

38

SERIAL NUMBER (Series of 1987) 07/977,385	PATENT DATE NOV 30 1993	PATENT NUMBER	5267314		
SERIAL NUMBER 07/977,385	FILING DATE 11/17/92	CLASS 380	SUBCLASS 24	GROUP ART UN 2202	*5267314*

LEON STAMBLER, PARKLAND, FL.

APPLICANTS

CONTINUING DATA***
VERIFIED
PZ

FOREIGN/PCT APPLICATIONS***
VERIFIED
PZ

FOREIGN FILING LICENSE GRANTED 12/11/92 ***** SMALL ENTITY *****

Foreign priority claimed 35 USC 119 conditions met	<input type="checkbox"/> yes <input checked="" type="checkbox"/> no <input type="checkbox"/> yes <input checked="" type="checkbox"/> no	AS FILED	STATE OR COUNTRY FL	SHEETS DRWGS. 15	TOTAL CLAIMS 63	INDEP. CLAIMS 18	FILING FEE RECEIVED \$1,383.00	ATTORNEY'S DOCKET NO. 6074-1
Verified and Acknowledged Examiner's Initials PZ								

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

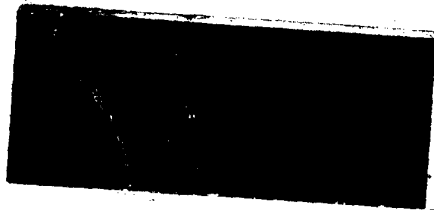
TITLE
SECURE TRANSACTION SYSTEM AND METHOD UTILIZED THEREIN

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

PARTS OF APPLICATION FILED SEPARATELY		NOTICE OF ALLOWANCE MAILED 7-22-93		PREPARED FOR ISSUE 7-22-93		CLAIMS ALLOWED	
		Assistant Examiner		Docket Clerk		Total Claims 27	
ISSUE FEE		SALVATORE CANGIALOSI PRIMARY EXAMINER ART UNIT 222 h. Cangialosi Primary Examiner				DRAWING	
Amount Due \$865.00	Date Paid 8-23-93					Sheets Drwg. 15	
		ISSUE CLASSIFICATION				ISSUE BATCH NUMBER	
		Class 380		Subclass 24		P08	
Label Area		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.					

m PTO-436
r. 9/90

07 1385



APPROVED FOR LICENSE ☐

INITIALS DEC 08 1992 36

Entered
or
Counted

CONTENTS

Received
or
Mailed

	1. Application	papers.	
1/27	2. Rejection 3mos		2-2-93
	3. Prior Art w/ AH		2-1-93
	4. Invt A		3-2-93
6/10	5. Rejection 30 days		6-11-93
	6. Election of B		7-1-93
7/22	7. Notice of Allowability		7-22-93
	8. Notice of Allowance		7-22-93
9/2	9. Final drawing (5 sheets)		9-2-93
	10. PTO GRANT NOV 30 1993		
	11.		
	12.		
	13.		
	14.		
	15.		
	16.		
	17.		
	18.		
	19.		
	20.		
	21.		
	22.		
	23.		
	24.		
	25.		
	26.		
	27.		

Staple Issue Slip Here

POSITION	INIT.	DATE
CLASSIFIER	211	12/4/92
EXAMINER		12-11-92
TYPIST	329	12-11-92
VERIFIER	291	12-14
CORPS CORR.		
SPEC. HAND		
FILE MAINT.		

INDEX OF CLAIMS

Claim	Final	Original	Date
1	1	13	9/2/93
2	2	3	9/2/93
3	3	5	9/2/93
4	4	6	9/2/93
5	5	7	9/2/93
6	6	8	9/2/93
7	7	9	9/2/93
8	8	10	9/2/93
9	9	11	9/2/93
10	10	12	9/2/93
11	11	13	9/2/93
12	12	14	9/2/93
13	13	15	9/2/93
14	14	16	9/2/93
15	15	17	9/2/93
16	16	18	9/2/93
17	17	19	9/2/93
18	18	20	9/2/93
19	19	21	9/2/93
20	20	22	9/2/93
21	21	23	9/2/93
22	22	24	9/2/93
23	23	25	9/2/93
24	24	26	9/2/93
25	25	27	9/2/93
26	26	28	9/2/93
27	27	29	9/2/93
28	28	30	9/2/93
29	29	31	9/2/93
30	30	32	9/2/93
31	31	33	9/2/93
32	32	34	9/2/93
33	33	35	9/2/93
34	34	36	9/2/93
35	35	37	9/2/93
36	36	38	9/2/93
37	37	39	9/2/93
38	38	40	9/2/93
39	39	41	9/2/93
40	40	42	9/2/93

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

Claim	Final	Original	Date
15	15	51	9/2/93
16	16	52	9/2/93
17	17	53	9/2/93
18	18	54	9/2/93
19	19	55	9/2/93
20	20	56	9/2/93
21	21	57	9/2/93
22	22	58	9/2/93
23	23	59	9/2/93
24	24	60	9/2/93
25	25	61	9/2/93
26	26	62	9/2/93
27	27	63	9/2/93
28	28	64	9/2/93
29	29	65	9/2/93
30	30	66	9/2/93
31	31	67	9/2/93
32	32	68	9/2/93
33	33	69	9/2/93
34	34	70	9/2/93
35	35	71	9/2/93
36	36	72	9/2/93
37	37	73	9/2/93
38	38	74	9/2/93
39	39	75	9/2/93
40	40	76	9/2/93
41	41	77	9/2/93
42	42	78	9/2/93
43	43	79	9/2/93
44	44	80	9/2/93
45	45	81	9/2/93
46	46	82	9/2/93
47	47	83	9/2/93
48	48	84	9/2/93
49	49	85	9/2/93
50	50	86	9/2/93
51	51	87	9/2/93
52	52	88	9/2/93
53	53	89	9/2/93
54	54	90	9/2/93
55	55	91	9/2/93

SEARCHED			
Class	Sub.	Date	Exmr.
380	23		
	24		
	25	1/11/93	P7
380	4	6/93	SR
380	4	7/93	SR

SEARCH NOTES		
	Date	Exmr.
Consulted with S. Calgialosi	1/7/93	P7

INTERFERENCE SEARCHED			
Class	Sub.	Date	Exmr.
380	4, 23, 25 24	7/93	guc

07 977385

PATENT APPLICATION SERIAL NO. _____

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

0320033 12/02/92 07977385 16-0235 020 201 1,303.0000 6074 1

97733

- 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.



6074-1

46

07 977385A

- 1 -

**SECURE TRANSACTION SYSTEM
AND METHOD UTILIZED THEREIN**

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.

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.

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
5 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
10 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
15 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

20 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
25 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
30 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
35 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 de-multiplexer 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

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,

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 ROCO and random number, RNO, are extracted from the originator's file at block 50. ROCO 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,
5 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
10 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
15 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
20 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,
25 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
30 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
35 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.

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

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.

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, 5 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 10 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 15 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, 20 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 25 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 30 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

5 "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

10 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

15 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.

20 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

25 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

30 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,

35 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

(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.

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.

30 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).

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, 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 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 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 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 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 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 should be the same as the actual INFO recorded on the credential.

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

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.

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.

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
5 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
10 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
15 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
20 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
25 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 RDBVAN, which is transmitted to the originator's bank, along with various transaction information and the information from the check. RDBVAN
30 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
35 table at block 260, whereby OBK and RDBK are extracted in the same manner as in block 252. The joint key JBK'

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

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

The redeemer's bank also communicates with the
5 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.

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

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

(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 CPKU 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

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

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,
5 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
10 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
15 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.
20 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
25 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.

30 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
35 is then transmitted along with CNU and PKU to the remote CPU over an unsecured medium. At the remote CPU, the

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

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

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.

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

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

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). 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 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.

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). 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 CNO previously recorded thereon. In this event, access to file no. 1 is unnecessary.

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 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, 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 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 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 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 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 information which appears at the bottom of an originator's check) or the originator's TIN and BIN.

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

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.

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.

CLAIMS

- Sub a'* → 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:
- 5 receiving a PIN from the party to be authenticated;
- 10 addressing the storage means using the predetermined address to locate the party information and to retrieve the first coded authentication information;
- 15 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
- 20 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.
- 25 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 information stored in the storage means are non-secret.
- 30 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.
- Sub B1* →

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.

Sub 4a
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;

associating the VAN with the transaction;

5 deriving the coded authentication information using the predetermined secret and non-secret codes; and

authenticating the VAN associated with the transaction using the derived coded authentication
10 information.

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

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

Sub 24 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.

Sub 24 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.~~

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:
receiving at a first site a personal
10 identification number from the party;
generating second coded authentication information by using the received personal identification number;
transmitting at least the second coded
15 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.

Sub 25
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
storing the joint code in a first storage
10 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 A6
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.

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.

5 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 6 37. The method of claim 5 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.

7 38. The method of claim 6 37, wherein the non-secret information associated with the party is the
30 coded secret address.

8 39. The method of claim 5 38, 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;

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

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

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

transmitting at least the first coded
15 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
25 authentication information and the coded secret address;
and

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

30 ⁸ 940. The method of claim 29, 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.

1041. 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.

1142. 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. 11

1243. 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.

1344. 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.

145. The method of claim 43, wherein the step
5 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
10 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.

Sub a 15 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:

20 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
25 funds transfer;

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

30 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.

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.

15 *Sub 28* 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.

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 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 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:

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 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 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 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.

¹⁶~~52~~. The method of claim ¹⁵~~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.

1753. The method of claim ¹⁵51, 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.

1854. The method of claim ¹⁵51, further comprising the step of revising the TSN, the secret number, and/or the coded address.

1955. The method of claim ¹⁵51, wherein the communication link is unsecured.

Sub 29
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:

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.

2060. A system for authenticating a party comprising:

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

10 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;

20 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.

2101. The system of claim 20, wherein the second storage means is a storage medium in the possession of the party.

30 2102. 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 *Sub a* 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.

addition

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

Inventor's Signature Leon Stambler

Date 11/16/92

Residence ~~Parkland~~ ~~Park Land~~, Florida FL JS 11/16/92

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 _____



Patent

Attorney Docket No. 6074-1

Applicant or Patentee: Leon Stambler
Serial or Patent No.: To Be Assigned
Filed or Issued: Filed Herewith
For: SECURE TRANSACTION SYSTEM AND METHOD UTILIZED THEREIN

**VERIFIED STATEMENT (DECLARATION) CLAIMING SMALL ENTITY STATUS
(37 CFR 1.9(f) and 1.27(b)) - INDEPENDENT INVENTOR**

As a below named inventor, I hereby declare that I qualify as an independent inventor as defined in 37 CFR 1.9(c) for purposes of paying reduced fees under Sections 41(a) and (b) of Title 35, United States Code, to the Patent and Trademark Office with regard to the invention entitled

SECURE TRANSACTION SYSTEM AND METHOD UTILIZED THEREIN
described in

☒ the specification filed herewith.
☐ Application Serial No. _____
Filed _____
☐ Patent No. _____
Issued _____

I have not assigned, granted, conveyed or licensed and am under no obligation under contract or law to assign, grant, convey or license, any rights in the invention to any person who could not be classified as an independent inventor under 37 CFR 1.9(c) if that person had made the invention, or to any concern which would not qualify as a small business concern under 37 CFR 1.9(d) or a nonprofit organization under 37 CFR 1.9(e).

Each person, concern or organization to which I have assigned, granted, conveyed, or licensed or am under an obligation under contract or law to assign, grant, convey or license any rights in the invention is listed below:

☒ no such person, concern or organization.
☐ persons, concerns or organizations listed below.*

*NOTE: Separate verified statements are required from each named person, concern or organization having rights to the invention averring to their status as small entities (37 CFR 1.27)

FULL NAME N/A
ADDRESS _____

☐ Individual ☐ Small Business Concern ☐ Nonprofit Organization

FULL NAME _____
ADDRESS _____

☐ Individual ☐ Small Business Concern ☐ Nonprofit Organization

I acknowledge the duty to file, in this application or patent, notification of any change in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the issue fee or any maintenance fee due after the date on which status as a small entity is no longer appropriate. (37 CFR 1.28(b))

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, any patent issuing thereon, or any patent to which this verified statement is directed.

Leon Stambler		
NAME OF INVENTOR	NAME OF INVENTOR	NAME OF INVENTOR
<i>Leon Stambler</i>		
Signature of Inventor	Signature of Inventor	Signature of Inventor
<i>11/16/92</i>		
DATE	DATE	DATE

PANITCH SCHWARZE JACOBS & NADEL
FIVE PENN CENTER PLAZA - 1601 Market St
SUITE 3600
PHILADELPHIA, PA 19103

FILE NO. 6074-1

EXPRESS MAIL LABEL NO. TB255327688

380/24

FIG. 1

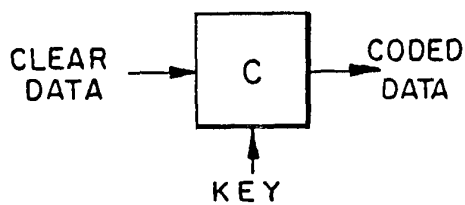


FIG. 2

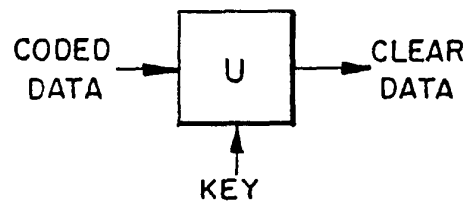


FIG. 3

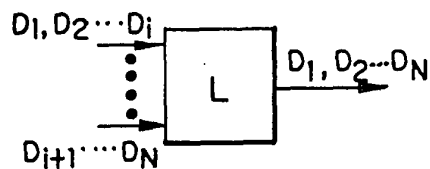


FIG. 4

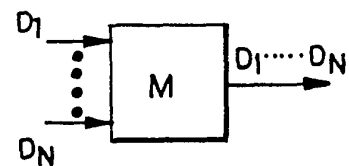


FIG. 5

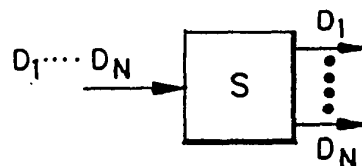
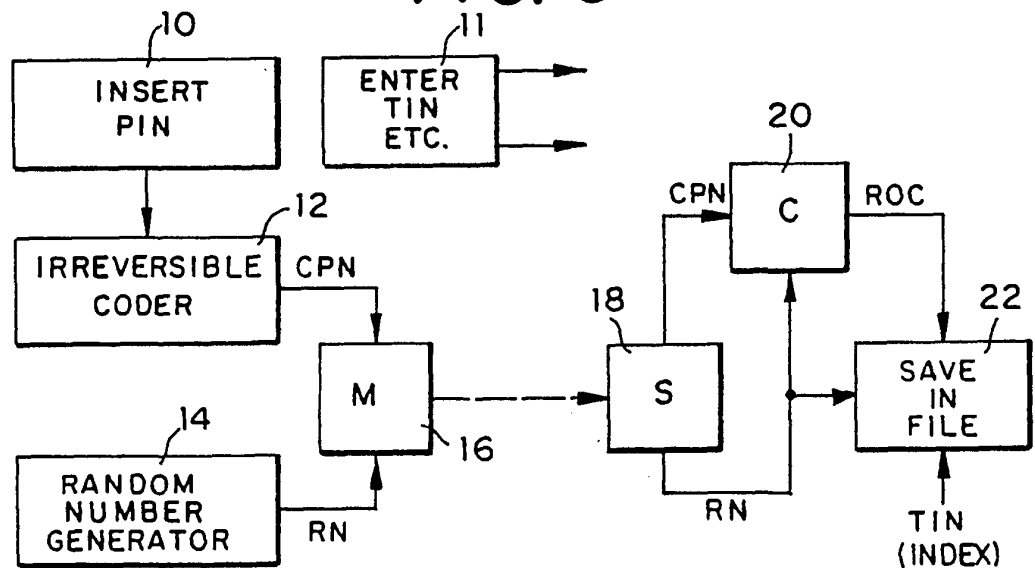
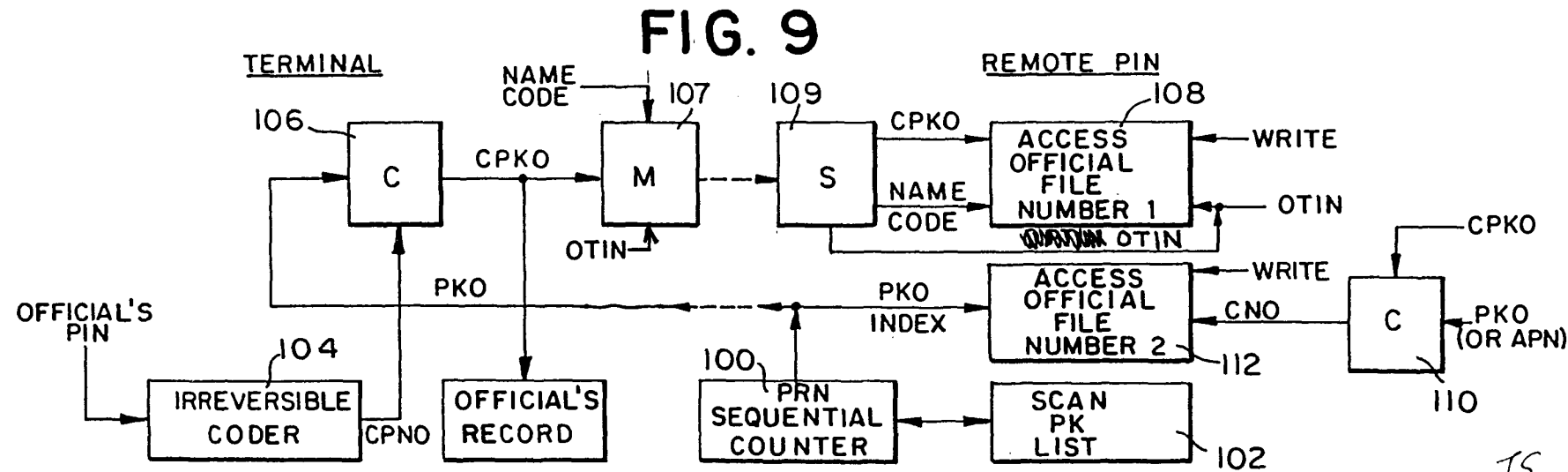
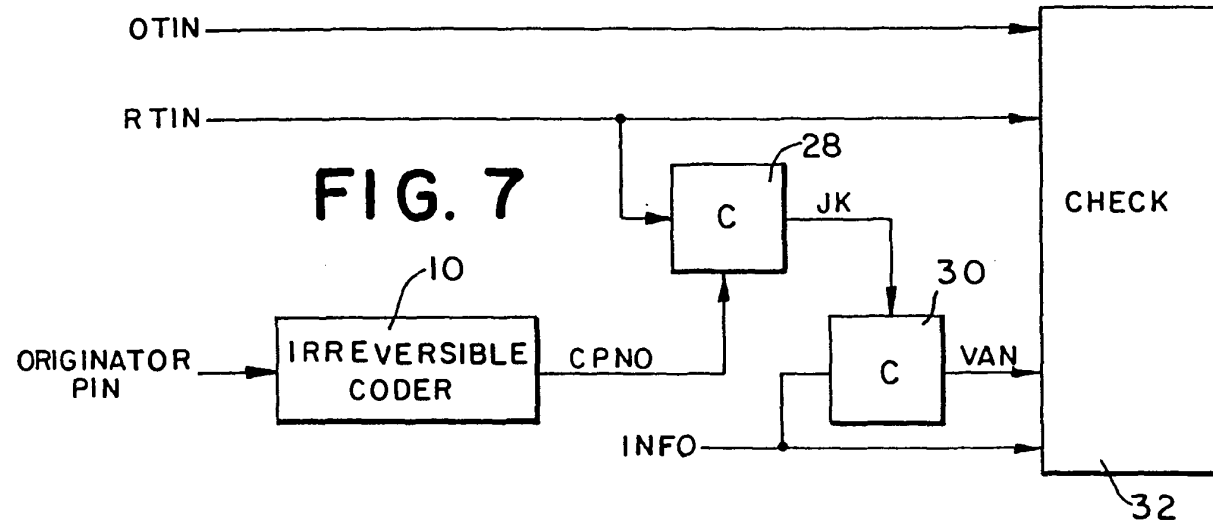


FIG. 6

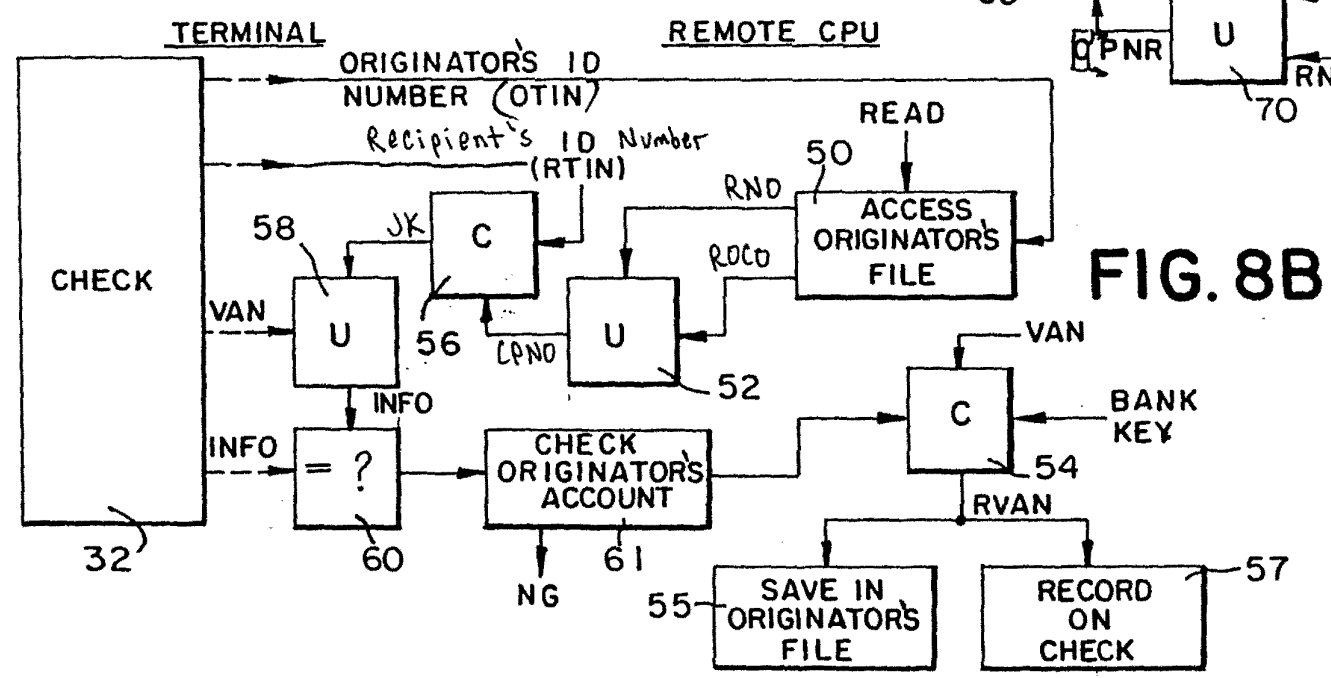
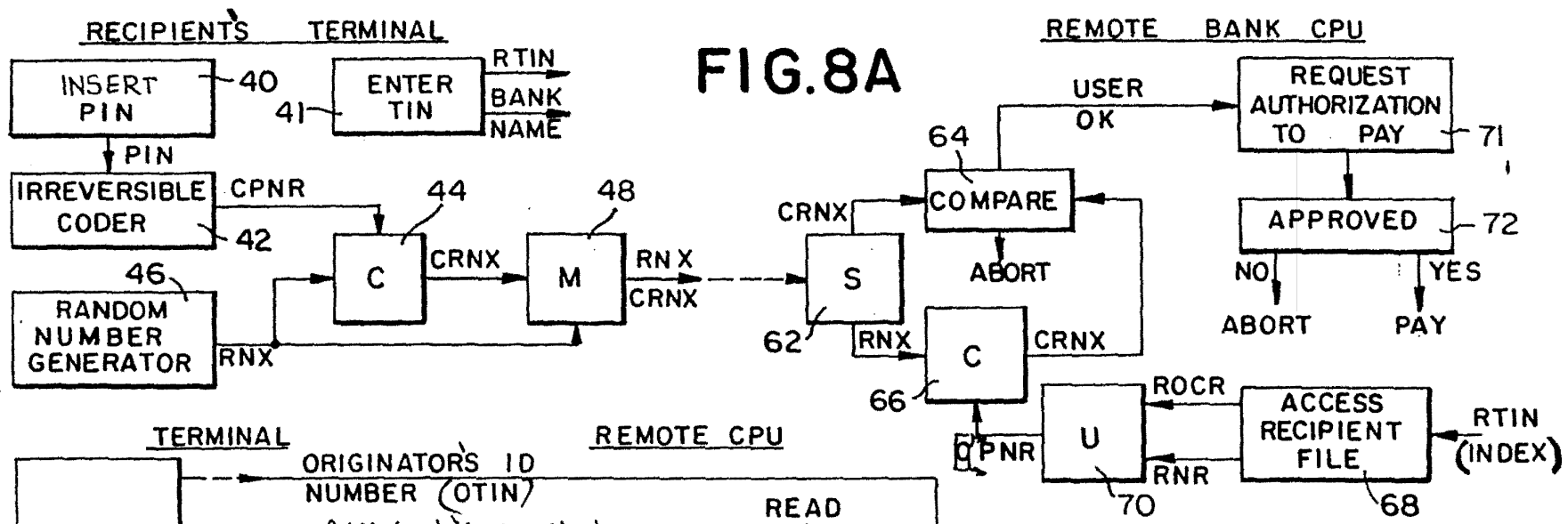




JS.
11/16/92

11 977305

NOT OF DRAWINGS
ORIGINALLY FILED



977385

JS
11/16/12

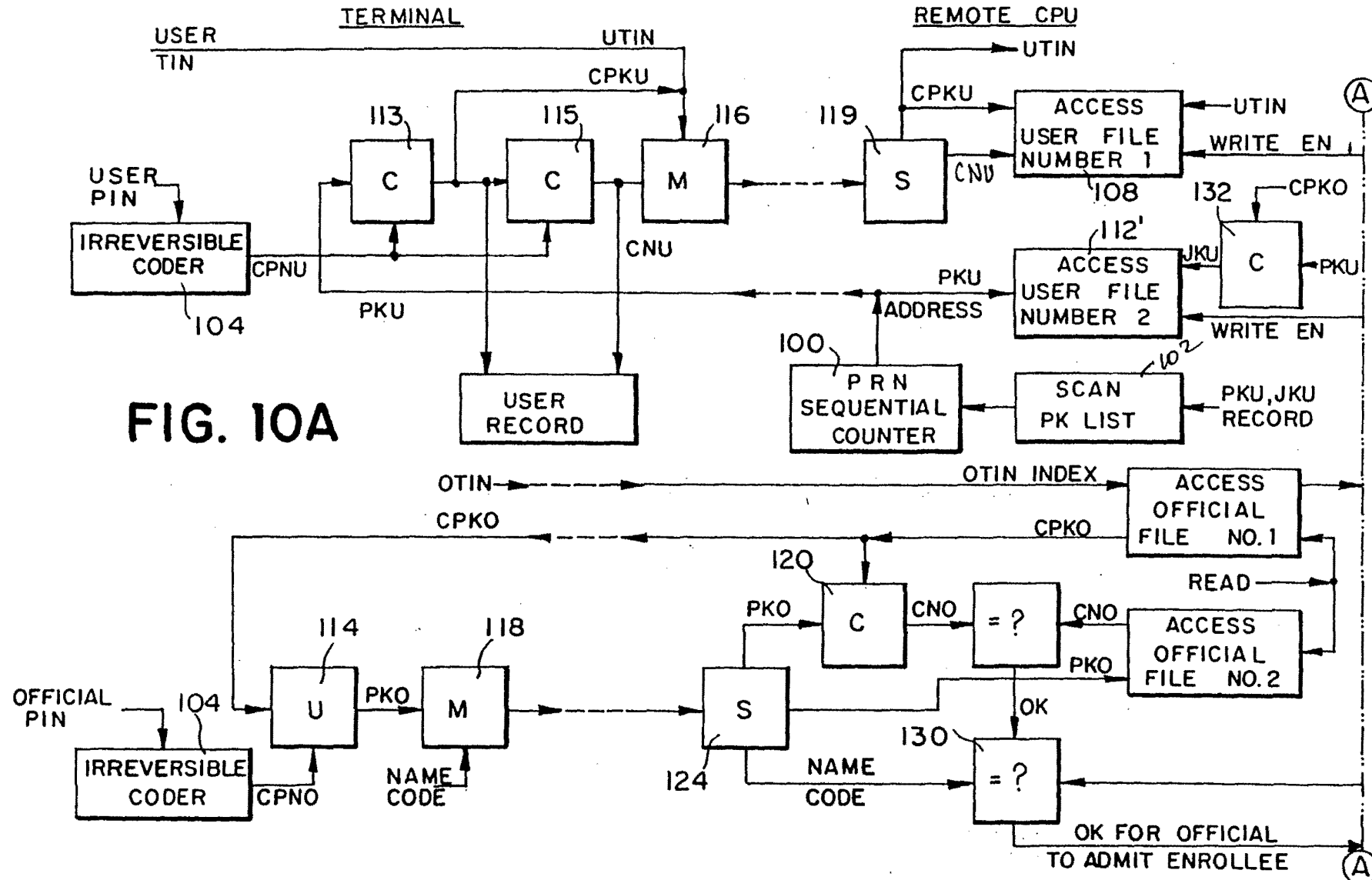


FIG. 10B

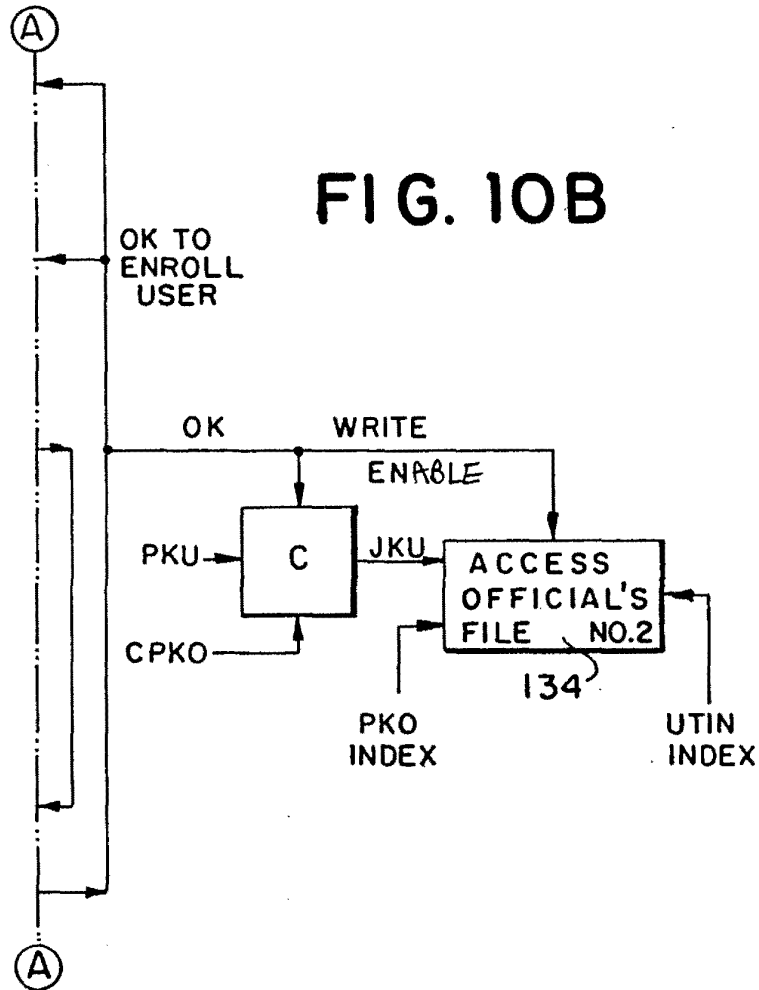
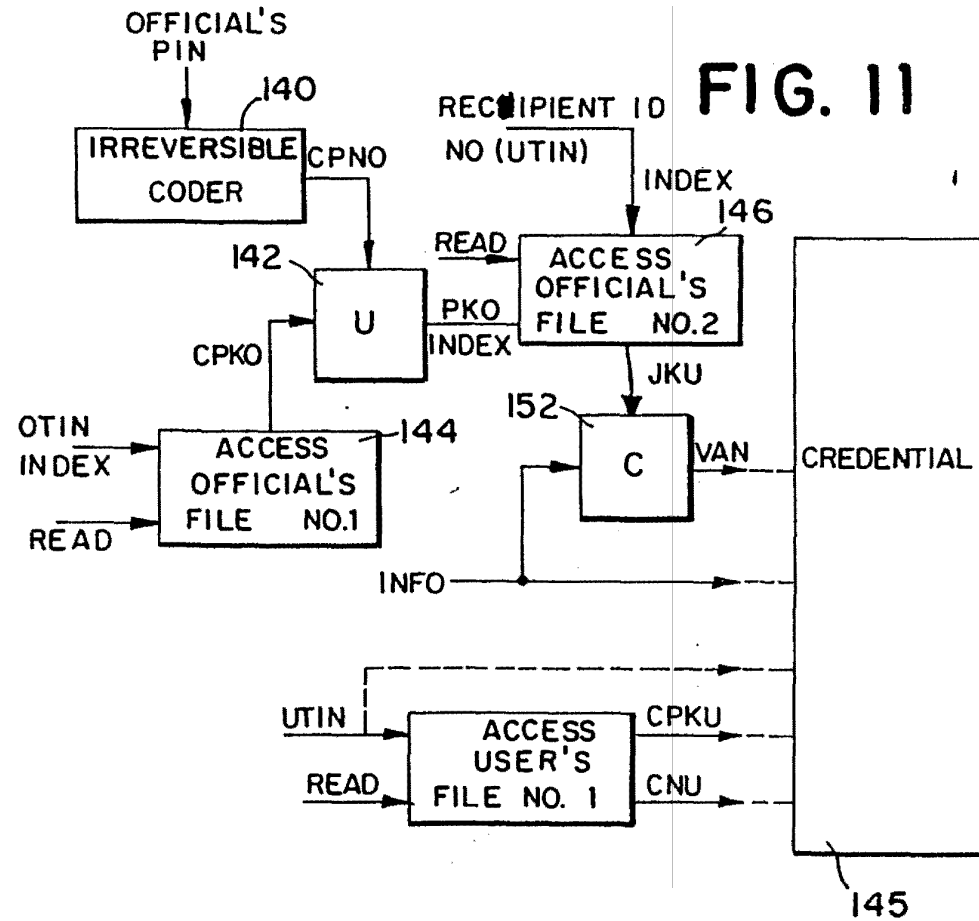


FIG. 11



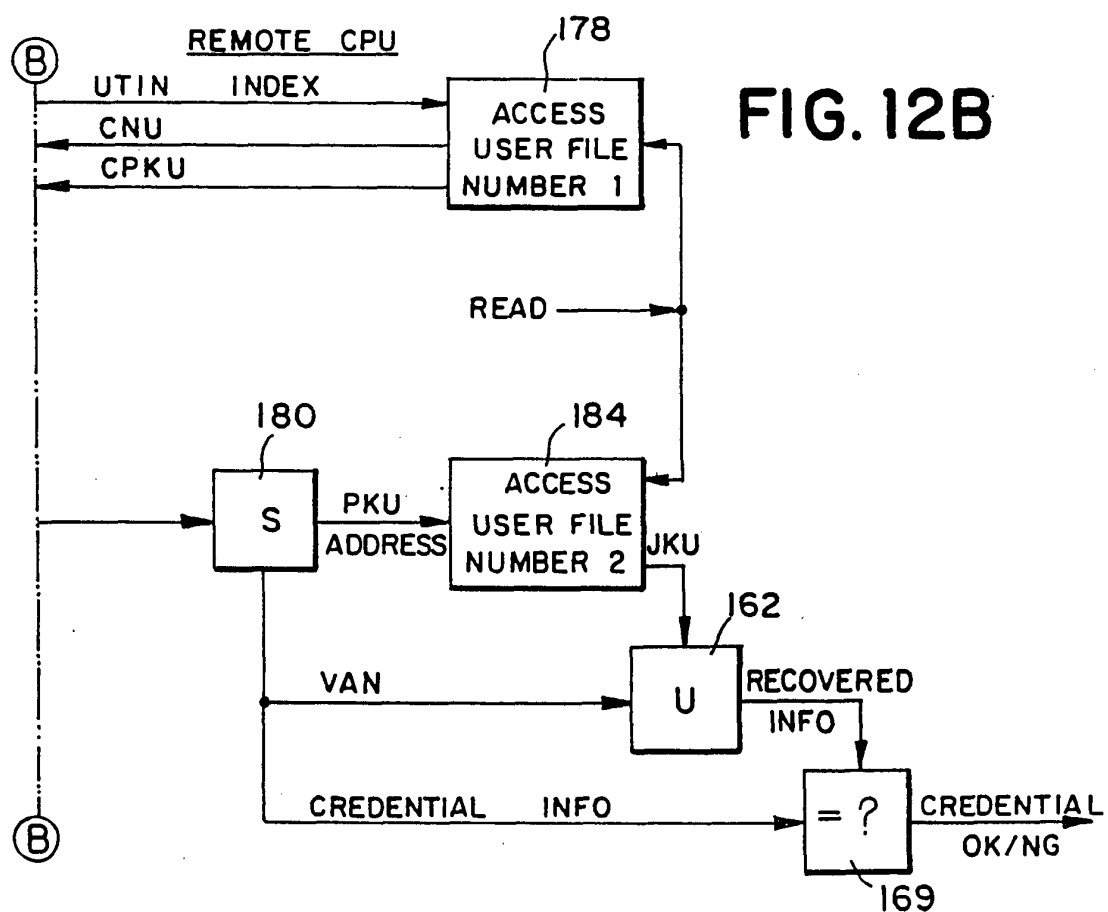
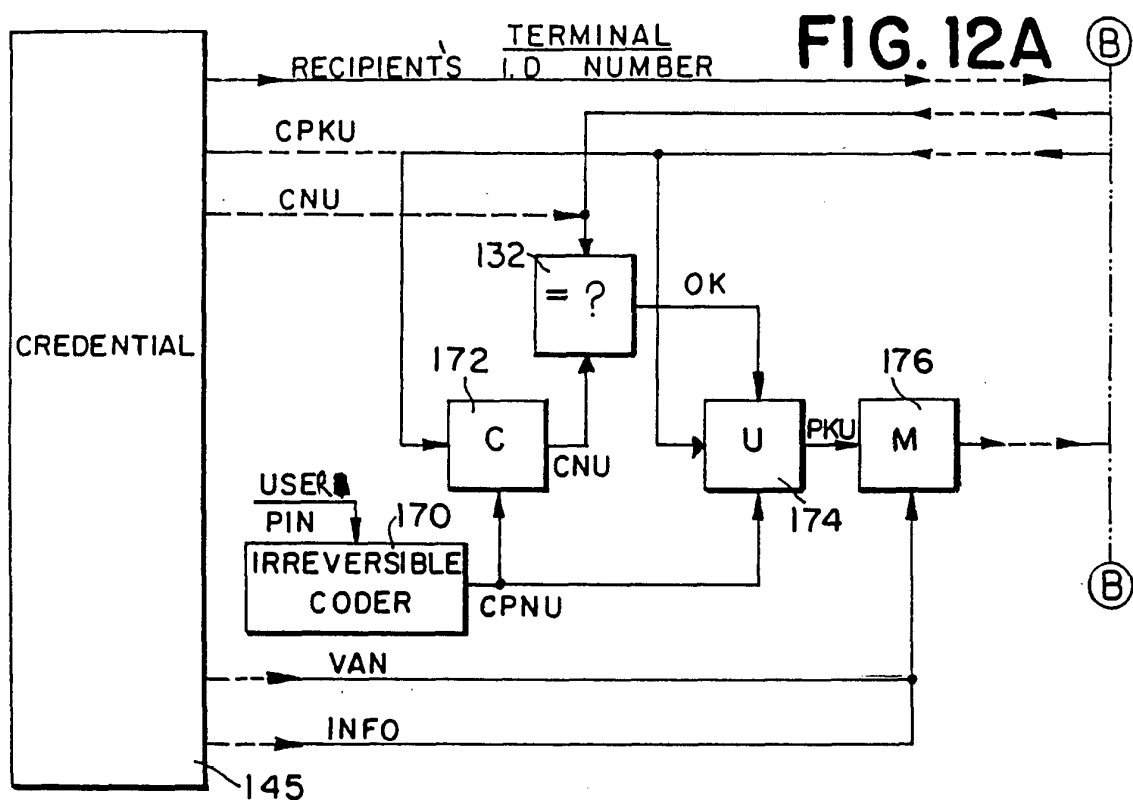
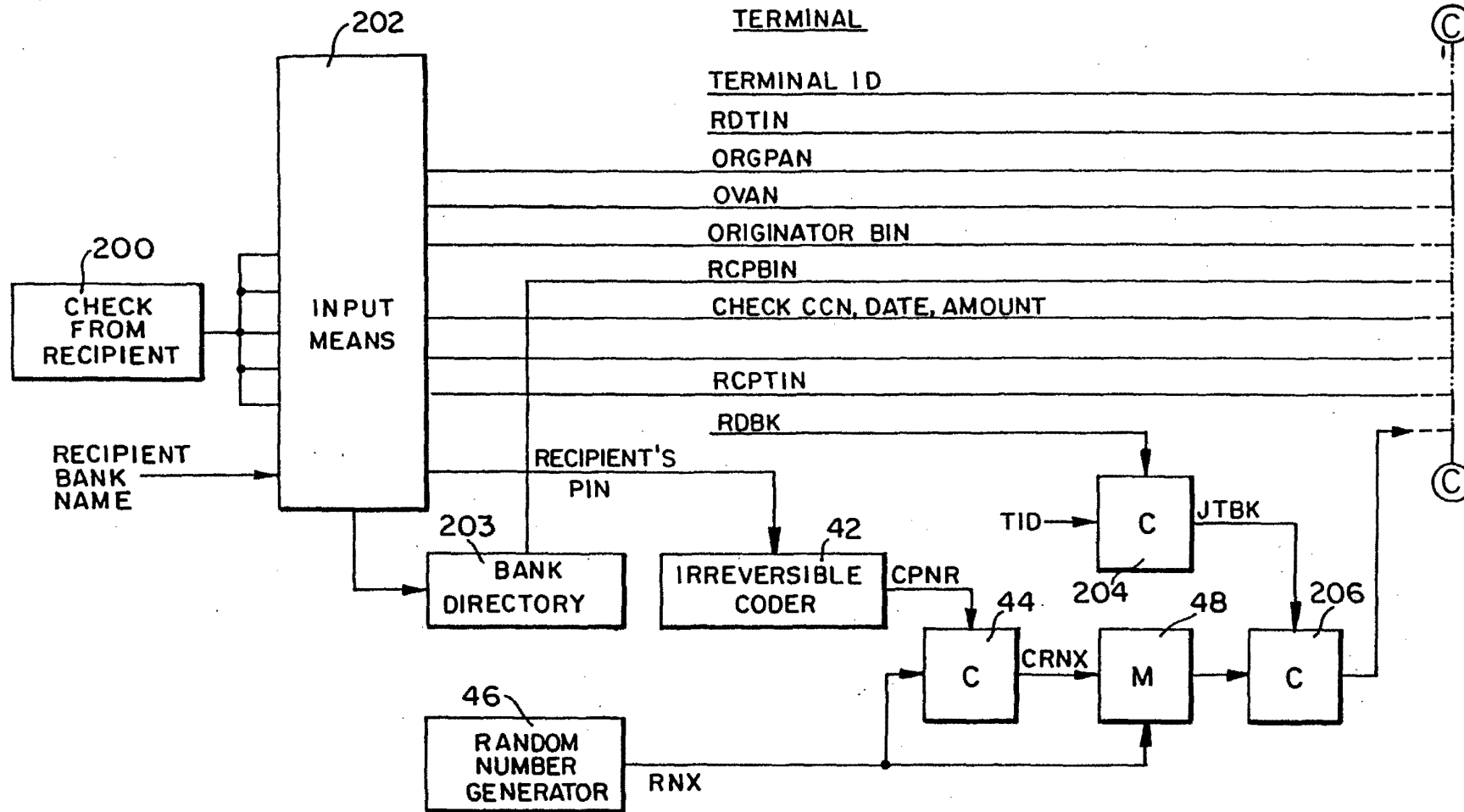


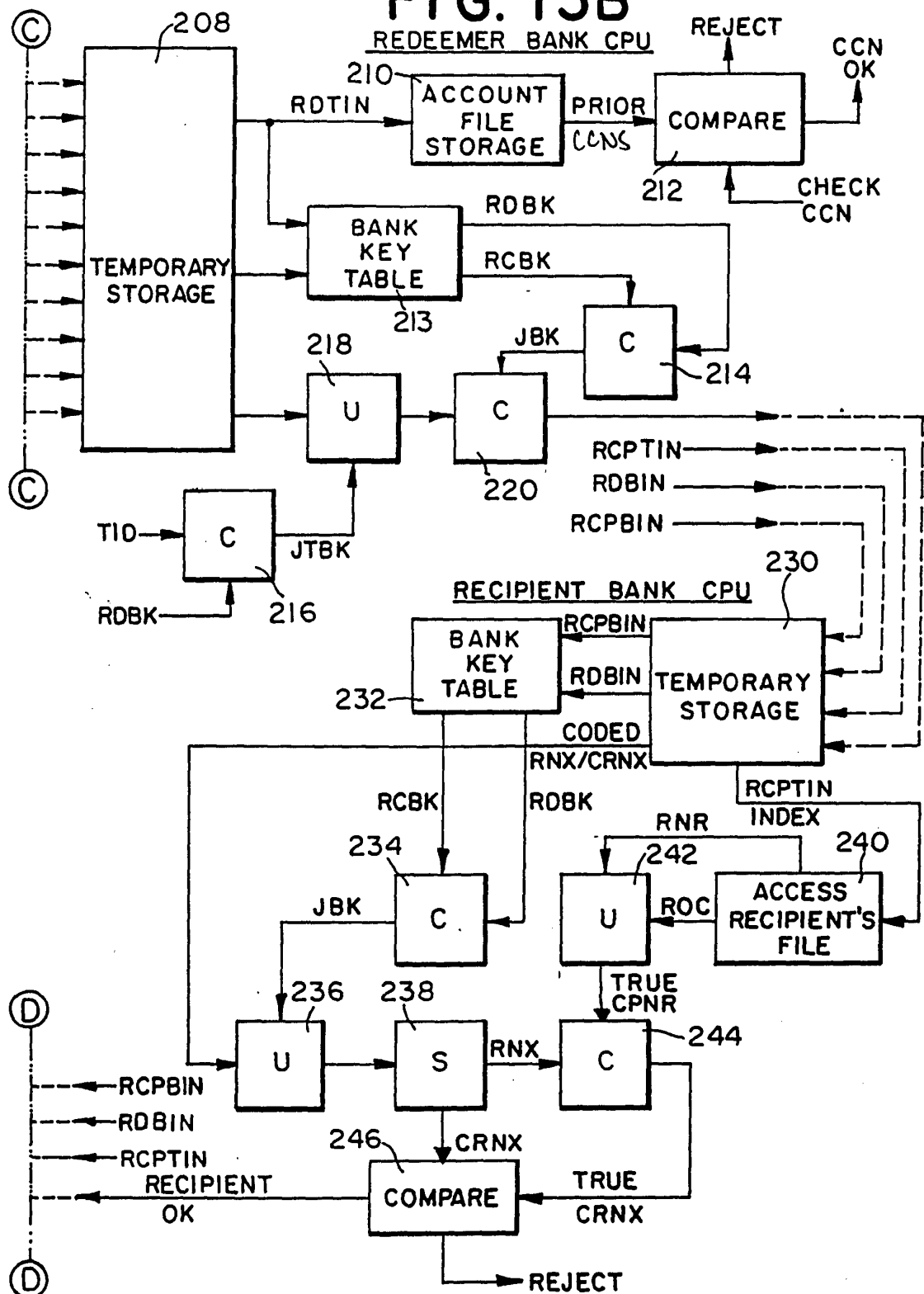
FIG. 13A



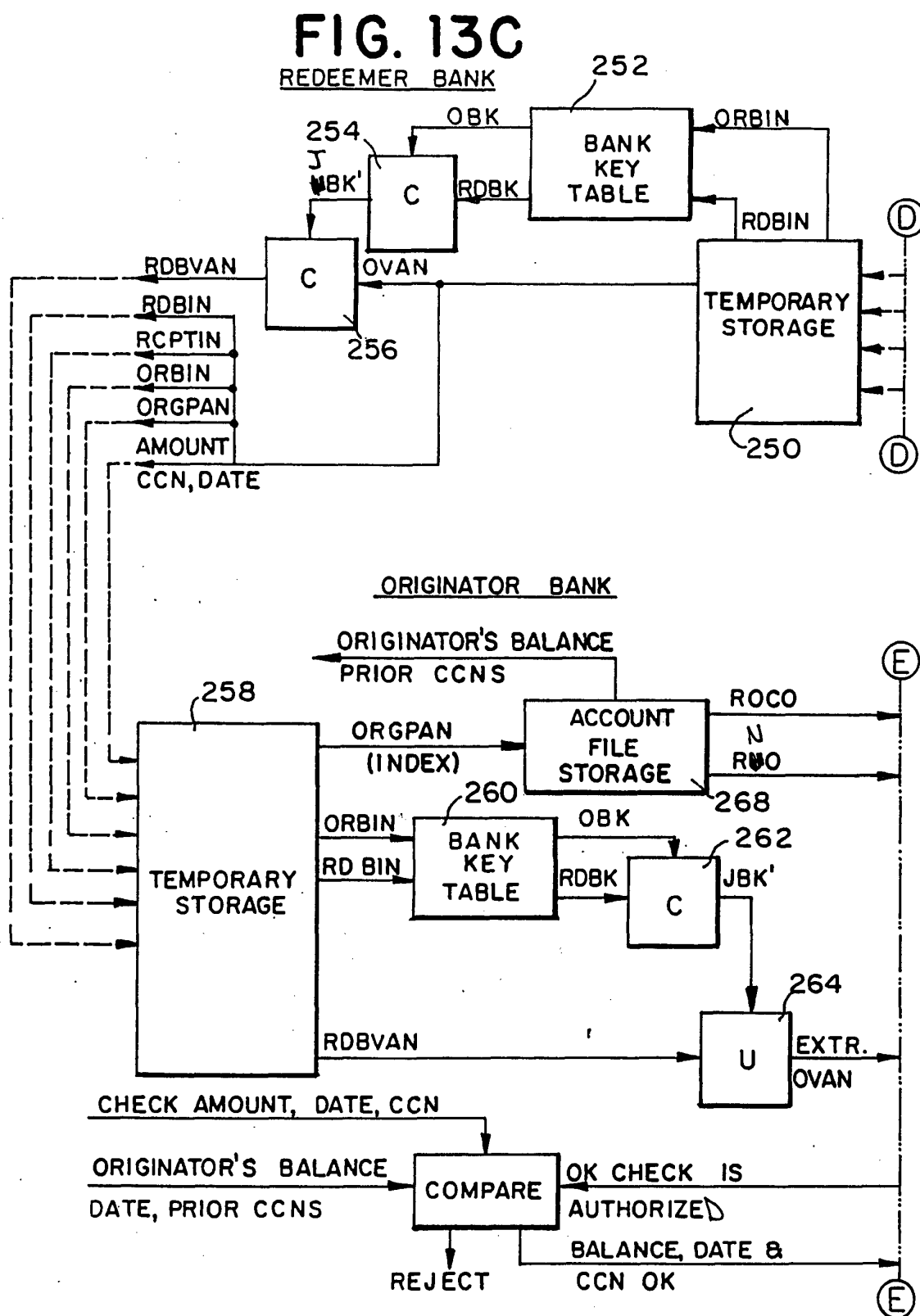
11 977385

07 977385

FIG. 13B

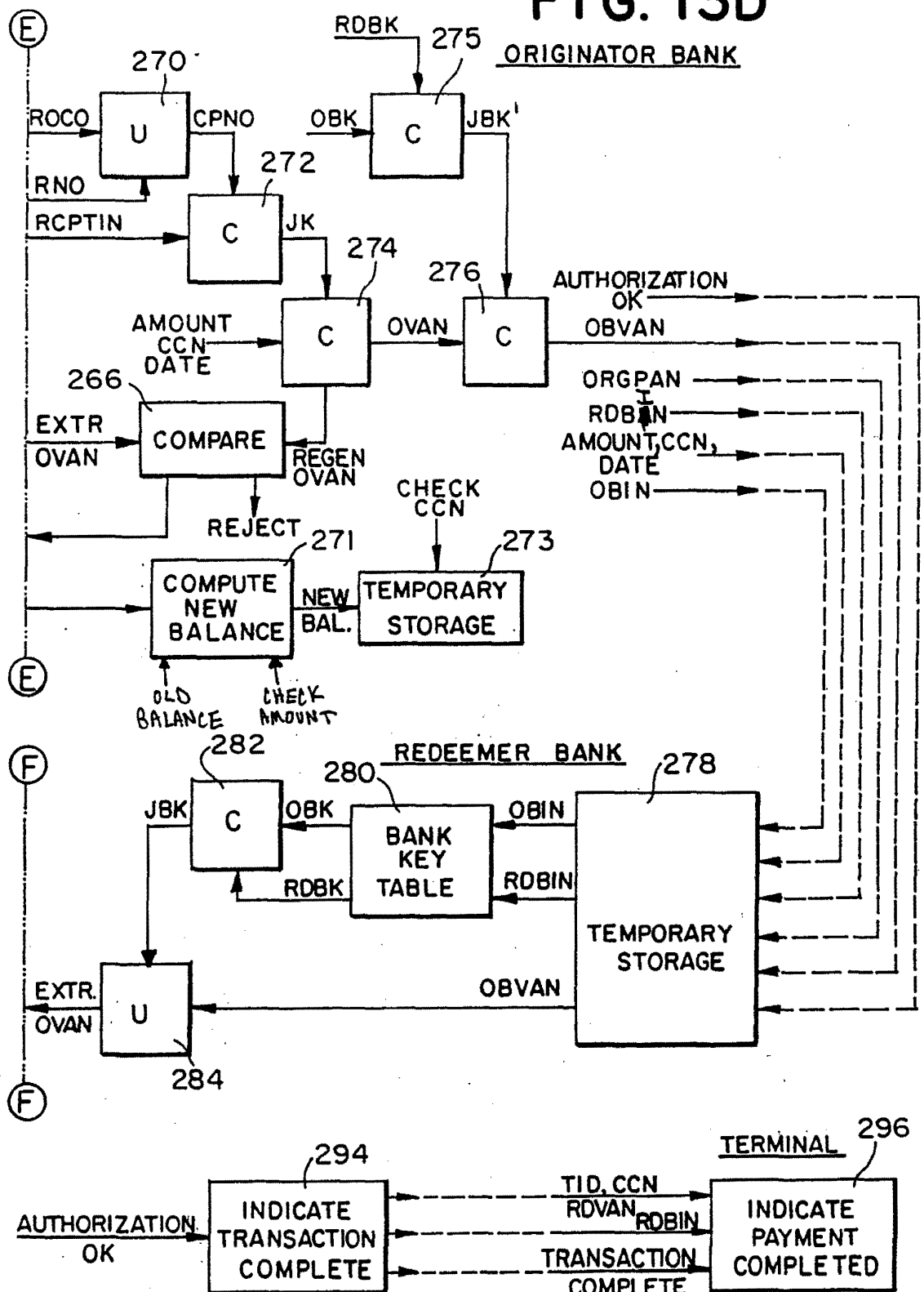


977385



977385

FIG. 13D



977385

FIG. 13E
REDEEMER BANK

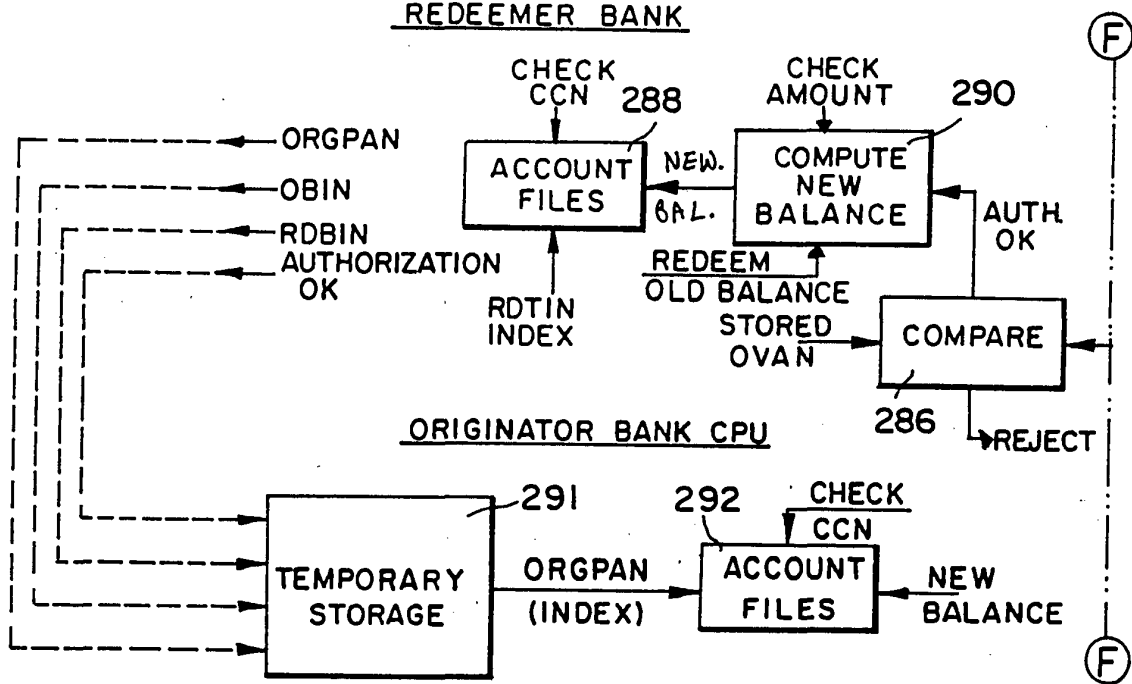
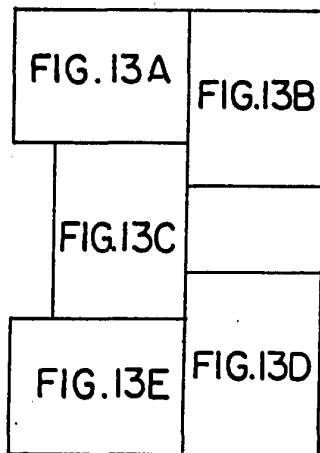


FIG. 14



CREDENTIAL ISSUE PROCESSING AGENCY TERMINAL / COMPUTER

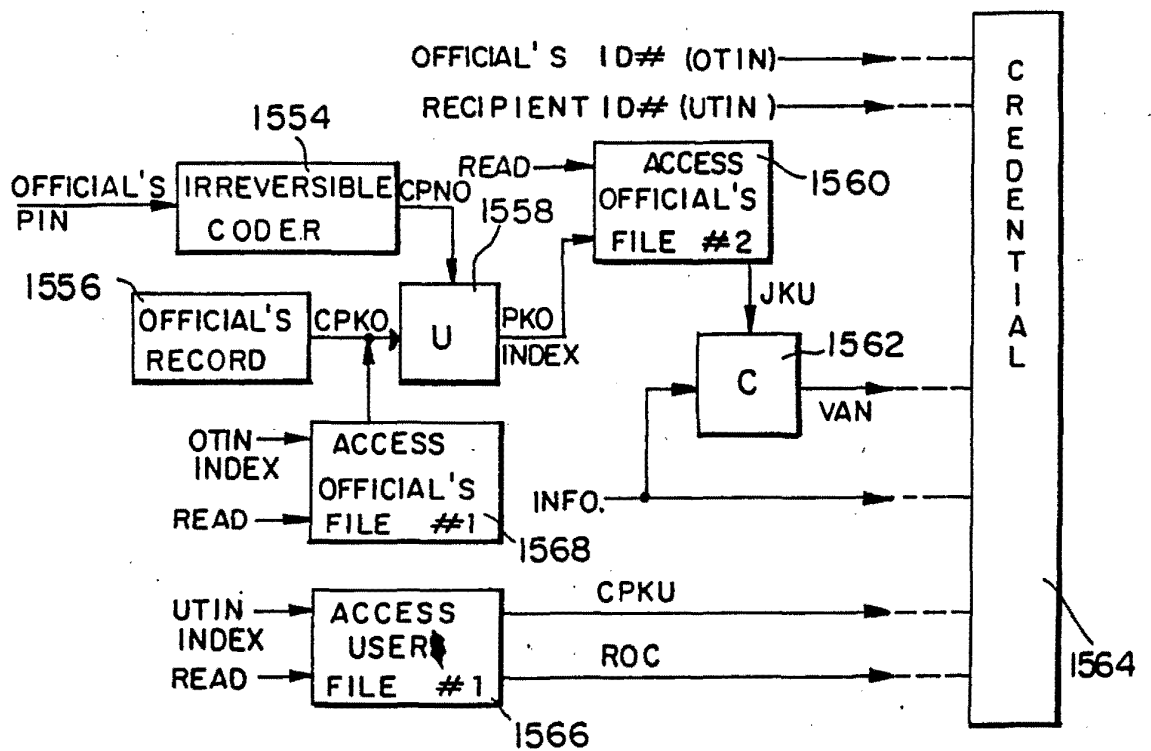


FIG. 15B

NOT OF DRAWINGS
ORIGINALLY FILED

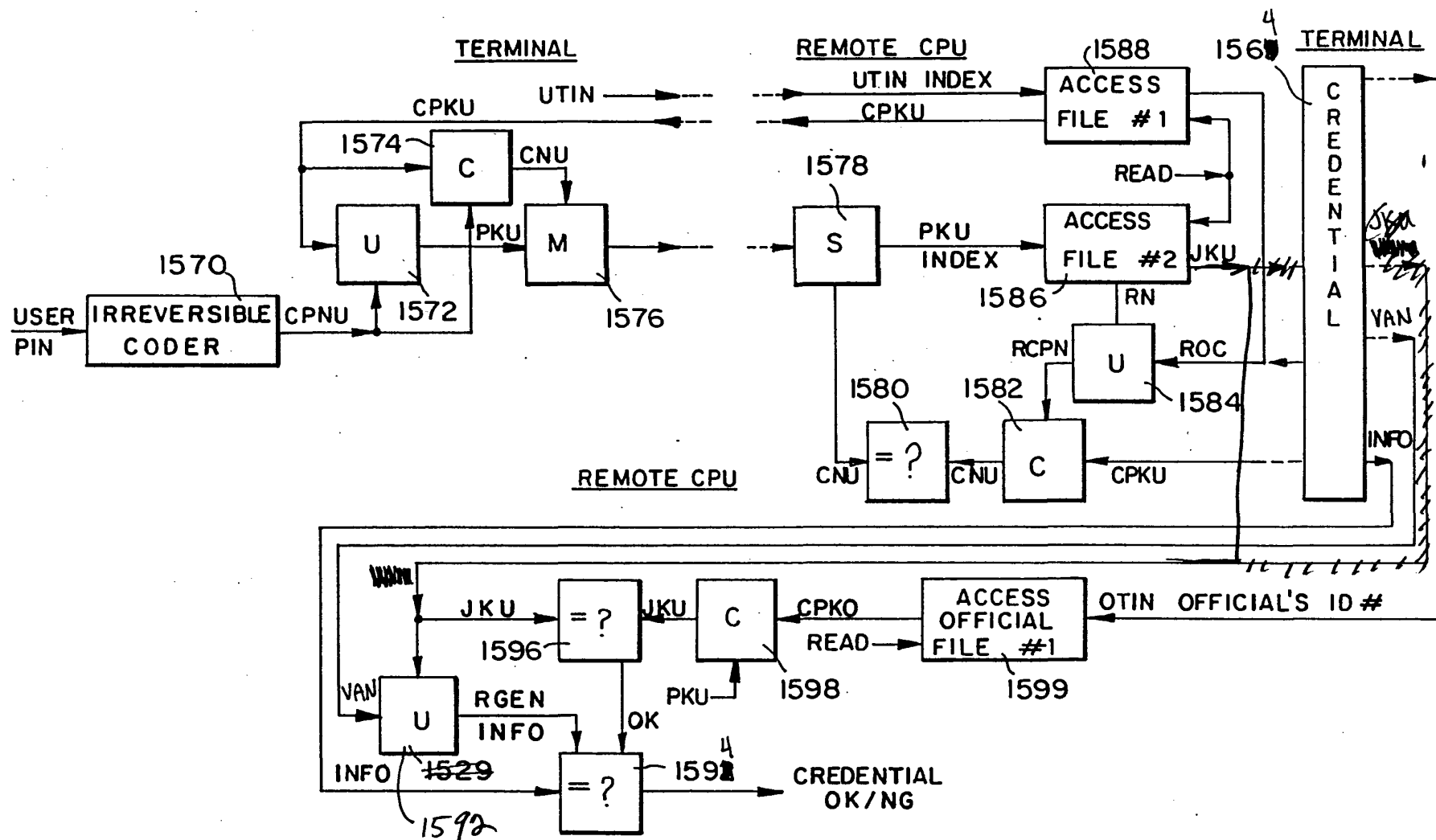


FIG. 15C

977385

IS
11/16/92

NOT OF DRAWINGS
ORIGINALLY FILED

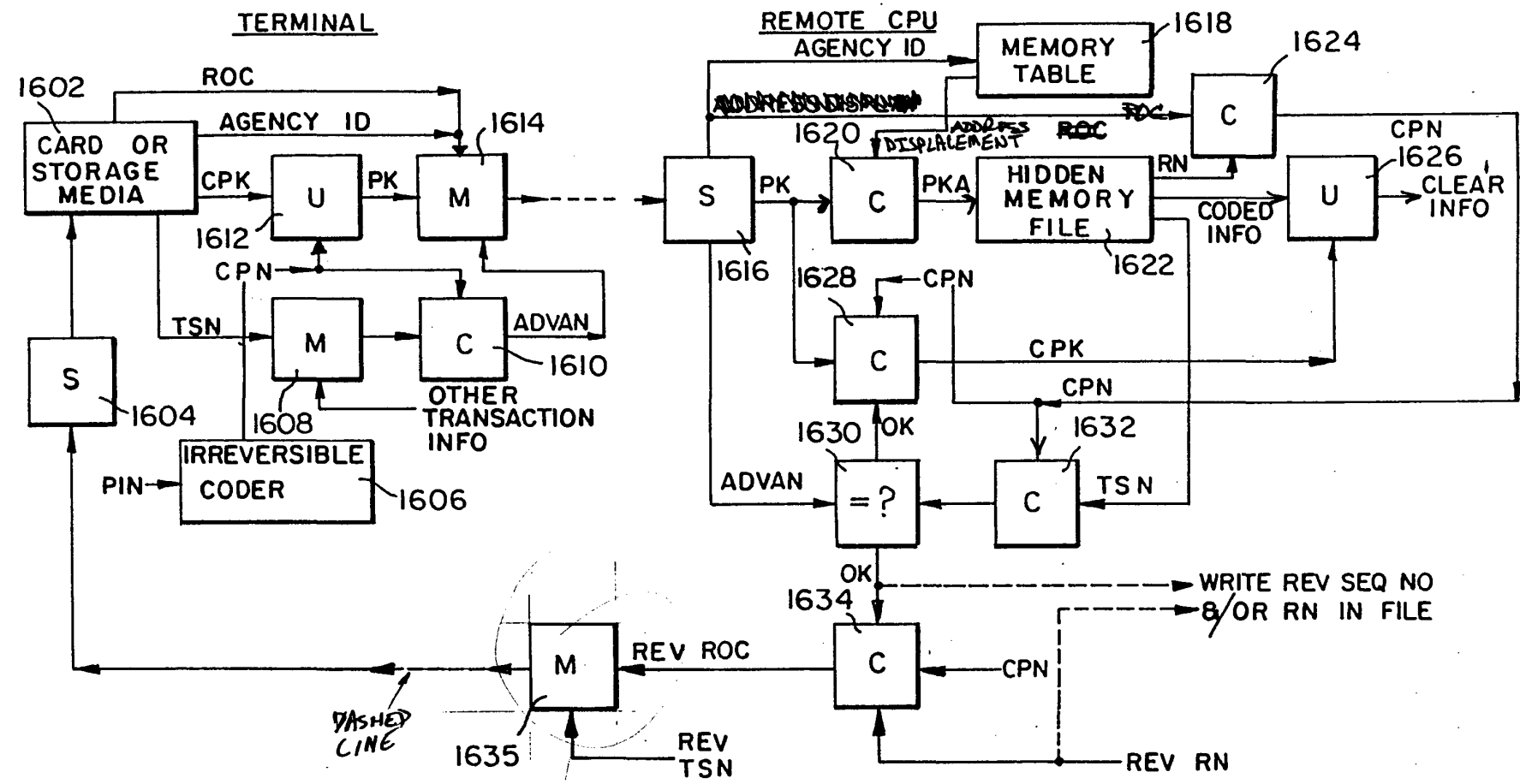


FIG. 16

120/11
D. P. 11/16/92

JS
11/16/92

11 977385

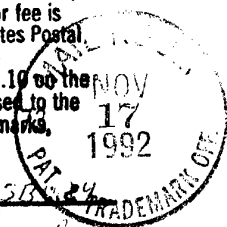
"Express Mail" mailing label
"number" TB 2553 58

Date of Deposit Nov-17, 1992

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 to the date indicated above and is addressed to the Commissioner of Patents and Trademarks, Washington, D.C. 20231.

Name: Ann M. Hansburg

Signed: Ann M. Hansburg



977385

PATENT

Attorney Docket
No. 6074-1

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

Attn: BOX PATENT APPLICATION

Transmitted herewith for filing is the utility patent
(type)

application of Inventor(s): Leon Stambler

For: SECURE TRANSACTION SYSTEM AND METHOD UTILIZED THEREIN

Enclosed are:

- ☒ Specification and claims with executed Declaration.
- ☐ Specification and claims with unsigned Declaration.
- ☒ Fifteen (15) sheets of drawings (informal) plus two copies.
- ☐ An assignment of the invention to _____
- ☐ A certified copy of Application No. _____
- ☒ A verified statement to establish small entity status under 37 CFR 1.9 and 37 CFR 1.27.
- ☐ Preliminary Amendment/Information Disclosure Statement.

The filing fee has been calculated as shown below:

CLAIMS	NO. FILED	NO. EXTRA
TOTAL	63 -20=	43
INDEPENDENT	18 -3=	15
MULTIPLE DEPENDENT CLAIMS PRESENT		

SMALL ENTITY		OR	LARGE ENTITY	
BASIC FEE	\$		BASIC FEE	\$
	355			710
x11=	\$ 473	OR	x22=	\$
x37=	\$ 555	OR	x74=	\$
115=	\$	OR	+230=	\$
TOTAL	\$1,383	OR TOTAL	\$	

The Commissioner is hereby authorized to charge payment of the following fees or credit any overpayment to Deposit Account No. 16-0235. Two additional copies of this sheet are enclosed.

☒ The above calculated filing fee \$1,383.00

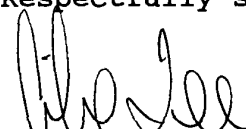
☒ Any additional fees required under 37 C.F.R. §1.16 or §1.17.

☒ 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).

Respectfully submitted,

11/17/92
(Date)

By:


Michael Q. Lee
Registration No. 35,239
PANITCH SCHWARZE JACOBS & NADEL
1601 Market Street - 36th Floor
Philadelphia, PA 19103
Telephone: 215-567-2020

MQL:amh
Enclosures



UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office

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

SERIAL NUMBER 07/97/883	FILING DATE 11/17/92	FIRST NAMED INVENTOR STAMBLER	ATTORNEY DOCKET NO. 8074-1
----------------------------	-------------------------	----------------------------------	-------------------------------

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

TARCZA EXAMINER

ART UNIT
2202

PAPER NUMBER

2

02/02/93

DATE MAILED:

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), 0 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 checked="" type="checkbox"/> Notice re Patent Drawing, PTO-948. |
| 3. <input type="checkbox"/> Notice of Art Cited by Applicant, PTO-1449. | 4. <input type="checkbox"/> Notice of Informal Patent Application, Form 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 1-63 are pending in the application.
Of the above, claims _____ are withdrawn from consideration.
2. ☐ Claims _____ have been cancelled.
3. ☐ Claims _____ are allowed.
4. ☒ Claims 1-63 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 re Patent Drawing, 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 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

Serial Number 0,362,102
Art Unit 2202

2

1. This application has been filed with informal drawings which are acceptable for examination purposes only. Formal drawings will be required when the application is allowed.

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. § 102 that form the basis for the rejections under this section made in this Office action:

"A person shall be entitled to a patent unless -

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States."

3. Claims 1-4, 6, 28, 29, 36-39, 44, 45, 51, 55, 57, 58 and 60-62 are rejected under 35 U.S.C. § 102 (b) as being anticipated by Atalla et al. Figure 2 of the reference shows all the elements of claim 1. Block 26 of figure 2 reads on claims 2 and 3. With regard to claim 4, the use of the account number to access a another storage means to retrieve the PIN verification number reads on the steps of claim 4. Column 8 lines 45-62 of the reference indicate that the account number, which was retrieved from a storage means and encoded under a PIN encryption key (block 36), is decoded and used to address the information which was retrieved from other storage means (block 70). The PVN that is retrieved is encrypted which reads on claim 6.

The enrollment method shown in figure 1 reads on the enrollment method of claims 28 and 29. The PIN is first encrypted in block 16 to create PTN which reads on CPN, and the PTN is encoded in block 22 to create PVN which reads on ROC. The bank key (20) is the predetermined arbitrary number, which is revisable at the bank's discretion.

The enrollment method shown in figure 1 reads on the enrollment method of claim 36. At enrollment a personal key (secret) and an account number (non-secret) are generated and stored on the user's card (a non-secret address). As described above, these numbers are used along with the PIN to address the PVN (secret) in a secret

Serial Number 0,,862,102
Art Unit 2202

3

(coded) address in the bank records (also see column 7 line 65 - column 8 line 2). With regard to claim 37, storage of the personal key reads on storing coded information. With regard to claim 38, the account number is the coded secret address, as described above. With regard to claim 39, the authentication method of figure 2 shows all of the authentication steps of the claim. With regard to claims 44 and 45, the method shown in figure 2 of using the account number which is encrypted and decrypted with the PIN (block 36), reads on the coding of the secret address with the PIN.

The transaction authorization process of figure 2 of the reference reads on the elements and steps of claim 51. The account number is the coded address (see column 7 line 65 - column 8 line 2). It is retrieved from storage on the user's card, encrypted with the PIN encryption key, transmitted to a second site, and used to generate a secret address which is used to retrieve coded authentication information for comparison. With regard to claim 55, column 8 lines 45-48 state that the information is transmitted using a conventional computer network which reads on the unsecure communication link.

The enrollment method shown in figure 1 reads on the enrollment method of claim 57. Column 7 lines 7-16 indicate that figure 1 also reads on claim 58. The operator entering the account number reads on an official's PIN number. The enrollment method shown in figure 1 reads on claim 60 and 61 (see rationale for claims 36-39). The authentication method shown in figure 2 reads on the authentication method of claim 62.

4. 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 negatived by the manner in which the invention was made. Subject matter developed by another person, which qualifies as prior art only under subsection (f) and (g) of section 102 of this title, shall not preclude patentability under this section where the subject matter and the

Serial Number 0,862,102
Art Unit 2202

4

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.

5. Claim 5 is rejected under 35 U.S.C. 103 as being unpatentable over Atalla et al. The applicant's claim is different than the reference in that the reference does not mention filling the memory with pseudo information prior to use so as to make used and unused memory indistinguishable. It would have been obvious to one skilled in the art to modify the reference to employ this common technique, since it would serve the objective of keeping the address of stored information secret (see column 7 line 65 - column 8 line 2).

6. Claims 40, 41 and 52-54 are rejected under 35 U.S.C. 103 as being unpatentable over Atalla et al in view of Dahbura. With regard to claims 40 and 41, Atalla differs from the claims in that it does not include the coding of the date and time with the authentication method. Dahbura teaches the use of the date and time of the transaction in the encryption algorithm in a system for preventing fraudulent use of credit cards (column 2 lines 21-67). It would have been obvious to modify the system in Atalla to include the use of the date and time to generate a unique authentication number associated with the transaction, because, as suggested in Dahbura, this would make it more difficult for a party to use the card fraudulently.

With regard to claims 52-54, Atalla differs from the claims in that an anti-duplication variable is not generated for each transaction and is not stored in a different place in memory. Further, Atalla does not store agency identification information. Dahbura teaches (column 2) the use of a unique anti-duplication variable for each transaction, each of which is stored in a different (revised) memory location at a credit card center. Further, the merchant's (agency's) identification is stored and later retrieved for verification along with the transaction information. It would have been obvious to one of ordinary skill in the art to modify Atalla to include these additional measures to prevent or resolve accounting mistakes made in a transaction and to make it more difficult for a party to use the card fraudulently.

Serial Number 6,862,102
Art Unit 2202

5

7. Claims 42 and 43 are rejected under 35 U.S.C. 103 as being unpatentable over Atalla et al in view of Campbell Jr. Atalla differs from the claims in that it does not generate semi-random numbers using a counter to code and uncode information. Campbell teaches a key management system in which a key is generated from a master key along with another key which is selected from a table via a counter (a semi-random number). The necessary information to synchronize the keys is sent to a host computer where the encrypted information is decrypted and authenticated. This technique results in a unique key for each transaction. It would have been obvious to modify the system in Atalla to alter the key with a semi-random number so that, as suggested in Campbell, even if coded PIN information is compromised, the system is still secure from adversaries.

8. Claims 7-13, 30-35, 46-50 and 63 are rejected under 35 U.S.C. § 102 (b) as being anticipated by Dahbura. All of the elements and steps of claims 7-13 are described in column 2 of the reference. Specifically, the predetermined secret code is the user's password, and the predetermined non-secret code is the time, date, etc. of the transaction. With regard to claims 46 and 47, all elements and steps of these claims are also recited in column 2 of the reference.

With regard to claim 30, column 2 lines 21-59 of the reference recite the generation of a joint code, storing of the code, and the inaccessibility of the information without the password which read on the steps of the claim. With regard to claim 31, the recording of the joint code on the receipt reads on the recording and issuing of the VAN on a credential (column 2 lines 32-42). All of the steps of claim 32 are also described in column 2 of the reference. The joint code is stored in the merchant's records, the central machine's record's and on a customer's receipt. Only the credit card center can access the information stored on the central machine, and authenticate the transaction. Likewise, the authentication process performed by the credit card center reads on claim 63.

Serial Number 6,862,102
Art Unit 2202

6

With regard to claims 33-35, all of the claimed elements and steps are described in column 2 of the reference. Specifically, the merchant's first verification code is a redemption VAN which must be compared with the central machine's second verification code for redemption.

With regard to claims 48-50, all of the elements and steps are described in column 2 of the reference. Specifically, the receipt generated is an invoice.

9. Claims 14-16 are rejected under 35 U.S.C. 103 as being unpatentable over Dahbura. Dahbura differs from the claims in that the methods are not applied to the dispensing of medical prescriptions. It would have been obvious to one of ordinary skill in the art to modify the reference to apply it to the dispensing of medical prescriptions, since, like credit card purchases and automatic teller transactions, it is a type of transaction that is subject to attempted fraud and requires authentication.

10. Claims 17-20, 22-27, 56 and 59 are rejected under 35 U.S.C. § 102 (b) as being anticipated by Bouricius et al. The reference describes a three party system (person, retailer, host system) which uses the person's encryption key and the retailer's encryption key to double encrypt transaction information which reads on the VAN generation of claim 17 and joint code of claim 19 (see column 5 line 61 - column 7 line 9). The same lines of the reference read on claims 56 and 59. While the person and retailer are present, the host system is absent, which reads on claim 18.

With regard to claim 20, the reference describes a system in which a host system performs the following steps which read on the steps of claim 20: receives coded authentication information (both singly and doubly encrypted); uses the transmitted information to retrieve secret (encryption keys) and non-secret (number of account, column 5 line 60); and compares the decrypted transmitted authentication information (see column 5 line 61 - column 7 line 9).

Serial Number 6,862,102
Art Unit 2202

7

With regard to claim 22, the personal data is first coded by the person and then received and doubly coded by the retailer which reads on the method of generating the second coded authentication information (see figure 5a). Column 5 line 67 - column 6 line 2 and column 7 lines 27-32 of the reference describe the use of coded date and time information to uniquely identify the transaction which reads on the ADVAN of claim 23. The decrypting of the date and time and performing a check at the host reads on claim 24. With regard to the steps of claims 25-27, the comparison at the host system of the singly and doubly encrypted common data (column 4 lines 29-62, figure 5a) reads on the formation, transmission and comparison of two the coded arbitrary numbers.

11. Claim 21 is rejected under 35 U.S.C. § 103 as being unpatentable over Bouricius. Bouricius differs from the claim in that it does not specifically mention that the communication medium is secure. It would have been obvious to one of ordinary skill in the art to transmit the transaction information over a secure communication medium to prevent eavesdroppers from obtaining any information that might help them defeat the system (such as the retailer's business number which is not encrypted).

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Patrick Finnan whose telephone number is (703) 308-0450. Any inquiry of a general nature or relating to the status of this application should be directed to the Group 2200 receptionist whose telephone number is (703) 308-0766.

P. Finnan

07



THOMAS H. TARCZA
SUPERVISORY PRIMARY EXAMINER
GROUP 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. 07/977,385		GROUP/ART UNIT 2202		ATTACHMENT TO PAPER NUMBER 2						
NOTICE OF REFERENCES CITED				APPLICANT(S) Stambler										
U.S. PATENT DOCUMENTS														
*		DOCUMENT NO.						DATE	NAME	CLASS	SUB-CLASS	FILING DATE IF APPROPRIATE		
	A	4	9	6	5	5	6	8	10/90	Atalla et al.	380	24		
	B	5	1	6	3	0	9	8	11/92	Dahbura	380	24		
	C	4	3	0	2	8	1	0	11/81	Bourgeois et al.	380	24		
	D	4	6	0	5	8	2	0	8/86	Campbell, Jr.	380	24		
	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 P. F. [Signature]								DATE 1/13/93						
* A copy of this reference is not being furnished with this office action. (See Manual of Patent Examining Procedure, section 707.05 (a).)														

GROUP

APPLICATION NUMBER

977385

NOTICE OF DRAFTSPERSON'S PATENT DRAWING REVIEW

THE PTO DRAFTSMEN REVIEW ALL ORIGINALLY FILED DRAWINGS REGARDLESS OF WHETHER THEY WERE DESIGNATED AS INFORMAL OR FORMAL. ADDITIONALLY, THE PATENT EXAMINER WILL ALSO REVIEW THE DRAWINGS FOR COMPLIANCE WITH THE REGULATIONS.

The drawings filed

11/17/92.

A. ☐ are approved by the draftsman.B. ☒ are objected to by the draftsman under 37 CFR 1.84 for the reason(s) checked below. The examiner will require submission of new, corrected drawings at the appropriate time. Corrected drawings must be submitted according to the instructions listed on the back of this Notice.

1. Paper and ink. 37 CFR 1.84(a)

☐ Sheet(s) _____ Poor.

2. Size of Sheet and Margins. 37 CFR 1.84(b)

Acceptable Paper Sizes and Margins

Margin	Paper Size		
	8 1/2 by 14 inches	8 1/2 by 13 inches	DIN size A4 21 by 29.7 cm.
Top	2 inches	1 inch	2.5 cm.
Left	1/4 inch	1/4 inch	2.5 cm.
Right	1/4 inch	1/4 inch	1.5 cm.
Bottom	1/4 inch	1/4 inch	1.0 cm.

☐ Proper Size Paper Required.
All Sheets Must be Same Size.
Sheet(s) _____☒ Proper Margins Required.
Sheet(s) 8A, 11, 15A☒ TOP ☐ RIGHT
☒ LEFT ☐ BOTTOM

3. Character of Lines. 37 CFR 1.84(c)

☐ Lines Pale or Rough and Blurred.
Fig(s) _____☐ Solid Black Shading Not Allowed.
Fig(s) _____4. ☐ Photographs Not Approved.

5. Hatching and Shading. 37 CFR 1.84(d)

☐ Shade Lines are Required.

Fig(s) _____

☐ Criss-Cross Hatching Not Allowed.

Fig(s) _____

☐ Double Line Hatching Not Allowed.

Fig(s) _____

☐ Parts in Section Must be Hatched.

Fig(s) _____

6. Reference Characters. 37 CFR 1.84(f)

☐ Reference Characters Poor or Incorrectly Sized.

Fig(s) _____

☐ Reference Characters Placed Incorrectly.

Fig(s) _____

7. Views. 37 CFR 1.84(i) & (j)

☐ Figures Must be Numbered Properly.☐ Figures Must Not be Connected.

Fig(s) _____

8. ☒ Identification of Drawings. 37 CFR 1.84(1)Extraneous Matter or Copy Machine
Marks Not Allowed. Fig(s) 1-169. ☐ Changes Not Completed from Prior
PTO-948 dated _____☒ Comments;

- Pencil & Red ink marks obj - Fig. 8A - 10A, 15A, 15C,

Telephone inquiries concerning this review should be directed to the Chief Draftsman at telephone number (703) 305-8404.

Tang
Reviewing Draftsman12/14/92
Date

Note: Any objection to the drawings made by the examiner will be communicated separately in an office action.

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 F. Wolf
DATE January 29, 1993



#3/Prior Art
1/24/93
J. G. Muds
2-16-93
RECEIVED

FEB 11 1993

PATENT

Box Non-Fee Amendment

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re:	Patent Application of Leon Stambler	:	Group Art Unit 2202
Serial No.:	07/977,385	:	Examiner: To Be Assigned
Filed:	November 17, 1992	:	Attorney Docket No. 6074-1
For:	SECURE TRANSACTION SYSTEM AND METHOD UTILIZED THEREIN	:	

INFORMATION DISCLOSURE STATEMENT

It is requested that the enclosed references 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 enclosed references are respectfully requested.

Respectfully submitted,

LEON STAMBLER

January 29, 1993
(Date)

By:

Michael Q. Lee
Registration No. 35,239
PANITCH SCHWARZE JACOBS & NADEL
1601 Market Street - 36th Floor
Philadelphia, PA 19103
Telephone: (215) 567-2020

MQL/amh-djw

Form P.O-1449
(REV. 8-83)

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE

ATTY. DOCKET NO.
6074-1

SERIAL NO.
07/977,385

Page 1 of 4 #3

INFORMATION DISCLOSURE CITATION
(Use several sheets if necessary)

APPLICANT
Leon Stambler

FILING DATE
November 17, 1992

GROUP
Art Unit 2202

U.S. PATENT DOCUMENTS													
EXAMINER INITIAL		DOCUMENT NUMBER							DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
SM		3	6	0	9	6	9	0	9/71	Nissman	340	149, R	
SM		3	6	1	1	2	9	3	10/71	Constable	340	149 A	
FOC		3	6	5	7	5	2	1	4/72	Constable	235	61.7 B	
FO		3	8	9	2	9	4	8	7/75	Constable	340	149 R	
FO		3	9	3	8	0	9	1	2/76	Atalla et al.	340	149 A	
FO		4	0	0	4	0	8	9	1/77	Richard et al.	178	22	
FO		4	0	1	6	4	0	5	4/77	McCune et al.	235	61.7 B	
FO		4	1	8	6	8	7	1	2/80	Anderson et al.	235	380	
FO		4	1	9	8	6	1	9	4/80	Atalla	340	149 A	
FO		4	2	0	8	5	7	5	6/80	Haltorf	235	380	
FO		4	2	2	3	4	0	3	9/80	Konheim et al.	375	2	

FOREIGN PATENT DOCUMENTS														
		DOCUMENT NUMBER							DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION	
													YES	NO

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

EXAMINER
S. Camgialosi

DATE CONSIDERED
6/93

*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.

TO-1449 U-83)		U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE		ATTY. DOCKET NO. 6074-1		SERIAL NO. 07/977,385							
INFORMATION DISCLOSURE CITATION (Use several sheets if necessary)				APPLICANT Leon Stambler									
				FILING DATE November 17, 1992		GROUP Art Unit 2202							
U.S. PATENT DOCUMENTS													
EXAMINER INITIALS	TRADEMARK OFFICE	DOCUMENT NUMBER		DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE					
gc		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	
me		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	
gn		4	3	1	7	9	5	7	3/82	Sendrow	178	22.08	
gn		4	3	2	8	4	1	4	5/82	Atalla	235	380	
gn		4	3	8	6	2	6	6	5/83	Chesarek	235	380	
gn		4	4	9	8	0	0	0	2/85	Decavele 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 6/93								
*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
(REV. 8-88)

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE

ATTY. DOCKET NO.
6074-1

SERIAL NO.
07/977,385

INFORMATION DISCLOSURE CITATION
(Use several sheets if necessary)

APPLICANT
Leon Stambler

FILING DATE
November 17, 1992

GROUP
Art Unit 2202

U.S. PATENT DOCUMENTS													
EXAMINER INITIALS	1993	DOCUMENT NUMBER							DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
gic		4	5	9	0	4	7	0	5/86	Koenig	340	825.31	
gic		4	6	0	5	8	2	0	8/86	Campbell, Jr.	178	22.09	
gic		4	6	6	5	3	9	6	5/87	Dieleman	380	23	
gic		4	6	8	6	3	5	7	8/87	Douno et al.	235	379	
gic		4	7	2	0	8	5	9	1/88	Aaro et al.	380	23	
gic		4	7	3	4	8	5	8	3/88	Schlaflly	364	408	
gic		4	7	5	5	9	4	0	7/88	Bracht1 et al.	364	408	
gic		4	7	9	7	9	2	0	1/89	Stein	380	24	
gic		4	7	9	9	0	6	1	1/89	Abraham et al.	340	825.34	
gic		4	9	0	8	8	6	1	3/90	Bracht1 et al.	380	25	
gic		4	9	2	8	0	9	8	5/90	Dannhaeuser	340	825.56	

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
6/93

*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 (REV. 8-83) U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE INFORMATION DISCLOSURE CITATION <i>(Use several sheets if necessary)</i>		ATTY. DOCKET NO. 6074-1 SERIAL NO. 07/977,385 APPLICANT Leon Stambler FILING DATE November 17, 1992 GROUP Art Unit 2202	
--	--	--	--

U.S. PATENT DOCUMENTS									
EXAMINER INITIALS	DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE			
	4 9 3 3 9 6 9	6/90	Marshall et al.	380	125				
	4 9 3 5 9 6 2	6/90	Austin	380	25				
	4 9 4 7 0 2 8	8/90	Gorog	235	381				
	4 9 6 5 5 6 8	10/90	Atalla et al.	340	825.340				
	4 9 7 7 5 9 5	12/90	Ohta et al.	380	24				
	4 9 9 2 7 8 3	2/91	Zdunek et al.	340	825.340				
	5 0 1 6 2 7 4	5/91	Micali et al.	380	23				
	5 0 2 3 9 0 8	6/91	Weiss	380	23				

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 6/93
----------------------------------	--------------------------------

*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.
20231, ON THE DATE INDICATED BELOW.

BY Anna M. Hansbury
DATE March 18, 1993

4/A
4-1-93
Patent SP/MS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Patent Application of : Group Art Unit 2202
Leon Stambler :
Serial No: 07/977,385 : Examiner: T. Tarcza
Filed: November 17, 1992 :
For: SECURE TRANSACTION SYSTEM :
AND METHOD UTILIZED THEREIN : Attorney Docket
No. 6074-1 **RECEIVED**

MAR 31 1993

AMENDMENT

This is in response to the Office Action mailed
February 2, 1993 (Paper No. Not Indicated) in connection with the
above-identified patent application. Kindly amend the
application, without prejudice, as follows:

In the Claims:

Please amend claims 1, 5, 6, 17, 19, 30, 33, 46, 48, 56,
59 and 63 as follows:

1. (Amended) In a system comprising a first storage
means addressable using a secret predetermined address and party
information associated with a party and stored in the first
storage means, the party information comprising first coded
authentication information previously generated by using a

CS1410B 04/01/93 07977385

16-0235 140 203

37.00CH

50

personal identification number (PIN) associated with the party, a method for authenticating the party comprising the steps of:

P1 (a) receiving a PIN from the party to be authenticated;

P1 (b) addressing the first storage means using the secret predetermined address to locate the party information and to retrieve the first coded authentication information;

P1 (c) generating second coded authentication information using the received PIN;

P1 (d) comparing at least part of the retrieved first coded authentication information to at least part of the generated second coded authentication information; and

P1 (e) 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[.];

P1 wherein the step of addressing the first storage means comprises the steps of:

P1 P (1) accessing a second storage means using a non-secret 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 secret predetermined address of the first storage means using the PIN;

P2 P (2) uncoding the coded address using the received PIN to generate the secret predetermined address; and

cancel!
117 (3) accessing the first storage means using the generated secret predetermined address to retrieve the first coded authentication information.

A2
38. (Amended) The method of claim [4] 1, wherein the first storage means is a part of a memory and wherein, prior to use of the memory, pseudo information is stored in the memory, thereby making unused portions of the memory indistinguishable from the first storage means.

48. (Amended) The method of claim [4] 1, wherein the party information also comprises secret information associated with the party.

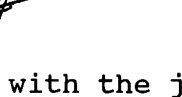
A3
17. (Amended) In a multi-party transaction system, a method for authenticating a transaction and parties to the transaction comprising the steps of:

nl
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


B
associating the VAN with the transaction.

19. (Amended) The method of claim 17, wherein the coding step comprises the steps of:

A4
Cont.
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 the information relevant to the transaction with the joint code to generate the VAN.

30. (Amended) 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 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 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.

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;

A6 determining whether [a] the recipient party [and the transaction are] is authentic by using the received recipient PIN; [and]

B 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:

A7 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;

As
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:

Ag
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:

Ag
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;

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

Q11 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. *B*

Please add new claim 64:

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

Q12 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 non-secret number with a predetermined secret number associated with the first party; and *B*

associating the VAN with the transaction.--

Please cancel claims 2, 4, and 18 without prejudice.

REMARKS

Claims 1, 3, 5-17, and 19-64 are pending in this application. At the outset, Applicant would like to express his appreciation for the Examiner's prompt and thorough examination of this application.

Claims 1, 5, 6, 17, 19, 30, 33, 46, 48, 56, 59 and 63 have been amended to more particularly point out and distinctly

claim what Applicant regards as the invention. Claims 2, 4 and 18 have been cancelled. Claim 64 has been added. No new matter has been added. Therefore, it is respectfully requested that the Examiner enter and duly consider the amendments.

In paragraph 3 of the Office Action, the Examiner has rejected claims 1-4, 6, 28, 29, 36-39, 44, 45, 51, 55, 57, 58, and 60-62 under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 4,965,568 to Atalla et al. (hereinafter "Atalla"). The rejection is respectfully traversed.

With regard to the rejection of claims 1, 3, and 6 (claims 2 and 4 having been cancelled), Applicant notes that claim 1 as amended is directed to a method for authenticating a party in a system comprising a first storage means addressable using a secret predetermined address (PK) and party information associated with the party and stored in the first storage means. The party information comprises first coded authentication information (CNU) previously generated by using a personal identification number (PIN) associated with the party. The method of claim 1 includes receiving a PIN from the party to be authenticated and addressing the first storage means using the secret predetermined address (PK) to locate and retrieve the first coded authentication information (CNU). More particularly, the first storage means is addressed by accessing a second storage means using a non-secret predetermined address (such as UTIN) to locate and to retrieve a coded address (such as CPKU) previously stored in the second

storage means. The coded address (CPKU) was previously generated by coding the secret predetermined address (PK) of the first storage means using the PIN. The secret predetermined address (PK) is then generated by uncoding the coded address (CPK) using the received PIN. The first storage means is then accessed using the generated secret predetermined address (PK) to retrieve the first coded authentication information (CNU).

The method of claim 1 also includes generating second coded authentication information (CNU) using the received PIN and comparing at least part of the retrieved first coded authentication information (CNU) to at least part of the generated second coded authentication information (CNU) and authenticating the party if the first and second coded authentication information match.

In contrast to claim 1 as amended, Atalla does not teach or suggest a first storage means which is addressable using a secret predetermined address or addressing the storage means using the secret predetermined address to locate and retrieve the first coded authentication information. Rather, Atalla discloses that the bank records 70 and the database 24 are accessed using a party's account number. As is well known, account numbers are not secret.

Additionally, Atalla does not teach or suggest accessing a second storage means using a non-secret predetermined address to locate and to retrieve a coded address previously stored in the

second storage means, uncoding the coded address using the received PIN to generate the secret predetermined address, and accessing the first storage means using the generated secret predetermined address to retrieve the first coded authentication information. The Examiner contends that Atalla (at column 8, lines 45-62) indicates that the account number, which was retrieved from a storage means and uncoded under a PIN encryption key, is decoded and used to address the information which was retrieved from other storage means. However, as noted above, the account number is not secret and, therefore, does not anticipate the secret predetermined address of claim 1. Also, since Atalla does not teach or suggest a secret predetermined address, Atalla does not teach or suggest a coded address which is generated by coding the secret predetermined address. Further, Applicant respectfully disagrees with the Examiner's position that the account number is uncoded under a PIN encryption key and stored in a storage means, as required in claim 1. Block 36 of Atalla Fig. 2 represents steps for transmitting PTN' and the account number from a site to an issuing bank. During the operation of block 36, the account number and PTN' are repeatedly encrypted and transferred from one location to another. In contrast to claim 1, Atalla does not teach or suggest that the encrypted account number is stored at any of the intermediate locations during the transmission from the site to the issuing bank.

For all of the above reasons, Applicant asserts that claim 1 is patentable over Atalla and respectfully requests that the Examiner reconsider and withdraw the rejection of claim 1. Applicant notes that claims 3 and 5 depend from claim 1. Therefore, Applicant asserts that claims 3 and 5 are patentable over Atalla for at least the same reasons as noted above with regard to claim 1, and requests that the Examiner reconsider and withdraw the rejection of claims 3 and 5.

With regard to the rejection of claims 28 and 29, Applicant notes that claim 28 is directed to a method for enrolling a party in a transaction system wherein the party is authenticated during at least one stage of a subsequent transaction, comprising the steps of receiving a personal identification number (PIN) from the party (block 10 of Fig. 6), irreversibly coding the PIN to produce a coded PIN, CPN (block 12 of Fig. 6), reversibly coding the CPN using a predetermined arbitrary number (RN) to produce a revisable owner code, ROC (block 20 of Fig. 6), and storing the predetermined arbitrary number (RN) and the ROC in a storage means (block 22 of Fig. 6) at a location associated with the party. It should be noted that since ROC was generated by reversibly coding the CPN with the predetermined arbitrary number (RN), CPN is derivable from the predetermined arbitrary number (RN) and the ROC.

In contrast to claim 28, Atalla teaches irreversibly encrypting the PTN (analogous to the CPN of claim 28) with the

bank key (analogous to the predetermined arbitrary number of claim 28) to produce PVN (analogous to ROC of claim 28). See, for example, block 22 of Atalla Fig. 1. Therefore, unlike claim 28, Atalla does not teach or suggest a coded personal identification number (CPN) which is generated using a PIN, and which is derivable from a predetermined arbitrary number and a revisable owner code. This is true since PTN is not derivable from PVN and the bank key. For the above reasons, Applicant respectfully asserts that claims 28 and 29 (claim 29 depending from claim 28) are patentable over Atalla and respectfully requests that the Examiner reconsider and withdraw the rejection of claims 28 and 29.

With regard to the rejection of claims 36-39, 44 and 45, Applicant notes that claim 36 is directed to a method for enrolling and authenticating a party including the steps of receiving a personal identification number (PIN) from the party, generating coded authentication information (CPNU) using the received PIN (block 1502 of Fig. 15A), generating a first secret number (RN) and a second non-secret number (ROC) such that the coded authentication information (CPN) is derivable from the first and second numbers (block 1518 of Fig. 15A), storing information comprising the secret number (RN) in a first storage means (block 1522 of Fig. 15A) using a predetermined secret address (PKU), generating a coded secret address (CPKU) using at least part of the predetermined secret address (PK) and the received PIN

(block 1504 of Fig. 15A), and storing the coded secret address (CPKU) and the non-secret number (ROC) in a second storage means (block 1520 of Fig. 15A) addressable using a predetermined non-secret address (UTIN). As shown in Fig. 15A, ROC is generated by reversibly coding CPN with RN in block 1518. Consequently, and as recited in claim 36, CPN (the coded authentication information) is derivable from RN (the first secret number) and ROC (the second non-secret number).

In contrast to claim 36, and as noted above with respect to claim 28, Atalla discloses generating PVN by irrevocably and irreversibly encrypting PTN with the bank key. Consequently, PTN is not derivable from PVN and the bank key. Additionally, Atalla does not teach or suggest a first storage means addressable using a predetermined secret address and a second storage means addressable using a predetermined non-secret address, as recited in claim 36. Atalla also does not disclose generating a coded secret address using at least part of a predetermined secret address. For at least the above reasons, Applicant asserts that claim 36 is patentable over Atalla and respectfully requests that the Examiner reconsider and withdraw the rejection of claim 36. Applicant notes that claims 37-39, 44 and 45 depend from claim 36. Consequently, Applicant asserts that claims 37-39, 44 and 45 are patentable over Atalla for at least the same reasons as given above for claim 36 and, therefore, respectfully requests that the Examiner reconsider and withdraw the rejection.

With regard to the rejection of claims 51 and 55, Applicant notes that claim 51 is directed to a method for authenticating a party and for authorizing access to a storage means (block 1622 of Fig. 16) associated with the party and addressable using a secret predetermined address (PK), and includes generating coded authentication information (CPN) using a personal identification number (PIN) wherein the coded authentication information (CPN) is derivable from a secret number (RN) stored in the storage means (block 1622) and a non-secret number (ROC) previously stored in a storage medium (card 1602 of Fig. 16) possessed by the party. Claim 51 also recites retrieving from the storage medium (card 1602) at least a coded address (CPK), wherein the coded address (CPK) was previously generated by coding at least a portion of the secret predetermined address (PK) using the coded authentication information (CPN), generating at least a portion of the secret predetermined address by uncoding the coded address (CPK) using the coded authentication information (CPN), and generating the secret predetermined address (PK) using the portion of the secret predetermined address (PK).

In contrast to claim 51, and as discussed above with regard to claims 28 and 36, Atalla discloses generating PVN by irreversibly encrypting PTN with the bank key such that PTN is not derivable from PVN and the bank key. Thus, Atalla does not teach or suggest CPN as recited in claim 51. Also, Atalla does not teach or suggest a storage means which is addressable using a

secret predetermined address, as recited in claim 51. Further, Atalla does not teach or suggest retrieving a coded address from a storage medium, the coded address representing a coded portion of the secret predetermined address, and regenerating the secret predetermined address by uncoding the coded address. For all of the above reasons, Applicant asserts that claim 51 is patentable over Atalla and respectfully requests that the Examiner reconsider and withdraw the rejection of claim 51. Additionally, since claim 55 depends from claim 51, Applicant asserts that claim 55 is patentable over Atalla and requests that the Examiner reconsider and withdraw the rejection of claim 55.

With regard to the rejection of claim 57, Applicant notes that claim 57 is similar to claim 28. Thus, Applicant asserts that claim 57 is patentable over Atalla for at least the same reasons given above for claim 28, and respectfully requests that the Examiner reconsider and withdraw the rejection of claim 57.

With regard to the rejection of claim 58, Applicant notes that claim 58 is directed to a transaction system for enrolling a party that includes means for coding information associated with the party (PKU) with information associated with an official (CPKO) to generate a joint code (JKU) (block 132 of Fig. 10A). The joint code (JKU) is subsequently associated with a transaction. Claim 58 also includes a storage means (block 112' in Fig. 10A) accessible only to someone with knowledge of a

personal identification number (PIN) associated with the party, and means for storing the joint code (JKU) in the storage means (block 112'). Note that the storage means as recited in claim 58 is accessible only to someone with knowledge of the PIN. Therefore, if no one exists with knowledge of the PIN, the joint code cannot be accessed from the storage means and, therefore, cannot be associated with a transaction.

Atalla discloses storing PVN in a database 24. In contrast to claim 58, the database 24 of Atalla is not accessible only to someone with knowledge of the PIN. Rather, the database 24, and the PVN stored therein, is accessible to anyone with knowledge of the party's account number, which generally represents readily available information. Therefore, the Atalla system is much less secure than the system of claim 58. For the above reasons, Applicant asserts that claim 58 is patentable over Atalla and respectfully requests that the Examiner reconsider and withdraw the rejection of claim 58.

With regard to the rejection of claims 60 and 61, Applicant notes that claim 60 is similar to claim 36. Therefore, Applicant asserts that claims 60 and 61 (claim 61 depending from claim 60) are patentable over Atalla for at least the same reasons as given above for claim 36, and respectfully requests that the Examiner reconsider and withdraw the rejection of claims 60 and 61.

With respect to the rejection of claim 62, the Examiner contends that the authentication method of Atalla Fig. 2 reads on claim 62. The rejection is respectfully traversed.

Claim 62 is directed to a method for authenticating a party (such as an official) for use in a system comprising a storage means (block 1548 in Fig. 15A) addressable using a secret predetermined address (PKO) and a first coded number (CNO) previously stored in the storage means (block 1548) and derivable from the secret predetermined address (PKO) and a coded address (CPKO) generated by coding the secret predetermined address (PKO) with first coded authentication information (CPNO). The method of claim 62 includes receiving a PIN from the party to be authenticated, generating second coded authentication information (CPNO) using the received PIN (block 1530), deriving the secret predetermined address (PKO) by uncoding the coded address (CPKO) using the second coded authentication information (CPNO) (block 1532), generating a second coded number (CNO) by coding the derived secret predetermined address (PKO) with the coded address (CPKO) (block 1534), using the derived secret predetermined address (PKO) to access the storage means (block 1548) and retrieve the first coded number (CNO) stored therein, and authenticating the party if the retrieved first coded number corresponds to the generated second coded number.

In contrast to claim 62, and as discussed further herein, Atalla does not teach or suggest a storage means

addressable using a secret predetermined address, a first coded number derivable from the secret predetermined address and a coded address generated by coding the secret predetermined address with first coded authentication information, deriving the secret predetermined address by uncoding the coded address using second coded authentication information, or generating a second coded number by coding the derived secret predetermined address with the coded address. Therefore, Applicant asserts that claim 62 is patentable over Atalla, and respectfully requests that the Examiner reconsider and withdraw the rejection of claim 62.

In paragraph 5 of the Office Action, the Examiner has rejected claim 5 under 35 U.S.C. § 103 as being unpatentable over Atalla. Applicant notes that claim 5 is dependent upon claim 1. Therefore, Applicant asserts that claim 5 is patentable over Atalla for at least the same reasons as noted above for claim 1, and requests that the Examiner reconsider and withdraw the rejection of claim 5.

In paragraph 6 of the Office Action, the Examiner has rejected claims 40, 41 and 52-54 under 35 U.S.C. § 103 as being unpatentable over Atalla in view of U.S. Patent No. 5,163,098 to Dahbura (hereinafter "Dahbura"). Applicant notes that claims 40 and 41 depend from claim 36. Therefore, the discussion above regarding claim 36 applies to claims 40 and 41, at least with regard to the application of Atalla to claims 40 and 41. Applicant asserts that Dahbura does not solve the deficiencies of

Atalla because Dahbura does not teach or suggest generating first and second numbers such that the coded authentication information is derivable from the first and second numbers. Also, Dahbura does not teach or suggest storing information comprising the secret number in a first storage means addressable using a predetermined secret address, generating a coded secret address using at least a part of the predetermined secret address, and storing the coded secret address and the non-secret number in a second storage means addressable using a predetermined non-secret address, as recited in claim 36. Therefore, Applicant asserts that claims 40 and 41 are patentable over Atalla and Dahbura for at least the same reasons as given above for claim 36, and respectfully requests that the Examiner reconsider and withdraw the rejection of claims 40 and 41.

With regard to the rejection of claims 52-54, Applicant notes that claims 52-54 depend from claim 51. Therefore, the discussion above regarding claim 51 applies to claims 52-54, at least with regard to the application of Atalla to claims 52-54. Applicant asserts that Dahbura does not solve the deficiencies of Atalla. Like Atalla, Dahbura does not teach or suggest generating coded authentication information which is derivable from a secret number and a non-secret number, storage means addressable using a secret predetermined address, a coded address representing a coded portion of the secret predetermined address, and regenerating the secret predetermined address by uncoding the coded address.

Therefore, Applicant asserts that claims 52-54 are patentable over Atalla and Dahbura for at least the same reasons as discussed above with regard to claim 51, and respectfully requests that the Examiner reconsider and withdraw the rejection of claims 52-54.

In paragraph 7 of the Office Action, the Examiner has rejected claims 42 and 43 under 35 U.S.C. § 103 as being unpatentable over Atalla in view of U.S. Patent No. 4,605,820 to Campbell (hereinafter "Campbell"). Applicant notes that claims 42 and 43 depend from claim 36 and, therefore, the discussion above regarding claim 36 also applies to claims 42 and 43, at least with regard to the application of Atalla to claims 42 and 43. Applicant asserts that Campbell does not solve the deficiencies of Atalla since Campbell does not teach or suggest generating first and second numbers such that the coded authentication information is derivable from the first and second numbers. Also, Dahbura does not teach or suggest storing information comprising the secret number in a first storage means addressable using a predetermined secret address, generating a coded secret number using at least a part of the predetermined secret address, and storing the coded secret address and the non-secret number in a second storage means addressable using a predetermined non-secret address, as recited in claim 36. Therefore, Applicant asserts that claims 42 and 43 are patentable over Atalla and Campbell for at least the same reasons as discussed above with regard to claim

36, and respectfully requests that the Examiner reconsider and withdraw the rejection of claims 42 and 43.

In paragraph 8 of the Office Action, the Examiner has rejected claims 7-13, 30-35, 46-50 and 63 under 35 U.S.C. § 102(b) as being anticipated by Dahbura. The rejection is respectfully traversed.

Referring to Figs. 6, 7 and 8B of the application, independent claim 7 is directed to a method for authenticating a transaction and at least one party to the transaction and comprises the steps of coding information relevant to a transaction, such as INFO, with information associated with at least one party, such as a joint key (JK), to generate a variable authentication number (VAN). The JK comprises coded authentication information, such as CPNO, and more particularly, is obtained by coding RTIN with CPNO in block 28 of Fig. 7. CPNO (or simply CPN) is derivable from a predetermined secret code, such as RN, and a predetermined non-secret code, such as ROC (see Fig. 6). CPNO is originally generated by coding a personal identification number (PIN), in an irreversible coder 12. The PIN is unrecoverable within the transaction system. In other words, the PIN is not stored anywhere in the transaction system.

The method of claim 7 also includes associating the VAN with a transaction, such as a check 32, deriving the CPNO from RN and ROC in block 52 of Fig. 8B, and authenticating the VAN

associated with the check 32 using the derived CPNO in blocks 56, 58, and 60 of Fig. 8B.

Dahbura is directed to a system which generates a first verification code by encrypting a user's password with a card number, a transaction date and time, and a merchant identification number. The Examiner contends that the user password is equivalent to the recited predetermined secret code and the transaction date and time are equivalent to the predetermined non-secret code. If the Examiner is correct, then the first verification code of Dahbura must be equivalent to the coded authentication information recited in claim 7. In Dahbura, the first verification code is associated with the transaction (that is, the first verification code is printed on the receipt). In contrast, in claim 7, the coded authentication information is not associated with the transaction. Rather, the VAN is associated with the transaction. Unlike claim 7, Dahbura does not generate a VAN and, consequently, does not associate the VAN with the transaction.

There are additional distinctions between claim 7 and Dahbura. Claim 7 recites a personal identification number (PIN) which is unrecoverable within the transaction system. Dahbura discloses only a user password, which the Examiner has equated to the recited predetermined secret code recited in claim 7. The Examiner has not identified a teaching in Dahbura which anticipates the PIN of claim 7. Applicant notes that the user

password of Dahbura cannot be equated with the PIN of claim 7 because Dahbura clearly teaches that the user password is stored within a system database. In other words, Dahbura clearly teaches that the user password is recoverable within the system (see column 2, lines 50-55). Therefore, unlike claim 7, Dahbura does not teach or suggest a PIN which is unrecoverable within the transaction system. For all of the above reasons, Applicant respectfully asserts that claim 7 is patentable over Dahbura, and respectfully requests that the Examiner reconsider and withdraw the rejection of claim 7. Additionally, since claims 8-13 depend upon claim 7, Applicant asserts that claims 8-13 are also patentable over Dahbura, and respectfully requests that the Examiner reconsider and withdraw the rejection of claims 8-13.

With regard to the rejection of claims 46 and 47, the Examiner contends that column 2 of Dahbura discloses all of the elements and steps of claims 46 and 47. Applicant respectfully disagrees.

Claim 46 as amended recites "determining whether the funds transfer is authentic by using the VAN", "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 funds transfer, such that the funds transfer is substantiated by the RVAN".

Dahbura discloses the generation of a first verification code and a second verification code, wherein if the first verification code matches the second verification code, then the merchant is credited with a receipt amount. In other words, if the first verification code and the second verification code match, then a funds transfer takes place. Unlike the invention of claim 46, Dahbura does not teach or suggest generating after transferring the authenticated funds to the recipient party account a redemption variable authentication number (RVAN). Neither the Dahbura first verification code nor the second verification code can be equated with the RVAN of claim 46 since both the first verification code and the second verification code are generated and utilized before the funds transfer takes place. In fact, the first and second verification codes are used to determine whether the funds transfer should take place. In contrast, the RVAN of claim 46 is generated after the funds transfer takes place, and is not used to determine whether the funds transfer takes place. For these reasons, Applicant asserts that claim 46 is patentable over Dahbura, and respectfully requests that the Examiner reconsider and withdraw the rejection of claim 46. Since claim 47 depends from claim 46, Applicant further asserts that claim 47 is patentable over Dahbura, and respectfully requests that the Examiner also reconsider and withdraw the rejection of claim 47.

With regard to the rejection of claim 30, the Examiner contends that Dahbura in column 2, lines 21-59, discloses generating a joint code and storing the joint code in a storage means, wherein the storage means is inaccessible without knowledge of a party password. Applicant respectfully disagrees.

Claim 30 as amended is directed to a method for enrolling a party into a transaction system to thereby enable the party to participate in subsequent transactions. Referring to Fig. 10A of the application, the method of claim 30 comprises the step of coding information associated with the party, such as PKU, with information associated with an official, such as CPKO, to generate a joint code, such as JKU, as depicted by block 132. The method of claim 30 also includes storing the joint code (JKU) in a first storage means, such as user file number 2 (block 112'), wherein the first storage means is accessible only to a party with knowledge of a first PIN associated with the party. In this manner, if no one exists with knowledge of the first PIN, the joint code (JKU) cannot be accessed from the first storage means and, therefore, the joint code (JKU) cannot be associated with a future transaction.

In contrast to claim 30, Dahbura is directed to a system and method for verifying a transaction. Unlike claim 30, Dahbura does not teach or suggest a method for enrolling a party to thereby enable the party to participate in future transactions. There are other distinctions between claim 30 and Dahbura. For

example, claim 30 requires the joint code (JKU) to be stored in a first storage means (user file number 2) wherein the first storage means is accessible only to someone with knowledge of the first PIN. In contrast, Dahbura does not teach or suggest any storage means wherein information stored therein is accessible only to a party with knowledge of a PIN. Dahbura does disclose that the password is stored in a database, but does not specify or even suggest that the database is accessible only to someone with knowledge of a PIN. Therefore, Applicant asserts that claim 30 is patentable over Dahbura and, therefore, respectfully requests that the Examiner reconsider and withdraw the rejection of claim 30. Additionally, since claims 31 and 32 are dependent on claim 30, Applicant respectfully asserts that claims 31 and 32 are patentable over Dahbura and requests that the Examiner reconsider and withdraw the rejection of claims 31 and 32.

With regard to the rejection of claims 33-35, the Examiner contends that Dahbura in column 2 discloses all of the elements and steps of claims 33-35. Applicant respectfully traverses the rejection.

Claim 33 as amended is directed to 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 a transaction, receiving a PIN from a recipient party, determining whether the recipient party is

authentic by using the received recipient PIN, determining whether the transaction is authentic, and authorizing the transaction if the recipient party and the transaction are authentic. Therefore, in claim 33, the transaction is processed only after the recipient is authorized using the received recipient PIN. In contrast to claim 33, in Dahbura the recipient party (i.e., the merchant) is not authorized prior to processing the transaction. That is, the transaction is processed without first authorizing the person who presents the transaction for processing. In fact, anyone can present the receipt to the credit card center for processing and payment. Thus, Dahbura is much less secure than claim 33. For the above reasons, Applicant asserts that claim 33 is patentable over Dahbura and requests that the Examiner reconsider and withdraw the rejection of claim 33. Additionally, since claims 34 and 35 depend from claim 33, Applicant asserts that claims 34 and 35 are patentable over Dahbura and requests that the Examiner reconsider and withdraw the rejection of claims 34 and 35.

With regard to the rejection of claims 48-50, the Examiner contends that Dahbura in column 2 discloses all of the elements and steps of claims 48-50. Applicant respectfully traverses the rejection.

Amended claim 48 is directed to a method for processing an invoice in an invoice processing system wherein a personal identification number (PIN) and a VAN are received from a payor party. The received PIN is used to authenticate the payor party

and the received VAN. As recited in amended claim 48, the received PIN is unrecoverable in the invoice processing system. In other words, the received PIN is not stored anywhere in the invoice processing system. In contrast, Dahbura discloses that the user password is stored and retrievable from a system database (column 2, lines 50-55 of Dahbura). Therefore, unlike claim 48, Dahbura does not teach or suggest a personal identification number which is unrecoverable in the system, as recited in claim 48. Additionally, it would not have been obvious to modify Dahbura to include an unrecoverable password since Dahbura validates transactions by comparing a first verification code with a second verification code, wherein the second verification code is generated using a password which is retrieved from a system database. Thus, the incorporation of an unrecoverable password into Dahbura would require fundamental structural and operational changes in the manner in which the second verification code was generated. For all of the above reasons, Applicant respectfully asserts that claim 48 is patentable over Dahbura and requests that the Examiner reconsider and withdraw the rejection of claim 48.

Additionally, since claims 49 and 50 are dependent upon claim 48, Applicant asserts that claims 49 and 50 are patentable over Dahbura for at least the same reasons as noted above with regard to claim 48. Also, Applicant notes that claim 49 recites steps for generating a redemption VAN (RVAN) and associating the RVAN with the invoice after the invoice has been processed.

Therefore, the discussion above regarding claim 33 also applies to claim 49. For all of the above reasons, Applicant asserts that claims 48-50 are patentable over Dahbura and requests that the Examiner reconsider and withdraw the rejection of claims 48-50.

With regard to the rejection of claim 63, the Examiner contends that the authentication process of Dahbura in column 2, lines 21-59, anticipates the steps of claim 63. Applicant respectfully traverses the rejection of claim 63. Claim 63 is directed to a method which includes a step for receiving a PIN from a party to be authenticated wherein the PIN is unrecoverable in the system. Therefore, claim 63 is similar to claim 48 (with regard to the PIN being unrecoverable in the system) and, therefore, the comments above pertaining to claim 48 are applicable to claim 63. Consequently, Applicant asserts that claim 63 is patentable over Dahbura for at least the same reasons as cited above for claim 48, and respectfully requests that the Examiner reconsider and withdraw the rejection of claim 63.

In paragraph 9 of the Office Action, the Examiner has rejected claims 14-16 under 35 U.S.C. § 103 as being unpatentable over Dahbura. The Examiner notes that Dahbura differs from claims 14-16 in that Dahbura is not applied to the dispensing of medical prescriptions. However, the Examiner contends that it would have been obvious to one of ordinary skill in the art to apply Dahbura to the dispensing of medical prescriptions since, like credit card purchases and automatic teller transactions, the

dispensing of medical prescriptions is subject to attempted fraud and, therefore, requires authentication. The rejection of claims 14-16 is respectfully traversed.

Applicant notes that claims 14-16 are dependent upon claim 7 and, therefore, are patentable over Dahbura for the same reasons as discussed above with regard to claim 7. There are additional distinctions between claims 14-16 and Dahbura. For example, in Dahbura, the receipt which is presented by the merchant to the credit card center includes a first verification code which was generated using inter alia the merchant's identification number. In other words, the receipt identifies the eventual payee (that is, the merchant) of the transaction. In contrast, the VAN associated with the medical prescription form is associated only with the originating physician and the patient. In contrast to Dahbura, the VAN associated with the medical prescription form does not identify the eventual payee (that is, the entity who processes the prescription form and who thereby identifies who is to receive payment for such processing).

Additionally, with regard to claim 16, Dahbura does not teach or suggest a correspondent physician licensed in a processing jurisdiction, or a step of obtaining authorization for processing a medical prescription form in the processing jurisdiction from the correspondent physician when the originating physician is not licensed to practice in the processing jurisdiction. For all of the above reasons, Applicant

respectfully asserts that claims 14-16 are patentable over Dahbura and, therefore, requests that the Examiner reconsider and withdraw the rejection of claims 14-16.

Applicant also asserts that the combination suggested by the Examiner is improper. It is well settled that when making a rejection under 35 U.S.C. § 103, the Examiner has the burden of establishing a prima facie case of obviousness. The Examiner can satisfy this burden only by showing an objective teaching in the prior art or that knowledge generally available to one of ordinary skill in the art would lead that individual to combine the relevant teachings of the references in the manner suggested by the Examiner. In re Fine, 5 U.S.P.Q.2d 1596, 1598 (Fed. Cir. 1988). Obviousness cannot be established by combining the teachings of the prior art to produce the claimed invention absent some teaching suggestion or incentive supporting the combination. In re Geiger, 2 U.S.P.Q.2d 1276, 1278 (Fed. Cir. 1987). Prior art references taken in combination do not make an invention obvious unless something in the particular prior art references would suggest the advantages to be derived from combining the teachings of the references. In re Sernaker, 217 U.S.P.Q. 1, 6 (Fed. Cir. 1983). The mere fact that the prior art could be modified in the manner proposed by the Examiner does not make the modification obvious unless the prior art suggests the desirability of the modification. Ex parte Dussaud, 7 U.S.P.Q.2d 1818, 1820 (PTO Bd. App. & Int. 1988). As the Court of Appeals

for the Federal Circuit points out, it is impermissible to use hindsight reconstruction to pick and choose among isolated disclosures in the prior art to deprecate the claimed invention. Fine, 5 U.S.P.Q.2d at 1600. "Something in the prior art as a whole must suggest the desirability, and thus the obviousness of [the invention]." Uniroyal Inc. v. Rudkin-Wiley Corp., 5 U.S.P.Q.2d 1434, 1438 (Fed. Cir. 1988) (emphasis added).

It is respectfully submitted that in making the present rejection, the Examiner has employed impermissible hindsight in using the Applicant's disclosure and claims to conduct a search of the prior art to locate a reference disclosing a transaction authorization system (i.e., Dahbura). Once the Dahbura reference was located, the Examiner concluded that it would have been obvious to one of ordinary skill in the art to modify the Dahbura reference to the dispensing of medical prescriptions. However, as discussed above, Dahbura does not teach, suggest or provide an incentive to make the improvement suggested by the Examiner. Accordingly, it is respectfully submitted that the combination suggested by the Examiner is improper and, therefore, the rejection of claims 14-16 under 35 U.S.C. § 103 is improper and should be withdrawn.

In paragraph 10 of the Office Action, the Examiner has rejected claims 17-20, 22-27, 56 and 59 under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 4,302,810 to Bouricius et

al. (hereinafter "Bouricius"). The rejection is respectfully traversed.

With regard to the rejection of claims 17-19, the Examiner contends that Bouricius discloses a three party system (person, retailer, and host system) which uses the person's encryption key and the retailer's encryption key to double encrypt transaction information. The Examiner contends that the person and the retailer are present when such encryption takes place and that the host system is absent. The rejection is respectfully traversed.

Claim 17 has been amended to more clearly define the VAN as being generated using information associated with at least one present party and with information associated with at least one absent party. The invention of claim 17 is very flexible in that not all parties to a transaction are required to be present when the transaction is created (for example, the recipient of a check need not be present when the originator writes the check). Despite this flexibility, the invention of claim 17 is very powerful with regard to its security features. In contrast, Bouricius requires that all parties to a transaction be present when the transaction is created. In particular, and as noted by the Examiner, both the person to the transaction and the retailer must be present when the doubled encrypted transaction information is created. Whether or not the host system is absent when the transaction is created is irrelevant. This is true since

information associated with the host system is not used to create the double encrypted transaction information. Consequently, claim 17 requires that the VAN be generated with information associated with present and absent parties, whereas Bouricius teaches that the double encrypted transaction information is created only from present parties. Therefore, Applicant respectfully asserts that claim 17 and its dependent claim 19 (note that claim 18 has been cancelled) are patentable over Bouricius and, therefore, respectfully request that the Examiner reconsider and withdraw the rejection of claims 17 and 19.

With regard to the rejection of claims 56 and 59, the Examiner contends that Bouricius anticipates claims 56 and 59 for the same reasons as noted above for claim 17. Claim 56 has been amended in a similar manner as claim 17 to more particularly define that the VAN is generated using information associated with at least one present party and with information associated with at least one absent party. Therefore, Applicant asserts that claim 56 is patentable over Bouricius for at least the same reasons as discussed above with regard to claim 17 and, therefore, requests that the Examiner reconsider and withdraw the rejection of claim 56.

Claim 59 has been amended to recite 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, 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. Bouricius does not teach or disclose means for generating an RVAN or means for associating the RVAN with the transaction after the transaction has been authorized and processed. Therefore, for at least the above reasons, Applicant respectfully asserts that claim 59 as amended is patentable over Bouricius, and requests that the Examiner reconsider and withdraw the rejection of claim 59.

With regard to claim 20, the Examiner contends that Bouricius discloses a system in which a host system receives coded authentication information (both singularly and doubly encryptic), uses transmitted information to retrieve secret information (encryption keys) and non-secret information (account number), and compares the decrypted transmitted authentication information.

Applicant respectfully traverses the rejection of claim 20.

Claim 20 is directed to a method for authenticating a party having a personal identification number (PIN) from which first coded authentication information (CPN) is generated, wherein the first coded authentication information is derivable from a predetermined secret number (RN) and a predetermined non-secret number (ROC). The method of claim 20 includes the steps of receiving at a first site a personal identification number (PIN) from the party (block 40 of Fig. 8A) and generating second coded

authentication information (CPNR generated at block 42 of Fig. 8A) by using the received PIN. The method of claim 20 also includes retrieving the secret number (RN) and the non-secret number (ROC) from a storage means (block 68), generating third coded authentication information (CPNR) using the secret and non-secret numbers (block 70), and comparing the second and third coded authentication information (blocks 44, 48, 62, 64, 66).

In contrast, Bouricius does not disclose or suggest the use of a personal identification number as recited in claim 20. None of the Bouricius figures show the receipt or use of a PIN. Figs. 5A, 5B and 5C depict a person's card number, but this differs greatly from a personal identification number which, as is well know, is secret (card numbers are not generally secret). Additionally, Bouricius does not teach or suggest comparing second coded authentication information and third coded authentication information. Instead, Bouricius discloses first deencrypting TM2 and TM1 and then comparing the decrypted codes. Further, Bouricius does not teach or suggest coded authentication information which is generated using a PIN, and which is also derivable from a secret number and a non-secret number. For all of the above reasons, Applicant respectfully asserts that claim 20 is patentable over Bouricius and respectfully requests that the Examiner reconsider and withdraw the rejection of claim 20.

Regarding the rejection of claims 22-27, Applicant notes that claims 22-27 are dependent upon claim 20. Therefore,

Applicant asserts that claims 22-27 are patentable over Bouricius for the same reasons as noted above for claim 20, and requests that the Examiner reconsider and withdraw the rejection of claims 22-27.

In paragraph 11 of the Office Action, the Examiner has rejected claim 21 under 35 U.S.C. § 103 as being patentable over Bouricius. Applicant notes that claim 21 is dependent upon claim 20. Therefore, Applicant asserts that claim 21 is patentable over Bouricius for at least the same reasons as discussed above for claim 20 and, therefore, respectfully requests that the Examiner reconsider and withdraw the rejection of claim 21.

New claim 64 has been added. The device recited in claim 64 is shown in Figs. 6 and 7. Therefore, no new matter is added by new claim 64. Applicant asserts that new claim 64 is patentable over the cited prior art for generally the reasons cited above. Specifically, claim 64 is patentable over the cited prior art because the cited prior art does not teach or suggest a VAN which is generated using at least information associated with a party wherein such party information is derivable by uncoding a predetermined non-secret number with a predetermined secret number. For at least the above reasons, Applicant asserts that claim 64 is patentable over the cited prior art and, therefore, respectfully requests that claim 64 be allowed.

In view of the foregoing discussion, it is respectfully submitted that the present application, including claims 1, 3,

5-17, and 19-64 as amended, is in condition for allowance and such action is respectfully requested.

Respectfully submitted,

LEON STAMBLER



Michael Q. Lee

Registration No. 35,239

PANITCH SCHWARZE JACOBS & NADEL

1601 Market Street, 36th Floor

Philadelphia, PA 19103

Telephone (215) 567-2020

3/18/93
(Date)

MQL:amh



**UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office**

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

Serial Number: 077879,085 Filing Date: 11/12/92 First Named Inventor: STONOLUK Attorney Docket No.: 0074-1

Examiner: DANGIAL

20M1/0611
PATENT SCHWARZE JACOBS & NADEL
1601 MARKET STREET
26TH FLOOR
PHILADELPHIA, PA 19103

ART UNIT: 2202 PAPER NUMBER: 5

DATE MAILED: 06/11/93

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 3/22/93 ☐ This action is made final.

A shortened statutory period for response to this action is set to expire THIRTY 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 re Patent Drawing, PTO-948. |
| 3. <input checked="" type="checkbox"/> Notice of Art Cited by Applicant, PTO-1449. | 4. <input type="checkbox"/> Notice of informal Patent Application, Form 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 1, 3, 5-17, 19-64 are pending in the application.
Of the above, claims 7-17, 19-35, 46-50, 56-59, 63 and 64 are withdrawn from consideration.
2. ☐ Claims _____ have been cancelled.
3. ☒ Claims 1, 3, 5, 6, 36-45, 51-55, 60 and 62 are allowed.
4. ☐ Claims _____ are rejected.
5. ☐ Claims _____ are objected to.
6. ☒ Claims 1, 3, 5-17, 19-64 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 re Patent Drawing, 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 on _____, has been ☐ approved. ☐ disapproved (see explanation).
12. ☐ Acknowledgment is made of the claim for priority under 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

Restriction to one of the following inventions is required under 35 U.S.C. 121:

I. Claims 1,3,5, 6, and 36-45, 51-55,60-62, drawn to Authentication by Secret Address System, classified in Class 380 subclass 23.

II. Claims 7-17,19, , 33-35, 46-47, 48-50,56,59,64 drawn to a Variable Authentication Number Method and Apparatus , classified in Class 380, subclass 24.

III. Claims 20-27, 63 , drawn to Authentication System, classified in Class 340, subclass 825.34.

IV. Claims 28-32, 57,58 drawn to a Method and Apparatus for Enrolling, classified in Class 340, subclass 825.31.

The inventions are distinct, each from the other because of the following reasons:

Inventions of Groups II, III, and IV and Group I are related as combination and subcombination. Inventions in this relationship are distinct if it can be shown that (1) the combination as claimed does not require the particulars of the subcombination as claimed for patentability, and (2) that the subcombination has utility by itself or in other combinations. (M.P.E.P. § 806.05(c)). In the instant case, the combination as claimed does not require the particulars of the subcombination as claimed because it does not require the secret address authentication . The subcombination has separate utility such as encrypted authentication method and apparatus.

Because these inventions are distinct for the reasons given above and have acquired a separate status in the art as shown by their different classifications restriction for examination purposes as indicated is proper.

07/977,385
Art Unit 2202

- 3 -


Applicant is advised that the response to this requirement to be complete must include an election of the invention to be examined even though the requirement be traversed.

During a telephone conversation with Leslie Kasten, Jr. on 6/8/93 a provisional election was made with traverse to prosecute the invention of Group I, claims 1,3,5, 6, and 36-45, 51-55,60-62. Affirmation of this election must be made by applicant in responding to this Office action. Claims 7-17, 18-35, 46-50, 56-59, 63, 64 stand withdrawn from further consideration by the Examiner, 37 CFR 1.142(b), as being drawn to a non-elected invention.

This application is in condition for allowance except for the presence of claims 7-17, 18-35, 46-50, 56-59, 63, 64 to an invention non-elected with traverse above. **APPLICANT IS GIVEN THIRTY DAYS FROM THE DATE OF THIS LETTER TO CANCEL THE NOTED CLAIMS OR TAKE OTHER APPROPRIATE ACTION (37 CFR 1.144).** Failure to take action during this period will be treated as authorization to cancel the noted claims by Examiner's Amendment and pass the case to issue. Extensions of time under 37 CFR 1.136(a) will not be permitted since this application will be passed to issue.

The prosecution of this case is closed except for consideration of the above matter.

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. 977,385		GROUP/ART UNIT 2202		ATTACHMENT TO PAPER NUMBER 5						
NOTICE OF REFERENCES CITED				APPLICANT(S) Stamler										
U.S. PATENT DOCUMENTS														
*		DOCUMENT NO.						DATE	NAME	CLASS	SUB-CLASS	FILING DATE IF APPROPRIATE		
	A	4	3	1	9	0	7	9	3/9/82	Best	380	4		
	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 S. Congiobesi								DATE 6/93						
* A copy of this reference is not being furnished with this office action. (See Manual of Patent Examining Procedure, section 707.05 (a).)														

22C
6-15-93
JUL 1 1993



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 June 29, 1993

RECEIVED

JUL 07 1993

GROUP 220

Patent

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Patent Application of : Group Art Unit 2207
Leon Stambler :
Serial No: 07/977,385 : Examiner: S. Cangialosi
Filed: November 17, 1992 :
For: SECURE TRANSACTION SYSTEM : Attorney Docket
AND METHOD UTILIZED THEREIN : No. 6074-1

AMENDMENT

In response to the Office Action mailed June 11, 1993,
with a shortened statutory period of response of thirty (30)
days, please amend the above-identified application as follows:

In the Claims:

Please amend claim 3 as follows:

2 1. (Amended) The method of claim 1, wherein the
[first coded authentication information] coded address is
extracted from a storage means which is in the possession of the
party.

Please cancel claims 7-17, 48-35, 46-50, 56-59, 63 and
64 without prejudice to the filing of a divisional application
with respect to each of these claims.

REMARKS

After the foregoing amendment, claims 1, 3, 5, 6, 36-45, 51-55, and 60-62 are active in the present application. The remaining claims have been cancelled as being drawn to a non-elected invention. Applicant hereby confirms the telephone election made to proceed with prosecution of the invention claimed in the claims of Group I, the only claims now remaining in the application. The remaining claims has been cancelled subject to the filing of a divisional application at a later date.

In the last Office Action, all of the claims of Group I, the only claims now remaining in the application, were indicated by the Examiner as being allowed. It is noted that the cover sheet to the last Office Action failed to indicate the allowance of claim 61, although this claim was indicated as being allowed as part of the claims of Group I on page 3 of the Office Action, and the Applicant assumes that the inconsistency is due to an error on the PTOL-326 cover sheet.

The foregoing amendment to claim 3 was made in order to make the language of claim 3 consistent with the language of claim 1 which was previously amended. Although prosecution on the merits is closed, the amendment to claim 3 adds no new matter to the application and does not change the substance of claim 3. Accordingly, entry of the amendment to claim 3 is respectfully requested.

12909.1

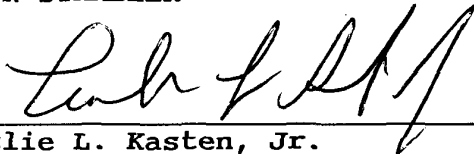
-2-

After the foregoing amendment and discussion, it is believed that the application, including claims 1, 3, 5, 6, 36-45, 51-55 and 60-62 is in condition for allowance and such action is respectfully solicited.

Respectfully submitted,

LEON STAMBLER

6/29/93
(Date)

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/amh



UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office

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

07/977,385 11/17/92 STAMBLER

L 6074-1

EXAMINER
CANGIALOSI, S

22M1/0722

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

ART UNIT

PAPER NUMBER

2202

7

DATE MAILED:

07/22/93

NOTICE OF ALLOWABILITY

PART I.

1. ☒ This communication is responsive to 7/1/93
2. ☒ 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.
3. ☒ The allowed claims are 1, 3, 5, 6, 36-45, 51-55, 60-62
4. ☐ The drawings filed on _____ are acceptable.
5. ☐ 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 _____.
6. ☐ Note the attached Examiner's Amendment.
7. ☐ Note the attached Examiner Interview Summary Record, PTOL-413.
8. ☐ Note the attached Examiner's Statement of Reasons for Allowance.
9. ☐ Note the attached NOTICE OF REFERENCES CITED, PTO-892.
10. ☐ 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).

1. ☐ 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.
2. ☒ APPLICANT MUST MAKE THE DRAWING CHANGES INDICATED BELOW IN THE MANNER SET FORTH ON THE REVERSE SIDE OF THIS PAPER.
 - a. ☒ Drawing informalities are indicated on the NOTICE RE PATENT DRAWINGS, PTO-948, attached hereto or to Paper No. 2. CORRECTION IS REQUIRED.
 - b. ☐ The proposed drawing correction filed on _____ has been approved by the examiner. CORRECTION IS REQUIRED.
 - c. ☐ Approved drawing corrections are described by the examiner in the attached EXAMINER'S AMENDMENT. CORRECTION IS REQUIRED.
 - d. ☒ 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

22M1/0722
PANITCH SCHWARZE JACOBS & NADEL
1601 MARKET STREET
36TH FLOOR
PHILADELPHIA, PA 19103

NOTICE OF ALLOWANCE
AND ISSUE FEE DUE

☐ 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
07/977,385	11/17/92	022	CANGIALOSI, S 2202	07/22/93
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 6074-1	380-024.000	P08	UTILITY	YES	\$585.00	10/22/93

THE APPLICATION IDENTIFIED 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, payment 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 a 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 communications prior to issuance to Box ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees.

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 Margaret A. Jones
DATE August 18, 1993

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re:	Patent Application of Leon Stambler	: Attn: Official Draftsman :
Serial No.:	07/977,385	: Group Art Unit: 2202 :
Filed:	November 17, 1992	: Batch No.: P08 :
For:	SECURE TRANSACTION SYSTEM AND METHOD UTILIZED THEREIN	: Attorney Docket : No. 6074-1 :

TRANSMITTAL OF FORMAL DRAWINGS

In accordance with the Notice of Allowability mailed
July 22, 1993, enclosed are fifteen (15) sheets of drawings (two
copies 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 on August 17, 1993.

Respectfully submitted,

August 18, 1993
Date

By Martin G. Belisario
MARTIN G. BELISARIO
Registration No. 32,886
PANITCH SCHWARZE JACOBS & NADEL
1601 Market Street, 36th Floor
Philadelphia, PA 19103
Telephone: (215) 567-2020

MGB/MES/maj

19517.1

5267314

977385

16
380 24

FIG. 1

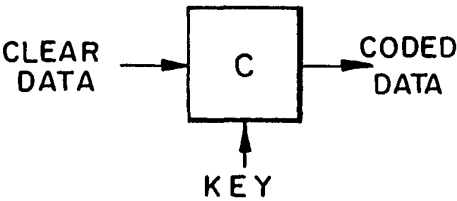


FIG. 2

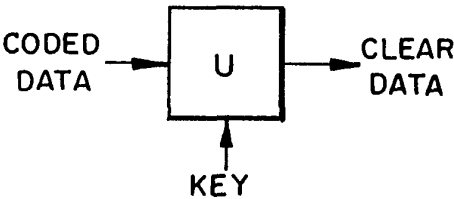


FIG. 3

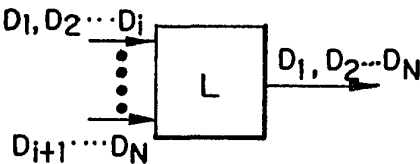


FIG. 4

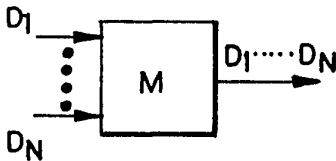


FIG. 5

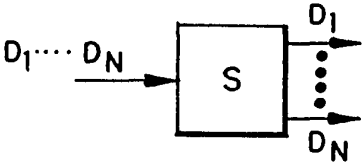
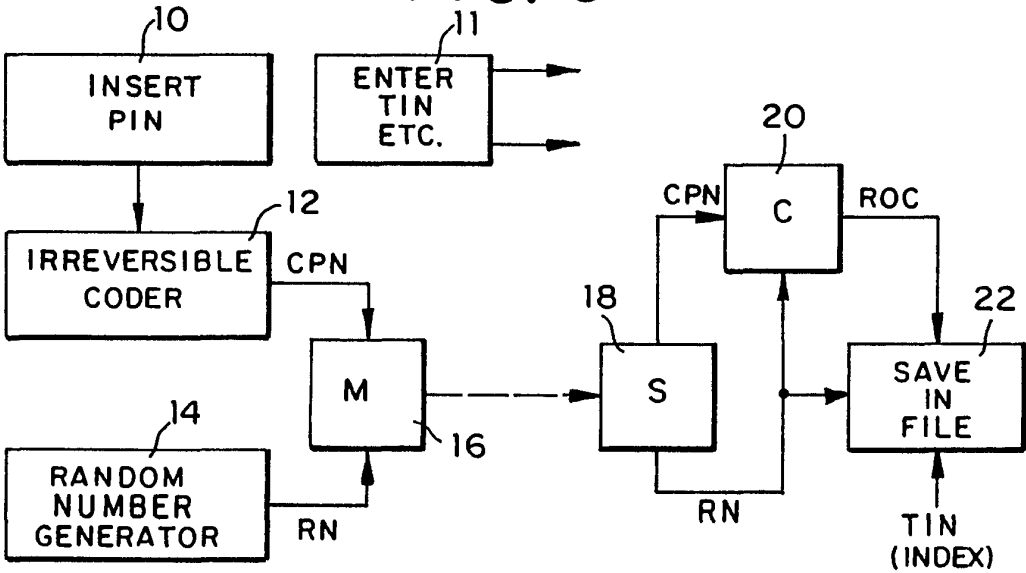
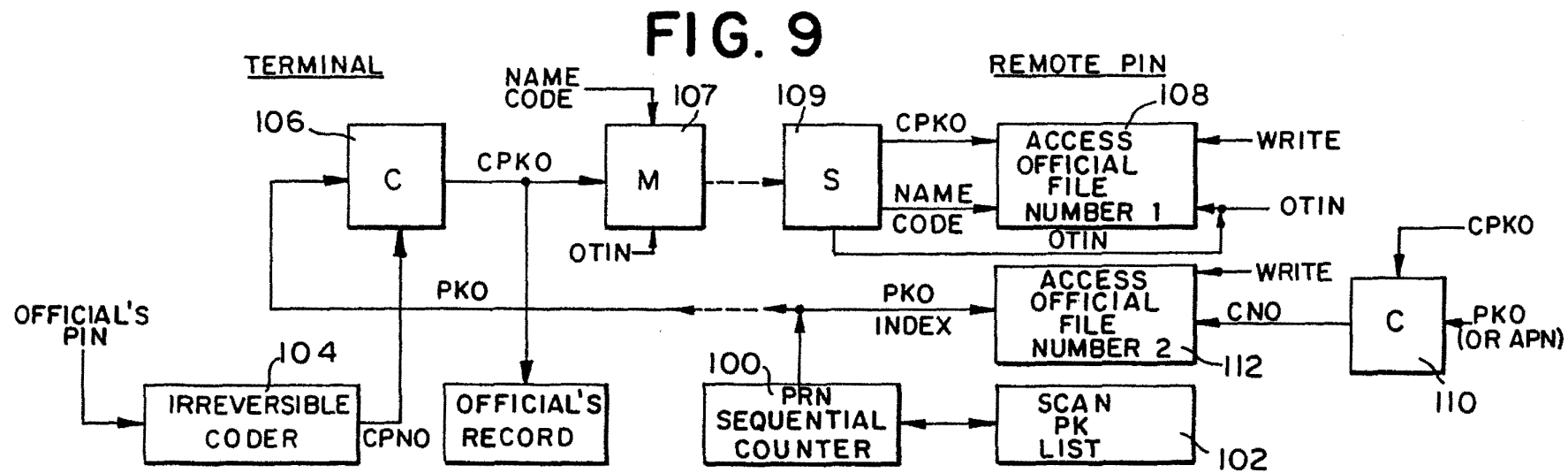
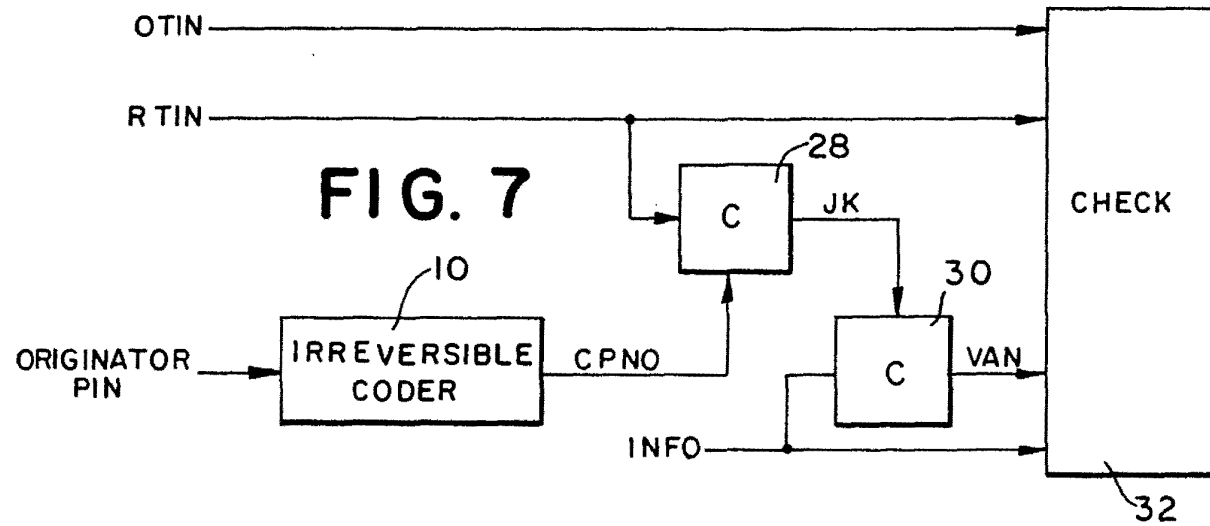
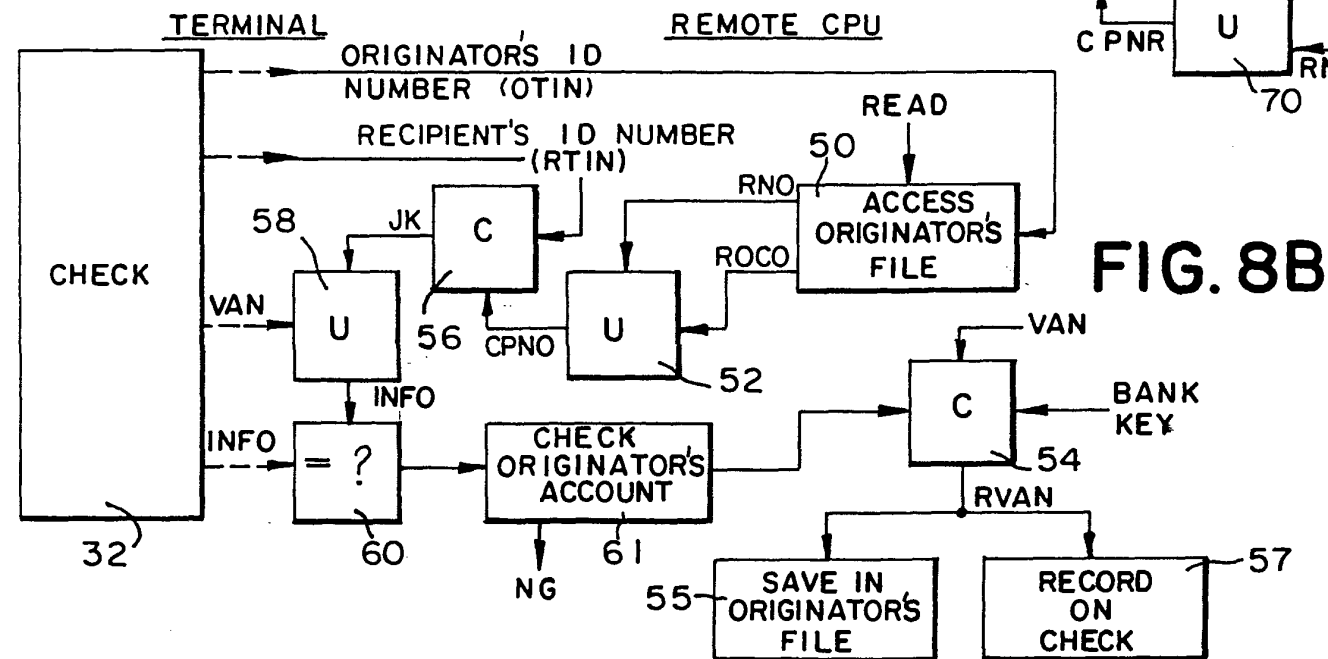
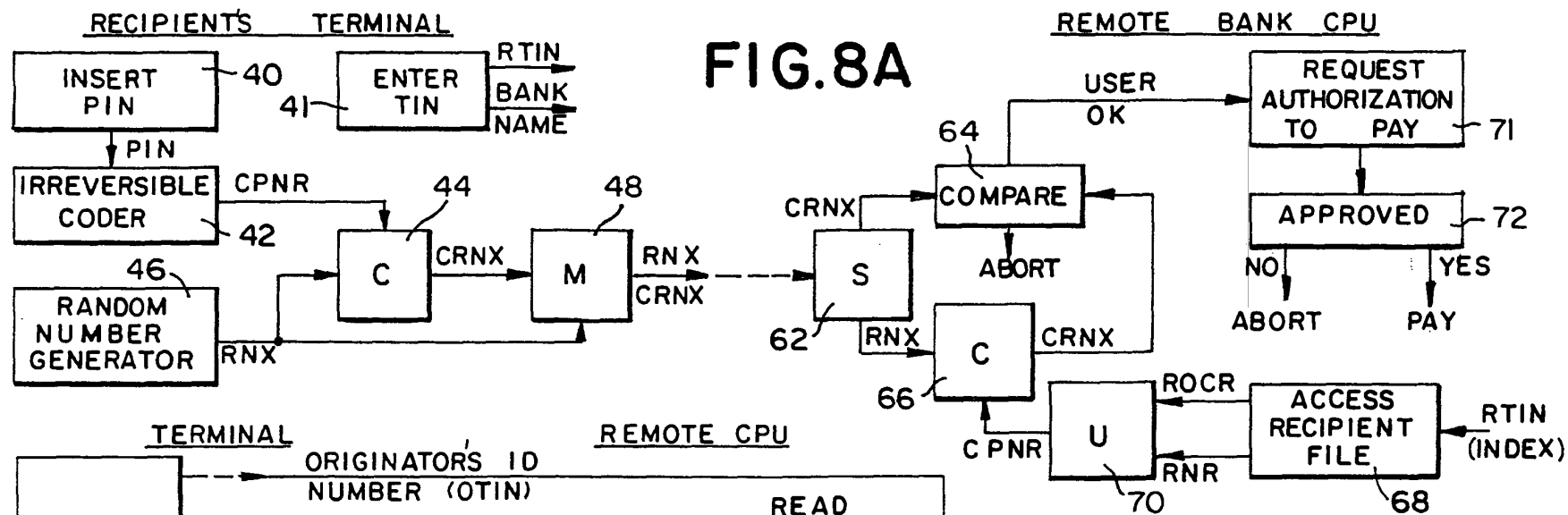
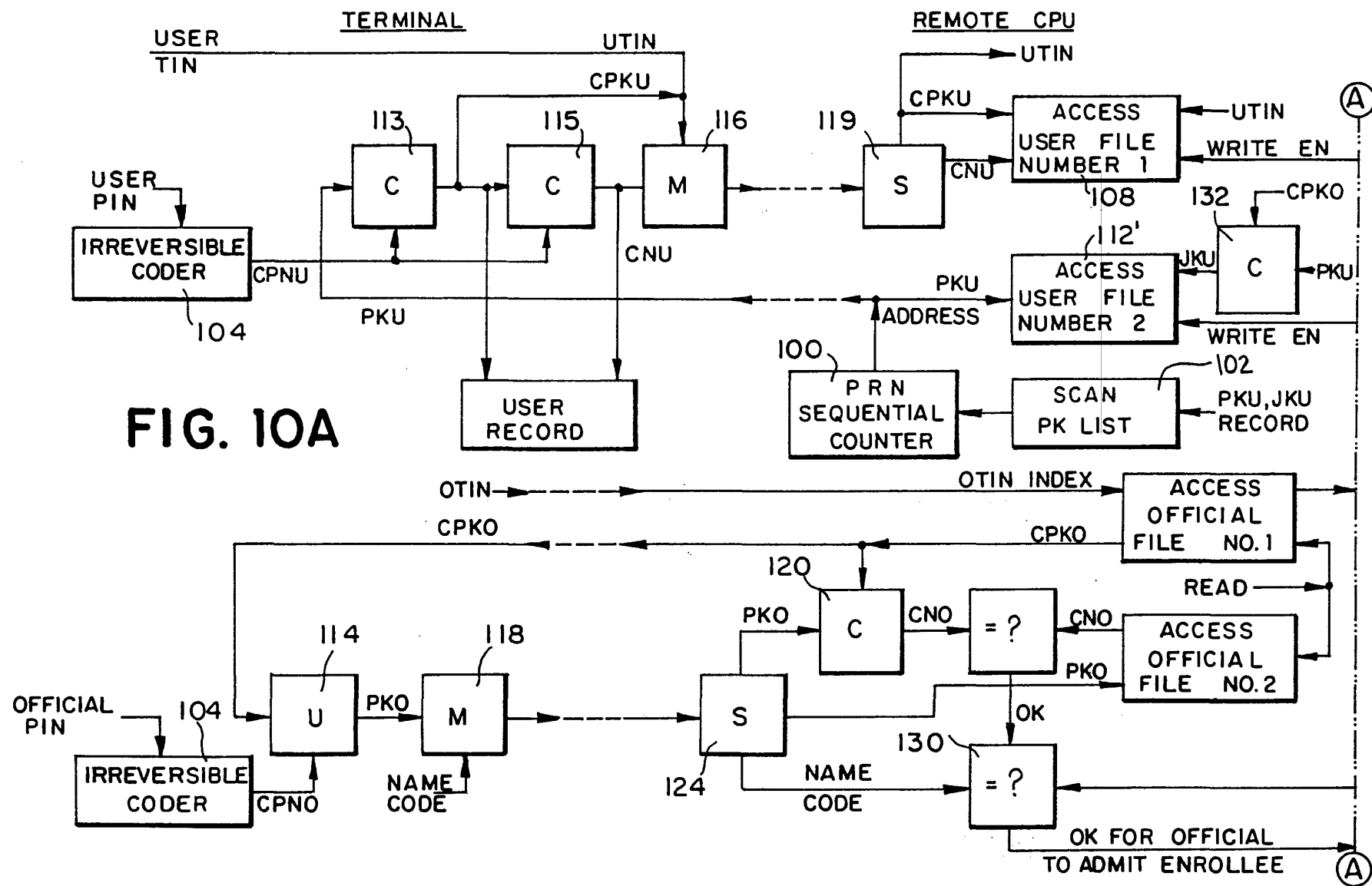


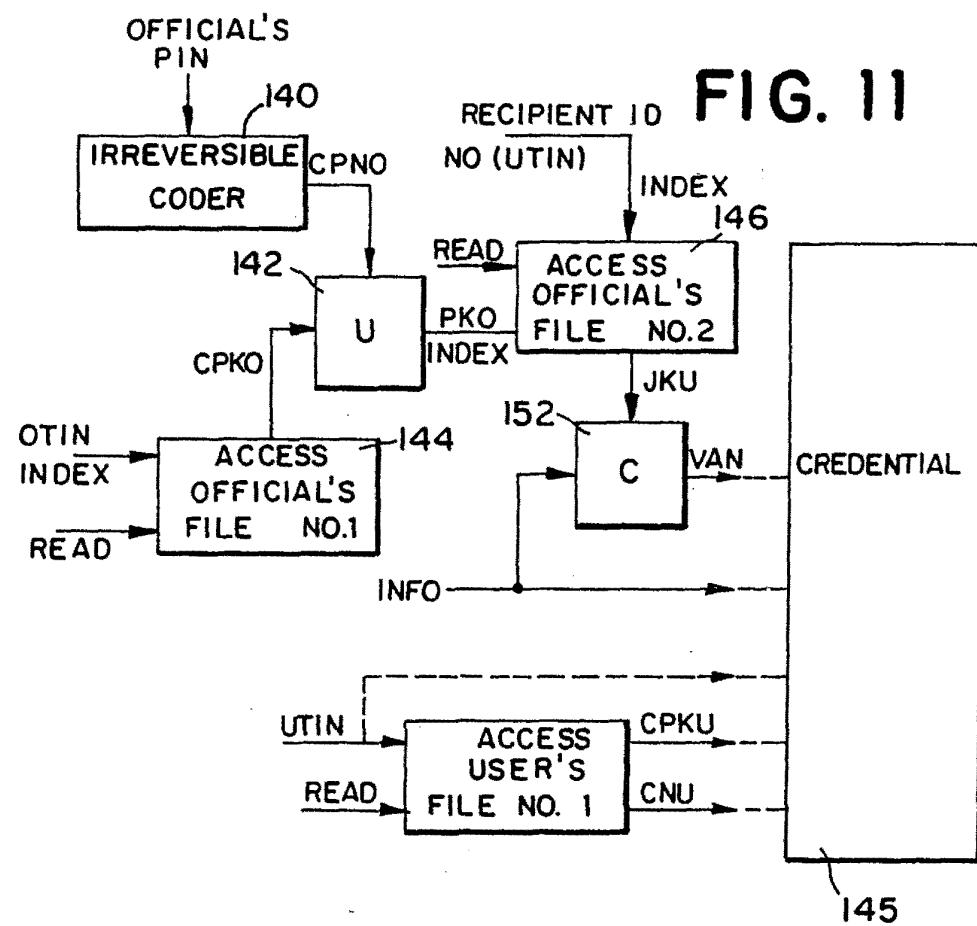
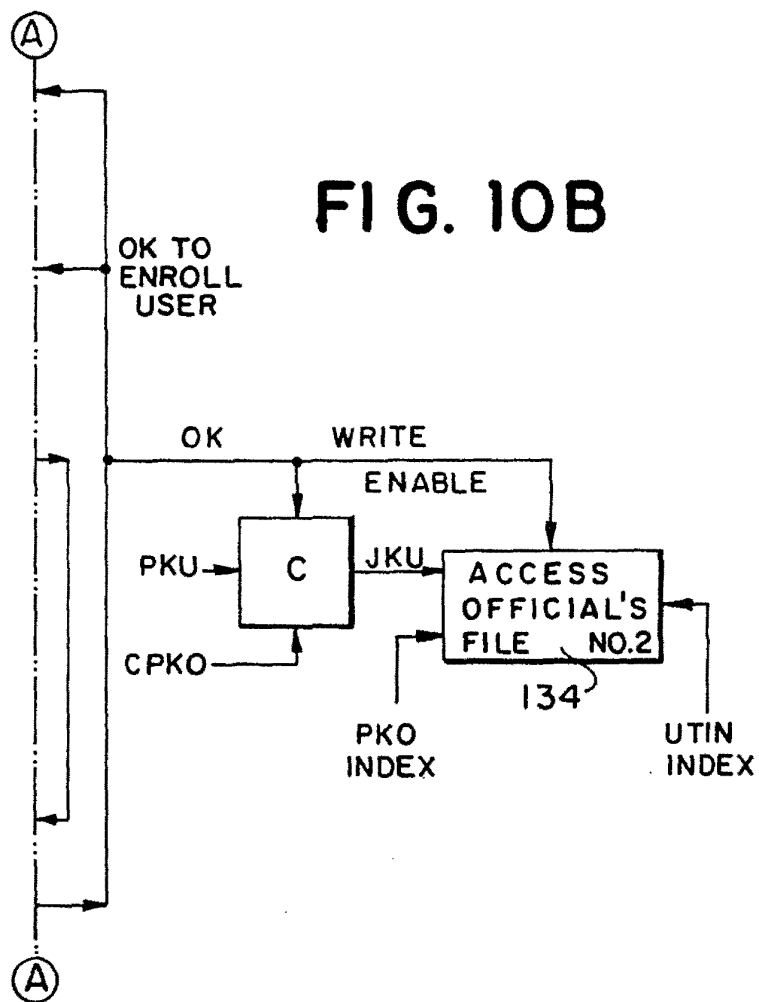
FIG. 6











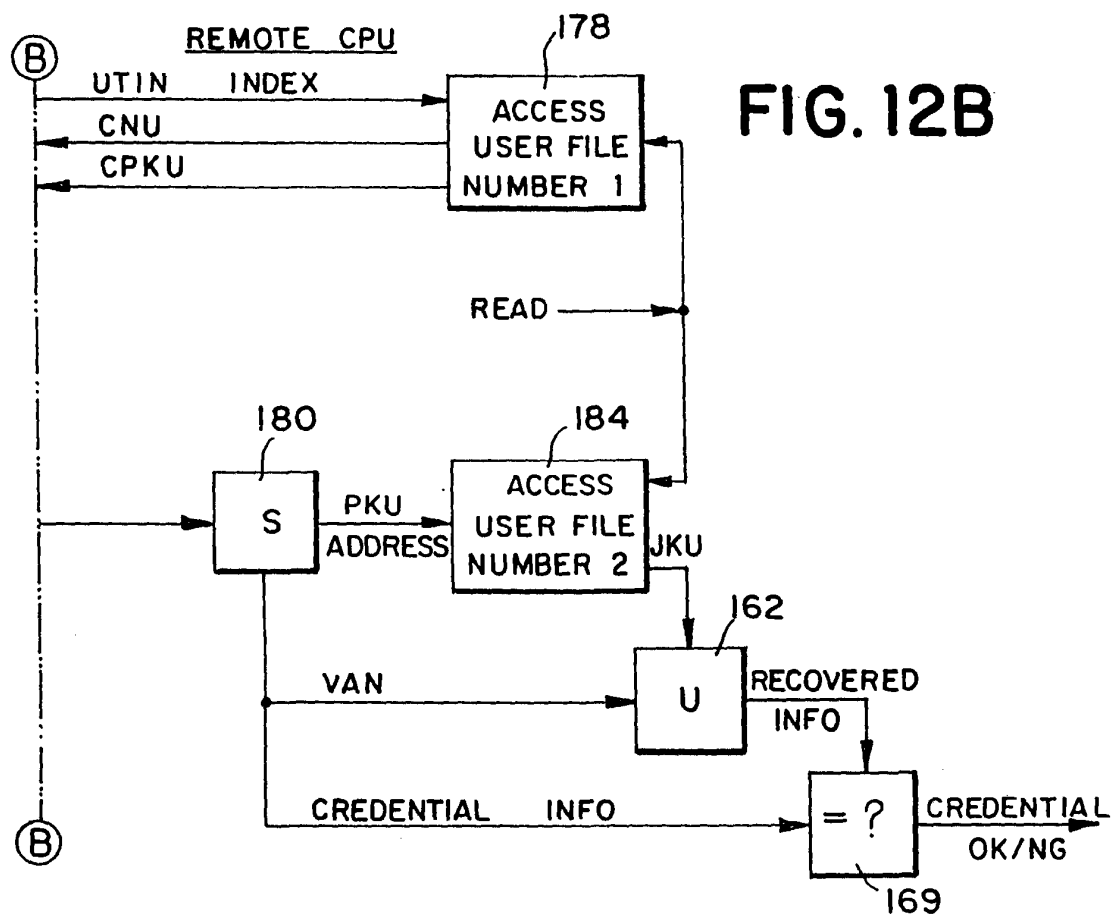
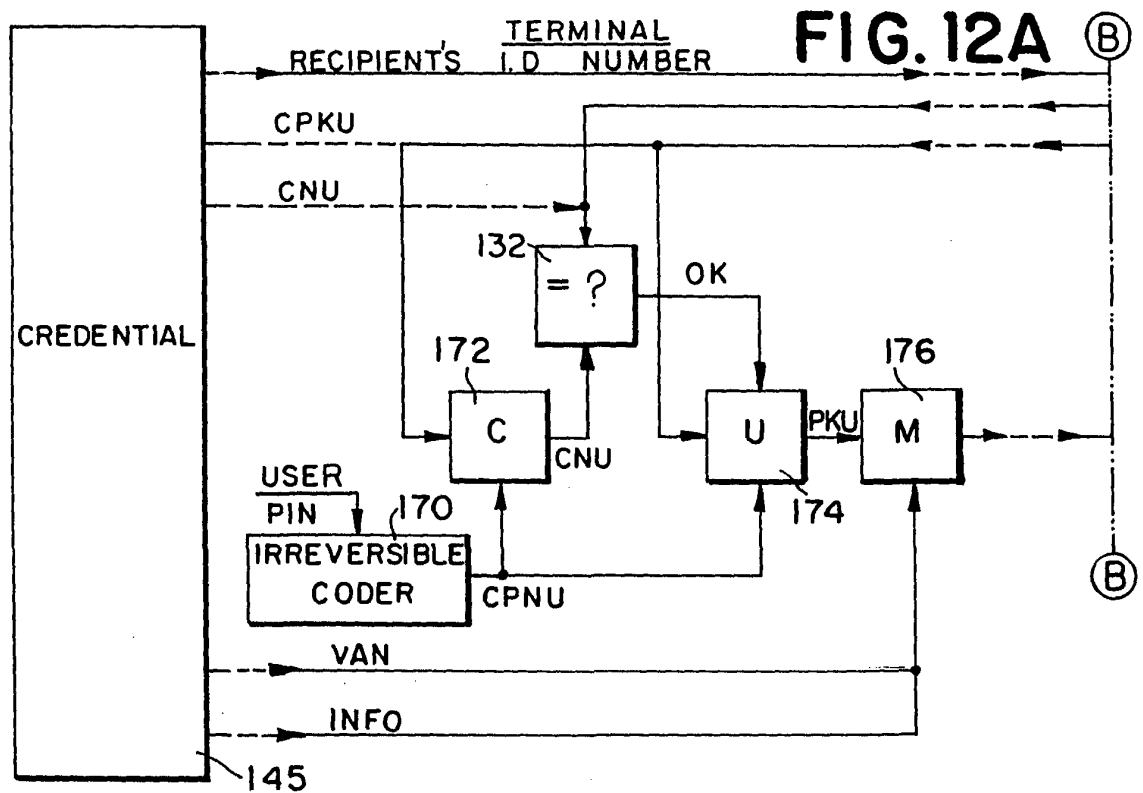
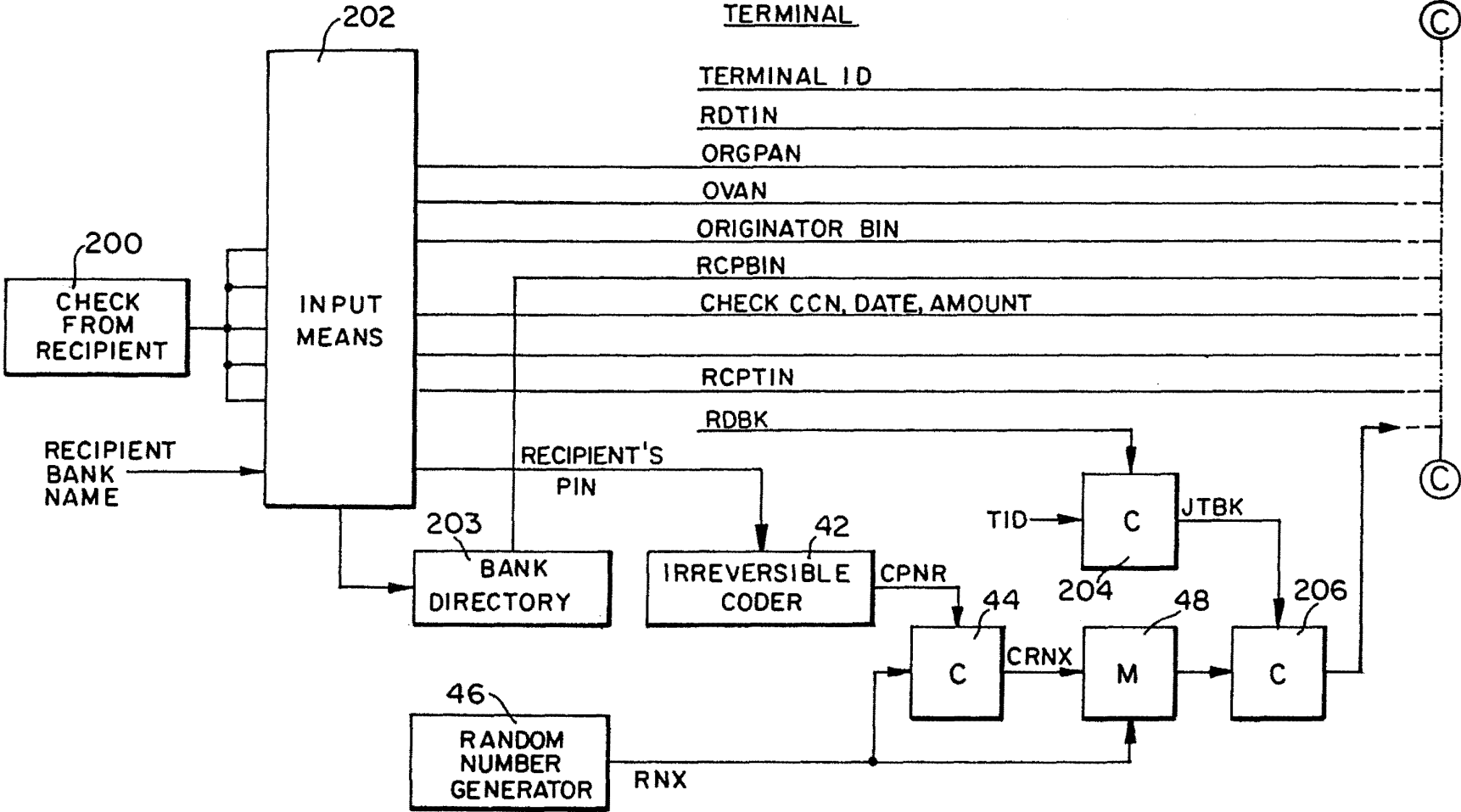
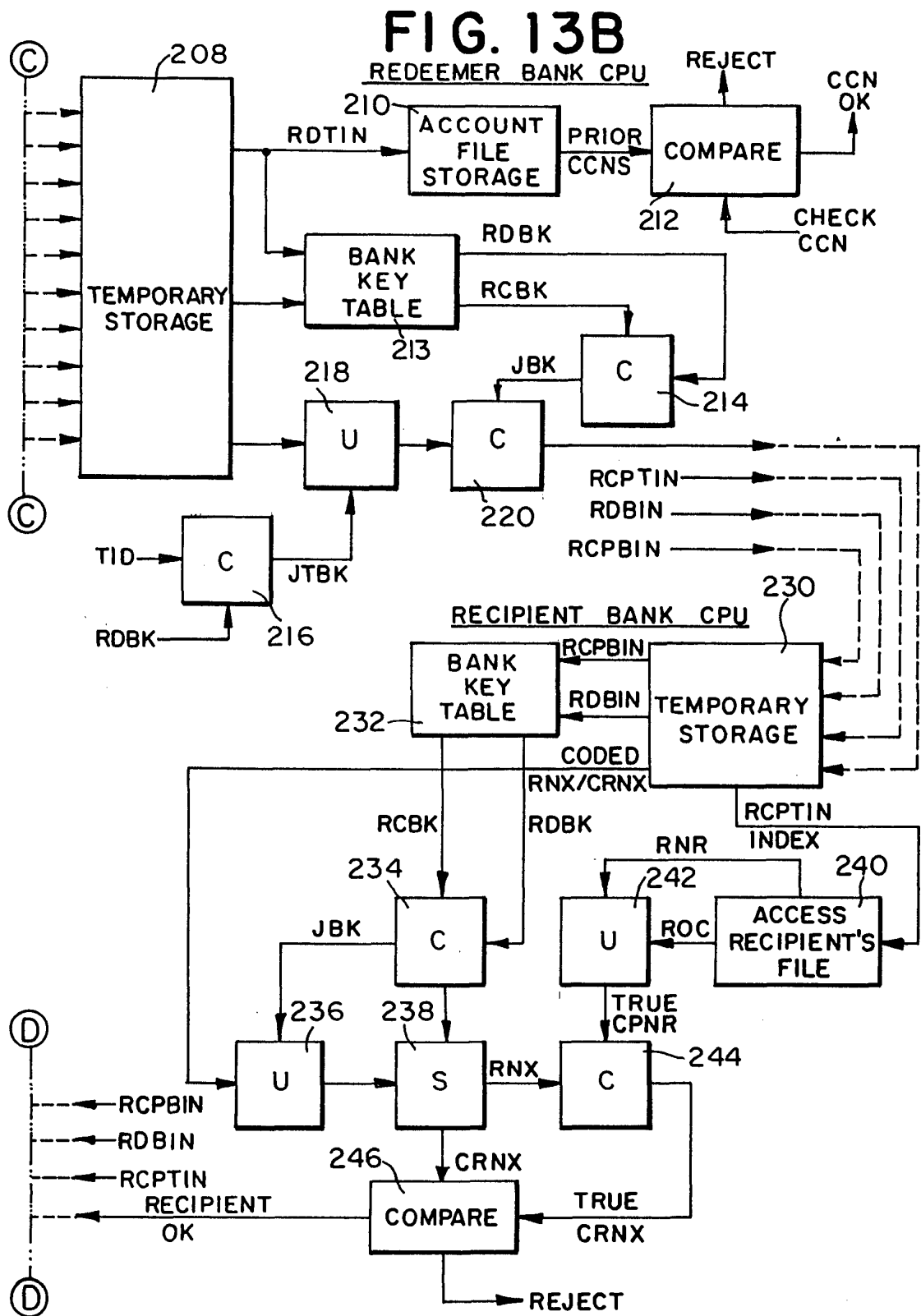


FIG. 13A





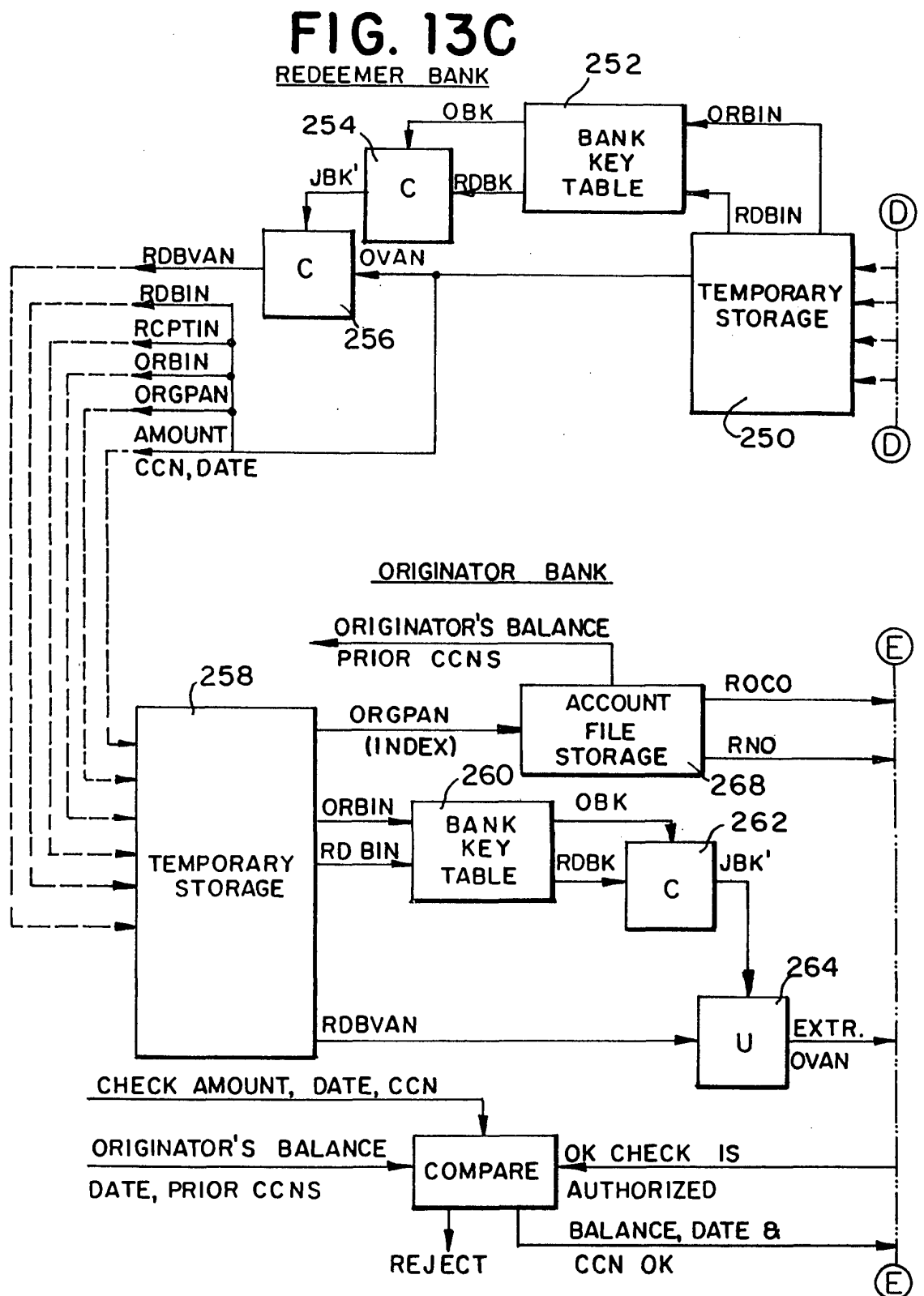
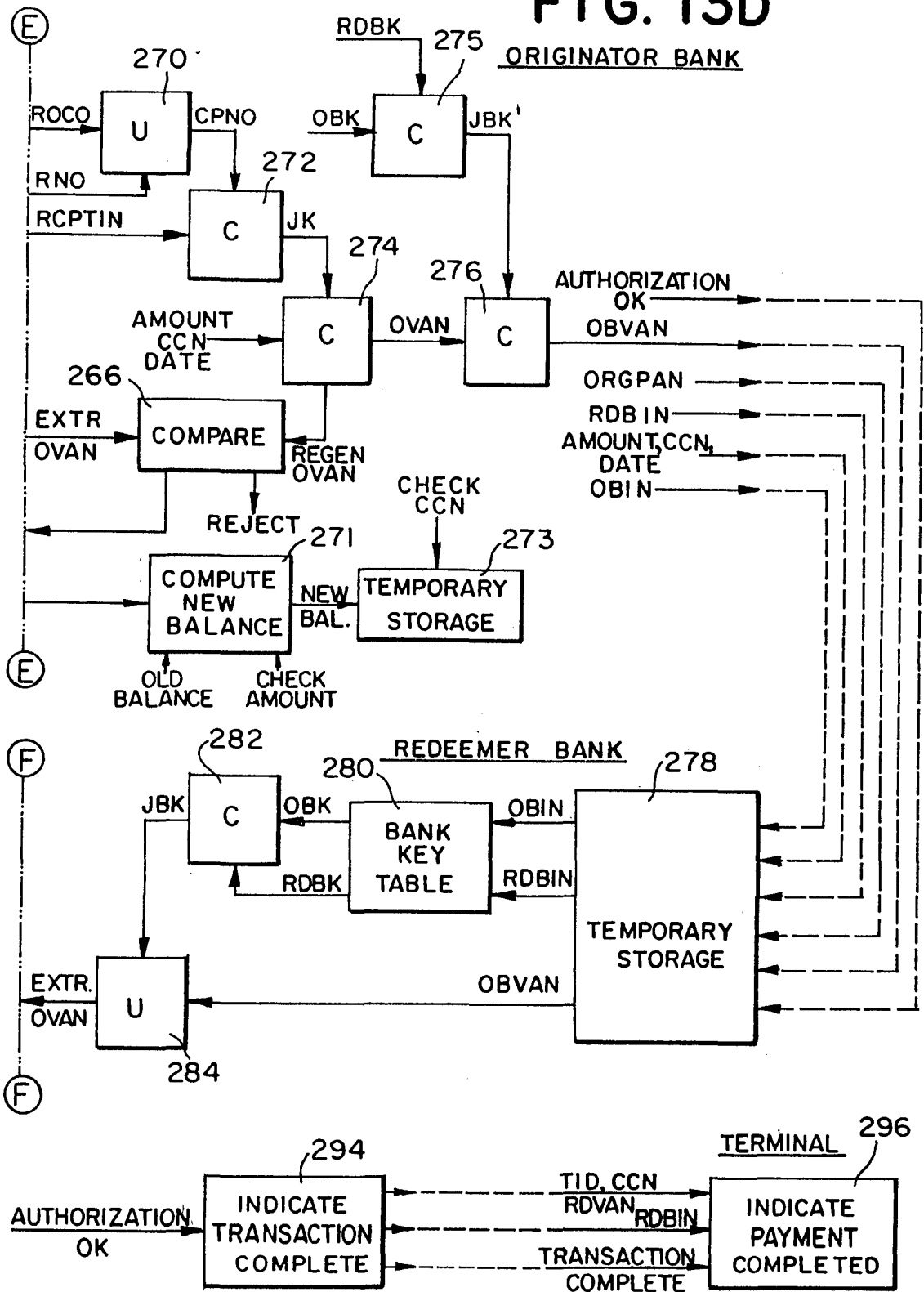
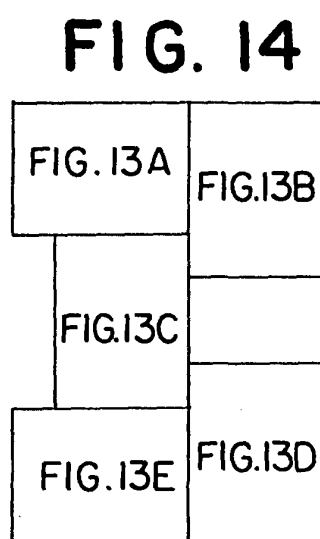
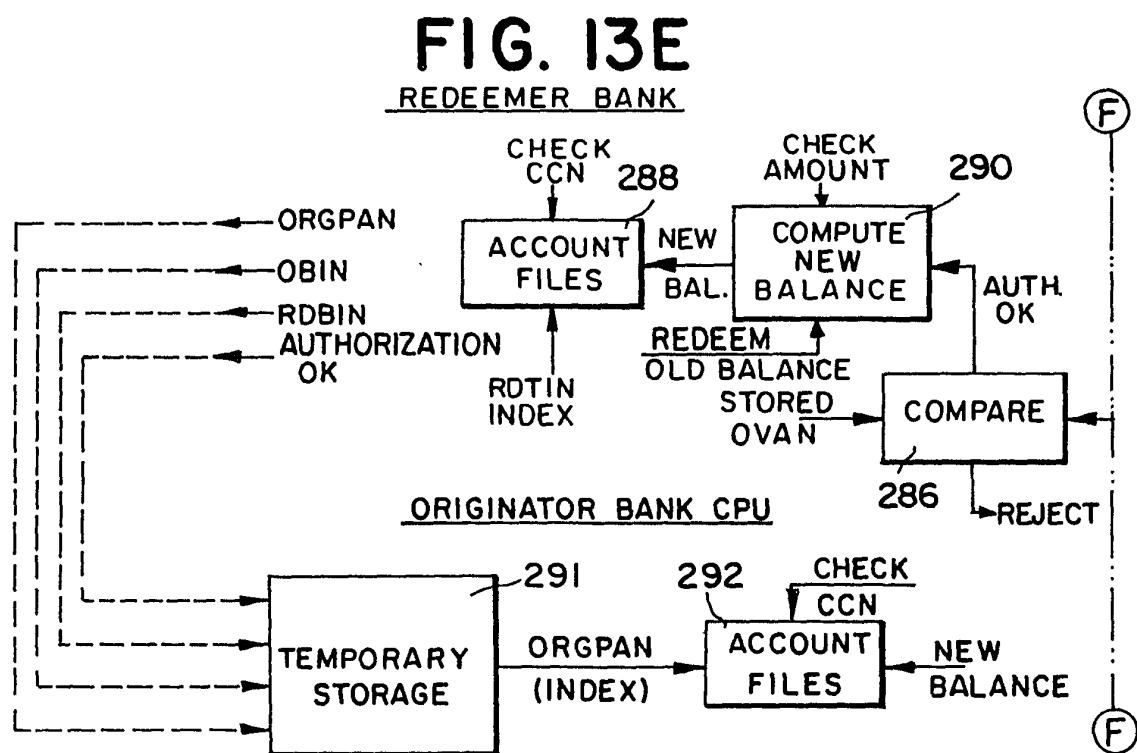


FIG. 13D





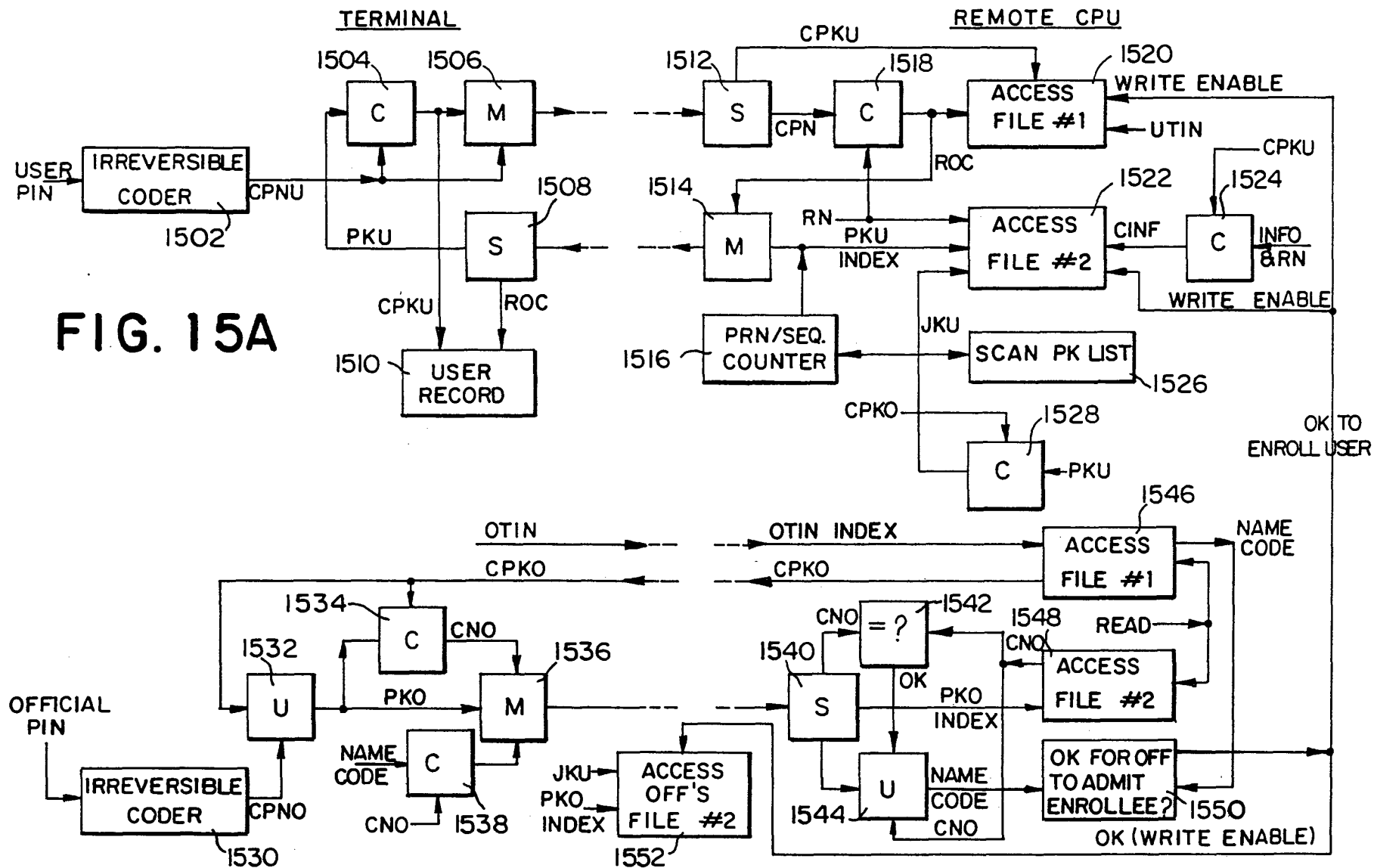


FIG. 15A

CREDENTIAL ISSUE PROCESSING AGENCY TERMINAL / COMPUTER

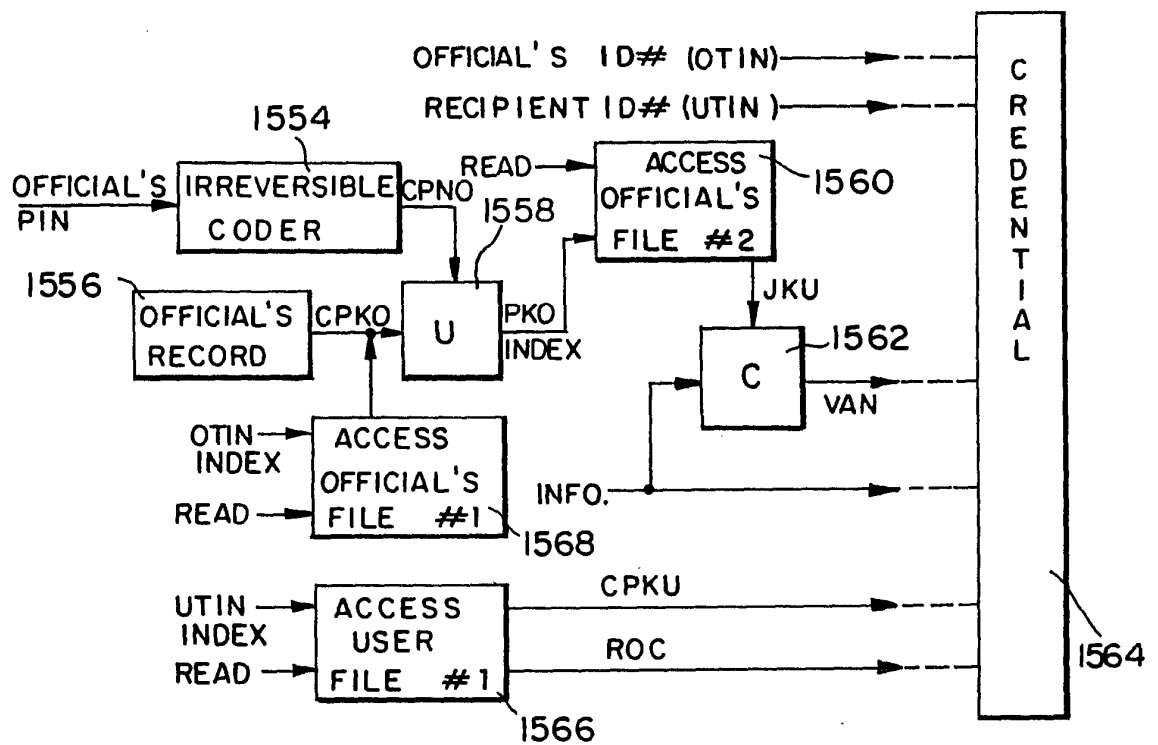


FIG. 15 B

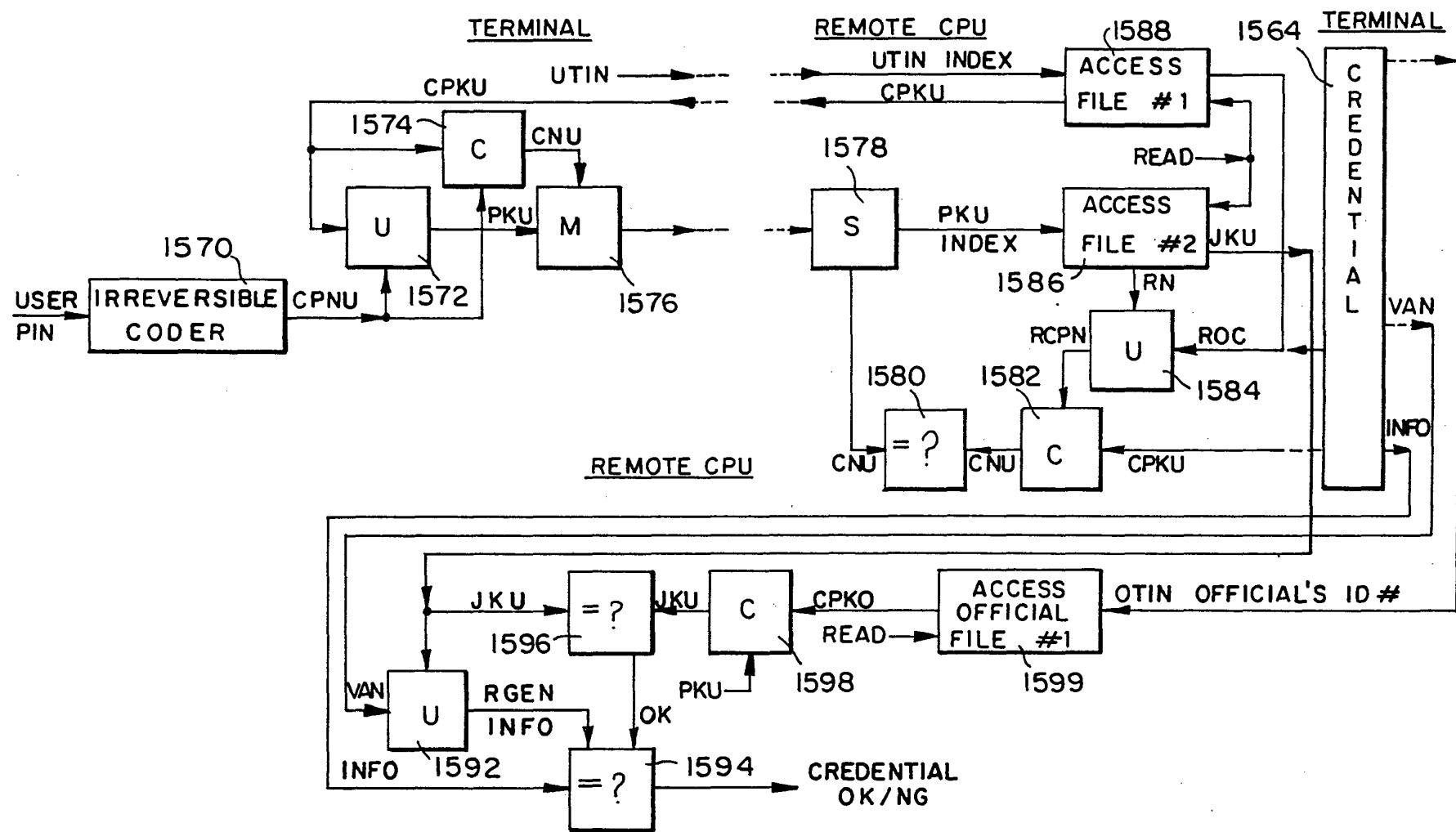
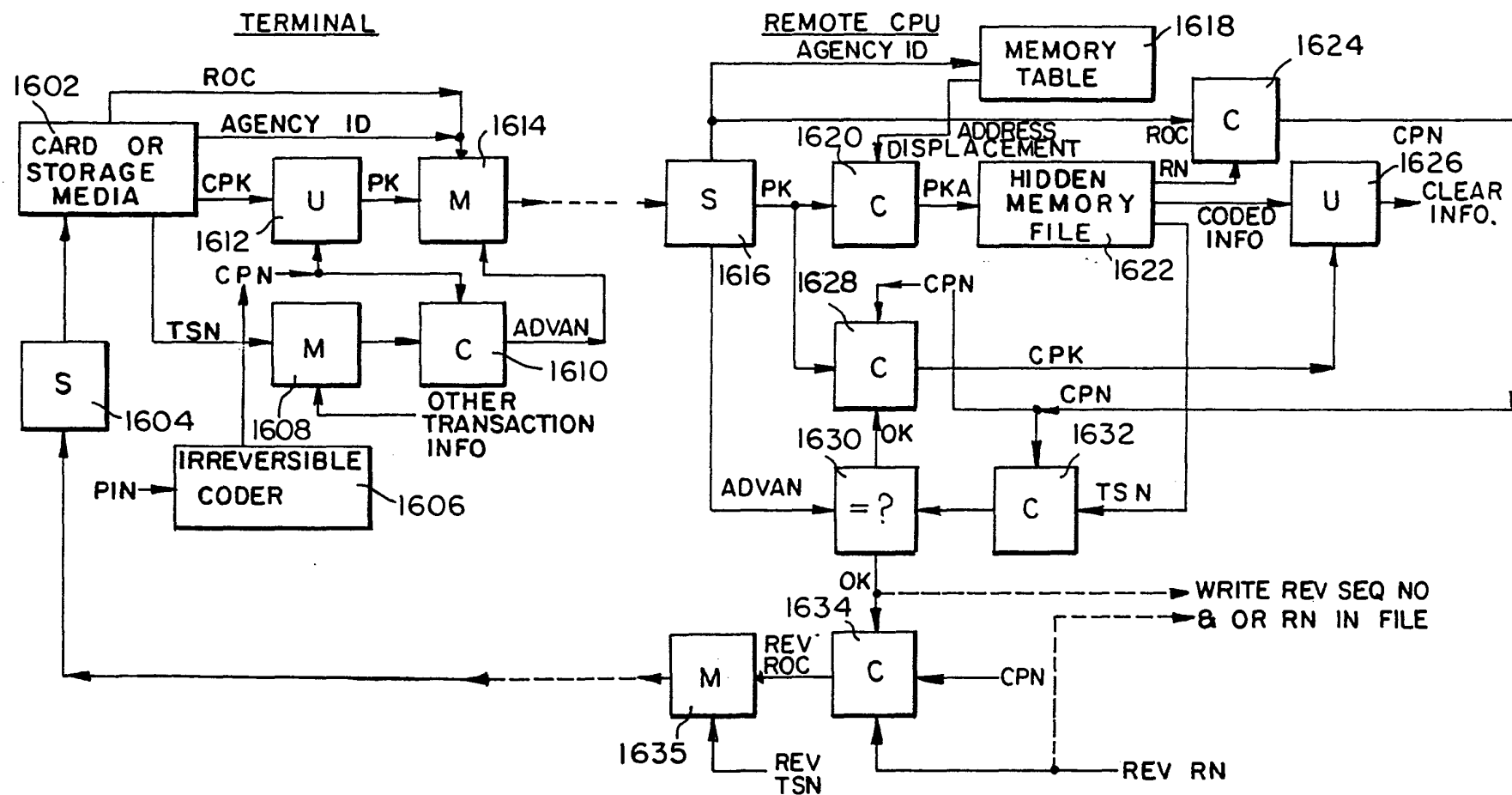


FIG. 15C



977 385

PART B - ISSUE FEE TRANSMITTAL

MAILING INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE. Blocks 2 through 5 should be completed where appropriate. All further correspondence including the Issue Fee Receipt, the Patent, advanced 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)
22M1/0722 PATENT ATTORNEYS SCHWARZE JACOBS & NADEL 120 MARKET STREET 36TH FLOOR PHILADELPHIA, PA 19103	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
07/977,385	11/17/92	022	CANGIALOSI, S	2202 07/22/93
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
6074-1	380-024.000	P08	UTILITY	YES	\$585.00	10/22/93

3. Further correspondence to be mailed to the following:

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

DS20209 09/01/93 07977385

DO NOT USE THIS SPACE

16-0235 020 242
16-0235 020 561

585.00CH
30.00CH

5. ASSIGNMENT DATA TO BE PRINTED ON THE PATENT (print or type)

(1) NAME OF ASSIGNEE:
(2) ADDRESS: (City & State or Country)
(3) STATE OF INCORPORATION, IF ASSIGNEE IS A CORPORATION
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.

6a. The following fees are enclosed:

☐ Issue Fee ☐ Advanced Order - # of Copies

6b. The following fees should be charged to: (Minimum of 10)

DEPOSIT ACCOUNT NUMBER 16-0235

(Enclose Part C)

☒ Issue Fee ☒ Advanced Order - # of Copies 10
☒ Any Deficiencies in Enclosed Fees (Minimum of 10)

The COMMISSIONER OF PATENTS AND TRADEMARKS is requested to apply the Issue Fee to the application identified above.

(Signature of party in interest of record)

(Date)

8/17/93

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

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 August 17, 1993
(Date)

MARY E SPERA
(Name of person making deposit)

Mary E Spera
(Signature)

August 17, 1993
(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 drawings, must have its own certificate of mailing.

This form is estimated to take 20 minutes to complete. Time will vary depending upon the needs of the individual applicant. Any comments on the amount of time you require to complete this form should be sent to the Office of Management and Organization, Patent and Trademark Office, Washington, D.C. 20231 and to the Office of Information and Regulatory Affairs, Office of Management and Budget, Washington, D.C. 20503.

PTO UTILITY GRANT

Paper Number 10

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

Matthew A. Thompson
Attest

PTO-1584



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 07977385 PATENT NUMBER 5267314

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

917385

CLAIMS AS FILED - PART I

(Column 1)

(Column 2)

FOR	NUMBER FILED	NUMBER EXTRA
BASIC FEE		
TOTAL CLAIMS	63 minus 20 =	43
INDEPENDENT CLAIMS	18 minus 3 =	15
MULTIPLE DEPENDENT CLAIM PRESENT		

* If the difference in column 1 is less than zero, enter "0" in column 2

SMALL ENTITY

OR

OTHER THAN SMALL ENTITY

RATE	FEE
	\$355.00
x\$11=	473
x 37=	555
+115=	
TOTAL	1383

RATE	FEE
	\$710.00
x\$22=	
x 74=	
+230=	
TOTAL	

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	62	63	-
Independent	19	18	1
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM			

SMALL ENTITY

OR

OTHER THAN SMALL ENTITY

RATE	ADDITIONAL FEE
x\$11=	
x 37=	37.0
+ 115=	
TOTAL ADDIT. FEE	37.0

RATE	ADDITIONAL FEE
x\$22=	
x 74=	
+230=	
TOTAL ADDIT. FEE	

(Column 1)

(Column 2)

(Column 3)

AMENDMENT B	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
Total	22	63	-
Independent	5	19	-
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM			

SMALL ENTITY

OR

OTHER THAN SMALL ENTITY

RATE	ADDITIONAL FEE
x\$11=	
x 37=	
+ 115=	
TOTAL ADDIT. FEE	

RATE	ADDITIONAL FEE
x\$22=	
x 74=	
+230=	
TOTAL ADDIT. FEE	

(Column 1)

(Column 2)

(Column 3)

AMENDMENT C	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
Total			
Independent			
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM			

SMALL ENTITY

OR

OTHER THAN SMALL ENTITY

RATE	ADDITIONAL FEE
x\$11=	
x 37=	
+115=	
TOTAL ADDIT. FEE	

RATE	ADDITIONAL FEE
x\$22=	
x 74=	
+230=	
TOTAL ADDIT. FEE	

* 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.

FORM PTO-875
(Rev.10-92)

Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE

PTO 1130

U.S. DEPARTMENT OF COMMERCE- PATENT & TRADEMARK OFFICE

1ST EXAMINER *G Smith*DATE *12-1-92*

(REV 11/81)

PACE DATA ENTRY CODING SHEET

2ND EXAMINER

DATE

APPLICATION NUMBER

TYPE
APPLFILING DATE
MONTH DAY YEARSPECIAL
HANDLINGGROUP
ART UNIT

CLASS

SHEETS OF
DRAWING*977385**1**11 17 92**0**2202**380**15*TOTAL
CLAIMSINDEPENDENT
CLAIMSSMALL
ENTITY?

FILING FEE

FOREIGN
LICENSE

ATTORNEY DOCKET NUMBER

*63**18**1**1383**1**6074-1*

CONTINUITY DATA

CONTINUITY
CODE

STATUS
CODE

PARENT APPLICATION
SERIAL NUMBER

0							
0							
0							
0							
0							

PARENT
PATENT NUMBER

PARENT
FILING DATE
MONTH DAY YEAR

PCT/FOREIGN APPLICATION DATA

FOREIGN
PRIORITY
CLAIMED

COUNTRY
CODE

PCT/FOREIGN APPLICATION SERIAL NUMBER

FOREIGN
FILING DATE
MONTH DAY YEAR
