded authentication information and the information relevant to the transaction.

11108. A system for authenticating a transaction and at least one party to the transaction comprising:

means for coding information relevant to a transaction with information associated with at least one party to the transaction for generating a variable authentication number (VAN), the information associated with the at least one party comprising encoded authentication information deriveable from a predetermined secret code and a predetermined non-secret code, the encoded authentication information being previously generated by encrypting a personal identification number (PIN) which is unrecoverable within the transaction system;

means for associating the VAN with the transaction;

57

means for deriving the encoded authentication information using the predetermined secret code and the predetermined non-secret code; and

means for authenticating the VAN associated with the transaction by using the derived coded authentication information and the information relevant to the transaction.

12109. A system for processing multiple party transactions comprising:

means for receiving a signal representative of information derived from a personal identification number (PIN) associated with at least one party to a transaction and for receiving a signal representative of other information relevant to the transaction and for generating therefrom a signal representative of a variable authentication number (VAN);

means for associating the VAN with the transaction;

means for receiving a signal representative of the PIN of a recipient party and for generating an encoded signal;

means for receiving the encoded signal and signals representative of the VAN and of the other information relevant to the transaction, for determining whether the recipient party and the transaction are authentic and for authorizing the transaction only if the recipient party and the transaction are authenticated.

15 ~~110~~. A system for automatically and instantaneously transferring funds from an account associated with an originator party to an account associated with a recipient party comprising:

means for receiving from the originator party a personal identification number (PIN) associated with the originator party, information identifying the account of the originator party, information for identifying the account of the recipient party, and fund transfer information including a transfer amount;

means for generating a variable authentication number (VAN) using the PIN of the originator party, the information identifying the account of the recipient party, and the fund transfer information;

means for determining whether the originator party is authentic by using the PIN of the originator party;

means for determining whether the fund transfer information is authentic by using the VAN;

means for transferring funds from the account of the originator party to the account of the recipient party only if the originator party and the funds transfer information are both determined to be authentic;

means for generating a redemption variable authentication number (RVAN) after the funds have been transferred to the account of the recipient party, the RVAN being generated using at least the funds transfer information; and

9
59

means for associating the RVAN with the funds transfer such that the funds transfer is substantiated by the RVAN.

17-111 A system for processing an invoice comprising:
means for generating a variable authentication number (VAN) using at least information associated with an invoice, the information associated with the invoice including information identifying an account of a payee party and payment information including at least a payment amount;

means for recording the VAN and the information associated with the invoice on the invoice;

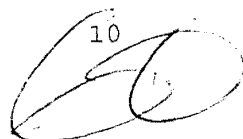
means for receiving the VAN and a personal identification number (PIN) from a payor party to the invoice, the received PIN being unrecoverable in the system;

means for determining whether the payor party and the VAN are authentic by using the information associated with the invoice and the received PIN;

means for receiving from the invoice the information identifying the account of the payee party and the payment information; and

means for transferring the payment amount to the account of the payee party from funds associated with the payor party only if the payor party and the VAN are determined to be authentic.--

10



REMARKS

After entry of the foregoing amendment, independent claims 107-111 and dependent claims 8-16, 34, 35, 47, 49 and 79 are active in the present application. All of the remaining claims have been cancelled. Entry of the foregoing amendment is respectfully requested because it is believed that the amended claims are now in condition for allowance.

Both the Applicant and his attorney would like to express their sincere appreciation to Examiner Cangialosi for the courtesies extended during the telephone interview conducted on June 28, 1995. During the interview, the newly presented independent claims were discussed and it was agreed that each of the new independent claims which are now in a system or apparatus format are sufficient to overcome the subject matter rejection under 35 U.S.C. § 101 which was imposed in the last Office Action. Per the discussion which occurred during the interview, all of the currently pending dependent claims have also been amended in substantially the same manner to place all of the dependent claims into an apparatus or system format. Accordingly, it is respectfully requested that the foregoing amendment be entered and that the rejection under 35 U.S.C. § 101 be withdrawn insofar as it may be applied to the currently pending claims.

The newly submitted independent claims are based upon and are closely related to corresponding independent method claims which now have been cancelled. The relationship between

the new claims and the previously pending independent claims is as follows:

<u>New Claim Number</u>	<u>Cancelled Claim Number</u>
107	7
108	7
109	33
110	46
111	48

A side-by-side comparison of the new claims with the previously pending claims will reveal that the new claims are substantively quite similar to the cancelled claims although in apparatus or system format. Accordingly, it is respectfully submitted that entry of the new claims raises no new issues which must be considered by the Examiner with respect to patentability.

In the last Office Action, all of the claims were rejected under 35 U.S.C. § 103 over the patent to Bracht1 et al. (U.S. Patent No. 4,747,050). It was the position of the Examiner that the Bracht1 reference discloses a transaction security system using time variant authentication parameters including a transaction variable for each transaction substantially as set forth in the claims and that the only difference was the use of the explicit term "variable authentication number". It was the belief of the Examiner that the transaction variable as employed in the Bracht1 et al. system is the functional equivalent of

Applicant's variable authentication number and that it would have been obvious to one of ordinary skill in the art to provide a similar arrangement because it is conventional and standard practice to employ a transaction variable for the authentication of each transaction. The Examiner also believed that the deficiencies of the art with respect to the dependent claims, if any, deal with conventional authentication schemes. For the reasons as set forth below and as presented in detail during the interview, the Applicant respectfully traverses the rejection as it may be applied to the currently pending claims.

The present invention relates to a system for authenticating a transaction and a party to the transaction. The present invention is probably best exemplified by new claim 107 which can be best understood when referring to Figs. 7 and 8B of the drawings. Claim 107 calls for means, in the embodiment of Fig. 7 and irreversible coder (10), for receiving a first signal representative of a personal identification number (PIN) of at least one party to the transaction (in Fig. 7, the originator), the PIN being unrecoverable within the system and for generating an encrypted signal (CPNO in Fig. 7) derived from the PIN. The system further includes means (coder 28 in Fig. 7) for receiving the encrypted signal and a signal representative of predetermined non-secret information (identification information of the recipient such as the recipient's account number or taxpayer identification number in the embodiment shown in Fig. 7) and for generating therefrom a signal representative of encoded

authentication information (the Joint Key in Fig. 7). The system further includes means (coder 30 in Fig. 7) for receiving the signal representative of the encoded authentication information and a signal representative of information relevant to the transaction (for example, the amount of the transaction) and for generating a signal representative of a variable authentication number (VAN). The claim further calls for means for associating the VAN with the transaction. In the embodiment shown in Fig. 7 in which a check is being employed, the VAN is printed directly onto the check along with all of the other pertinent information normally on the check such as the account number of the recipient, account information of the originator, the amount of the check, etc. The check then goes forward to the recipient and, referring to Fig. 8, the system further includes means (coder 56) for receiving a second signal representative of the PIN (CPNO) and a signal representative of the predetermined non-secret information (from the check) and for deriving therefrom a signal representative of the encoded authentication information (Joint Key). The system further includes means (58, 60 in Fig. 8B) for authenticating the VAN associated with the transaction using the derived encoded authentication information (Joint Key) and the information relevant to the transaction, in the embodiment shown in Fig. 8B, the transaction amount taken from the check. The dependent claims relate to more specific features of the invention and the other independent claims relate to slightly different variations of the same invention.

The Bracht1 et al. patent is directed to a transaction security system which employs time variant parameters in combination with time invariant parameters to generate session keys. In the Bracht1 system, each user is supplied with a "smart" user card which includes a microprocessor, an encryption device, and storage or memory. The storage portion of the card is employed for storing a great deal of information including a personal key (KP), a personal account number (PAN), and various other parameters. The parameters stored within the memory of the card remain the same and, therefore, are said to be time invariant. When a user wishes to conduct a transaction in the Bracht1 system, the user inserts the card into an on-line terminal which is connected via a communications link to a computer processing center of the entity which issued the card; i.e., a bank or other financial institution. Without using any type of PIN entered by the card user, the local terminal obtains certain information from the user card (PAN and KP) and generates a session key (KSTR1) and a message authentication code (MAC) which are transmitted in a transaction request message along with certain information to the data processing center of the card issuer. The message authentication code (MAC) is generated on the card (by the microprocessor) utilizing the time variant transaction session key (KSTR1), which is generated from two time variable parameters (T_{term} and T_{card}) and a transaction key generated from the PAN and the KP on the user card. The message authentication code (MAC) is then attached to the transaction

message sent from the local terminal to the processing facility of the user. The issuer data processing facility then uses the MAC to authenticate the transaction request message, and also generates a time variant transaction authentication parameter (TAP), based upon a time variable (T_{issuer}), and a pre-stored version of the card user's personal key (KP), personal account number (PAN), and PIN. A response message which includes the TAP and a response MAC is generated by the issuer data processing facility and sent with other information to the terminal to indicate that the transaction is authorized or rejected. The terminal uses the MAC in the response message to authenticate the transaction response. The card user then inputs his or her PIN which is processed on the card (i.e., in the microprocessor) with the personal key (KP) to provide a derived TAP which is compared with the received TAP from the card issuer's processing facility in the terminal as a confirmation that the card user is authorized.

As discussed in substantial detail during the interview, it is abundantly clear that while the Bracht1 et al. patent teaches the concept of using some type of encoded signal or accompanying messages passing between the terminal and the processing facility for authentication purposes, the message authentication code employed in Bracht1 is generated in a completely different way than that called for in the claims of the present application. The system in Bracht1 et al. does not use and does not suggest the use of a personal identification

number (PIN) which is encoded with non-secret information including the recipient's account number and the amount of the transaction for generating the message authentication code. Instead, the Bracht1 system employs a separate smart card for storing certain secret keys which are obtained from the card and are combined with certain other secret time varying parameters to generate a message authentication code (MAC). Clearly, one of ordinary skill in the art would not look to the complex Bracht1 system in developing the relatively simple, elegant system developed by the Applicant. In the Applicant's system, there is no need for any type of smart card or other card, there is no need for the storage of multiple secret keys or codes, and there is no particular need for a user to be on line with the card issuing facility through the point of sale terminal or other terminal.

The foregoing discussion concerning the Bracht1 reference and the differences between the Bracht1 reference and the present invention, as set forth in the claims, is believed to be a good summary of the discussion during the telephone interview. In view of the foregoing discussion and the discussion at the telephone interview, it is respectfully submitted that new independent claims 107-111 and the amended dependent claims 8-16, 34, 35, 47, 49 and 79 distinguish patentably over the Bracht1 reference and, therefore, it is respectfully requested that these claims all be entered.

In view of the foregoing amendment and discussion, it is respectfully submitted that the present application is in condition for allowance and such action is respectfully solicited.

Respectfully submitted,

LEON STAMBLER

Jul 19, 1995
(Date)

By:

Leslie L. Kasten, Jr.
Registration No. 28,959
PANITCH SCHWARZE JACOBS & NADEL, P.C.
1601 Market Street - 36th Floor
Philadelphia, PA 19103-2398
Telephone: (215) 567-2020
Facsimile: (215) 567-2991

LLK:amh



UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

SERIAL NUMBER	FILING DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET NO.
08/122,071	09/14/93	STAMBLER	L 60741U1

22M2/0731
PANITCH SCHWARZE JACOBS & NADEL
1601 MARKET STREET - 36TH FLOOR
PHILADELPHIA, PA 19103

CANGIALOSI EXAMINER

ART UNIT	PAPER NUMBER
2202	15

DATE MAILED: 07/31/95

NOTICE OF ALLOWABILITY

PART I.

- ☒ This communication is responsive to 7/21/95
- ☒ All the claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice Of Allowance And Issue Fee Due or other appropriate communication will be sent in due course.
- ☒ The allowed claims are 8-16, 34, 35, 47, 49, 79, 107-111
- ☐ The drawings filed on _____ are acceptable.
- ☐ Acknowledgment is made of the claim for priority under 35 U.S.C. 119. The certified copy has ☐ been received. ☐ not been received. ☐ been filed in parent application Serial No. _____, filed on _____.
- ☐ Note the attached Examiner's Amendment.
- ☐ Note the attached Examiner Interview Summary Record, PTOL-413.
- ☐ Note the attached Examiner's Statement of Reasons for Allowance.
- ☐ Note the attached NOTICE OF REFERENCES CITED, PTO-892.
- ☐ Note the attached INFORMATION DISCLOSURE CITATION, PTO-1449.

PART II.

A SHORTENED STATUTORY PERIOD FOR RESPONSE to comply with the requirements noted below is set to EXPIRE THREE MONTHS FROM THE "DATE MAILED" indicated on this form. Failure to timely comply will result in the ABANDONMENT of this application. Extensions of time may be obtained under the provisions of 37 CFR 1.136(a).

- ☐ Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL APPLICATION, PTO-152, which discloses that the oath or declaration is deficient. A SUBSTITUTE OATH OR DECLARATION IS REQUIRED.
- ☒ APPLICANT MUST MAKE THE DRAWING CHANGES INDICATED BELOW IN THE MANNER SET FORTH ON THE REVERSE SIDE OF THIS PAPER.
 - ☒ Drawing informalities are indicated on the NOTICE RE PATENT DRAWINGS, PTO-948, attached hereto or to Paper No. 7. CORRECTION IS REQUIRED.
 - ☐ The proposed drawing correction filed on _____ has been approved by the examiner. CORRECTION IS REQUIRED.
 - ☐ Approved drawing corrections are described by the examiner in the attached EXAMINER'S AMENDMENT. CORRECTION IS REQUIRED.
 - ☒ Formal drawings are now REQUIRED.

Any response to this letter should include in the upper right hand corner, the following information from the NOTICE OF ALLOWANCE AND ISSUE FEE DUE: ISSUE BATCH NUMBER, DATE OF THE NOTICE OF ALLOWANCE, AND SERIAL NUMBER.

Attachments:

- Examiner's Amendment
- Examiner Interview Summary Record, PTOL-413
- Reasons for Allowance
- Notice of References Cited, PTO-892
- Information Disclosure Citation, PTO-1449
- Notice of Informal Application, PTO-152
- Notice re Patent Drawings, PTO-948
- Listing of Bonded Draftsmen
- Other

Salvatore Cangialosi
SALVATORE CANGIALOSI
PRIMARY EXAMINER
ART UNIT 222



UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office

Address: Box ISSUE FEE
COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

PANITCH SCHWARZE JACOBS & NADOL
1601 MARKET STREET 36TH FLOOR
PHILADELPHIA, PA 19103

NOTICE OF ALLOWANCE
AND ISSUE FEE DUE

16

- ☐ Note attached communication from the Examiner
☐ This notice is issued in view of applicant's communication filed _____

SERIES CODE/SERIAL NO.	FILING DATE	TOTAL CLAIMS	EXAMINER AND GROUP ART UNIT	DATE MAILED
08/122,071	09/14/93	019	CANGIALOSI, S	07/31/95
First Named Applicant	STAMBLER, LEON			

TITLE OBSCURE TRANSACTION SYSTEM AND METHOD UTILIZED THEREIN
INVENTION

ATTY'S DOCKET NO.	CLASS-SUBCLASS	BATCH NO.	APPLN. TYPE	SMALL ENTITY	FEE DUE	DATE DUE
2 60741U1	380-004.000	N77	UTILITY	YES	\$605.00	10/31/95

**THE APPLICATION IDENTIFIES ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT.
PROSECUTION ON THE MERITS IS CLOSED.**

**THE ISSUE FEE MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS
APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED.**

HOW TO RESPOND TO THIS NOTICE:

- I. Review the SMALL ENTITY Status shown above.
If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

- A. If the status is changed, pay twice the amount of the FEE DUE shown above and notify the patent and Trademark Office of the change in status, or
B. If the Status is the same, pay the FEE DUE shown above.

If the SMALL ENTITY is shown as NO:

- A. Pay FEE DUE shown above, or
B. File verified statement of Small Entity Status before, or with, pay of 1/2 the FEE DUE shown above.

- II. Part B of this notice should be completed and returned to the Patent and Trademark Office (PTO) with your ISSUE FEE. Even if the ISSUE FEE has already been paid by charge to deposit account, Part B should be completed and returned. If you are charging the ISSUE FEE to your deposit account, Part C of this notice should also be completed and returned.
III. All communications regarding this application must give series code (or filing date), serial number and batch number. Please direct all communication prior to issuance to Box ISSUE FEE unless advised to contrary.

IMPORTANT REMINDER: Patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PATENT AND TRADEMARK OFFICE COPY

PTOL-85B (REV. 4-94) (0651-0033)



I HEREBY CERTIFY THAT THIS CORRESPONDENCE IS BEING
DEPOSITED WITH THE UNITED STATES POSTAL SERVICE AS
FIRST CLASS MAIL IN AN ENVELOPE ADDRESSED TO:
COMMISSIONER OF PATENTS AND TRADEMARKS, WASHINGTON, D.C.
20231, ON THE DATE INDICATED BELOW.

BY Donna M. Eaton
DATE 9-13-95

BOX ISSUE FEE
PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re	: Patent Application of	: Office of Publication
	: Leon Stambler	:
	:	: Batch No. N77
Serial No	: 08/122,071	:
	:	: Allowed July 31, 1995
Filed	: September 14, 1993	:
	:	:
For	: SECURE TRANSACTION SYSTEM	: Attorney Docket
	: AND METHOD UTILIZED	: No. 6074-1U1
	: THEREIN	:

TRANSMITTAL LETTER

Although it is Applicant's opinion that the claims
filed by way of amendment are substantially embraced in the
statement of invention or in the claims originally filed,
Applicant herewith files a Supplemental Declaration for
precautionary purposes under 37 CFR 1.67.

Respectfully submitted,

LEON STAMBLER

Sept 13, 1995
(Date)

By:

Leslie L. Kasten, Jr.
LESLIE L. KASTEN, JR.
Registration No. 28,959
PANITCH SCHWARZE JACOBS & NADEL, P.C.
1601 Market Street - 36th Floor
Philadelphia, PA 19103
Telephone: (215) 567-2020

LLK:MES:dme
Enclosure



PSJ&N File No. 6074-1U1

SUPPLEMENTAL DECLARATION
(Related Application)

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed, as amended by any and all amendments entered during the prosecution of the patent application identified herein, and for which a patent is sought on the invention entitled **SECURE TRANSACTION SYSTEM AND METHOD UTILIZED THEREIN** the specification of which was filed on **September 14, 1993** as Application Serial No. **08/122,071**.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any and all amendments entered during the prosecution of the application identified herein and during the prosecution of the related patent applications identified below.

I acknowledge the duty to disclose information which is material to patentability in accordance with Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application(s) in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose information material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56 which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

<u>07/977,385</u>	<u>November 17, 1992</u>	<u>Patented (5,267,314)</u>
(Application Serial No.)	(Filing Date)	(Status-patented, pending, abandoned)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issues thereon.

Full name of sole or
first inventor

Leon Stambler

Inventor's Signature

Leon Stambler

Date

09/05/95

Residence

Parkland, Florida

Citizenship

U.S.A.

Post Office

Address

7803 Boulder Lane

Parkland, Florida 33067

PART B—ISSUE FEE TRANSMITTAL

MAILING INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE. Blocks 2 through 6 should be completed where appropriate. All further correspondence including the Issue Fee Receipt, the Patent, advance orders and notification of maintenance fees will be mailed to addressee entered in Block 1 unless you direct otherwise, by: (a) specifying a new correspondence address in Block 3 below; or (b) providing the PTO with a separate "FEE ADDRESS" for maintenance fee notifications with the payment of Issue Fee or thereafter. See reverse for Certificate of Mailing.

1. CORRESPONDENCE ADDRESS		2. INVENTOR(S) ADDRESS CHANGE (Complete only if there is a change)		
PANITCH SCHWARZE JACOBS & NADEL 1601 MARKET STREET - 36TH FLOOR PHILADELPHIA, PA 19103 22M2/0731 E		INVENTOR'S NAME		
		Street Address		
		City, State and ZIP Code		
		CO-INVENTOR'S NAME		
		Street Address		
		City, State and ZIP Code		
		<input type="checkbox"/> Check if additional changes are on reverse side		
SERIES CODE/SERIAL NO.	FILING DATE	TOTAL CLAIMS	EXAMINER AND GROUP ART UNIT	DATE MAILED
08/122,071	09/14/93	019	CANGIALOSI, S	2202 07/31/95
First Named Applicant	STAMBLER, LEON			

TITLE OF INVENTION SECURE TRANSACTION SYSTEM AND METHOD UTILIZED THEREIN

	ATTY'S DOCKET NO.	CLASS-SUBCLASS	BATCH NO.	APPLN. TYPE	SMALL ENTITY	FEE DUE	DATE DUE
2	60741U1	380-024.000	N77	UTILITY	YES	\$605.00	10/31/95

3. Correspondence address change (Complete only if there is a change)	4. For printing on the patent front page, list the names of not more than 3 registered patent attorneys or agents OR, alternatively, the name of a firm having as a member a registered attorney or agent. If no name is listed, no name will be printed.
	1. PANITCH 2. SCHWARZE 3. JACOBS & NADEL, P.C.

DO NOT USE THIS SPACE

AG00360	10/17/95	08122071	16-0235	060	242	605.00CH
AG00361	10/17/95	08122071	16-0235	060	561	30.00CH

5. ASSIGNMENT DATA TO BE PRINTED ON THE PATENT (print or type)

(1) NAME OF ASSIGNEE:	5a. The following fees are enclosed: <input type="checkbox"/> Issue Fee <input type="checkbox"/> Advance Order - # of Copies
(2) ADDRESS: (CITY & STATE OR COUNTRY)	5b. The following fees should be charged to: 16-0235 DEPOSIT ACCOUNT NUMBER (ENCLOSE PART C) <input type="checkbox"/> Issue Fee <input checked="" type="checkbox"/> Advance Order - # of Copies 10 <input type="checkbox"/> Any Deficiencies in Enclosed Fees
A. <input checked="" type="checkbox"/> This application is NOT assigned. <input type="checkbox"/> Assignment previously submitted to the Patent and Trademark Office. <input type="checkbox"/> Assignment is being submitted under separate cover. Assignments should be directed to Box ASSIGNMENTS. PLEASE NOTE: Unless an assignee is identified in Block 5, no assignee data will appear on the patent. Inclusion of assignee data is only appropriate when an assignment has been previously submitted to the PTO or is being submitted under separate cover. Completion of this form is NOT a substitute for filing an assignment.	The COMMISSIONER OF PATENTS AND TRADEMARKS is requested to apply the Issue Fee to the application identified above. (Authorized Signature) <i>Robert H. A.</i> (Date) 9/21/95 NOTE: The Issue Fee will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the Patent and Trademark Office.

TRANSMIT THIS FORM WITH FEE-CERTIFICATE OF MAILING ON REVERSE

PTOL-85B (REV. 4-94) (0851-0033)

Certificate of Mailing

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to:

Box ISSUE FEE
Commissioner of Patents and Trademarks
Washington, D.C. 20231

on SEPT. 27, 1995
(Date)
MARY E SPERA
(Name of person making deposit)
Mary E Spera
(Signature)
Sept 27, 1995
(Date)

Note: If this certificate of mailing is used, it can only be used to transmit the Issue Fee. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing.

Burden Hour Statement: This form is estimated to take .2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Office of Information Systems, Patent and Trademark Office, Washington, D.C. 20231, and to the Office of Information and Regulatory Affairs, Office of Management and Budget, (Project 0651-0033), Washington, D.C. 20503. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner of Patents and Trademarks, Box Issue Fee, Washington, DC 20231.



I HEREBY CERTIFY THAT THIS CORRESPONDENCE IS BEING DEPOSITED WITH THE UNITED STATES POSTAL SERVICE AS FIRST CLASS MAIL IN AN ENVELOPE ADDRESSED TO: COMMISSIONER OF PATENTS AND TRADEMARKS, WASHINGTON, D.C. 20231, ON THE DATE INDICATED BELOW.

BY Elizabeth A. McLeod
DATE 10/24/95

[Handwritten signature]
[Handwritten initials]

PATENT
BOX ISSUE FEE
IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re:	Patent Application of Leon Stambler	: Attn: Official Draftsman
Appln. No.:	08/122,071	: Allowed July 31, 1995
Filed:	September 14, 1993	: Batch No.: N77
For:	SECURE TRANSACTION SYSTEM AND METHOD UTILIZED THEREIN	: Attorney Docket No. 6074-1U1

TRANSMITTAL OF FORMAL DRAWINGS

In accordance with the Notice of Allowability accompanying the Notice of Allowance mailed July 31, 1995, enclosed are fifteen (15) sheets of drawings (2 copies each), figures 1 through 15B, concerning the above-identified application.

It is respectfully submitted that the enclosed copies of Formal Drawings place this application in condition to be issued. The issue fee was paid on September 27, 1995.

Respectfully submitted,

LEON STAMBLER

October 24, 1995
(Date)

Martin G. Belisario
MARTIN G. BELISARIO
Reg. No. 32,886
PANITCH SCHWARZE JACOBS & NADEL, P.C.
1601 Market Street, 36th Floor
Philadelphia, PA 19103
(215) 567-2020

MGB:MES:eam

PSJN2/9053.1



UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office

Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20230

SERIAL NUMBER	FILING DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET NO.
66/122,877	09/14/95	STANDLER	10-27-95

4102/0103
PANITCH SCHWARZE JACOBS & NADEL 1601 MARKET STREET - 35TH FLOOR PHILADELPHIA, PA 19103

EXAMINER	
ART. UNIT	PAPER NUMBER

DATE MAILED:

NOTICE OF DRAWING REQUIREMENTS

☒ Corrected/substituted drawings for the above-identified application, received at the PTO on 10-27-95, are still considered informal for the reasons identified on the attached Form PTO-948.

☐ Applicant has the time remaining in the response period set in the Notice of Allowability or Notice of Drawing Requirements mailed _____ to overcome the objections raised in the attached Form PTO-948. This response period may be extended under the provisions of 37 CFR 1.136 (a) by filing the appropriate request and fee before the end of the six month statutory period for response.

☒ The PTO delayed in reviewing the corrected drawings. Applicant is given ONE MONTH TIME LIMIT from the date of this letter to provide corrected drawings. NO EXTENSION OF THIS TIME LIMIT MAY BE GRANTED UNDER EITHER 37 CFR 1.136(a) or (b). See MPEP 704.08. However, the response period set in the Notice of Allowability or Notice of Drawing Requirements mailed 7-13-95 may be extended under the provisions of 37 CFR 1.136(a) by filing the appropriate request and fee before the end of the six month statutory period for response.

☐ The PTO delayed in reviewing the corrected drawings. Applicant is given ONE MONTH TIME LIMIT from the date of this letter to provide corrected drawings. NO EXTENSION OF THIS TIME LIMIT MAY BE GRANTED UNDER EITHER 37 CFR 1.136(a) or (b). See MPEP 704.08.

☒ ATTACHMENT: PTO-948

John Chan
PATENT AND TRADEMARK OFFICE

12-15-95
DATE

NOTICE OF DRAFTSPERSON'S PATENT DRAWING REVIEW

PTO Draftpersons review all originally filed drawings regardless of whether they are designated as formal or informal. Additionally, patent examiners will review the drawings for compliance with the regulations. Direct telephone inquiries concerning this review to the Drawing Review Branch, 703-305-8404.

The drawings filed (insert date) 10-27-95 are
A. ☐ not objected to by the Draftsperson under 37 CFR 1.84 or 1.152.
B. ☒ objected to by the Draftsperson under 37 CFR 1.84 or 1.152 as indicated below. The Examiner will require submission of new, corrected drawings when necessary. Corrected drawings must be filed in accordance with the instructions on the back of this Notice.

1. DRAWINGS. 37 CFR 1.84(a): Acceptable categories of drawings:
Black ink. Color.
☐ Not black solid lines. Fig(s) _____
☐ Color drawings are not acceptable until petition is granted. Fig(s) _____
2. PHOTOGRAPHS. 37 CFR 1.84(b)
☐ Photographs are not acceptable until petition is granted. Fig(s) _____
☐ Photographs not properly mounted (must use dry-rot board or photographic double-weight paper). Fig(s) _____
☐ Poor quality (half-tone). Fig(s) _____
3. GRAPHIC FORMS. 37 CFR 1.84(d)
☐ Chemical or mathematical formula not labeled as separate figure. Fig(s) _____
☐ Group of waveforms not presented as a single figure, using common vertical axis with time extending along horizontal axis. Fig(s) _____
☐ Individuals waveform not identified with a separate letter designation adjacent to the vertical axis. Fig(s) _____
4. TYPE OF PAPER. 37 CFR 1.84(e)
☐ Paper not flexible, strong, white, smooth, nonshiny, and durable. Sheet(s) _____
☐ Erasures, alterations, overwritings, interlineations, cracks, creases, and folds copy machine marks not accepted. Fig(s) _____
☐ Mylar, velum paper is not acceptable (too thin). Fig(s) _____
5. SIZE OF PAPER. 37 CFR 1.84(f): Acceptable sizes:
21.6 cm. by 35.6 cm. (8 1/2 by 14 inches)
21.6 cm. by 33.1 cm. (8 1/2 by 13 inches)
21.6 cm. by 27.9 cm. (8 1/2 by 11 inches)
21.0 cm. by 29.7 cm. (DIN size A4)
☐ All drawing sheets not the same size. Sheet(s) _____
☐ Drawing sheet not an acceptable size. Sheet(s) _____
6. MARGINS. 37 CFR 1.84(g): Acceptable margins:

Paper size

21.6 cm. X 35.6 cm. (8 1/2 X 14 inches)	21.6 cm. X 33.1 cm. (8 1/2 X 13 inches)	21.6 cm. X 27.9 cm. (8 1/2 X 11 inches)	21.0 cm. X 29.7 cm. (DIN Size A4)
T 5.1 cm. (2")	2.5 cm. (1")	2.5 cm. (1")	2.5 cm.
L .64 cm. (1/4")	.64 cm. (1/4")	.64 cm. (1/4")	2.5 cm.
R .64 cm. (1/4")	.64 cm. (1/4")	.64 cm. (1/4")	1.5 cm.
B .64 cm. (1/4")	.64 cm. (1/4")	.64 cm. (1/4")	1.0 cm.

Margins do not conform to chart above.

Sheet(s) _____
Top (T) Left (L) Right (R) Bottom (B)

7. VIEWS. 37 CFR 1.84(h)
REMINDER: Specification may require revision to correspond to drawing changes.
☐ All views not grouped together. Fig(s) _____
☐ Views connected by projection lines or lead lines. Fig(s) _____
Partial views. 37 CFR 1.84(h) 2

- ☐ View and enlarged view not labeled separately or properly. Fig(s) _____
Sectional views. 37 CFR 1.84 (h) 3
☐ Hatching not indicated for sectional portions of an object. Fig(s) _____
☐ Cross section not drawn same as view with parts in cross section with regularly spaced parallel oblique strokes. Fig(s) _____
8. ARRANGEMENT OF VIEWS. 37 CFR 1.84(i)
☐ Words do not appear on a horizontal, left-to-right fashion when page is either upright or turned so that the top becomes the right side, except for graphs. Fig(s) _____
9. SCALE. 37 CFR 1.84(k)
☐ Scale not large enough to show mechanism with crowding when drawing is reduced in size to two-thirds in reproduction. Fig(s) _____
☐ Indication such as "actual size" or scale 1/2" not permitted. Fig(s) _____
10. CHARACTER OF LINES, NUMBERS, & LETTERS. 37 CFR 1.84(l)
☒ Lines, numbers & letters not uniformly thick and well defined, clean, durable, and black (except for color drawings). Fig(s) 1-16 (Roucut)
11. SHADING. 37 CFR 1.84(m)
☐ Solid black shading areas not permitted. Fig(s) _____
☐ Shade lines, pale, rough and blurred. Fig(s) _____
12. NUMBERS, LETTERS, & REFERENCE CHARACTERS. 37 CFR 1.84(p)
☒ Numbers and reference characters not plain and legible. 37 CFR 1.84(p)(l) Fig(s) 1-16
☐ Numbers and reference characters not oriented in same direction as the view. 37 CFR 1.84(p)(l) Fig(s) _____
☐ English alphabet not used. 37 CFR 1.84(p)(2) Fig(s) _____
☐ Numbers, letters, and reference characters do not measure at least .32 cm. (1/8 inch) in height. 37 CFR(p)(3) Fig(s) _____
13. LEAD LINES. 37 CFR 1.84(q)
☐ Lead lines cross each other. Fig(s) _____
☐ Lead lines missing. Fig(s) _____
14. NUMBERING OF SHEETS OF DRAWINGS. 37 CFR 1.84(t)
☐ Sheets not numbered consecutively, and in Arabic numerals, beginning with number 1. Sheet(s) _____
15. NUMBER OF VIEWS. 37 CFR 1.84(u)
☐ Views not numbered consecutively, and in Arabic numerals, beginning with number 1. Fig(s) _____
☐ View numbers not preceded by the abbreviation Fig. Fig(s) _____
16. CORRECTIONS. 37 CFR 1.84(w)
☐ Corrections not made from prior PTO-948. Fig(s) _____
17. DESIGN DRAWING. 37 CFR 1.152
☐ Surface shading shown not appropriate. Fig(s) _____
☐ Solid black shading not used for color contrast. Fig(s) _____

COMMENTS:

ATTACHMENT TO PAPER NO. 19REVIEWER J. CHASEDATE 12-15-95



I HEREBY CERTIFY THAT THE CORRESPONDENCE IS BEING DEPOSITED WITH THE UNITED STATES POSTAL SERVICE AS FIRST CLASS MAIL IN AN ENVELOPE ADDRESSED TO: COMMISSIONER OF PATENTS AND TRADEMARKS, WASHINGTON, D.C. 20231, ON THE DATE INDICATED BELOW.

BY Elizabeth A. Stambler
DATE 1/23/96

4/10 1/3

B
#20
#4

PATENT
BOX ISSUE FEE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re:	Patent Application of Leon Stambler	: Attn: Official Draftsman :
Appln. No.:	08/122,071	: Allowed July 31, 1995 :
Filed:	September 14, 1993	: Batch No.: N77 :
For:	SECURE TRANSACTION SYSTEM AND METHOD UTILIZED THEREIN	: Attorney Docket No. 6074-1U1 :

RESPONSE TO NOTICE OF DRAWING REQUIREMENTS

In response to the above NOTICE, mailed January 3, 1996, enclosed are fifteen (15) replacement sheets of drawings (1 copy each), figures 1 through 16, concerning the above-identified application.

It is respectfully submitted that the enclosed copies of Formal Drawings place this application in condition to be issued. The issue fee was paid September 27, 1995.

Respectfully submitted,

LEON STAMBLER

January 22, 1996
(Date)

Martin G. Belisario
MARTIN G. BELISARIO
Reg. No. 32,886
PANITCH SCHWARZE JACOBS & NADEL, P.C.
1601 Market Street, 36th Floor
Philadelphia, PA 19103
(215) 567-2020

MGB:MES:eam

5524073

FIG. 1

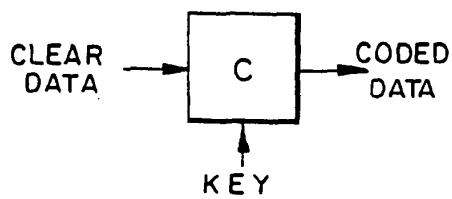


FIG. 2

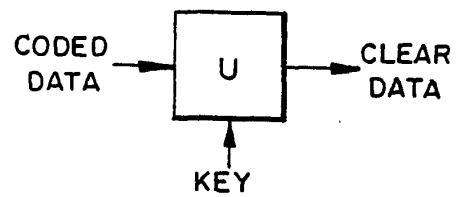


FIG. 3

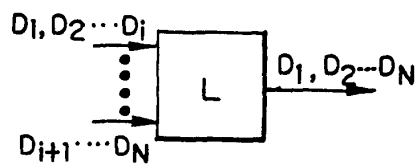


FIG. 4

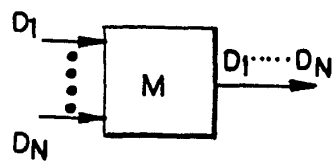


FIG. 5

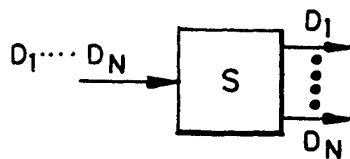
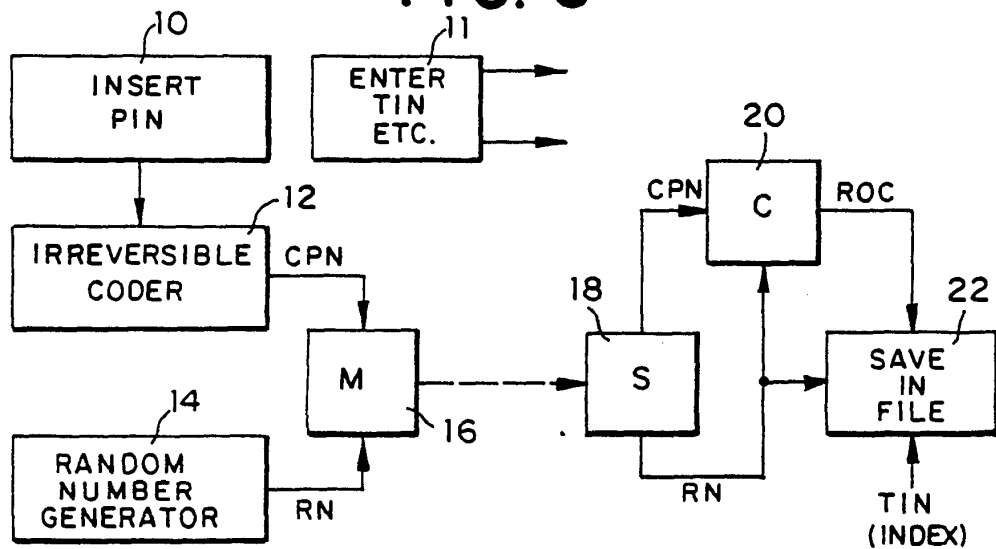


FIG. 6



BY
 DATE

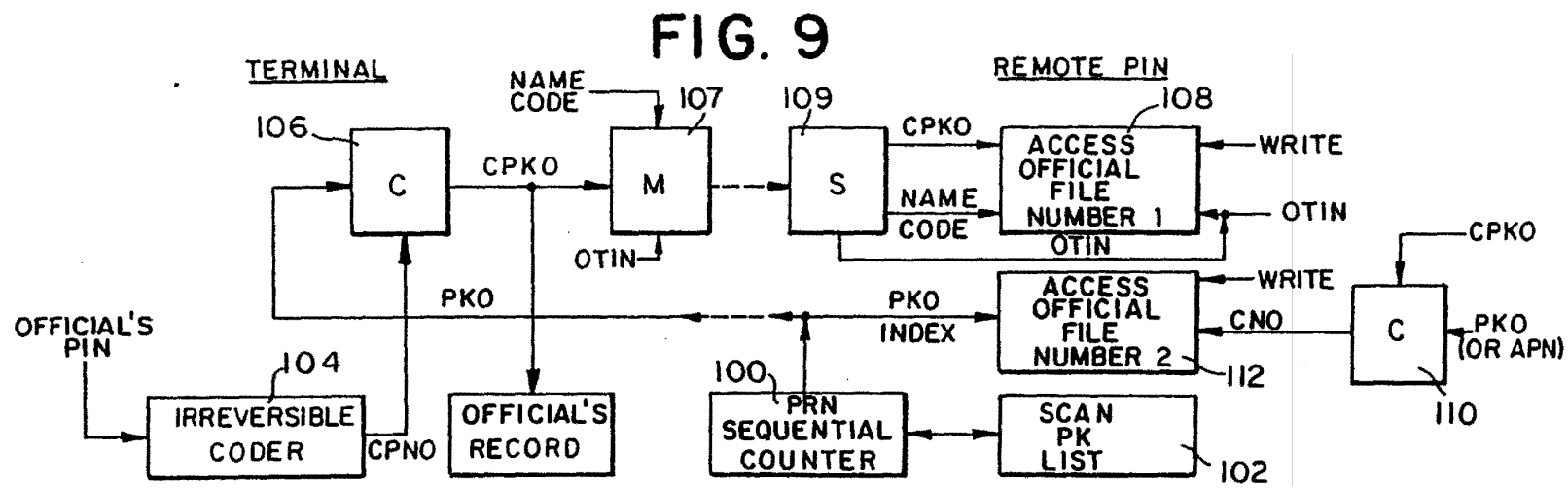
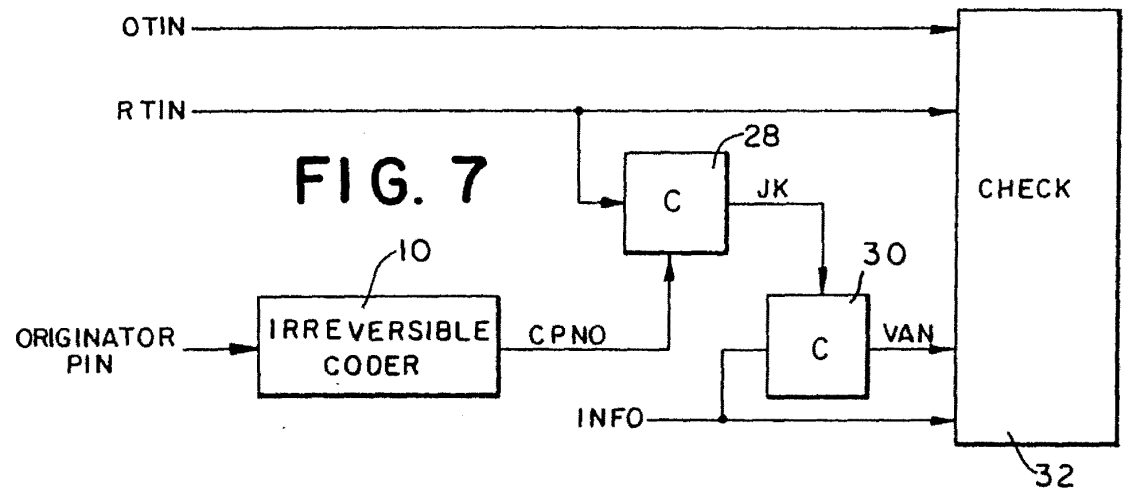


FIG. 8A

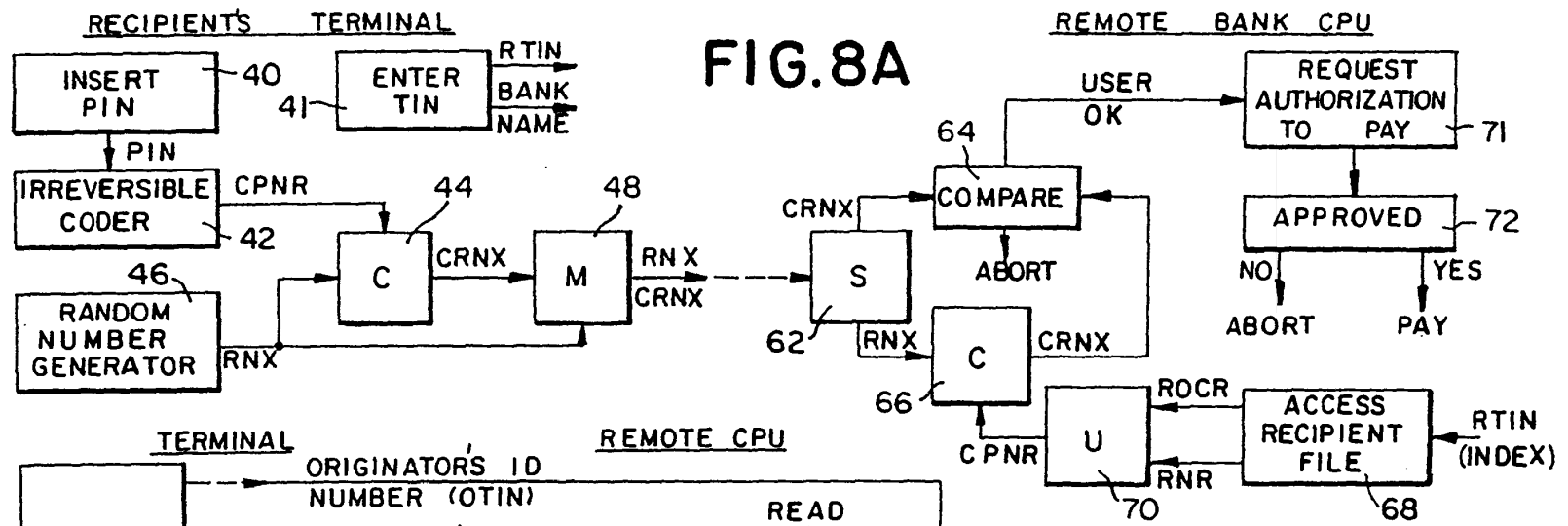


FIG. 8A

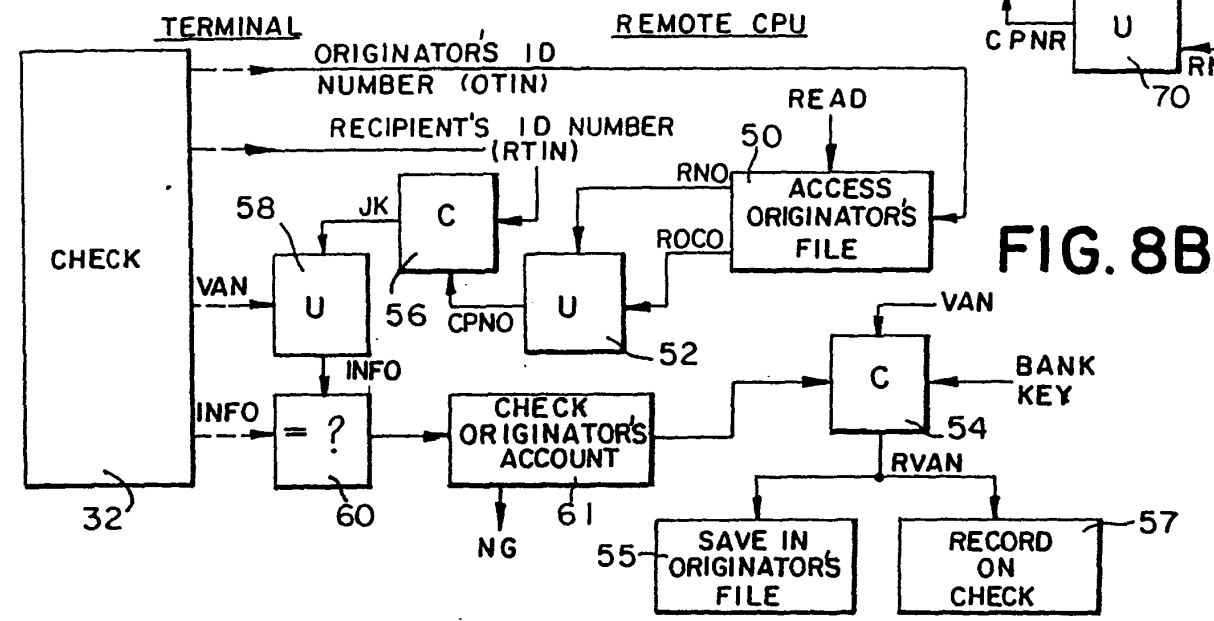


FIG. 8B

SECRET
 57
 INTERNAL

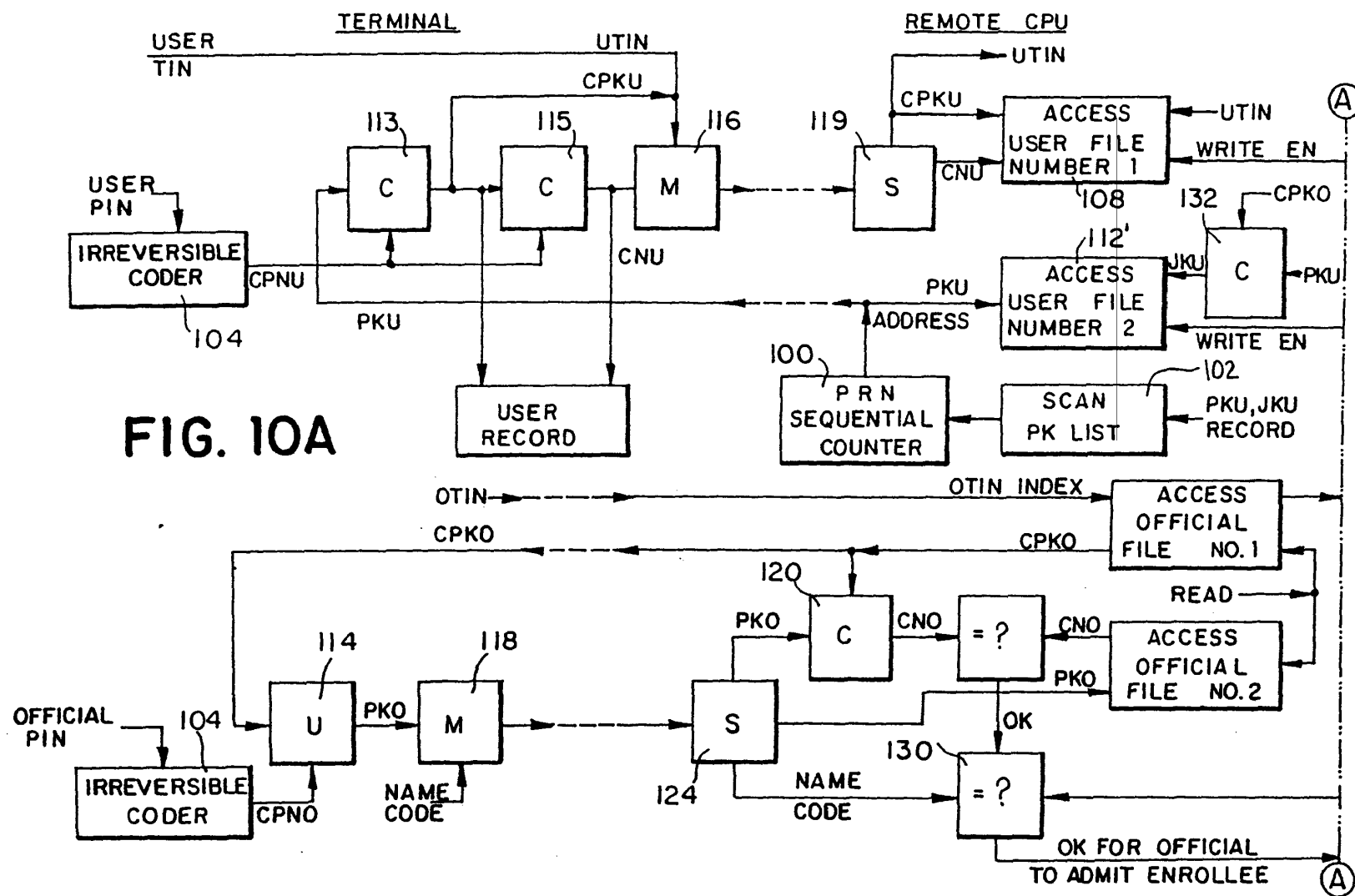
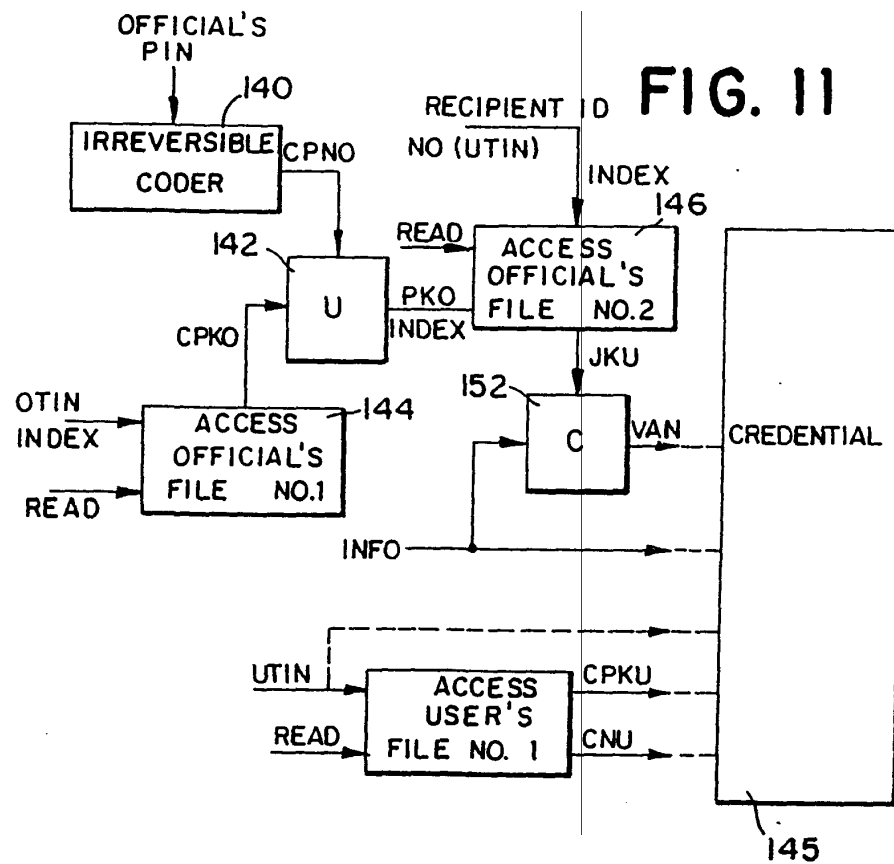
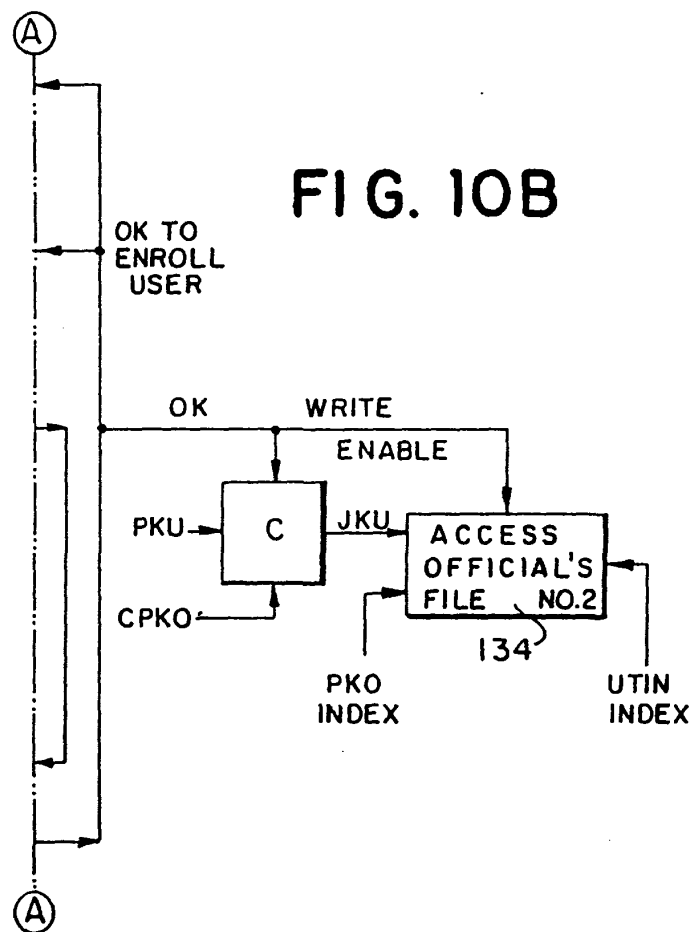


FIG. 10A

SECRET
 BY []
 DATE []
 CONTROL []



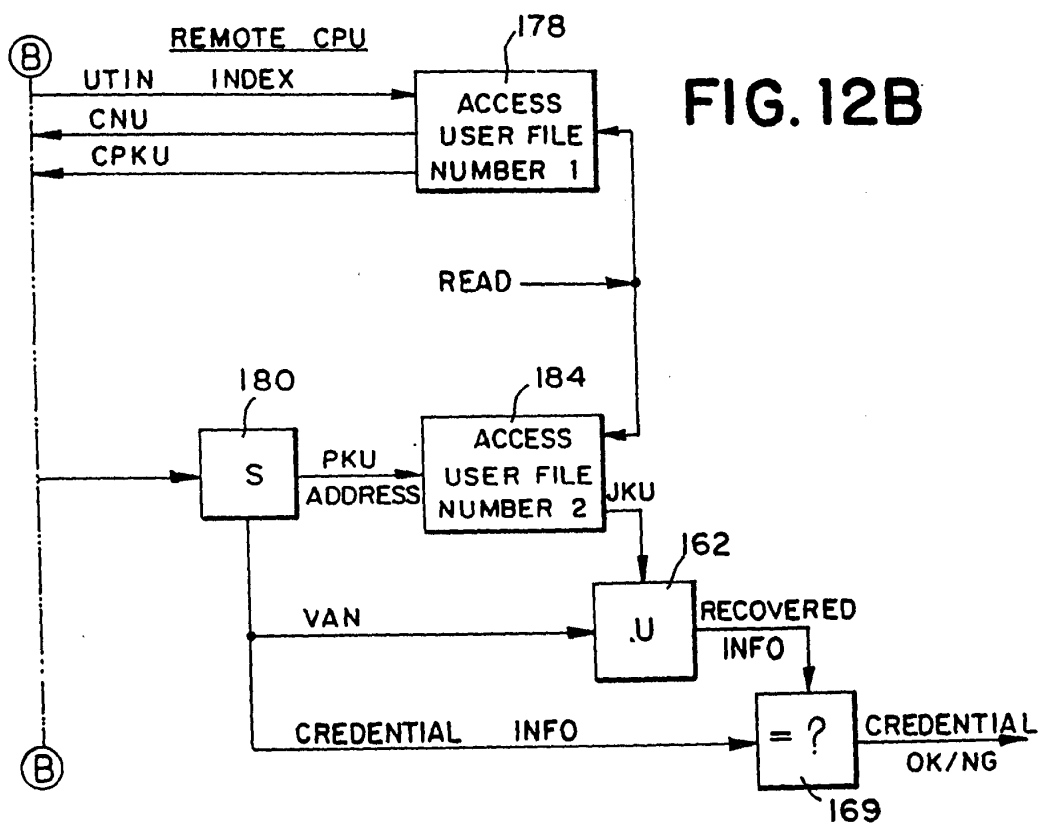
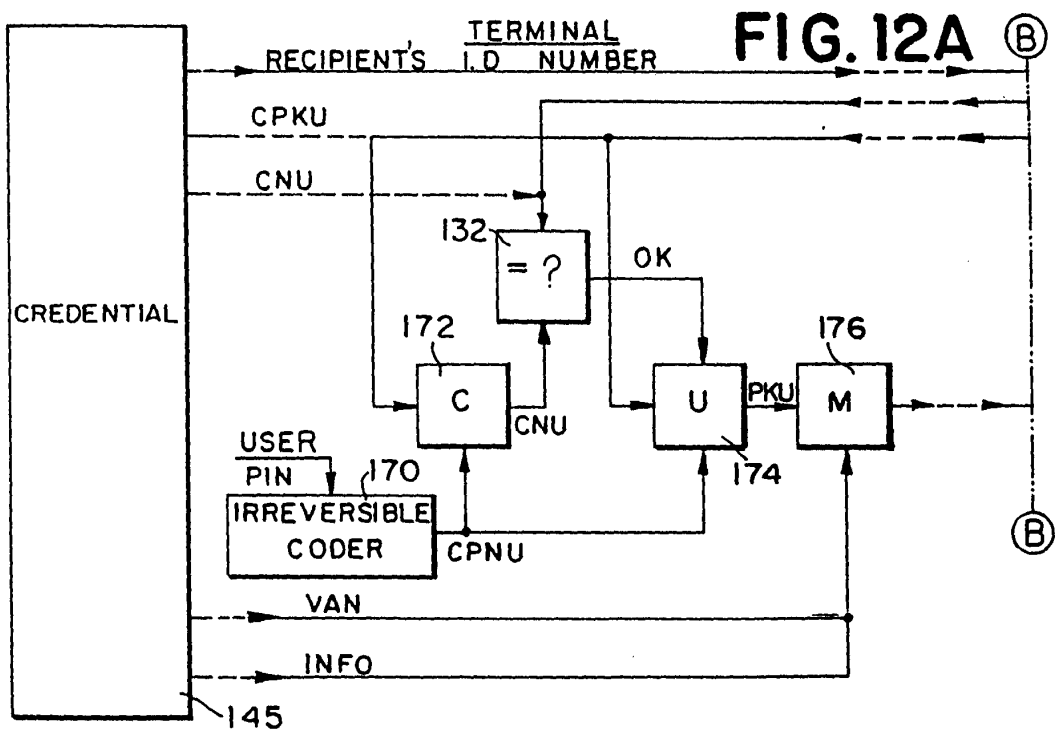


FIG. 13A

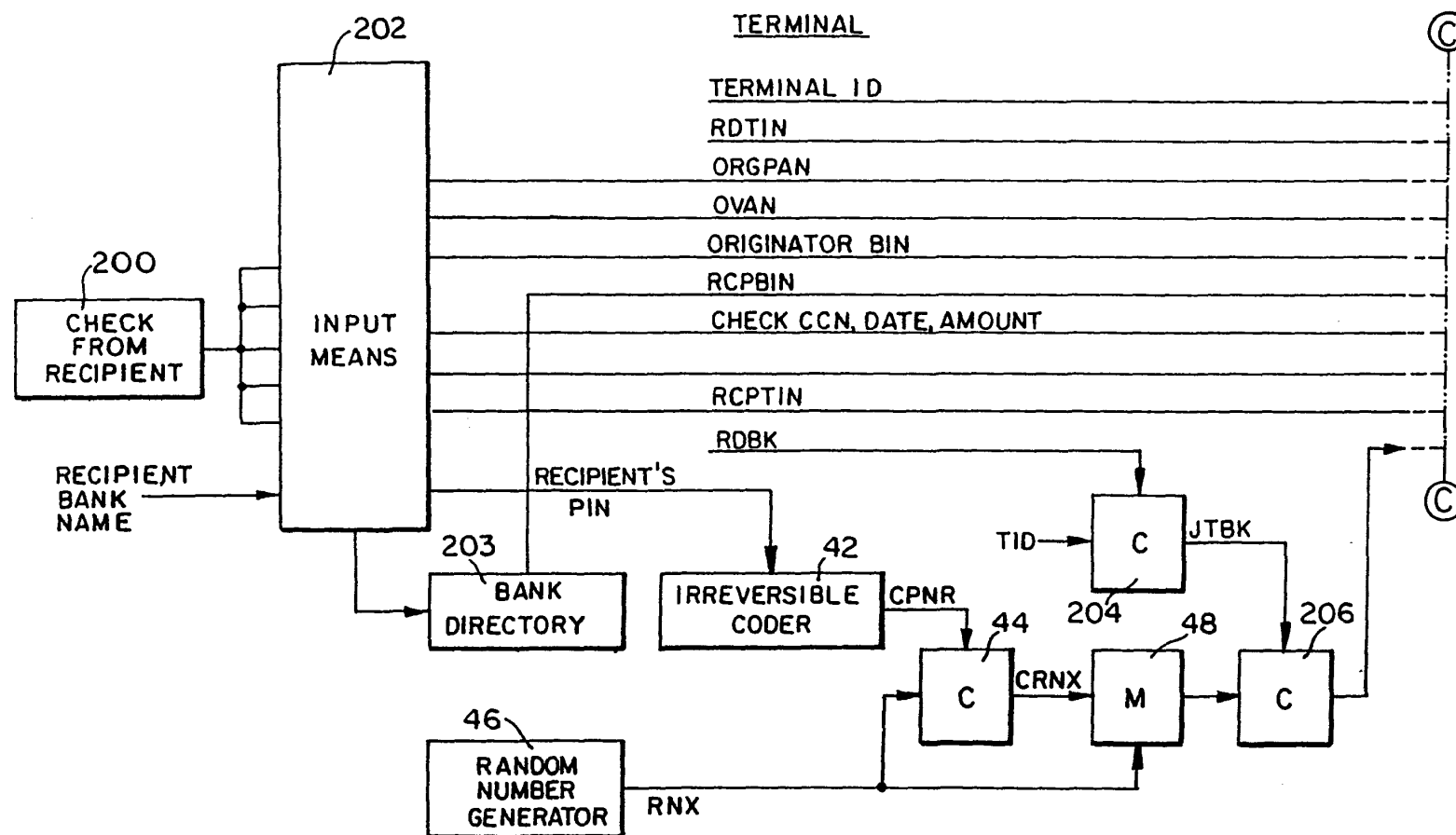


FIG. 13B

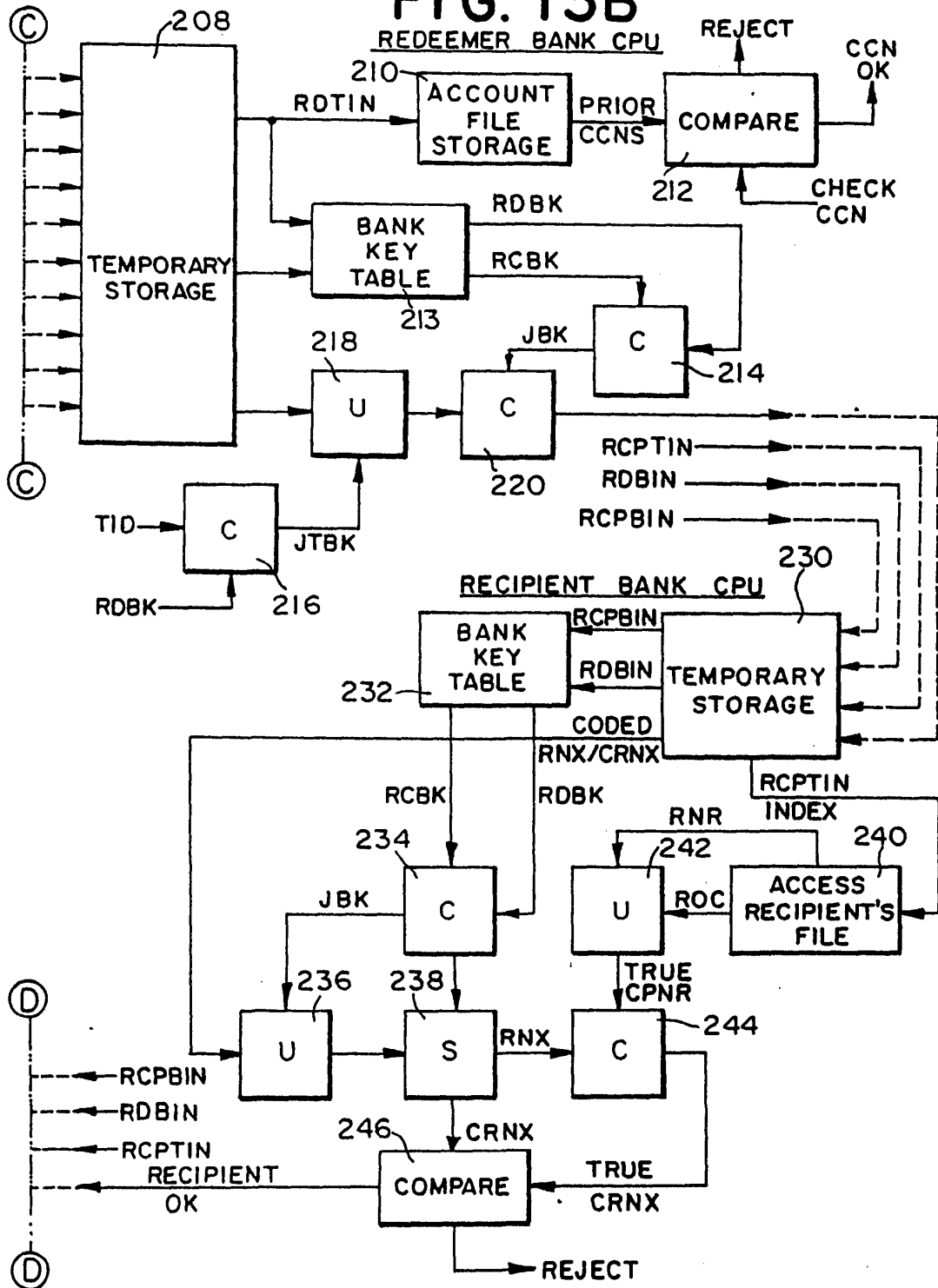


FIG. 13C

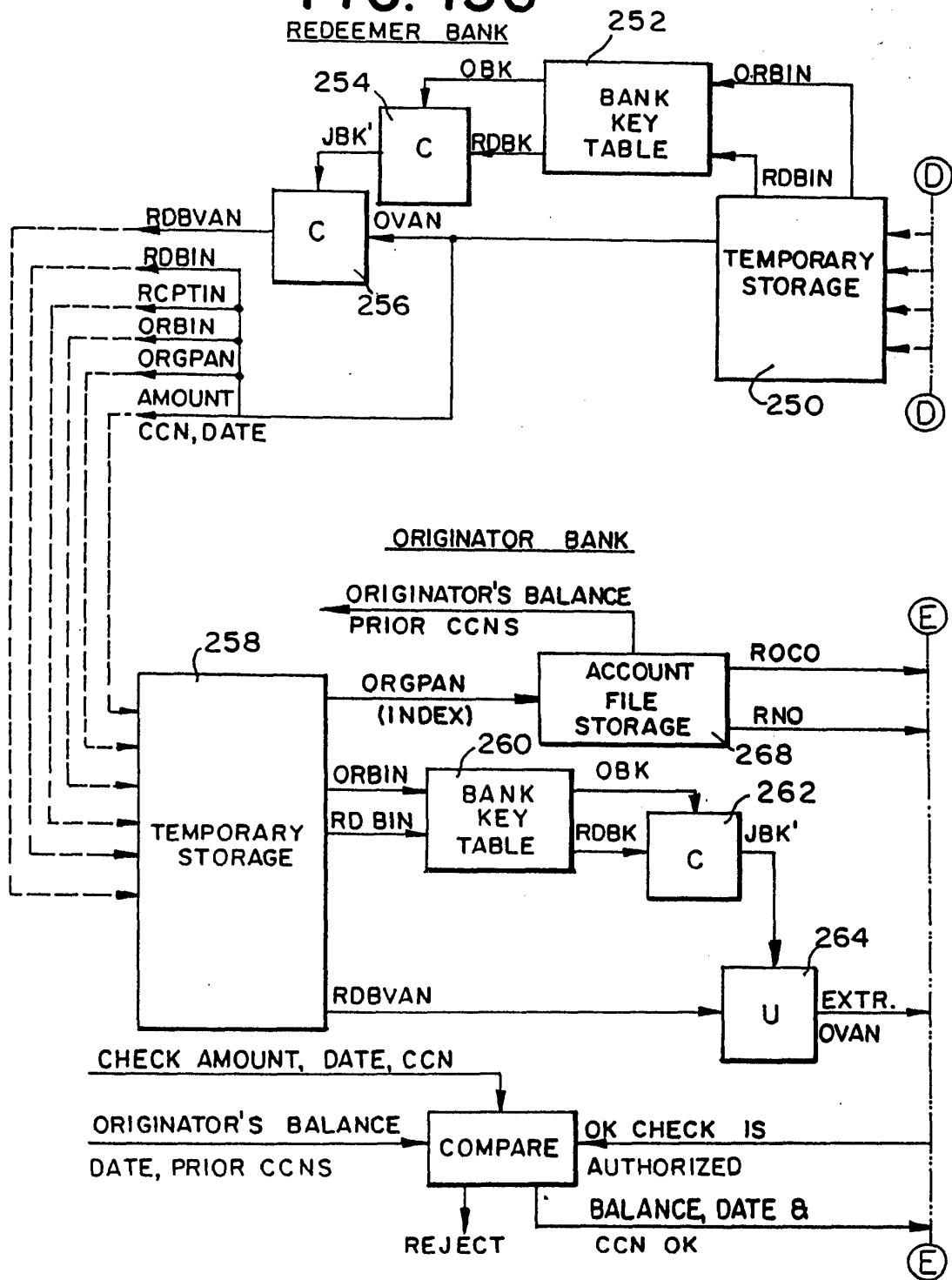


FIG. 13D

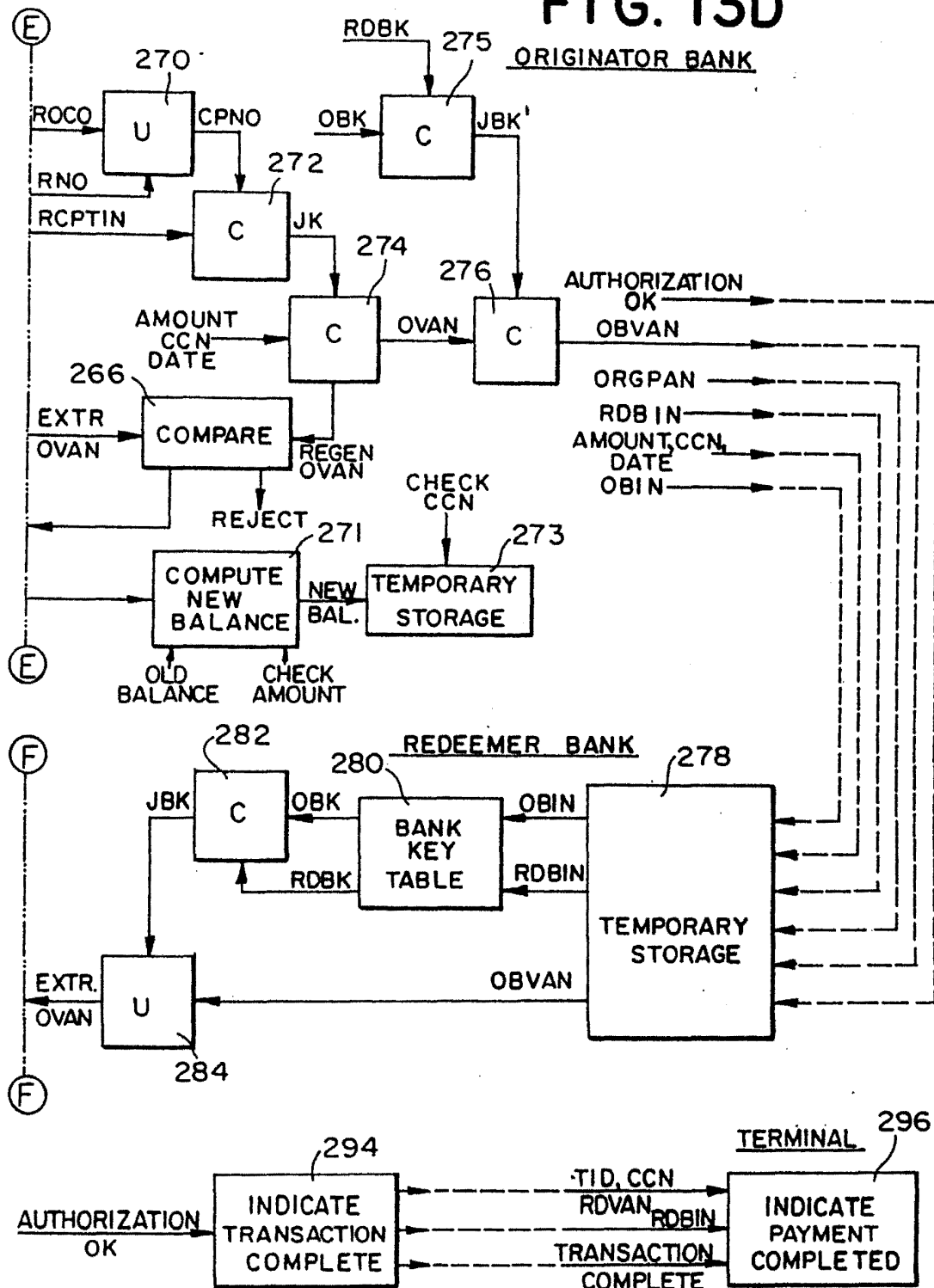


FIG. 13E

REDEEMER BANK

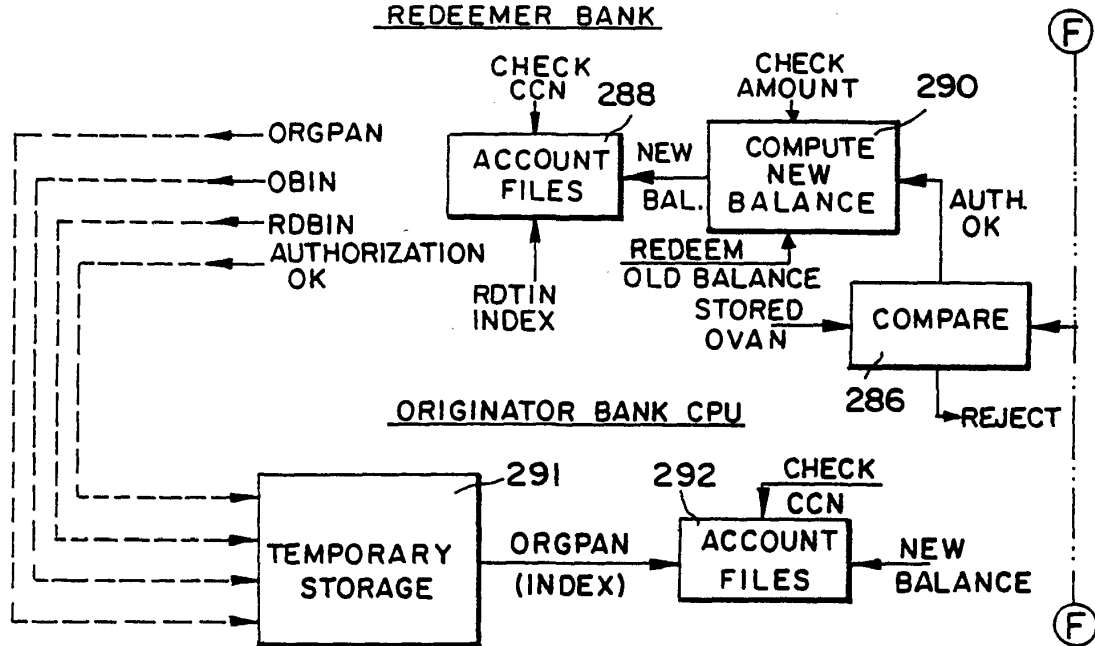


FIG. 14

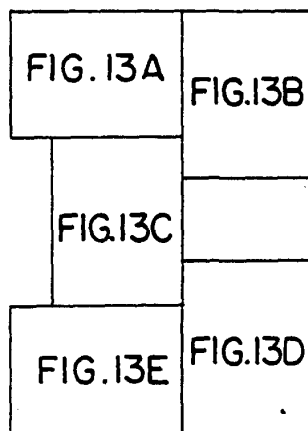
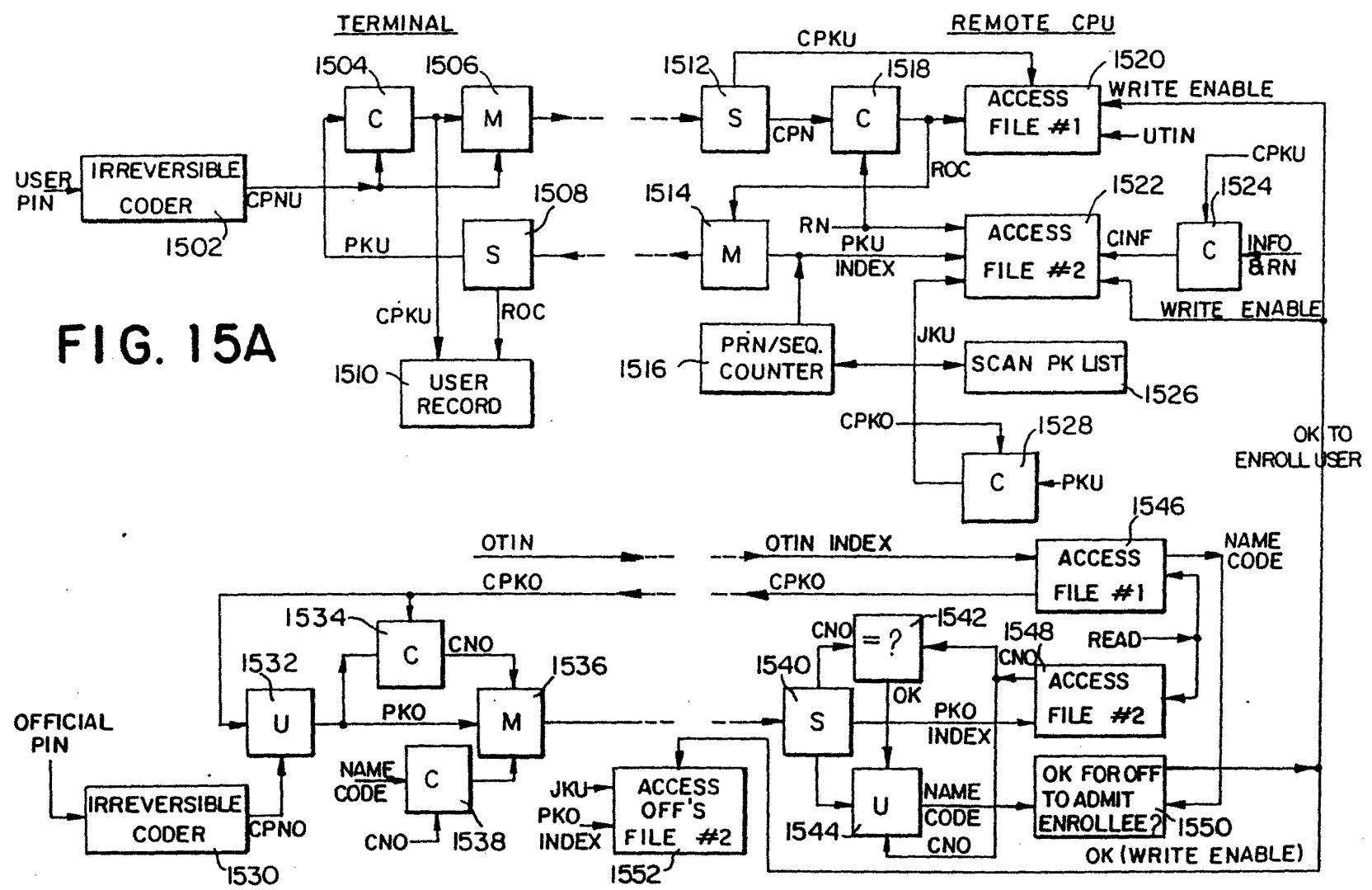


FIG. 15A
 BY [Signature]
 DATE [Date]
 TITLE [Title]
 [Stamp]





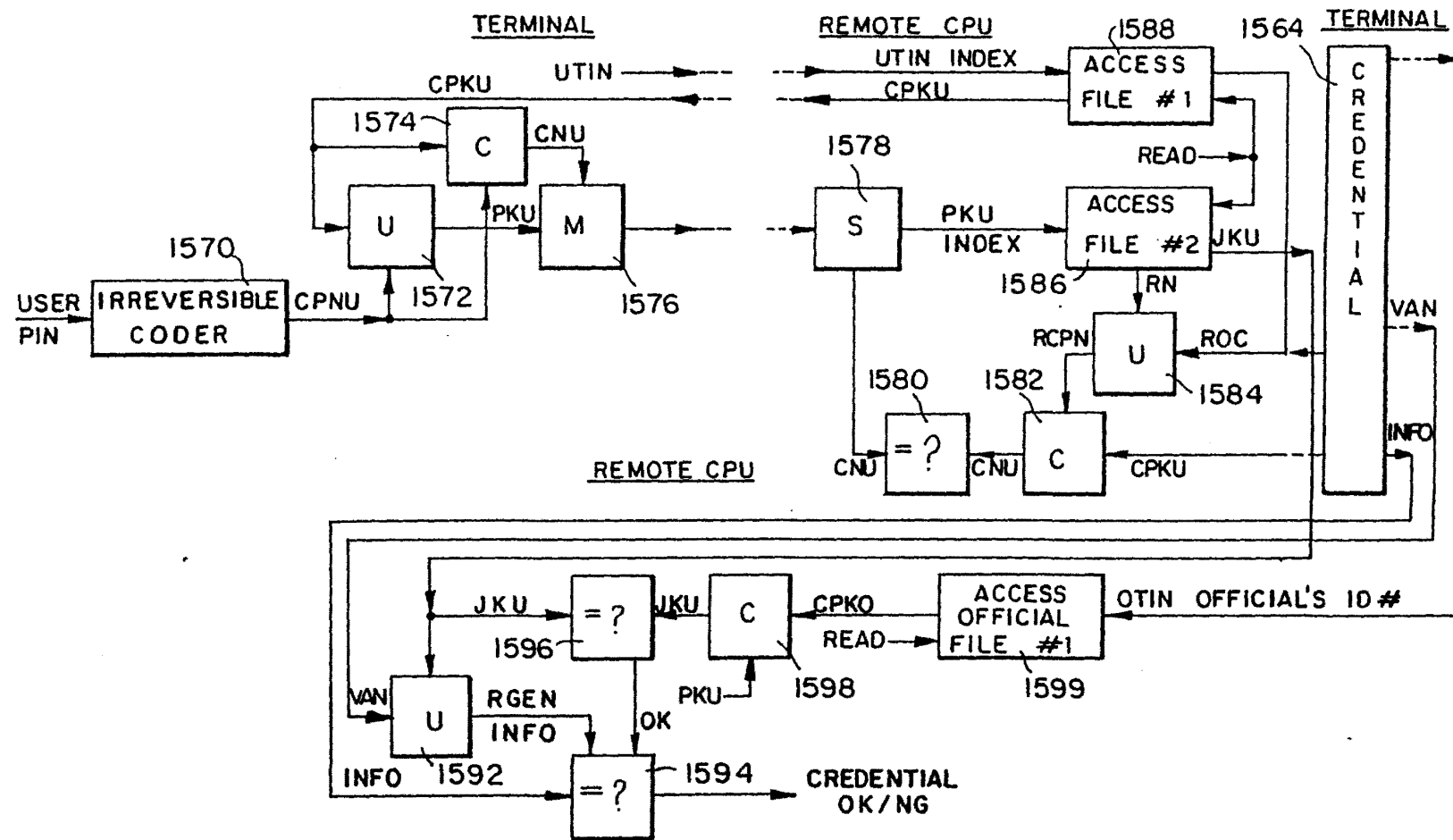


FIG. 15C

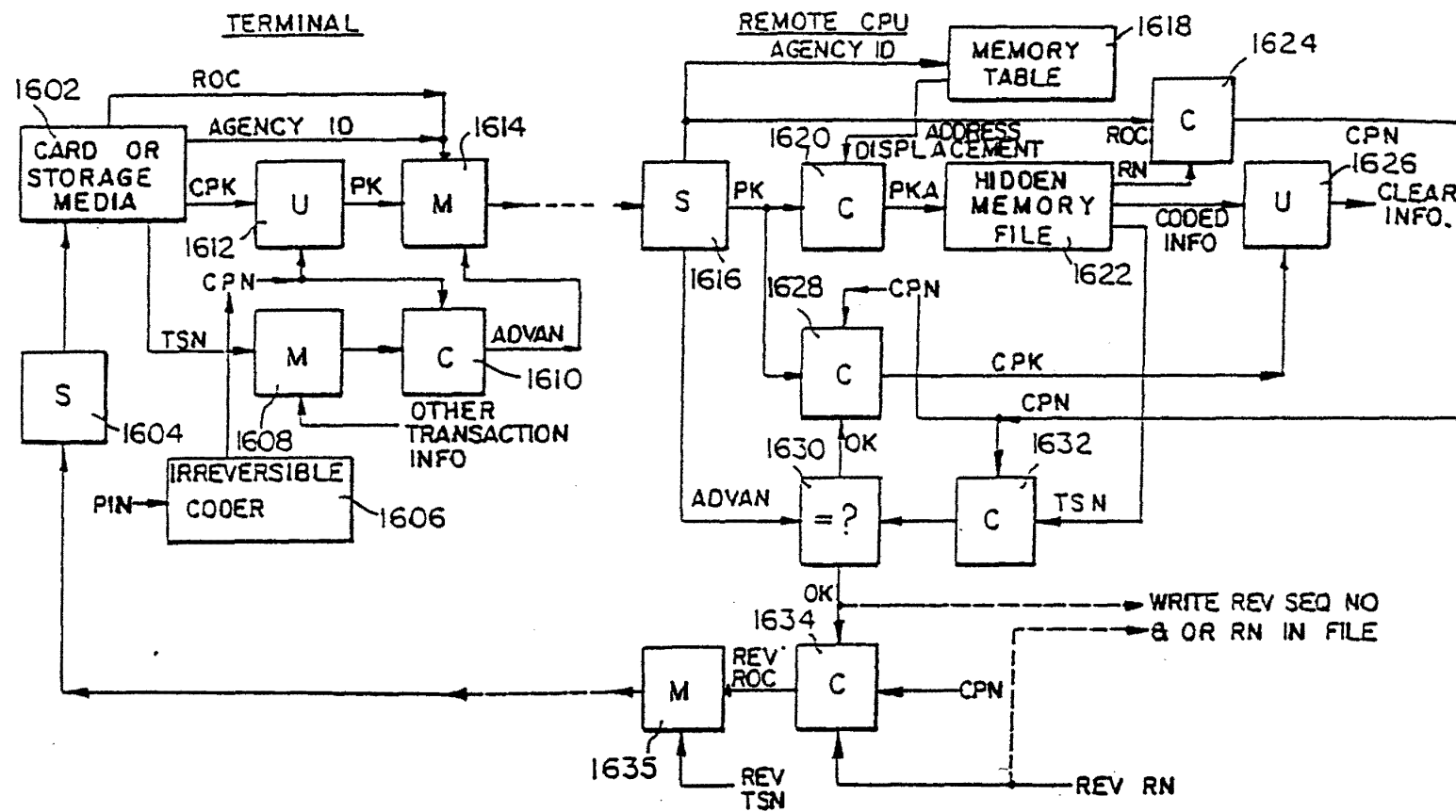


FIG. 16

PTO UTILITY GRANT

Paper Number 21

The
United
States
of
America



The Commissioner of Patents
and Trademarks

*Has received an application for a patent
for a new and useful invention. The title
and description of the invention are en-
closed. The requirements of law have
been complied with, and it has been de-
termined that a patent on the invention
shall be granted under the law.*

Therefore, this

United States Patent

*Grants to the person or persons having
title to this patent the right to exclude
others from making, using or selling the
invention throughout the United States
of America for the term of seventeen
years from the date of this patent, sub-
ject to the payment of maintenance fees
as provided by law.*

Bence Lehman

Commissioner of Patents and Trademarks

Margaret V. Turner

Attest

PTO-1584



C. f. c

PATENT

HEREBY CERTIFY THAT THIS CORRESPONDENCE IS BEING DEPOSITED WITH THE UNITED STATES POSTAL SERVICE AS FIRST CLASS MAIL IN AN ENVELOPE ADDRESSED TO: COMMISSIONER OF PATENTS AND TRADEMARKS, WASHINGTON, D.C. 20231, ON THE DATE INDICATED BELOW.

BY Louisa Drain DATE July 12, 1996

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re:	U.S. Patent No.	: Group Art Unit: 2202
	5,524,073	:
		:
Issued:	June 4, 1996	: Examiner: S. Cangialosi
		:
For:	SECURE TRANSACTION	: Attorney Docket
	SYSTEM AND METHOD	: No. 6074-1U1
	UTILIZED THEREIN	:

Attention: Decision and Certificate of Correction
Branch of the Patent Issue Division

REQUEST FOR CERTIFICATE OF CORRECTION
OF PATENT FOR PTO MISTAKE (37 CFR 1.322(a))

1. Attached, in duplicate, is Form PTO-1050, with at least one copy being suitable for printing

2. The exact page and line number where errors are shown correctly in the application file are:

Correction to column 26, line 23: see page 8, line 19 of Amendment After Final filed July 19, 1995 (entered by USPTO on July 21, 1995).

Correction to column 27, line 7: see page 10, line 3 of the Amendment After Final filed July 19, 1995 (entered by USPTO on July 21, 1995).

3. Please send the Certificate to:

Leslie L. Kasten, Esq.
PANITCH SCHWARZE JACOBS & NADEL, P.C.
1601 Market Street, 36th Floor
Philadelphia, PA 19103

Respectfully submitted,

LEON STAMBLER

July 11, 1996
(Date)

Leslie L. Kasten, Jr.
LESLIE L. KASTEN, JR.
Reg. No. 28,959
PANITCH SCHWARZE JACOBS & NADEL, P.C.
1601 Market Street, 36th Floor
Philadelphia, PA 19103
Telephone: (215) 567-2020
Facsimile: (215) 567-2991

LLK:lcd

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 5,524,073
DATED : June 4, 1996
INVENTOR(S) : Leon Stambler

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Column 26, line 23: "decoded" should read "encoded".
Column 27, line 7: "RVAN." should be inserted at the end of the line.

MAILING ADDRESS OF SENDER:

Leslie L. Kasten, Jr.
PANITCH SCHWARZE JACOBS & NADEL, P.C.
1601 Market Street, 36th Floor
Philadelphia, PA 19103

PATENT NO. 5,524,073

No. of add'l copies
@ 50¢ per page





UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office

ASSISTANT SECRETARY AND COMMISSIONER
OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

CHANGE OF ADDRESS/POWER OF ATTORNEY

LOCATION 9200 SERIAL NUMBER 08122071 PATENT NUMBER 5524073

THE CORRESPONDENCE ADDRESS HAS BEEN CHANGED TO CUSTOMER # 570

THE PRACTITIONERS OF RECORD HAVE BEEN CHANGED TO CUSTOMER # 570

THE FEE ADDRESS HAS BEEN CHANGED TO CUSTOMER # 570

ON 07/10/98 THE ADDRESS OF RECORD FOR CUSTOMER NUMBER 570 IS:

PANITCH SCHWARZE JACOBS & NADEL
ONE COMMERCE SQUARE
2005 MARKET STREET 22ND FLOOR
PHILADELPHIA PA 19103

AND THE PRACTITIONERS OF RECORD FOR CUSTOMER NUMBER 570 ARE:

22130	22825	25918	27363	27633	28959	28959	29546	32886	34626
35039	35039	35837	36317	36317	40961	40961	40961		

PTO INSTRUCTIONS: PLEASE TAKE THE FOLLOWING ACTION WHEN THE
CORRESPONDENCE ADDRESS HAS BEEN CHANGED TO CUSTOMER NUMBER:
RECORD, ON THE NEXT AVAILABLE CONTENTS LINE OF THE FILE JACKET,
'ADDRESS CHANGE TO CUSTOMER NUMBER'. LINE THROUGH THE OLD
ADDRESS ON THE FILE JACKET LABEL AND ENTER ONLY THE 'CUSTOMER
NUMBER' AS THE NEW ADDRESS. FILE THIS LETTER IN THE FILE JACKET.
WHEN ABOVE CHANGES ARE ONLY TO FEE ADDRESS AND/OR PRACTITIONERS
OF RECORD, FILE LETTER IN THE FILE JACKET.

PATENT APPLICATION FEE DETERMINATION RECORD Effective October 1, 1992						Application or Docket Number 12371	
CLAIMS AS FILED - PART I (Column 1) (Column 2)							
FOR	NUMBER FILED	NUMBER EXTRA					
BASIC FEE							
TOTAL CLAIMS		38	minus 20 = *	18			
INDEPENDENT CLAIMS		13	minus 3 = *	10			
MULTIPLE DEPENDENT CLAIM PRESENT							
* If the difference in column 1 is less than zero, enter "0" in column 2							
CLAIMS AS AMENDED - PART II (Column 1) (Column 2) (Column 3)							
AMENDMENT A		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		
	Total	* 59	Minus	**	=		
	Independent	* 17	Minus	***	=		
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM						
	(Column 1) 14 (Column 2) (Column 3)						
AMENDMENT B		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		
	Total	* 18	Minus	** 75	=		
	Independent	* 6	Minus	*** 13	=		
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM						
	(Column 1) (Column 2) (Column 3)						
AMENDMENT C		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		
	Total	*	Minus	**	=		
	Independent	*	Minus	***	=		
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM						
	(Column 1) (Column 2) (Column 3)						
						SMALL ENTITY OR OTHER THAN SMALL ENTITY	
						RATE	FEE
						x\$11=	\$355.00
						x 37=	198
						+115=	313
						TOTAL	973
						RATE	FEE
						x\$22=	\$710.00
						x 74=	
						+230=	
						TOTAL	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in Column 1.

PTO 1130		U.S. DEPARTMENT OF COMMERCE- PATENT & TRADEMARK OFFICE										1ST EXAMINER <i>Middleton</i>		DATE <i>10-20-93</i>			
(REV 11/91)		PACE DATA ENTRY CODING SHEET										2ND EXAMINER		DATE			
APPLICATION NUMBER				TYPE APPL	FILING DATE			SPECIAL HANDLING	GROUP ART UNIT		CLASS		SHEETS OF DRAWING				
08/122071				1	09/14/93			2	2202		380		115				
TOTAL CLAIMS		INDEPENDENT CLAIMS		SMALL ENTITY?		FILING FEE		FOREIGN LICENSE		ATTORNEY DOCKET NUMBER							
-38		-13		1		-947		X		60741111							
CONTINUITY DATA																	
CONTINUITY CODE		STATUS CODE	PARENT APPLICATION SERIAL NUMBER					PARENT PATENT NUMBER				PARENT FILING DATE					
01		2	7977385									11/17/92					
PCT/FOREIGN APPLICATION DATA																	
FOREIGN PRIORITY CLAIMED		COUNTRY CODE			PCT/FOREIGN APPLICATION SERIAL NUMBER										FOREIGN FILING DATE		
															MONTH DAY YEAR		

MULTIPLE DEPENDENT CLAIM FEE CALCULATION SHEET (FOR USE WITH FORM PTO-875)							SERIAL N 122071	FILING DATE					
							APPLICANT(S)						
CLAIMS													
	AS FILED		AFTER 1st AMENDMENT		AFTER 2nd AMENDMENT			*		*		*	
	IND.	DEP.	IND.	DEP.	IND.	DEP.		IND.	DEP.	IND.	DEP.	IND.	DEP.
1							51						
2							52						
3							53						
4							54						
5							55						
6							56	/					
7	/						57	/					
8		/					58	/					
9		/					59	/					
10		/					60						
11		/					61						
12		/					62						
13		/					63	/					
14		/					64						
15		/					65						
16		/					66						
17	/						67						
18		/					68						
19		/					69						
20	/						70						
21		/					71						
22		/					72						
23		/					73						
24		/					74						
25		/					75						
26		/					76						
27		/					77						
28	/						78						
29		/					79						
30	/						80						
31		/					81						
32		/					82						
33	/						83						
34		/					84						
35		/					85						
36	/						86						
37							87						
38							88						
39							89						
40							90						
41							91						
42							92						
43							93						
44							94						
45	/						95						
46	/						96						
47		/					97						
48	/						98						
49		/					99						
50	/	/					100						
TOTAL IND.	8						TOTAL IND.	5					
TOTAL DEP.	25						TOTAL DEP.						
TOTAL CLAIMS	33						TOTAL CLAIMS	5					

PTO-1360 (3-78)

*MAY BE USED FOR ADDITIONAL CLAIMS OR AMENDMENTS

U.S. DEPARTMENT of COMMERCE
Patent and Trademark Office

Staple Issue Slip Here

POSITION	ID NO.	DATE
CLASSIFIER	18	6/14/93
EXAMINER	76	10-20-93
TYPIST	219	10-20-93
VERIFIER	338	10-20-93
CORPS CORR.		
SPEC. HAND		
FILE MAINT.		
DRAFTING		

INDEX OF CLAIMS

Claim	Date
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	
25	
26	
27	
28	
29	
30	
31	
32	
33	
34	
35	
36	
37	
38	
39	
40	
41	
42	
43	
44	
45	
46	
47	
48	
49	
50	

Claim	Date
Final	
Original	
5	
10	
7	
94	
95	
51	
52	
53	
54	
55	
56	
57	
58	
59	
60	
61	
62	
63	
64	
65	
66	
67	
68	
69	
70	
71	
72	
73	
74	
75	
76	
77	
78	
79	
80	
81	
82	
83	
84	
85	
86	
87	
88	
89	
90	
91	
92	
93	
94	
95	
96	
97	
98	
99	
100	

SYMBOLS

- ✓ Rejected
- Allowed
- (Through numeral) Canceled
- + Restricted
- N Non-elected
- I Interference
- A Appeal
- O Objected

(LEFT INSIDE)