PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 5 : G07F 7/10, G06K 7/08	A1	(11) International Publication Number: WO 94/17498
		(43) International Publication Date: 4 August 1994 (04.08.94)

(21) International Application Number: PCT/US94/00715

(22) International Filing Date: 18 January 1994 (18.01.94)

(30) Priority Data:
104422 18 January 1993 (18.01.93) IL

(71) Applicant *(for all designated States except US)*: ENCO-TONE LTD. [IL/IL]; 6 Shlomo Ben-Yosef Street, P.O. Box 15110, 32961 Haifa (IL).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: LABATON, Isaac, J. [IL/IL]; 6 Shlomo Ben-Yosef Street, P.O. Box 25110, 32961 Haifa (IL). KELLY, Michael, K. [US/US]; 2915 East Redfield, Phoenix, AZ 85032 (US).

(74) Agents: LECHTER, Michael, A. et al.; Streich Lang, 2100 First Interstate Bank Plaza, 100 West Washington, Phoenix, AZ 85003 (US).

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

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: METHODS AND APPARATUS FOR MAGNETICALLY STORING AND RETRIEVING CREDIT CARD TRANSACTION INFORMATION

(57) Abstract

A smart credit card holder module (3) is provided to read an account information stored on a magnetic strip (1) on a card (2), when it is inserted into the module. The information on the card can be erased, such that the card cannot be used for transactions. The card may be stored outside of the module in the meantime. When the card will be used for transactions, the information must be rewritten on the card. The card must be again inserted into the module and the stored information will be rewritten onto the erased strip. Also the informations of various cards can be stored in the memory (24) of the holders module and may be rewritten on a blank or new card and may be erased again. Thus only one card is necessary instead of many various cards. The informations stored in the memory may be read on a display (11). New codes may be written by means of a keypad (6). The module comprises an input/output slot (3, 7), an alarm or audio transducer (8), a reader/writer (27) and an erasing mechanism (30).

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.

AT	Austria	**GB**	United Kingdom	**MR**	Mauritania
AU	Australia	**GE**	Georgia	**MW**	Malawi
BB	Barbados	**GN**	Guinea	**NE**	Niger
BE	Belgium	**GR**	Greece	**NL**	Netherlands
BF	Burkina Faso	**HU**	Hungary	**NO**	Norway
BG	Bulgaria	**IE**	Ireland	**NZ**	New Zealand
BJ	Benin	**IT**	Italy	**PL**	Poland
BR	Brazil	**JP**	Japan	**PT**	Portugal
BY	Belarus	**KE**	Kenya	**RO**	Romania
CA	Canada	**KG**	Kyrgystan	**RU**	Russian Federation
CF	Central African Republic	**KP**	Democratic People's Republic of Korea	**SD**	Sudan
CG	Congo			**SE**	Sweden
CH	Switzerland	**KR**	Republic of Korea	**SI**	Slovenia
CI	Côte d'Ivoire	**KZ**	Kazakhstan	**SK**	Slovakia
CM	Cameroon	**LI**	Liechtenstein	**SN**	Senegal
CN	China	**LK**	Sri Lanka	**TD**	Chad
CS	Czechoslovakia	**LU**	Luxembourg	**TG**	Togo
CZ	Czech Republic	**LV**	Latvia	**TJ**	Tajikistan
DE	Germany	**MC**	Monaco	**TT**	Trinidad and Tobago
DK	Denmark	**MD**	Republic of Moldova	**UA**	Ukraine
ES	Spain	**MG**	Madagascar	**US**	United States of America
FI	Finland	**ML**	Mali	**UZ**	Uzbekistan
FR	France	**MN**	Mongolia	**VN**	Viet Nam
GA	Gabon				

METHODS AND APPARATUS FOR MAGNETICALLY STORING AND RETRIEVING CREDIT CARD TRANSACTION INFORMATION

Inventors: Isaac Labaton and Michael K. Kelly

Technical Field

The present invention generally relates to methods and apparatus for securing credit card transaction information, and more particularly, to a device for selectively erasing and writing credit card account information onto a magnetic strip associated with a credit card, bank account, or the like.

Background Art and Technical Problems

The use of plastic cards bearing a magnetic strip for effecting sales, banking, and other financial transactions is becoming increasingly popular. In part because of the ease with which such cards may be legitimately used to effect financial transactions, the unauthorized use of such cards for fraudulent purposes is also widespread. Consequently, for many applications of transaction cards of the type having a magnetic strip, the holder or user of the card is required to enter a pass code (e.g., a Personal Identification Number or PIN), for example in the context of a banking transaction using an Automatic Teller Machine (ATM).

While the use of PINs reduces the ease with which a card may be used for an unauthorized purpose, many credit card sales transactions do not lend themselves to the use of a PIN. This is particularly true in the context of a conventional Point of Sale (POS) device, wherein a credit card or debit card is slid through a POS verification device at a seller's place of business. In such cases, the fraudulent use of a card may not be identified as fraudulent until after the transaction has occurred.

In addition, many consumers carry a plurality of transaction cards, such that if a consumer's wallet or purse is lost or stolen, the consumer is potentially subject to fraudulent use of a large number of cards, resulting in substantial economic hardship.

A system is thus needed which affords a cardholder the ease, convenience, and simplicity of use of a transaction card, yet which also provides sufficient security against unauthorized use of such cards.

Summary Of The Invention

The present invention provides methods and applications which overcome the shortcomings of the prior art.

In accordance with one aspect of the present invention, a Smart Credit Cardholder (SCCH) Module is configured to receive a credit card therewithin, and to "read" the account information embedded in the magnetic strip associated with the card. In accordance with a further aspect of the invention, the SCCH Module includes an integral memory array for storing the information contained in the magnetic strip.

In accordance with one mode of operation of the SCCH Module, the magnetic strip is erased once the information contained therein is stored within the module's memory array. In its erased configuration, the card cannot be used in an unauthorized manner to defraud the owner of the account represented by the card. When the owner of the card desires to effect a transaction using the card, he enters the card into the SCCH Module and, by entering a predetermined pass code into the Module, retrieves the account information from the memory array and rewrites the information to the credit card's magnetic strip. When the sale or other transaction is completed using the card, it may again be erased, thus rendering the card unsuitable for fraudulent use. In accordance with the foregoing mode of operation of the SCCH Module, a consumer having a number of credit cards, bank cards, debit cards and the like may "reissue" a particular card for purposes of a single transaction, and thereafter erase the card until the next transaction.

In accordance with an alternate mode of operation of the subject SCCH Module, the original card issued by the card issuer

(e.g., *VISA*™, *MASTERCARD*™, and the like) may be inserted into the Module, whereupon the information stored in the card's magnetic strip is stored in the Module's array. Thereafter, the card may be retrieved from the Module with the magnetic information intact. The owner of the card may then maintain the card permanently in a secure place rather than carrying the card around in a wallet, purse, or the like. For example, the card owner may wish to maintain such cards in a safe deposit box, safe or the like. When it is desired to effect a transaction using the account represented by a card which is permanently stored, the user may simply insert a blank "dummy" card into the SCCH Module and write the account information to the "dummy" card. After closing the transaction with the "dummy" card, it may be reinserted into the Module and erased. In this way, a single blank card may be used for a large number of unrelated transactions; that is, the "dummy" card may alternately function as a bank card, debit card, or a credit card, as desired.

In accordance with a further aspect of the invention, information pertaining to a particular account may be stored in the SCCH memory array in accordance with a pass code selected by the owner of the SCCH Module. This pass code may correspond to the PIN number associated with the card, or may comprise any arbitrary number selected by the user. When the user desires to rewrite the information to an originally-issued (but erased) card or desires to write the information to a "dummy" card, the account information may be retrieved from the Module's memory by entering the pass code associated with that card, for example via a keypad associated with the SCCH Module.

In accordance with a further aspect of the present invention, the SCCH Module may be equipped with an alarm or other warning mechanism which may be configured to alert the card owner in the event the card is not erased within a predetermined period of time after being reissued. For example, when a card owner desires to charge merchandise to a credit card, either the

originally issued (but blank) credit card or a "dummy" card may be inserted into the Module, and the account information written onto the magnetic strip associated with the card, immediately prior to effecting the sales transaction. After the sales transaction is completed, the alarm or other warning device associated with the SCCH Module may be configured to alert the owner to erase the information from the card within a predetermined time, for example, 90 seconds after issuing the card.

In accordance with yet another further aspect of the invention, the personal/biographical information (i.e., photograph, signature, name) may appear on the outside of the SCCH Module, either in addition to or instead of appearing on the cardholder's credit card.

In accordance with a further aspect of the invention, after entering a password into the SCCH Module, a plastic or paper card bearing a magnetic strip may be issued by the SCCH and signed by the owner of the account, which card may be retained by the seller as a receipt or proof of approval of the transaction. The amount, date, and other data associated with the transaction may also be written onto the paper/plastic card which, in effect, has been issued for a single transaction and kept by the seller as a Magnetic Card Receipt (MCR).

In accordance with yet a further aspect of the invention, the magnetic material comprising the magnetic strip associated with a card of the type discussed herein may be made from a material or otherwise configured such that the magnetic information in the strip remains intact for a short, predetermined period of time. In this way, the card may be used immediately after issuing for a predetermined time thereafter, but will be incapable of effecting a transaction beyond the predetermined period of authorization inasmuch as the magnetic information is calculated to degrade a short time after the card is issued. The use of such a Transitory Magnetic Card (TMC) permits the owner of the

card to reissue the card on the spot, in order to effect a sales transaction with the ease and simplicity of conventional cards, yet the card can be abandoned after the transaction, and the likelihood that the card will be used for an unauthorized purpose in the event it is lost or stolen is minimized.

Brief Description Of The Drawing Figures

The subject invention will hereinafter be described in conjunction with the appended drawing figures, wherein like numerals denote like elements, and:

Figure 1 is a schematic diagram of an exemplary SCCH Module in accordance with one aspect of the invention;

Figure 2 is an exemplary Magnetic Card Receipt (MCR) in accordance with one aspect of the invention;

Figure 3 is an exemplary block diagram of the Module shown in Figure 1 setting forth various functional aspects of the Module;

Figure 4 is a schematic diagram of an exemplary transaction card for use in conjunction with the Module shown in Figure 1; and

Figure 5 depicts a credit card verification device of the type typically employed at Point of Sale (POS) transaction sites.

Detailed Description Of Preferred Exemplary Embodiments

Referring now to Figures 1, 4 and 5, an exemplary Smart Credit Cardholder (SCCH) Module 3 in accordance with the present invention suitably comprises a keypad 6, for example a conventional alphanumeric telephone-type keypad, an alphanumeric display 11, an audio transducer (speaker) 8, a first inlet slot 7, a second inlet slot 4 having an erasing mechanism 30, for example a permanent magnet associated therewith, and a selectively actuable mode switch 60.

As is well known, financial, sales and other transactions which are effectuated through the use of a transaction card of the type bearing a magnetic strip often employ a verification

device (Figure 5), typically located at the seller's place of business. In order to authorize a transaction, it is often appropriate to swipe or draw the transaction card through a slot 62 associated with verification device 5, such that magnetic strip 1 associated with card 2 is integrated by an appropriate card reading mechanism associated with device 5. The account or other information imbedded within strip 1 is read by device 5 and used to authorize the transaction, for example by transmitting the information to a central computer maintained by the card issuer (for example to confirm or deny the transaction). For example, if the card has been reported stolen or if the amount of the transaction exceeds the cardholder's available credit limit, the transaction may be denied.

In accordance with one aspect of the present invention, the account information imbedded within magnetic strip 1 may be stored in memory within module 3, thus permitting the owner of the card to erase the information from the card and to write the information back to the original card or to another card only when desired, for example immediately prior to effecting a transaction with the card. In this way, if the card is lost or stolen between transactions, the likelihood that the card may be used in an unauthorized manner is reduced inasmuch as the card does not bear the account information within its magnetic strip, and further in view of the fact that an unauthorized user is unlikely to also have access to the cardholder's SCCH Module and/or knowledge of the pass code used to retrieve the account information from Module 3.

Referring now to Figure 3, Module 3 may be configured to house circuitry for electronically effecting the functions described herein. More particularly, Module 3 comprises a serial input/output port 33, a CPU 21 including a clock 32, a display circuit 22, a read-only memory (ROM) 23, a random access memory (RAM) 24, an alarm 8, a power source 26, a keyboard 6, and a card reader/

card writer 27 operatively associated with input slot 4 and output slot 7.

With continued reference to Figures 1, 3 and 4, the information imbedded in the magnetic strips of various bank cards, ATM cards, credit cards, debit cards, charge cards and the like may be stored within Module 3 and selectively retrieved by the owner of Module 3 in order to effect the transaction with one of the foregoing cards. More particularly, a typical transaction card, for example a *VISA*™ or *MASTERCARD*™, is issued to the card owner with the account information imbedded in the magnetic strip associated with the card. In a preferred embodiment of the present invention, the card may be inserted into slot 7 of Module 3, whereupon instructions resident in ROM 23 instruct display 22 to display a command to the user requesting that the user enter a pass code, for example a password comprising up to 10 or more alpha/numeric characters. In accordance with a particular preferred embodiment, the user may enter a 4-digit pass code into Module 3 via keypad 6. This pass code may later be used by the cardholder to retrieve information from Module 3 corresponding to the same card, as discussed in greater detail below.

Upon entering the pass code, an address is assigned in RAM 24 wherein information pertaining to the particular pass code may be stored. More particularly, once the card is inserted into Module 3 and a pass code entered, Card Reader 27 "reads" the information imbedded in the magnetic strip of the card and stores the information in RAM 24 in the location corresponding to the password associated with the card. In accordance with a further aspect of the present invention, the owner of Module 3 may thereafter operate the Module in accordance with one of at least two modes: in the context of the illustrated embodiment, the user may select either mode A operation or mode B operation via switch 60.

If mode A operation is employed, the card may then be removed from Module 3 through slot 7 with the information imbedded within

the magnetic strip intact. In accordance with mode A operation, the cardholder may then retain the originally issued card, with the magnetically coded information intact, in a safe place, for example a safe or safety deposit box. That is, in accordance with mode A operation, it is not necessary that the cardholder carry the credit card in a purse or wallet; rather, a facsimile or substitute for the card may be generated by the user for a particular transaction, as discussed in greater detail below.

In accordance with mode B operation, once a pass code is assigned to a particular transaction and the information is retrieved from the card and stored in RAM 24, the card may be removed through slot 4, whereupon the card interacts magnetically with magnet 30 to thereby erase the information from the magnetic strip 1. In this way, the cardholder may carry the card in a wallet or purse so that the card can be "reactivated" at a later time as discussed in greater detail below.

While it is still possible to use an erased card in an unauthorized manner, the likelihood of such unauthorized use is reduced inasmuch as a card without its magnetically encoded information typically may not be used to authorize a typical sales transaction of the type which employs a POS device 5.

When the owner of a transaction card desires to utilize the card to effect a transaction, whether it be a banking, debit, charge, sales, or other transaction, Module 3 may be used to reissue the card in the following manner:

When a cardholder desires to reissue a card, the user inserts a card into Module 3, for example by inserting the card into slot 4. In this regard, the card may be the originally issued card which was previously erased in accordance with mode B operation (described above), or the card may comprise a blank, "dummy" card, for example a generic or universal-type card which may be used as a credit card, debit card, bank card, or charge card, as desired. Upon inserting a card into Module 3, display 11 may instruct the user to enter a user I.D. as a threshold to

operating the device. In this regard, such a user I.D. may be unrelated to a particular card, and may simply constitute a threshold authorization step which must be performed by the user each time any card is "reissued." Thereafter, display 11 may instruct the user to enter a pass code pertaining to a particular card. Alternatively, the aforementioned "threshold" step may be eliminated, such that the user simply enters a single password into Module 3 (via keypad 6) corresponding to the particular card which the user is to reissue.

Upon entering the pass code corresponding to a particular card, the account information corresponding to that card is retrieved from RAM 24 and written on the magnetic strip of the card then resident in the Module by card writer 27. The reissued card is then removed from the Module through slot 7 and used to effect the sales, banking, charge, debit or other transaction.

In accordance with a further aspect of the invention, the user may reinsert the card into Module 3, for example through slot 4, upon completion of the transaction for which the card was reissued. That is, once the card has been used to effect the transaction, it may again be erased, thereby inhibiting the unauthorized use of the card in the event that it becomes lost or stolen. Alternatively, the cardholder may simply retain the card, with its account information intact within the magnetic strip, until it is desired to erase the information. For this purpose, Module 3 may be configured to remind the user of the option to erase the information from the card at a predetermined time following the time at which the card was reissued. For example, Module 3 may be configured such that alarm circuit 8 emits a buzz, tone, or voice synthesized command at a convenient time following reissue of the card. In accordance with a preferred embodiment, such an alarm signal may be emitted by Module 3 in the range of 30 seconds to 30 minutes, and most preferably in the range of about 90 seconds, following the issuance of a card. The period of time between the reissuance of

a card and the alarm signal should be of sufficient length to conveniently effect a transaction with a newly-reissued card.

In accordance with a further aspect of the invention, Module 3 may be used to store account information pertaining to a plurality of transactions and other type cards, in a single universal card used to reissue each of a plurality of cards stored within Module 3. In this way, a cardholder need only carry with him his personal SCCH Module 3 and one or more universal cards, rather than carrying a large number of credit cards, debit cards, bank cards, charge cards and the like.

In accordance with a further aspect of the invention, Module 3 may be configured to authorize a transaction directly, i.e., without the need for reissuing a card and swiping the card through a POS device such as POS device 5. More particularly, it may be desirable to connect Module 3 directly to a telephone line (if Module 3 is equipped with a modem) or to a POS device through input port 33. The authorization or other account information may thus be transmitted and/or received directly by Module 3, thus eliminating the need for the intervening steps of issuing a card and utilizing the magnetic strip associated with the card to convey the account information.

In accordance with a further aspect of the invention, information and/or data pertaining to transaction cards may be downloaded directly into RAM 24 via input port 33, without the need for inserting a card into the Module. In this way, rather than issuing a card bearing a magnetic strip having account information embedded therein, the information may be loaded into Module 3 via a port 33 from a computer, modem, telephone or other device. In accordance with this aspect of the invention, credit card and other card-issuing companies need not send the cards through the mail; rather, they may simply download the account information directly into Module 3, whereupon the consumer may issue his own transaction card via Module 3 as needed.

In accordance with the foregoing embodiments, and particularly in the context of mode B operation wherein information is erased from the transaction card and not rewritten until the card is used in a transaction, consumers are afforded an extra layer of security against unauthorized use of their cards. The present invention permits this additional security layer, for example in the form of a pass code required to retrieve the information from memory and reissue a card advantageously implemented through the use of Module 3. Thus, existing ATM's, POS devices, and the like, need not be altered, and may be used in their conventional fashion.

Even if Module 3 is lost or stolen, the account information remains secure to the extent an unauthorized user is without knowledge of the pass codes needed to retrieve account information from memory.

Referring now to Figure 2, an exemplary Magnetic Card Receipt (MCR) 9 comprises a thin, planar card including a magnetic strip 10 and various other indicia pertaining to a transaction, for example the cardholder's name, signature, transaction date, amount of transaction, the nature of the transaction, and the like. In accordance with an alternate embodiment of the present invention, MCR 9 may function as a universal card which may be entered into Module 3 whenever it is desired to effect a transaction. MCR 9 may be used to effect the transaction, and thereafter may be left with either the merchant (seller), bank, or other entity with whom the cardholder engages in a transaction as a receipt or other record evidencing authorization for the transaction. In this way, the card issued for a particular transaction by Module 3 can also function as a sales receipt or other permanent record of the transaction. For this purpose, MCR 9 may advantageously comprise paper, plastic, or other suitable material.

In accordance with the further aspect of the invention, the magnetic material which comprises magnetic strip 1 of card 2 (or,

alternatively, magnetic strip 10 of MCR 9) suitably comprises a magnetic material designed to retain the information stored therein for a predetermined period of time. Thus, the card issued by Module 3 may have a predetermined useful life, so that in the event it is lost or stolen, the information contained in the magnetic strip will be degraded, rendering the card unusable by an unauthorized user. Such a Transitory Magnetic Card (TMC) may contain magnetic material which causes the information written thereon to decay within a predetermined period of time, for example the range of 1 to 20 minutes, and most preferably in the range of 3 to 5 minutes, if the card is issued immediately prior to effecting a transaction. Alternatively, the magnetic strip may be configured as such that the information therein decays, for example due to thermal effects, or due to the interaction with magnetic fields present in normal commercial environments, within a period of one hour up to 1 or 2 days or more, for example in the context of a relatively short business trip. In yet a further embodiment, the magnetic strip may be configured such that the information written therein decays after a relatively long period of time, for example 2 to 4 weeks or more; this would be particularly advantageous in the situation where a card is issued for a vacation or other extended trip, but which is desired to be cancelled or otherwise rendered unusable at the end of the trip.

The use of a TMC-type magnetic strip is particularly advantageous in the context of MCR 9 to the extent such a receipt is left in the hands of a merchant; hence, the merchant may use MCR 9 for accounting and other administrative purposes, but would be unable to use the card to authorize another transaction once the information contained within the magnetic strip is eroded.

In accordance with a further aspect of the invention, Module 3 may be figured to display instructions, prompts, announcements, and the like to permit expanded functionality and flexibility for the user. For example, Module 3 may be configured to disclose a

message to the user when it is time to replace or recharge power source 26 (e.g., batteries).

In this regard, Module 3 may be configured to execute various accounting features, for example by storing data pertaining to various transactions so that the status of the various accounts maintained by Module 3 may be conveniently displayed for the user. For example, each time a transaction is closed for a particular account (e.g., a *VISA* credit card), an on-going balance of payments and charges for the user's *VISA* account may be maintained within RAM 24, such that the user may display his current available credit prior to effecting a transaction with his *VISA* card.

In accordance with a further embodiment of the invention, Module 3 may be adapted to include additional security apparatus, for example including a fingerprint detection circuit, a voice recognition circuit, and other security measures for the purpose of unambiguously identifying an authorized user.

Although the invention has been described herein in conjunction with the appended drawings and figures, the scope of the invention as set forth in the Appended Claims is not so limited. For example, although the apparatus and method of this invention has been described in the context of transaction cards, the invention may be utilized in the context of virtually any application wherein information is desired to be stored and retrieved in magnetic form. Various other modifications in the selection in the arrangement of the various components and method steps discussed herein may be made without departing from the spirit of the invention as set forth in the Appended Claims.

Claims:

1. A method for issuing cards having information embedded on a magnetic strip comprising:

reading the information embedded in the magnetic strip of the card using a hand-held device;

storing said information in an electronic circuit of said device; and

thereafter magnetically writing said information onto a magnetic strip of said card or another compatible card.

2. The method of Claim 1, further comprising the step of erasing said magnetic information from said card after said reading step and before said writing step.

3. The method of Claim 2, further comprising the steps of:

requesting a selection of a password when reading and storing the information embedded in the magnetic strip of a particular card; and

entering said password into said device in order to enable said rewriting step.

4. The method of Claim 3, wherein said entering step comprises entering a Personal Identification Number in order to prevent the unauthorized reissuing of said Card.

5. The method of Claim 4, wherein a blank card is issued instead of the original one, such blank card being capable of replacing the original one as a means for completing a transaction.

6. The method of Claim 5, wherein said writing step comprises writing information onto a card containing indicia pertaining to a sales transaction.

7. A transaction card encoder, comprising:

a processor, having embedded circuitry for effecting instructions pertaining to the operation of said device;

means for entering data into said device;

a slot for inserting and removing a transaction card having a magnetic strip from said device;

means for magnetically reading data embedded into said magnetic strip associated with said card;

memory means for storing data retrieved from said card;

means for erasing magnetic information from said magnetic strip associated with said card; and

means for writing on said magnetic strip of said card.

8. The device of Claim 7, further comprising means for sensing said card within said device.

9. The device of Claim 7, further comprising means for displaying user prompts.

10. The device of Claim 7, further comprising alarm means configured to generate an alarm at a predetermined period of time after said card is inserted into said device.

11. A portable electronic storage apparatus for storing the information pertaining to a card bearing a magnetic strip, comprising:

(a) a slot for facilitating insertion and removal of the card into and out of the apparatus;

(b) a memory circuit for storing information pertaining to the card;

(c) means for entering data into the apparatus;

(d) a card reader circuit configured to read information from the magnetic strip when the card is inserted into the apparatus; and

(e) a card writer circuit configured to write account information retrieved from said memory circuit onto the magnetic strip associated with the card in response to entry of a password into said entering means.

12. The apparatus of Claim 11, further comprising display means for displaying user prompts.

13. The apparatus of Claim 11, further comprising means, disposed proximate said slot, for selectively erasing information contained in the magnetic strip.

14. A method of securing account information of the type embedded in a magnetic strip on a credit card, comprising the steps of:

(a) inserting the credit card into an electronic storage module;

(b) assigning a code to the credit card;

(c) reading account information from the magnetic strip associated with the credit card within said module;

(d) storing said information read from the magnetic strip in a memory circuit within said module; and

(e) removing the card from said module.

15. The method of Claim 14, wherein said step of removing the credit card from said module comprises erasing said information from the magnetic strip.

16. The method of Claim 14, further comprising the steps of:

(a) inserting a card having a blank magnetic strip into said module;

(b) entering said code into said module;

(c) retrieving information from said memory circuit in accordance with said code;

(d) writing said retrieved information onto said blank magnetic strip associated with said card while said second card is within said module; and

(e) thereafter removing said second card from said module with said information embedded in said magnetic strip on said second card.

17. The method of Claim 14, further comprising the step of generating an alarm signal at a predetermined time following said step of inserting said card into said module.

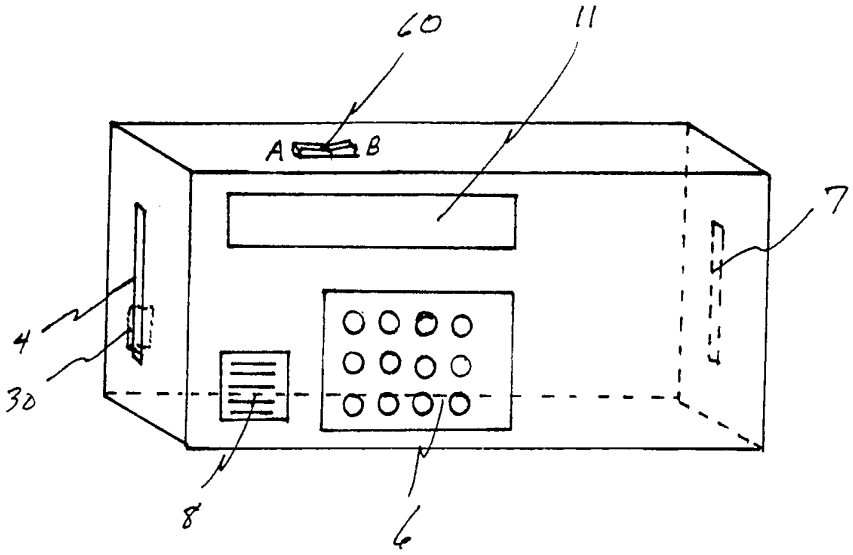
18. The method of Claim 14, wherein said step of assigning a code to said card comprises manually entering a PIN associated with said Card into said Module.

19. The method of Claim 14, further comprising the step of preconfiguring said module to function in accordance with one of at least two operational modes, wherein a first of said modes comprises the step of erasing said information from the magnetic strip as the card is removed from said module, and wherein a second of said operational modes comprises leaving the information embedded in said magnetic strip intact as the card is removed from said module.

20. The method of Claim 14, wherein said step of writing said information onto said magnetic strip comprises writing information pertaining to said account onto said magnetic strip, and further comprises the step of writing information onto said magnetic strip pertaining to a particular transaction.

21. The method of Claim 14, wherein said step of writing said information onto said magnetic strip comprises writing information onto a second card other than a first card from which information was read from a magnetic strip.

FIG. 1



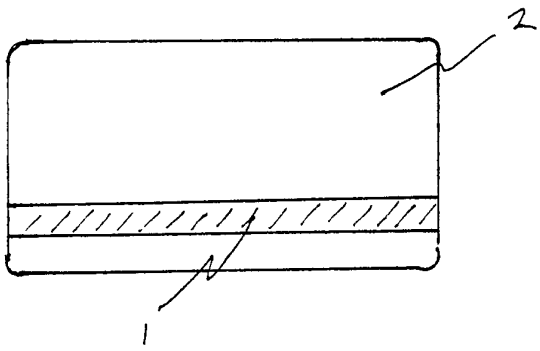


FIG. 4

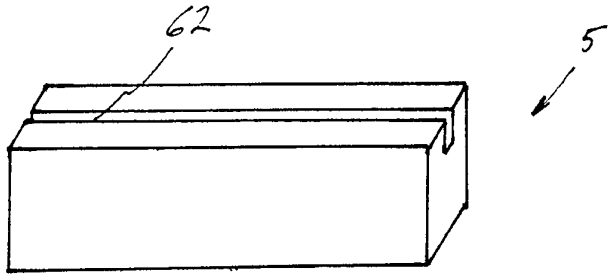


FIG. 5

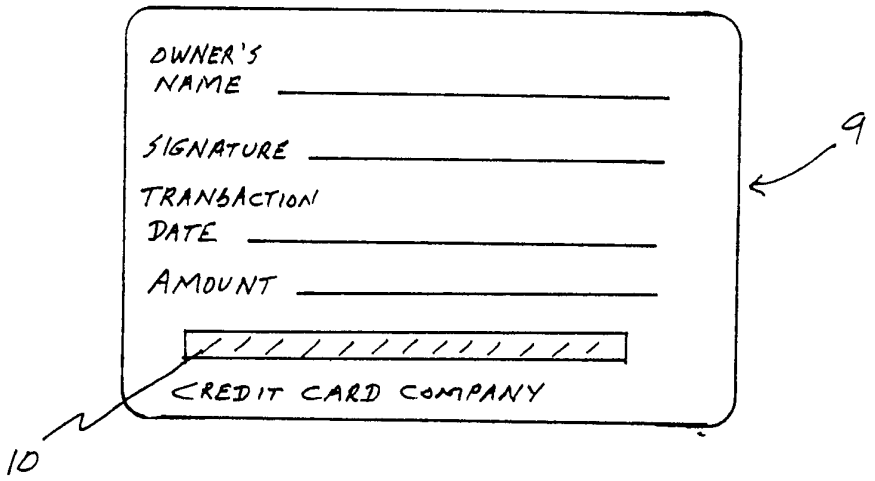

OWNER'S NAME
SIGNATURE
TRANSACTION DATE
AMOUNT
CREDIT CARD COMPANY
9
10

FIG. 2

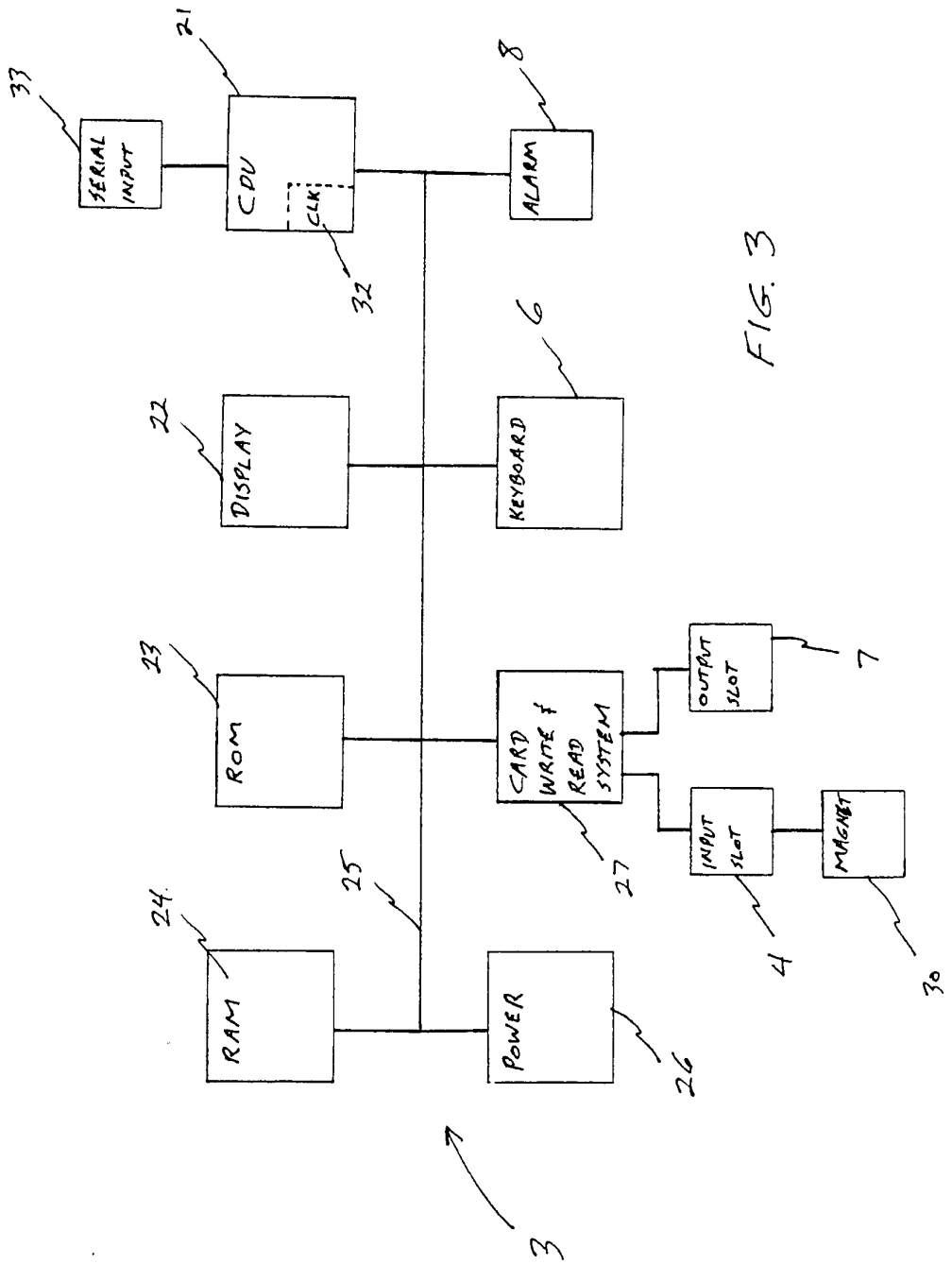

SERIAL INPUT
CPU
CLK
ALARM
DISPLAY
KEYBOARD
ROM
CARD WRITE & READ SYSTEM
OUTPUT SLOT
INPUT SLOT
MAGNET
RAM
POWER
21
33
8
32
6
22
23
7
27
4
30
24
25
26
3

FIG. 3

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 94/00715

A. CLASSIFICATION OF SUBJECT MATTER

G 07 F 7/10,G 06 K 7/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G 07 F,G 06 K,G 06 F 15/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP, A2, 0 397 512 (NIHON CARD TRANSFER CORP.) 14 November 1990 (14.11.90), claims 1-3,8; fig. 4.	1,3,4, 7,11
Y	EP, A1, 0 306 892 (DETHLOFF) 15 March 1989 (15.03.89), column 21, 1st paragraph; column 22, lines 22-56; figs. 4-7,9.	1,3,4, 7,11
A	column 21, 1st paragraph; column 22, lines 22-56; figs. 4-7,9.	2,5,6, 8-10, 12-15

☐ Further documents are listed in the continuation of box C.

☐ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 May 1994	10. 06. 94

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+ 31-70) 340-2040, Tx. 31 651 epo nl, Fax (+ 31-70) 340-3016	BISTRICH e.h.

Form PCT/ISA/210 (second sheet) (July 1992)

ANHANG

zum internationalen Recherchenbericht über die internationale Patentanmeldung Nr.

ANNEX

to the International Search Report to the International Patent Application No.

ANNEXE

au rapport de recherche international relatif á la demande de brevet international n°

PCT/US 94/00715 SAE 86098

In diesem Anhang sind die Mitglieder der Patentfamilien der im obengenannten internationalen Recherchenbericht angeführten Patentdokumente angegeben. Diese Angaben dienen nur zur Unterrichtung und erfolgen ohne Gewähr.

This Annex lists the patent family members relating to the patent documents cited in the above-mentioned international search report. The Office is in no way liable for these particulars which are given merely for the purpose of information.

La présente annexe indique les membres de la famille de brevets relatifs aux documents de brevets cités dans le rapport de recherche international visée ci-dessus. Les renseignements fournis sont donnés á titre indicatif et n'engagent pas la responsibilité de l'Office.

Im Recherchenbericht angeführtes Patentdokument Patent document cited in search report Document de brevet cité dans le rapport de recherche	Datum der Veröffentlichung Publication date Date de publication	Mitglied(er) der Patentfamilie Patent family member(s) Membre(s) de la famille de brevets	Datum der Veröffentlichung Publication date Date de publication
EP A2 397512	14-11-90	EP A3 397512 JP A2 2297297	05-06-91 07-12-90
EP A1 306892	15-03-89	CN A 1031902 CN B 1009398 DD A5 282306 DD A5 282308 DE C0 3867001 EP B1 306892 HU A2 50257 HU B 206555 JP A2 1145798 US A 4837422 US A 4968873	22-03-89 29-08-90 05-09-90 05-09-90 30-01-92 18-12-91 28-12-89 30-11-92 07-06-89 06-06-89 06-11-90