

## CREDIT AUTHORIZATION SYSTEM AND METHOD

### FIELD OF THE INVENTION

[0001] The present invention relates to a system and method for preventing credit card fraud by comparing the location of a given transaction with the location of a pre-determined communication device.

### BACKGROUND OF THE INVENTION

[0002] Millions of individuals enjoy the convenience of utilizing transaction cards such as credit cards, charge cards, debit cards, and/or currency or "smart" cards as a convenient way in which to purchase goods and/or services. By utilizing transaction cards, an individual may enter into a transaction without having to have cash or currency in hand or otherwise. In the case of credit cards and charge cards, the individual, in effect obtains an instant loan of the funds needed to make a purchase and/or enter into a transaction. In the case of currency or "smart" cards, the individual may "store" an amount of money on the card(s) and, thereafter, utilize the card(s), instead of cash or currency, in order to make purchases and/or enter into transactions.

[0003] Millions of individuals also enjoy the benefits of having savings accounts, checking accounts and/or automated teller machine accounts which allow them to enjoy the security of saving their money in accounts which are usually insured and which allow them to, in some instances, earn interest on their money. In the case of checking accounts, individuals enjoy the convenience of writing checks and/or other transaction instruments which allow them to draw against their money without having to undergo the inconvenience of going to the bank or financial institution to withdraw their money, in currency form, and traveling to, in some cases, a distant location to either make a purchase, payment and/or to otherwise settle an account. In this regard, the ability to write checks, drafts and/or other instruments against an account is a very convenient manner in which to conduct transactions of any kind.

[0004] Many individuals also enjoy the convenience of owning and/or using wireless, mobile or cellular telephones or devices as a means by which to make telephone calls when a conventional line or permanent telephone is not within reach and/or when the individual is "on the go", such as in an automobile, on foot, and/or in any other type of environment, such as away from home, when a conventional line or permanently fixed telephone is not available.

[0005] Unfortunately, with the convenience of each of the above credit cards, charge cards, debit cards, and/or currency or "smart" cards, savings accounts, checking accounts, automated teller machine accounts, and cellular telephones or cellular communications devices, comes many disadvantages and the opportunity for theft and/or fraud. In the case of credit cards, charge cards and/or debit cards, hundreds of millions, if not billions, of dollars a year are lost as a result of the theft of, and/or the fraudulent use of, credit cards, charge cards and/or debit cards, or the account numbers which correspond thereto.

[0006] A lost or stolen card may be utilized by an unauthorized individual to spend upwards of thousands of dollars before the unauthorized use is detected and/or before the

cardholder can ascertain, and/or be notified, either by the card issuer or servicing institution or when the cardholder detects the unauthorized transaction on his or her monthly account statement, that the card is lost or stolen. Similarly, even in the absence of the physical card, an unauthorized individual may utilize the account number which corresponds to the card in order to make certain transactions, for example by telephone or the Internet.

[0007] While card holders are usually protected by various types of coverage which shield them from the liabilities associated with the fraudulent use of a card or the corresponding account number, the card issuers, credit, charge and/or debit card issuing companies and/or institutions, and/or their insurance companies end up paying for the above described thefts and/or fraudulent and/or unauthorized uses. Ultimately, the consumer also shoulders the burden of the costs associated with these thefts and/or fraudulent and/or unauthorized uses in the form of increased prices.

[0008] While authorization terminals and/or devices are utilized at a point-of-sale and/or at the vendor's, the seller's, or the service provider's, location, these authorization terminals and/or devices typically are utilized to obtain an authorization from the card issuer or account servicing institution, which usually entails a screening of whether the card has been lost, stolen, cancelled, de-activated and/or whether the cardholder has exceeded and/or will exceed his or her credit limit. This current authorization practice fails to prevent the use of a lost or stolen card, or the unauthorized use of either the card or the account number corresponding thereto, if the card has not been reported, and/or discovered, to be lost, stolen or used without authorization and/or if the account credit limit has not yet been reached.

[0009] Current practices do not entail and/or do not include the provision for obtaining an authorization, and/or for providing notice to the cardholder before, during and/or shortly after a transaction, which cardholder authorization and/or notification procedure would be helpful and prove to be essential in preventing the fraudulent use and/or unauthorized use of a card and/or the account number corresponding thereto, in an unauthorized transaction and/or shortly after an unauthorized transaction has occurred, thereby minimizing the fraudulent and/or unauthorized use of the card and/or the account number corresponding thereto.

[0010] In the case of currency or "smart" cards, which typically may serve as bearer instruments, the monetary credit on these cards may be completely depleted before the card owner even discovers same to be lost or stolen.

[0011] In the case of savings accounts, checking accounts, and/or automated teller machine accounts, these accounts may be accessed, and funds be withdrawn, without the account owner's notification and/or knowledge. In the case of savings accounts and checking accounts, these accounts may be accessed, and/or funds may be withdrawn therefrom, when checks drawn on insufficient funds are returned, and/or when the account number is inadvertently and/or fraudulently utilized in an endorsement, or otherwise, by an individual attempting to cash or perform a transaction with a fraudulent instrument, a forged instrument and/or an otherwise "bad" check. In these instances, the accounts and/or funds involved are usually accessed, invaded, and/or