A merchant specific debit card verification system which includes a debit card having at least one ID property stored thereon and a merchant's terminal having at least one ID property stored thereon so that the ID property stored on the debit card relates to the ID properties stored on the merchant's terminal in a predetermined manner. The merchant's terminal retrieves the ID properties stored on the debit card so as to provide a retrieved ID property and then transmits to an intelligent network platform the retrieved ID property and the ID properties stored on the merchant's terminal. The intelligent network platform matches the ID properties stored on the terminal with the retrieved ID property and then transmits a validation whereby the debit card may be used at the merchant's terminal.

8 Claims, 4 Drawing Sheets
Figure 1

10

Figure 2

64

22

26

22

18

24

28

72

73

14

12

Merchant Terminal Interface Unit

Intelligent Network Platform Computer

Response Unit Interface

Database Program

Response Unit
$S_0$ Consumer presents debit card.

$S_1$ Merchant "swipes" debit card through card reader connected to merchants terminal.

$S_2$ Merchant inputs transaction amount via keypad provided with merchants terminal.

$S_3$ M.T. connects with INP and transmits validation access codes and encrypted data field from card.

$S_4$ INP decrypts the encrypted data fields.

$S_5$ INP compares data fields with the associated validation access codes. If the data fields do not match the associated validation access codes, then reject the transaction. If they do match then next step.

$S_6$ INP notifies M.T. of rejection and then closes the connection with the M.T.

$S_7$ INP debits or credits account balance associated with the card number.

$S_8$ INP notifies M.T. of acceptance and then closes the connection with M.T.

$S_9$ M.T. provides receipt.
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$S_0$</td>
<td>Consumer calls INP</td>
</tr>
<tr>
<td>$S_1$</td>
<td>Consumer inputs account number.</td>
</tr>
<tr>
<td>$S_2$</td>
<td>INP checks to see if valid account number. If valid then $S_3$, if not then $S_1$.</td>
</tr>
<tr>
<td>$S_3$</td>
<td>Consumer inputs destination number.</td>
</tr>
<tr>
<td>$S_4$</td>
<td>INP checks to see if destination answers, if so $S_5$, if not cancel.</td>
</tr>
<tr>
<td>$S_5$</td>
<td>INP checks to see if account balance = 0 if so, then disconnect, if not then $S_7$.</td>
</tr>
<tr>
<td>$S_6$</td>
<td>INP checks to see if account balance = value where only one or two minutes are remaining if so, then $S_8$, if not, then $S_5$.</td>
</tr>
<tr>
<td>$S_7$</td>
<td>Warn consumer of remaining time, then go to $S_8$.</td>
</tr>
<tr>
<td>$S_8$</td>
<td>Debit account balance at predetermined rate.</td>
</tr>
</tbody>
</table>
Upon successful activation of the debit card, the consumer may use the activated debit card for the purchase of goods or services, principally from participating retail locations.

The merchant no longer has a large initial expenditure since the non-activated debit cards have no initial intrinsic value. The consumer can not use the debit card at an unauthorized location since the debit card can only be used at terminals encoded with the correct ID property. Theft is no longer a concern since the non-activated debit cards have very little value.

**BRIEF DESCRIPTION OF THE DRAWINGS**

FIG. 1 is a rear view of a debit card for use in the present invention.

FIG. 2 is a schematic, diagrammatic view of an intelligent network platform.

FIG. 3 is a flow chart illustrating a preferred sequence of steps to be followed in the distribution of the debit card of FIG. 1.

FIG. 4 is a diagrammatic view illustrating the creation of the encrypted data field.

FIG. 5 is a schematic, diagrammatic view of a merchant's terminal for use in the present invention.

FIG. 6 is a diagrammatic view illustrating the decryption of the encrypted data field.

FIG. 7 is a diagrammatic view illustrating a preferred sequence of steps to be followed when using the debit card of FIG. 1 to make a transaction.

FIG. 8 is a diagrammatic view illustrating a preferred sequence of steps to be followed when using the debit card of FIG. 1 for making long distance telephone calls.

**DESCRIPTION OF THE PREFERRED EMBODIMENT**

Shown in FIG. 1 and designated by the general reference numeral 10 is a debit card for use in the present invention. The debit card 10 comprises a card 12 which has a magnetic stripe 14 containing information which is capable of being read by an appropriate card reader (not shown) such as the card reader provided with a Verifone Trans 330 merchant's terminal provided from Verifone, Inc. of Three Lagoon Drive, Suite 400, Redwood City, Calif. 94065. The information contained on the magnetic stripe comprises a card record, which preferably contains the following encrypted data fields: merchant ID and card number. As explained below, the card record may further contain the following optional encrypted data fields: terminal ID and store ID.

Debit cards are well known in the art. The debit card 10 may be any type of debit card.

As shown in FIG. 2, an intelligent network platform 16 is maintained for the use and the activation of debit cards, such as the debit card 10. The intelligent network platform 16 is comprised of a computer 18 which is loaded with a database program 20, the computer 18 being connected to a merchant's terminal interface unit 22 and to a response unit interface 24 via signal paths 26 and 28 respectively. The computer 18 may be a DOS or UNIX based computer such as an IBM PS/2. The database program 20 may be a program developed from a developer's toolkit, such as VOS available from Parity Software of 870 Market St., #1155, San Francisco, Calif. 94102. The program developed from the developer's toolkit, such as VOS, may be selectively customizable as is customary in the art. The merchant's termi-
The encrypted data field is output via signal path 36 to a database loading system 34 where the terms from the contract 30 are loaded into the database 28. Optionally, the contract may contain and the database may be loaded with the following terms: store ID, terminal ID or retailer greeting prompt.

After the contract terms are loaded into the database 28 by the database loading system 34, the merchant ID, store ID, terminal ID, card number and originating telephone number terms are transferred via signal path 36 to a card encoding system 38 wherein the encrypted data field in accordance with the encryption algorithm and the encoding service is available from FastCards, Inc. which can be located at 903 North Bowser Dr., St., 200, Richardson, Tex. 75081.

Now referring to FIG. 4, the generation of the encrypted data fields is accomplished by an electronic element 44, which is preferably a microprocessor that has been programmed with an encryption algorithm. The electronic element 44 receives as inputs a data field to be encrypted and the originating telephone number via signal paths 46 and 48. The electronic element 44 then produces the encrypted data field in accordance with the encryption algorithm and the data field to be encrypted and the originating phone number inputs. The encrypted data field is output via signal path 36 to the card encoding system 38 wherein the encrypted data field is encoded onto the magnetic stripe 14 of the debit card 10.

The encryption algorithm may be any of a number of encryption algorithms which are known in the art. For example, an encryption algorithm may generate the encrypted data field by altering the characters of the two inputs. Alternatively, the encryption algorithm may concatenate the two inputs to generate the encrypted data field. Although the two preferred inputs are the data field to be encrypted and the originating telephone number, it is to be understood that the present invention is not limited to only using either or both of these inputs. For example, the encrypted data field may be generated using the data field to be encrypted and using a date or a time as the two inputs.

FIG. 5 shows a merchant's terminal 50 which has been programmed with an ID property which corresponds in a predetermined manner with the merchant ID field encrypted on the debit card 10. The merchant's terminal is provided with a central processing unit 51, a card reader 52, a keypad 54 and a communication interface 56. The card reader 52, the keypad 54 and the communication interface 56 are connected to the central processing unit 51 via respective signal paths 58, 60 and 62.

When making a transaction, the debit card 10 is passed through the card reader 52 to read the encrypted data fields, such as merchant ID and card number for example, which are stored on the magnetic stripe 14 of the debit card 10. The encrypted data fields, merchant ID and card number, are transmitted along signal path 58 to the central processing unit 51. A transaction amount is then punched into the keypad 54 which transmits the transaction amount to the central processing unit 51 via signal path 60.

The communication interface 56 then connects with the merchant terminal interface unit 22 (FIG. 2) of the intelligent network platform 16 via signal path 64. The encrypted data fields, merchant ID and card number, along with the transaction amount and the ID property are then transmitted sequentially along signal paths 62, 64 and 26 to the intelligent network platform computer 18. The intelligent network platform computer 18 operates in accordance with a decryption algorithm 66 (FIG. 6) which decrypts the encrypted data fields, card number and merchant ID. The merchant ID field from the debit card 10 is then compared with the ID property programmed into the merchant's terminal 50. If the two codes match, then the transaction may continue. However, if the two codes do not match, then the transaction is not allowed to proceed.

If the two codes match and the transaction is allowed to continue, the intelligent network platform computer 18 debits or credits an account balance associated with the card number by the transaction amount. The merchant's terminal 50 is then notified in reverse by the intelligent network platform computer 18 via sequential signal paths 26 and 64 wherein the merchant's terminal 50 provides a receipt for the transaction.

In this manner, the merchant can be assured that the debit card 10 may not be used except at merchant's terminals, such as the merchant's terminal 50, authorized by the merchant. That is, the debit card 10 may only be used at merchant's terminals that have been programmed with an ID property that corresponds in a predetermined manner to the ID property stored on the debit card 10. The use of the debit card 10 may be confined to a particular store of a retail chain by matching the optional store ID field on the debit card 10 with the ID property relating to the optional store ID field stored on the merchant's terminal 50. The use of the debit card 10 may be further confined to a particular merchant's terminal 50 in a store by matching the optional terminal ID field on the debit card 10 with the optional ID property relating to the terminal ID field stored on the merchant's terminal 50.

As shown in FIG. 6, the decryption algorithm 66 receives a first input via signal path 68 and a second input via signal path 70 and outputs a decrypted data field via signal path 71. The first input is preferably the encrypted data field and the second input is preferably the originating telephone number which is sensed from a telephone line where the connection from the merchant's terminal 50 originated. The sensed originating telephone number must be identical to the originating telephone number which was used in the encryption of the encrypted data field. In the event that the two originating telephone numbers are not identical, then the encrypted data field will not be decrypted properly.
The above stated sequence of steps followed when making the transaction as set forth above are summarized in the step chart of FIG. 7. The consumer presents the debit card 10 to the merchant at a step S0, At a step S1, the Merchant swipes the debit card 10 through the card reader 52 which is connected to the merchant’s terminal 50. The merchant inputs the transaction amount via the keypad 54 which is provided with the merchant’s terminal 50, at a step S2.

The merchant's terminal 50 connects with the intelligent network platform 16 and then transmits to the intelligent network platform 16 the ID properties which are stored on the merchant's terminal 50 and the encrypted data fields which are stored on the debit card 10, at a step S3. At a step S4, the intelligent network platform's decryption algorithm 66 then decrypts the encrypted data fields.

At a step S5, the intelligent network platform 16 compares the data fields, such as merchant ID, terminal ID and store ID, with the associated ID properties. If the data fields do not match the associated ID properties then the transaction is rejected. At a step S6, the intelligent network platform 16 notifies the merchant’s terminal 50 of the rejection of the transaction and then closes the connection with the merchant’s terminal 50. However, if the data fields do match the associated ID properties, then the intelligent network platform 16 accepts the transaction and debits or credits the account balance associated with the card number, at a step S7. The intelligent network platform 16 notifies the merchant’s terminal 50 of the acceptance of the transaction and then closes the connection with the merchant’s terminal 50, at a step S8. And at a step S9, the merchant’s terminal provides a receipt for the consumer.

Customizing a merchant’s terminal for a particular merchant is well known in the art. The merchant may be provided with any merchant’s terminal which may be programmed with ID properties, such as the Verifone Trans 330. The Verifone Trans 330 may be provided with the ID properties preprogrammed. That is, Verifone will customize the merchant’s terminal 50 for the merchant.

The term “transaction” as used herein is intended to mean any transfer of value between two entities, such as the consumer and the merchant. For example, the transaction would occur when the consumer would be adding value to the debit card 10 or when the consumer would be buying goods or services with the debit card 10.

The debit card 10 may further be used for making long distance calls. Referring again to FIG. 2, when the debit card 10 is used for making long distance calls, the consumer calls into the response unit interface 24 of the intelligent network platform 16 via signal path 72 from a response unit 73, such as a touch tone telephone. Upon connection, the consumer then punches an account number into the response unit 73 which is transmitted to the response unit interface 24 via signal path 72.

The account number is transmitted from the response unit interface 24 to the intelligent network platform computer 18 via signal path 28 where the intelligent network platform computer 18 checks the validity of the account number punched in by the consumer. If the account number is a valid number, then the consumer is prompted via signal path 72 to enter in a destination telephone number. If the account number is not a valid number, then the consumer is prompted to reenter the account number, at a step S10. If the account number is not a valid number, then the consumer is prompted to reenter the account number, at a step S11. At a step S12, the intelligent network platform 16 checks to see if the destination answers. If the destination does not answer the telephone, then the process is cancelled. However, if the destination does answer the telephone, either automatically or manually, then the intelligent network platform 16 enters into a monitoring cycle starting at step S13.

At step S14, the intelligent network platform 16 checks to see if the consumer's account balance is equal to zero. If the consumer's account balance is equal to zero, then the intelligent network platform disconnects the call. However, if the consumer's account balance is not equal to zero, then the intelligent network platform executes the next step (S15) wherein the intelligent network platform checks to see if there is only a few minutes worth of value remaining in the consumer's account. If there is only a few minutes worth of value remaining in the consumer's account, then the intelligent network platform 16 warns, either audibly or visually, the consumer of the remaining time, at a step S16, then debits the consumer's account at a step S17. If there is more than a few minutes worth of value remaining in the consumer's account, then the consumer's account balance is debited at a step S18. After step S18, the sequence repeats starting at step S13.

Changes may be made in the steps or sequence of steps of the methods described herein without departing from the spirit and the scope of the invention as defined in the following claims.

What is claimed is:

1. A method of making a transaction, the method comprising the steps of:
   a. providing a debit card having at least one ID information stored thereon;
   b. providing a terminal having at least one ID information stored thereon prior to the transaction wherein the ID information stored on the debit card relates to the ID information stored on the terminal in a predetermined manner;
   c. retrieving via the terminal the ID information stored on the debit card so as to provide a retrieved ID information;
   d. transmitting to a computer the retrieved ID information and the ID information stored on the terminal;
   e. matching via the computer the ID information stored on the terminal with the retrieved ID information; and
   f. transmitting via the computer a validation to the terminal.
2. The method of claim 1 wherein the ID information is selected from a group of ID information consisting of merchant ID, terminal ID and store ID.

3. A method of making a transaction, the method comprising the steps of:
   a. providing a debit card having at least one encrypted ID information stored thereon;
   b. providing a terminal having at least one ID information stored thereon wherein the ID information stored on the debit card relates to the ID information stored on the terminal in a predetermined manner;
   c. retrieving via the terminal the encrypted ID information stored on the debit card so as to provide a retrieved encrypted ID information;
   d. communicating means for transmitting the ID information stored on the debit card to determine whether the transaction is valid; and
   e. communication means for transmitting the ID information stored on the debit card and the ID information stored on the terminal to the computer means such that the ID information stored on the debit card and the ID information stored on the terminal can be matched by the computer means.

4. The method of claim 3 wherein the encrypted ID information is selected from a group of encrypted ID information consisting of merchant ID, terminal ID and store ID.

5. An apparatus of making a transaction, the apparatus comprising:
   a. providing a debit card having at least one ID information stored thereon which is related to an ID information stored on a terminal in a predetermined manner;
   b. providing a terminal having at least one ID information stored thereon prior to the transaction wherein the ID information stored on the terminal relates to the ID information stored on the debit card in a predetermined manner;
   c. card reader means communicating with the terminal for retrieving the ID information stored on the debit card;
   d. computer means disposed remotely from the terminal for matching the ID information stored on the terminal with the ID information stored on the card to determine whether the transaction is valid; and
   e. communication means for transmitting the ID information stored on the debit card and the ID information stored on the terminal to the computer means such that the ID information stored on the debit card and the ID information stored on the terminal can be matched by the computer means.

6. The apparatus of claim 5 wherein the ID information stored on the debit card is further defined as being selected from a group of ID information consisting of a merchant ID, a terminal ID and a store ID.

7. A method for making long distance telephone calls using a debit card verification system, the method comprising the steps of:
   a. providing a debit card having at least one encrypted ID information stored thereon which is related to an ID information stored on a terminal in a predetermined manner;
   b. providing a response unit;
   c. connecting, via the response unit, to a computer;
   d. transmitting, from the response unit, a destination telephone number and an account number to the computer;
   e. checking, by the computer, the validity of the account number transmitted from the response unit;
   f. generating a signal indicative of the validity or invalidity of the account number wherein upon the signal being indicative of an invalid account number the computer is interrupted and upon the signal being indicative of a valid account number, dialing, by the computer, the destination telephone number transmitted by the response unit so that a telephone call is placed by an individual who is calling from the response unit.

8. The method of claim 7 wherein the encrypted ID information is selected from a group of encrypted ID information consisting of merchant ID, terminal ID and store ID.