PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L	A2	(11) International Publication Number: **WO 97/40600**
		(43) International Publication Date: 30 October 1997 (30.10.97)

(21) International Application Number: PCT/US97/06838

(22) International Filing Date: 23 April 1997 (23.04.97)

(30) Priority Data:

60/015,525	23 April 1996 (23.04.96)	US
60/015,527	23 April 1996 (23.04.96)	US
60/015,529	23 April 1996 (23.04.96)	US

(71) Applicant *(for all designated States except US)*: ASCOM HASLER MAILING SYSTEMS, INC. [US/US]; 19 Forest Parkway, Shelton, CT 06484 (US).

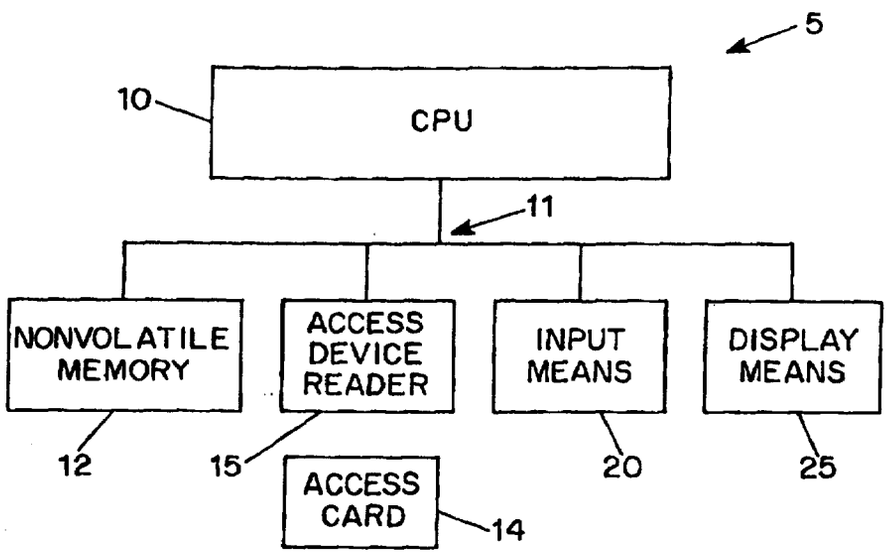
(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: BROOKNER, George [US/US]; 11 Surrey Drive, Norwalk, CT 06851 (US).

(74) Agent: FERENCE, Stanley, D., III; Oppedahl & Larson, Suite 309, 1992 Commerce Street, Yorktown Heights, NY 10598-4412 (US).

(81) Designated States: CA, JP, US, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: SYSTEM FOR IDENTIFYING THE USER OF POSTAL EQUIPMENT



(57) Abstract

An improved system for identifying the user of postal equipment. A user provides identifying information, and if access is not appropriate based on that information, an additional comparison is performed before access is denied. This permits the user to select the identifying information needed for access from a set of predefined information, thereby permitting the user to change identifying information needed for access in the event the information has been or is suspected of having been compromised. Additional security may also be obtained by requiring the user to supply additional identifying information randomly selected from a predetermined set after valid first identifying information has been entered. Identifying information supplied by the user may include personal digital data, such as a digital fingerprint or retina eye scan.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

SYSTEM FOR IDENTIFYING THE USER OF POSTAL EQUIPMENT

RELATED APPLICATIONS

This application claims priority from pending U.S. Provisional Application Serial Nos. 60/015,525, 60/015,527, and 60/015,529, all filed on April 23, 1996, which are hereby incorporated by reference.

TECHNICAL FIELD

This invention is directed to a system for identifying the user of a particular device, such as postal devices, and limiting operation of such device to authorized users.

BACKGROUND ART

In countries throughout the world, a postal customer may obtain postage from the postal authority in several ways, including the purchase of stamps and the use of a postage meter. The customer has at least two security concerns no matter what method is used to obtain postage from the postal authority. First, the customer is concerned that only his authorized agents purchase postage from the postal authority. Second, the customer is concerned with limiting usage of the purchased postage to authorized persons. This is a particular concern in an office environment where there are a large number of personnel.

When stamps are involved, their purchase may be controlled through various accounting techniques, and their use is generally limited by physically controlling the stamps themselves. For example, the stamps are kept in a locked location, such as a drawer, and only

authorized personnel have access to the stamps. Such physical controls may also be used for limiting access to postage machines. Due to the size of postage machines, however, such physical control mechanisms may be of great inconvenience.

Typically, a postage meter is left out in an open area where there is little access control to the physical area itself. Thus, limiting the operation of the machine must be accomplished in a manner in which it is not necessary to limit access to the area containing the machine. In some postage machines, limiting operation to authorized personnel has be accomplished through use of physical means, most typically a key without which the machine will not operate. Physical controls similar to those used for stamps are then used to limit access to the key to authorized personnel.

With electronic postage meters, it may be possible to limit operation of the machine to authorized personnel through the use of a Personal Identification Number (PIN), in addition to physical controls, or in combination therewith. Furthermore, some electronic postage meters are capable of purchasing postage remotely, obviating the necessity of physically taking the postage meter to the postal authority for the addition of postage, and a PIN may be used to limit those persons who are authorized to purchase additional postage. When a PIN is involved, however, there is a risk that some unauthorized person may obtain knowledge of the PIN, for example, by observing the entry of the PIN by an authorized person. When the PIN becomes compromised, or knowledge of it is no longer limited to authorized personnel, the PIN ceases to be an effective means of limiting the operation of the postage meter to authorized personnel.

When a PIN has been compromised, or is suspected of having been compromised, the PIN must be changed in order to once again become an effective means of limiting the operation of the postage meter to authorized personnel. Changing a PIN, however, is not a trivial matter. Generally, the supplier of the postage meter must be consulted, which at a minimum, increases the amount of time the compromised PIN is no longer an effective control means.

DISCLOSURE OF THE INVENTION

In accordance with the present invention, there is provided a greatly improved system for user identification of postal equipment in connection with the use of an access device. According to the invention, it is provided that the access device may be associated with a number of access codes, or Personal Identification Numbers (PINs), and the active code may be selected at the user's discretion. Additional security may also be provided for by prompting for additional information randomly selected from a predetermined set after the entry of a valid PIN. In keeping with the invention, data supplied by the user used to identify the user may include biometric personal digital data, such as a digital fingerprint, voice pattern or a retina eye scan.

BRIEF DESCRIPTION OF DRAWINGS

Fig. 1 is a block diagram of the system of the present invention used with a postage meter.

Fig. 2 is a flow chart of the user identification method according to the invention.

Fig. 3 is a flow chart of the user identification method according to another embodiment of the invention.

Fig. 4 is a flow chart of the user identification method according to another embodiment of the invention.

Fig. 5 is a flow chart of the user identification method according to another embodiment of the invention.

MODES FOR CARRYING OUT THE INVENTION

Referring to Fig. 1, a user identifying system is shown generally at 5 and includes a CPU 10, nonvolatile memory 12, an access device 14, an access device reader 15, input means 20, and display means 25, wherein CPU 10, access device reader 15, input means 20,and display means 25 are coupled with each other by system bus 11. Such a system may be integrated into postal equipment, for example by using the components of the postal equipment, or may be a stand alone system connected for controlling the postal equipment.

When access device 14 is inserted into access device reader 15, CPU 10 prompts the user by means of display means 25 to enter an input through input means 20. The access device may be a card with magnetically encoded information, or a "smart card," or the like. The CPU 10 then compares the user input with either a value previously encoded on the access device 14 or contained within nonvolatile memory 12, or both, which are related to the user indicated by access device 14. If the user input matches one or both of the other values, as

previously selected, user identity is verified and access to the postal equipment is permitted.

Referring now to Fig. 2, a flow chart is shown wherein the identification is based upon a predetermined number of PINs, and the active PIN is changeable by the user at the user's discretion. When the CPU 10 in the user identifying system 5 shown in Fig. 1 referred to above, compares the user input (S1) with one or both of the other values (S2), as previously selected, and there is no match with the user input, a secondary comparison (S4) is performed against secondary values contained in at least memory 12 of access control system 5. This secondary comparison is performed until a match is found, or the number of permissible secondary values has been exceed and no match has been found. If the secondary comparison results in no match (S7), the user is not permitted to access the postal equipment. If, however, a match is found (S5), the memory 12 or access device 14, or both, are updated to note the new value, and alternatively, it is indicated the old value may not be used in the future, and the user is permitted to assess the postage device (S6).

In this embodiment, a number of PINs are allocated to a user's access device at the time of creation. These PINs are now forevermore linked to the specific user and the user identification system. This invention which allows the user to select among the PINs assigned to the user's access device provides the same type of access security as issuing a new access device.

The number of PINS preassigned is only limited to the number a user can remember (by memory, written, logged, etc.), but would typically be more than one. Should a user decide to change his/her PIN, any of the

preassigned PINs are valid. Once a new PIN is used for the first time, the user identity system recognizes this PIN is one of the preassigned PINs and will now expect this new PIN to be the standard PIN for this user. Once the last preassigned PIN has been selected, the PIN may no longer be changed by the user.

If one of the user's access devices is lost, stolen, or misplaced, the meter manufacturer may supply a replacement access device and the user may immediately change the PIN. If the lost access device is found, it is still valid with the new PIN. If the access device was stolen, it is useless. Further, this system permits the vendor of the postal equipment the option of asking the user to change the active PIN, due to some reason of security. Thus, this is effectively the same as issuing a new access device without the costs or logistics involved with new issues.

Referring now to Fig. 3, a flow chart is shown wherein the identification is based upon providing additional information randomly selected from a predetermined set after entry of a valid PIN. When the CPU 10 in the user identification system 5 shown in Fig. 1 referred to above, compares the user input (S10) with one or both of the other values (S11), as previously selected, and there is no match with the user input (S12), the user is not permitted to access the postage meter. If there is a match, however, the CPU 10 prompts the user to enter additional information randomly selected from a pre-selected amount of information contained in memory 12 (S14). Such additional information may be in the nature of "birth date," "Social Security No.," "Address," other unique user-specific data, or the like. This additional information will be doubled, tripled, etc., such that the request for

additional information will not be the same for each use of the access device.

It is preferred the prompt for additional information alternate (randomly or sequentially) amongst the additional values contained in memory 12. If the secondary comparison results in no match (S15), the user is not permitted to access the postage meter; if it results in a match (S16), access is permitted. This method of verifying user identity minimizes the possibility of an access device 14 or security code being fraudulently obtained and then used. This embodiment of the invention may be used with an access device only having the possibility of one PIN, or with an access device capable of having multiple PINs, as is shown in Fig. 2.; it may also be used in connection with the initial access code.

Referring now to Fig. 4, a flow chart is shown wherein the identification is based upon providing some unique personal digital data, or biometric, such as a digital finger print, voice pattern or retina eye scan. When the CPU 10 in the user identification system 5 shown in Fig. 1 referred to above, compares the user input (S20) with one or both of the other values (S21), as previously selected, and there is no match with the user input (S22), the user is not permitted to access the postage meter. If there is a match (S23), access is permitted.

In this embodiment, the user input consists of the user's digital finger print, voice pattern or retina eye scan. If the identify verification process is a closed loop process between the user, the access device 14 and the CPU 10, then the personal digital data can be compared against the value in the access device 14 and in

turn the value in memory 12. Alternatively, the comparison may be only against the value in the access device 14. Further, the comparison may be only against the value in memory 12 if the access device is restricted in band pass, memory, or the like. The level of security desired may relate to the magnitude of biometric data comparison necessary in that a low level of security could command an abbreviated biometric data comparison (e.g., major finger print classification features), while high levels of security would command a comprehensive "all features" evaluation of the data. In a small office environment, the biometric data comparison requirements could be reduced to only several unique finger print, voice pattern or retina scan features or the like. In such a configuration, the time to verify would be rapid and the identity data content would be small.

This embodiment eliminates the present need for a series of user commands or interactive network commands to validate the use of franking/postage equipment. By utilizing the personal digital data, it is no longer necessary to additionally validate the related equipment to be used for franking/postage processing. Rather, the personalized digital data is predefined for the system to which the user is authorized. Furthermore, the input means 20 may be contained in access device 14.

Referring now to Fig. 5, a flow chart is shown wherein the present invention is used in connection with the remote purchasing of postage. Telemeter setting (TMS) may be carried out as set forth in EPO pub. no. EP 442761, or as set forth in PCT pub. no. WO 86-05611, each of which is incorporated herein by reference. Once CPU 10 in the user identification system 5 shown in Fig. 1 referred to above, compares the user input (S24) with the possible values (S25), and there is no match with the

user input (S24), the user is not permitted to access the postage meter (S26). The user input may be textual, biometric, or another type of data. If there is a match, however, the TMS Data Center requests additional data (S27) to determine if the user is authorized to purchase postage. Such additional data may be either textual, biometric, or randomly selected in accordance with the present invention. If there is no match between the additional data and that maintained by the Data Center, the purchase does not proceed; if there is a match, the purchase proceeds.

While there have been described what are believed to be the preferred embodiments of the invention, those skilled in the art will recognize that other and further modifications may be made thereto without departing from the invention and it is intended to claim all such changes and modifications as fully within the scope of the invention.

I CLAIM:

1. A system for verifying the user of postal equipment, comprising:

input means for input of information, said information including data associated with a user of said system;

means for storing a plurality of data associated with said user, one such datum being the preferred data;

means responsive to said input means for:

receiving said user identifying data;

comparing said user identifying data against said stored data, including said preferred stored data;

updating said preferred stored data to be one of said stored data.

2. The system as described in Claim 1, wherein said user identifying data includes a user's digital finger print.

3. The system as described in Claim 2, wherein said user identifying data includes a user's retina eye scan.

4. A system for verifying the user of postal equipment, comprising:

input means for input of information, said information including data associated with a user of said system;

means for storing a plurality of data associated with said user;

means for prompting the user to input one of the plurality of data associated with said user, said data being randomly selected;

means responsive to said input means for:

receiving said user identifying data;

comparing said user identifying data against said randomly selected stored data associated with said user.

5. A system for verifying the user of postal equipment, comprising:

input means for input of information, said information including first data associated with a user of said system;

means for storing a plurality of data associated with said user;

means responsive to said input means for:

receiving said user identifying first data;

comparing said user identifying first data against said stored data;

means for input of second information, said information including second data associated with a user of said system;

means responsive to said input means for:

receiving said user identifying second data;

comparing said user identifying second data against said stored data.

6. A method for verifying the identity of a user of postage equipment, comprising the following steps:

(a) obtaining first user identifying information from an access device provided by the user;

(b) prompting the user to enter second identifying information;

(c) comparing said user supplied second identifying information against primary identifying information previously associated with said first user identifying information;

(d) comparing said user supplied second identifying information against secondary identifying information previously associated with said first user identifying information;

(e) updating said primary identifying information from said secondary identifying information.

7. The method as described in Claim 6, wherein said user second identifying data includes a user's digital finger print.

8. The method as described in Claim 6, wherein said user second identifying data includes a user's voice pattern.

9. The method as described in Claim 6, wherein said user second identifying data includes a user's retina eye scan.

10. A method of verifying the identity of a user of postal equipment, comprising the following steps:

(a) obtaining first user identifying information from an access device provided by the user;

(b) prompting the user to enter second identifying information;

(c) comparing said user supplied second identifying information against identifying information previously associated with said first user identifying information;

(d) prompting the user to enter third identifying information randomly selected from a set of information previously associated with said user first identifying information.

11. The method as described in Claim 10, wherein said user second identifying data includes a user's digital finger print.

12. The method as described in Claim 10, wherein said user second identifying data includes a user's voice pattern.

13. The method as described in Claim 10, wherein said user second identifying data includes a user's retina eye scan.

14. A method of verifying the identity of a user of postal equipment, comprising the following steps:

(a) obtaining first user identifying information from an access device provided by the user;

(b) prompting the user to enter second identifying information;

(c) comparing said user supplied second identifying information against identifying information previously associated with said first user identifying information;

(d) obtaining third identifying information from the user;

(e) comparing said third identifying information against identifying information previously associated with said first user identifying information.

15. The method described in Claim 14, wherein said third identifying information was requested from the user by random selection from a set of information previously associated with said user first identifying information.

16. The method described in Claim 14, wherein said third identifying information is biometric data.

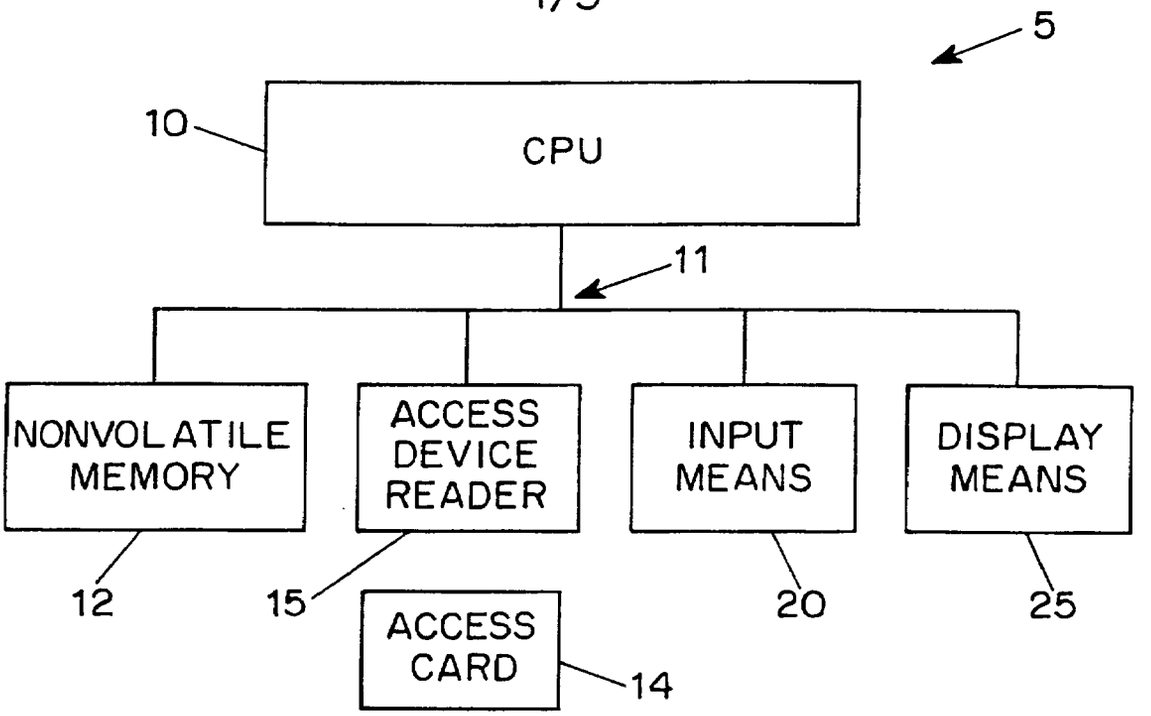

5
10
CPU
11
NONVOLATILE MEMORY
ACCESS DEVICE READER
INPUT MEANS
DISPLAY MEANS
12
15
20
25
ACCESS CARD
14

FIG. 1

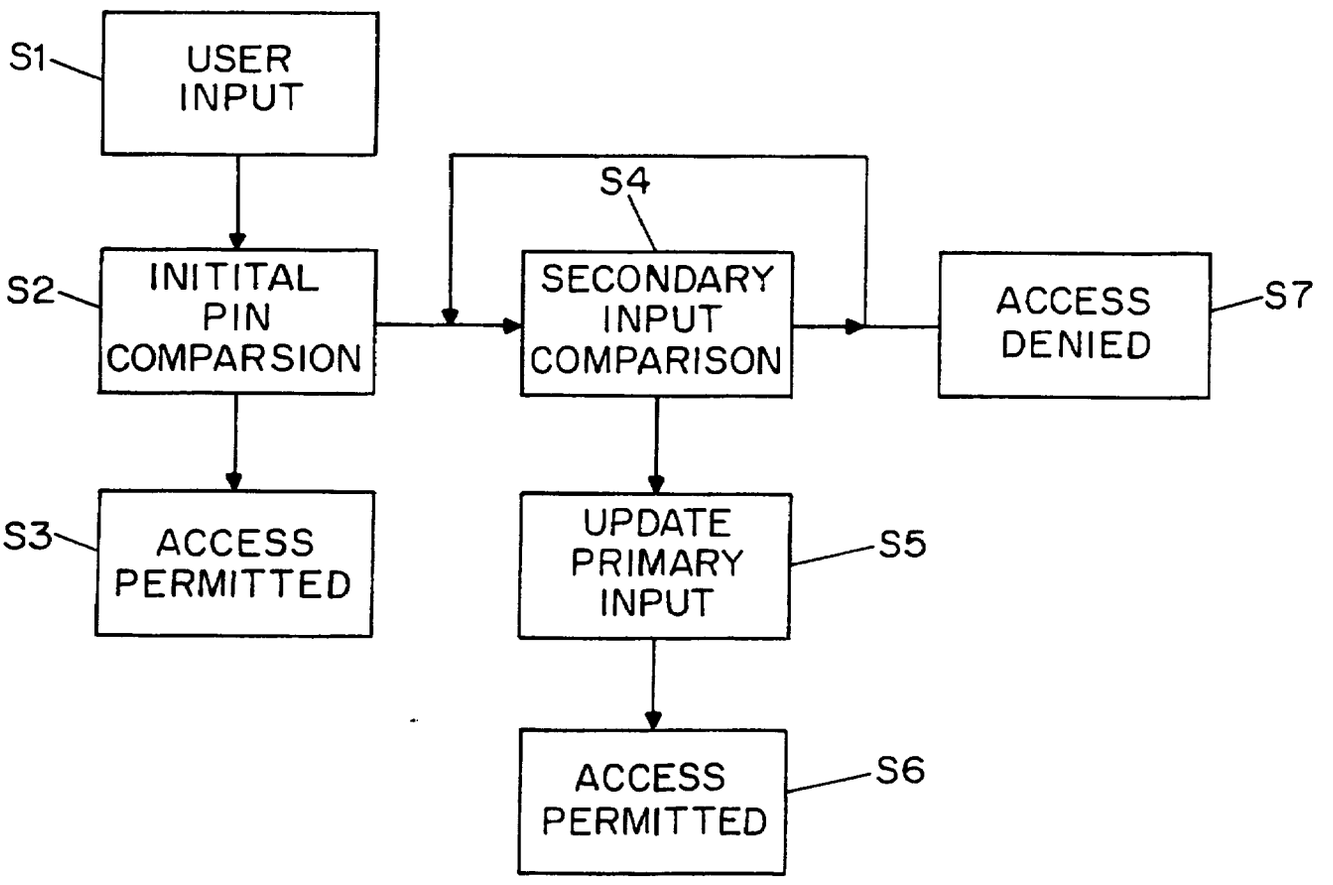

S1
USER INPUT
S4
S2
INITITAL PIN COMPARSION
SECONDARY INPUT COMPARISON
ACCESS DENIED
S7
S3
ACCESS PERMITTED
UPDATE PRIMARY INPUT
S5
ACCESS PERMITTED
S6

FIG. 2

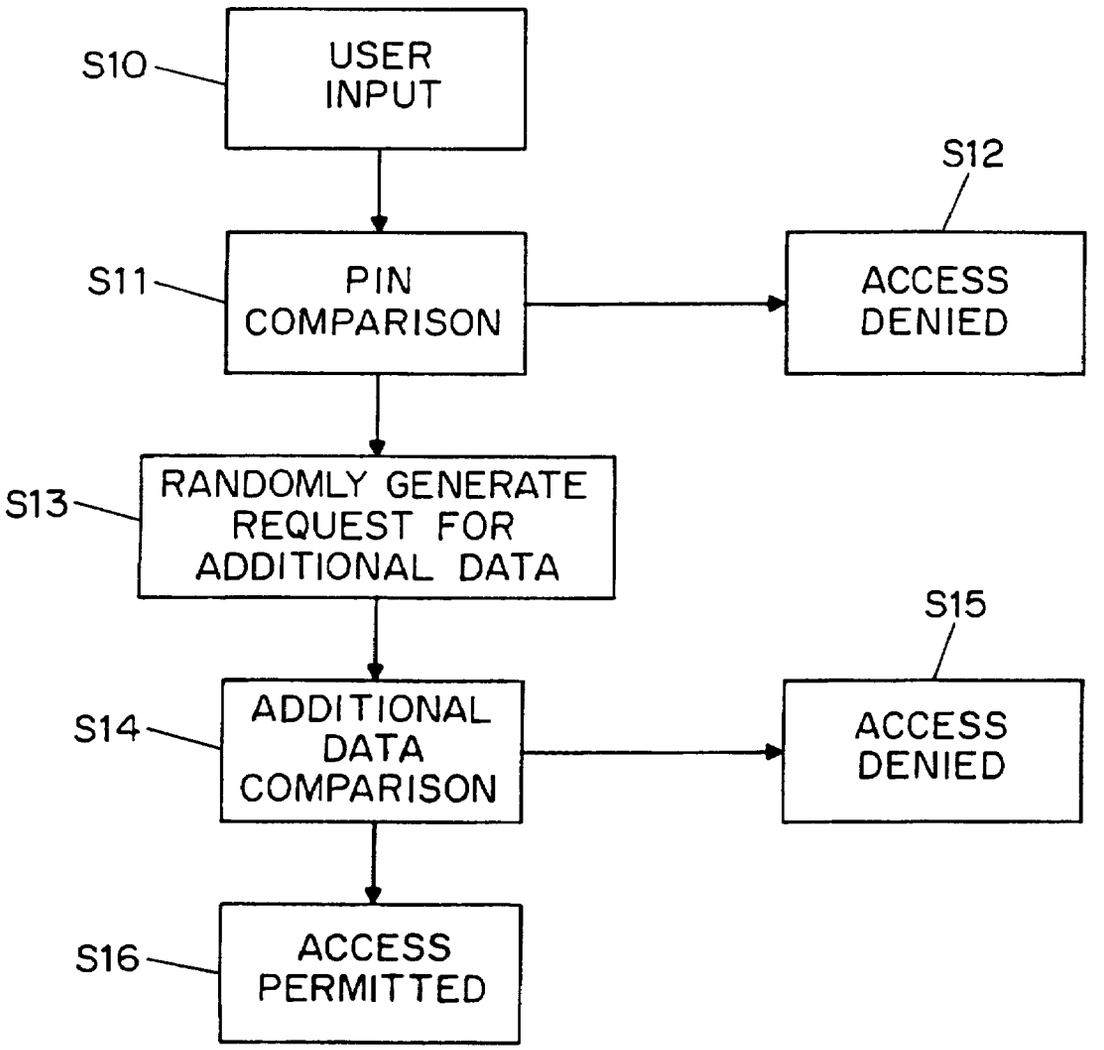

S10
USER INPUT
S12
S11
PIN COMPARISON
ACCESS DENIED
S13
RANDOMLY GENERATE REQUEST FOR ADDITIONAL DATA
S15
S14
ADDITIONAL DATA COMPARISON
ACCESS DENIED
S16
ACCESS PERMITTED

FIG. 3

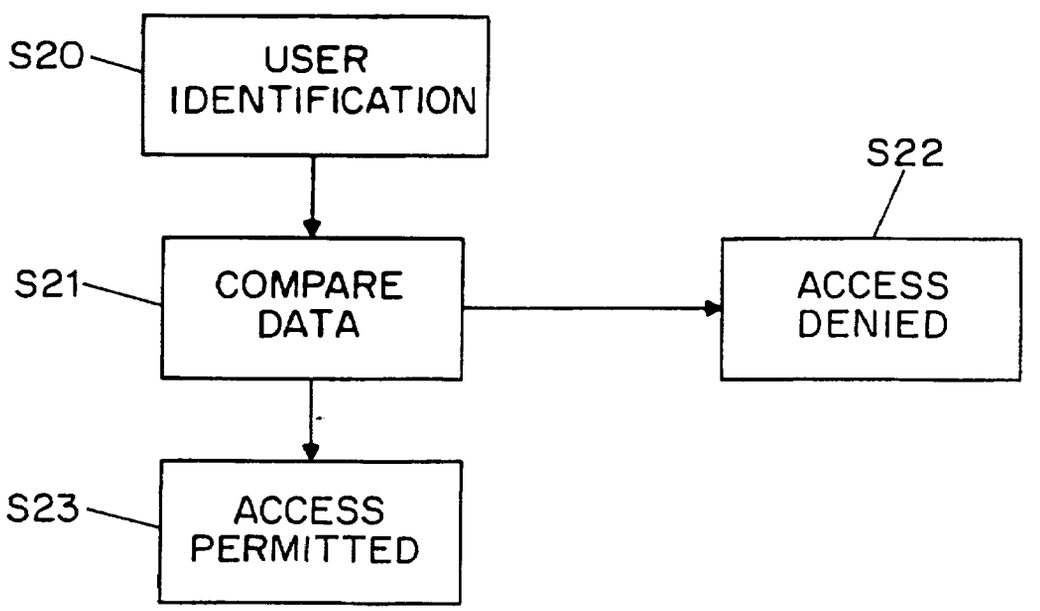

S20
USER IDENTIFICATION
S22
S21
COMPARE DATA
ACCESS DENIED
S23
ACCESS PERMITTED

FIG. 4

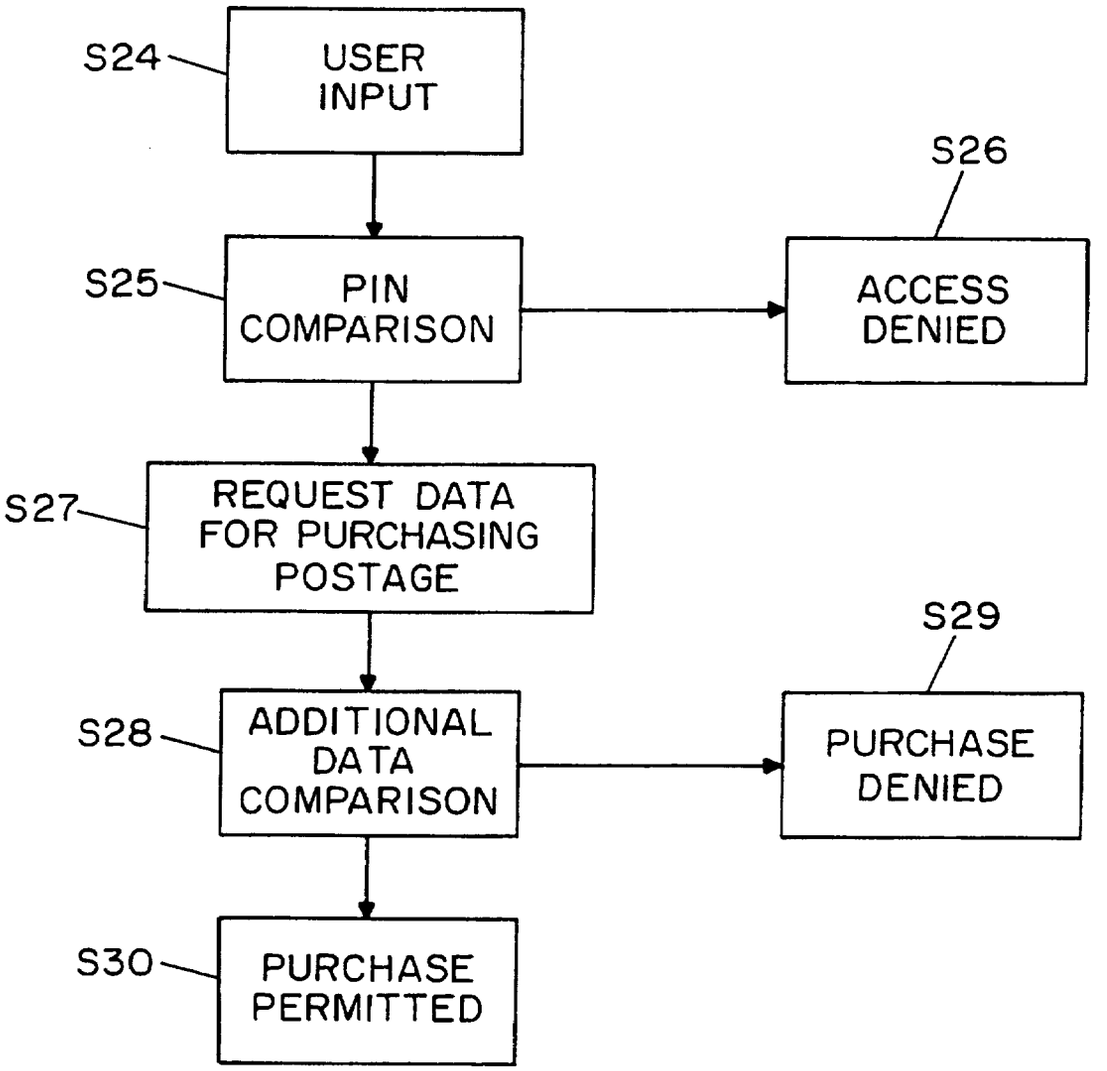

S24
USER INPUT
S26
S25
PIN COMPARISON
ACCESS DENIED
S27
REQUEST DATA FOR PURCHASING POSTAGE
S29
S28
ADDITIONAL DATA COMPARISON
PURCHASE DENIED
S30
PURCHASE PERMITTED

FIG. 5