

access message, and to send the access message to a merchant computer. Because the access message is tied to a particular product and a particular merchant computer, the access message can not be generated until the user sends the payment message to the payment computer. Because the access message is different from existing credit card formats, the access message is ill-suited for phone/mail orders and other traditional credit card transactions.

[0015] U.S. Pat. No. 5,883,810 (Franklin et al.) describes an online transaction system in which a user of the Internet or the like clicks on an icon to receive a proxy transaction number from a credit card provider. This proxy number stands in for the user's regular credit card number during transmission over the Internet, but expires after a short time (e.g., one hour) to reduce the chance that the number will be effectively intercepted and fraudulently used. The processing that occurs when a bank receives transaction information from a merchant involves checking whether the proxy number is a valid number and whether the transaction value and merchant match. There is no additional processing triggered when the bank processing system receives the proxy number. In addition, a significant drawback of the Franklin et al. system is that an unscrupulous merchant or a criminal who is capable of accessing or intercepting order details can then turn around and use the proxy number a number of times before the lapse of the expiration term. Thus, more than one transaction can occur within the duration of the expiration term. The Franklin et al. system has nothing in place to prevent this type of fraud. The Franklin et al. system merely depends upon an assumption that fewer criminals could obtain the proxy number and reuse it within the expiration term of the proxy transaction number set by the issuing bank than the total number of criminals capable of gaining access to credit card numbers used for online commerce. Also, the inclusion of specific transaction information does not prevent a fraudulent merchant from recurrent unauthorized charges within the expiry time of the proxy number. The user will not be aware of this misuse of his/her credit card details until the receipt of the statement, which will typically not be until several weeks later.

[0016] There are also specific electronic transaction systems such as "Cyber Cash," "Check Free" and "First Virtual." Unfortunately, there are perceived problems with what has been proposed to date. First, any form of reliance on encryption is a challenge to those who will then try to break it. The manner in which access has been gained to extremely sensitive information in government premises would make anyone wary of any reliance on an encryption system. Second, a further problem is that some of the most secure forms of encryption system are not widely available due to government and other security requirements. Limiting the electronic trading systems and security systems for use to the Internet is of relatively little use. In addition, entirely new electronic payment systems require changes in how merchants handle transactions and this represents an important commercial disadvantage for such systems.

[0017] Additionally, various approaches have been taken to make "card present" transactions more attractive. For instance, Japanese Patent Publication No. Hei 6-282556 discloses a one-time credit card settlement system for use by, e.g., teenage children of credit card holders. This system employs a credit card which can be used only once in which

various information such as specific personal information, use conditions, and an approved credit limit identical to those of the original credit card are recorded on a data recording element and displayed on the face of the card. The one-time credit card contains the same member number, expiration date, card company code, and the like as on existing credit card, as well as one-time credit card expiration date not exceeding the expiration date of credit card, available credit limit for the card, and the like. The one-time credit card makes use of some of the same settlement means as the conventional credit card. However, the system also requires use permission information to be recorded on the credit card, the information permitting the credit card to be used only once or making it impossible to use the credit card when the credit limit has been exceeded. A special card terminal device checks the information taken from the card for correctness and imparts use permission information for when the card is not permitted to be used on the transmission to the credit card issuing company. The use permission information takes the form of a punched hole on the card itself. This system has obvious drawbacks, such as the card terminal having to be modified for additional functions (e.g., punching holes, detected punched holes, imparting additional information, etc.). Also, such a system offers little additional security insofar as fraud can still be practiced perhaps by covering the holes or otherwise replacing the permission use information on the credit card. Further, such a system would require a change in nearly all card terminal equipment if it were adopted.

[0018] U.S. Pat. Nos. 5,627,355 and 5,478,994 (Rahman et al.) disclose another type of system that uses a plurality of pin numbers which are added to a credit card number on an electronic display. U.S. Pat. No. 5,627,355 discloses a credit card having a memory element containing a series of passwords in a predetermined sequence. These passwords are identical to another sequence stored in a memory of a host control computer. Further, the card contains a first fixed field containing an account number (e.g., "444 222 333"). In operation, the memory element of the credit card device provides a unique password from the sequence with each use of the credit card device. This permits verification by comparing the account number and the password provided with each use of the device with the account number and the next number in sequence as indicated by the host computer. The host computer deactivates the password after the transaction. Among the drawbacks with this type of system is the need for a power supply, a display, a memory device, a sound generator and the need to recycle a limited sequence of pin numbers. Such a system is not readily adapted to current credit card transactions because it lacks the ability of providing a check sum of the card number and cannot be read by a standard card reader. Also, if the card is lost or stolen, there is little to prevent a person from using the card until it is reported to be lost or stolen by the correct holder. See, also, U.S. Pat. No. 5,606,614 (Brady et al.).

[0019] Other attempts have been made to make funds available to an individual, but with limitations. For example, U.S. Pat. No. 5,350,906 (Brody et al.) and U.S. Pat. No. 5,326,960 (Tannenbaum et al.) disclose issuing temporary PINs for one time or limited time and limited credit access to an account at an ATM. These patents disclose a currency transfer system and method for an ATM network. In this system, a main account holder (i.e., the sponsor) sets up a subaccount that can be accessed by a non-subscriber by