

INCREASED SECURITY FOR ELECTRONIC TRANSACTIONS

Field of the Invention

- 5 The present invention relates to a method of increasing security in electronic transactions and apparatus for achieving the method. The method has particular application in conducting an online electronic transfer of money.

Background of the Invention

- 10 The present e-commerce environment and systems do not provide people with confidence in shopping online. Consumers are concerned about security issues when using their credit cards/debit cards to make purchases. They are worried that by using their credit cards/debit cards to make purchases online, that it will compromise the security of their credit cards/debit cards and they will be vulnerable to fraud. Should credit card
15 information go into the wrong hands, credit card owners may be liable for transactions not conducted by them.

The present invention provides a process that adds security to the transaction to alleviate some of the risks involved.

20

Summary of the Present Invention

In accordance with the present invention there is provided a method of conducting an online transaction, said method including the steps of:

- 25 providing a transaction manager;
 identifying a registered user to the transaction manager by a login process;
 receiving a transaction request from the identified user;
 generating a unique identifier and sending the unique identifier to the identified
user;
 associating the unique identifier with the transaction;
30 providing the unique identifier to the transaction manager;
 validating the unique identifier; and

performing the transaction in the event that the unique identifier is valid.

Preferably the transaction is the transfer of money. More preferably the transaction is a financial transaction to pay a merchant for the purchase of a product or service.

- 5 Alternatively the transaction is the transfer of money to a third party. In one embodiment the transaction is the transfer of money from one bank account to another.

Preferably the product or service is provided externally to the transaction process.

- 10 Preferably the method further comprises the step of registering the user with the transaction manager.

- Preferably the method further comprises the step of requesting the unique identifier, which follows receiving the transaction request. Preferably a user making a transaction request comprises requesting the unique identifier from transaction manager.
- 15

- Preferably the method further comprises the step of registering the merchant with the transaction manager. Preferably the merchant receives the transaction request from the user and provides the transaction request to the transaction manager. Preferably performing the transaction includes transaction manager causing the payment to occur. Typically performing the transaction includes the transaction manager providing the merchant with a unique transaction receipt number. Typically the payment is made into the merchant's bank account.
- 20

- 25 Preferably the login process comprises verifying the identify of the user by providing a password to match a user name, wherein a confirmation password is stored by the transaction manager, with the password provided by the user compared to the confirmation password to verify the identity of the user.

- 30 Preferably the unique identifier is unique to the transaction. Preferably the unique identifier is send to the user via a different communications means to the

communications means over which the user engages in the login process. Preferably the communications means includes a mobile telephone. Alternatively the unique identifier is send to the user in a different session (at a different time) to the transaction request.

- 5 Preferably the step of validation of the unique identified provides a second level of verification of the user's identity, which is unique to the transaction before the transaction is performed.

10 Preferably the transaction is conducted via an on-line banking service, such that the transaction manager comprises an on-line banking service computer server. Typically the transaction is provided by the on-line banking service.

15 In one embodiment the transaction is one session with one or more sub-transactions being provided by the on-line banking service. Preferably a fee is paid to the on-line banking service provider for each transaction. Alternatively a fee is paid to the on-line banking service provider for each session. Alternatively a fee is paid to the on-line banking service provider for the overall provision of the on-line banking service.

20 Preferably the provision of the product or service is triggered by the transaction.

Preferably the transaction manager comprises an user identification component.
Preferably the transaction manager comprises a transaction control component.
Preferably the transaction manager comprises a unique identifier generation component and unique identifier validation component.

25

Also in accordance with the present invention there is a method of identifying a user comprising the steps of:

- 30 providing an identification means;
providing facilitation means for conducting a transaction;
identifying the user to the identification means;
issuing an identity authenticated code to the identified user;

receiving a request from the user to access an on-line service or purchase of a product by electronic transaction;

requesting the user supply the identity authenticated code to the facilitation means;

5 receiving the identity authenticated code at the facilitation means;

transferring the identity authenticated code from the facilitation means to the identification means;

validating the identity authenticated code as being that provided to the identified user by the user identification means; and

10 facilitating the electronic transaction.

Preferably sending the identity authenticated code to the user is via a different mode of communication;

15 Also in accordance with the present invention there is a transaction manager comprising:
means for identifying a registered user to the transaction manager by a login process;

means for generating a unique identifier and sending the unique identifier to the identified user when a transaction request is made by the registered user;

20 means for recording an association of the unique identifier with the transaction;

means for receiving the unique identifier from the registered user;

means for validating the unique identifier; and

means for facilitating performance of the transaction in the event that the unique identifier is valid.

25

Preferably the transaction manager deducts money from a user's account to cover the money paid to the merchant. Preferably the transaction manager deducts money at the time of the request of the unique transaction identifier. Alternatively the transaction manager deducts money at the time of the transfer of money to the merchant.

30

Preferably the user's account is with a financial institution. Alternatively the user's

account is with the transaction manger, the account may be a credit account or a charge account. Preferably the transaction manager issues a new account that corresponds to an existing account with a financial institution, whereby the new account details are used by the user and merchant in place of the existing account details. Preferably the transaction
5 manager uses the new account details to look up the existing account details and the existing account details are used by the transaction manager with the financial institution.

Preferably the user requests the unique transaction identifier by an Internet connection. Preferably the user's registration details are stored in a database of the transaction
10 manager. Preferably the merchant's registration details are stored in the database including a unique merchant identification.

Preferably the user's request for the unique transaction identifier is validated by checking the user's details stored in the database of the transaction manager. Preferably when the
15 merchant forwards the unique identification number to the transaction manager, the merchants unique identifier is sent to the transaction manager, whereby validating the merchants identification is checked by the transaction manager before sending the identification number.

20 Preferably the transaction manager checks if sufficient funds are available to cover the transaction and the transaction number is only provided to the merchant if sufficient funds are available.

Preferably the merchant links to the transaction manager by the Internet or a dedicated
25 secure line to request the transaction number and the transfer of funds. Preferably the link between the user and the transaction manager, and the merchant and the transaction manager are secured by encryption.

Detailed Description of the Invention

30 In order to provide a better understanding a preferred embodiment of the present invention will now be described in detail, by way of example only, with reference to the

accompanying drawings, in which:

Figure 1 is a diagrammatic view of the relationship between entities using the method of the present invention;

Figure 2 is a diagrammatic flow chart representing an example of a transaction process in accordance with the present invention;

Figure 3 is a block diagram of a system architecture of the transaction manager of the present invention;

Figure 4 is a block diagram of a database structure of the transaction manager; and

Figure 5 is a block diagram of a data validation process conducted by the transaction manager.

Referring to Figure 1, entities using the method of the present invention are shown. A transaction manger 2 is provided. The transaction manager is referred to as ZIPFUND in the drawings. A user 4 uses the method of the present invention to conduct an electronic fund transfer transaction. Each user must have an account with the transaction manager to use the facility. The account is specific to each registered user. Information held by the transaction manager in relation to each user is held in confidence and in compliance with privacy laws. A user may maintain an Internet financial account with the transaction manager. The transaction manager will have the discretion to issue financial accounts to approved clients.

An e-commerce merchant 3 is a person or entity that uses an Internet site to do business with Internet clients. E-commerce merchants may register with the transaction manager to use the facility provided by the present invention. The registration process ensures that the e-commerce merchant site is a secure site and Internet clients are aware of this certification by the transaction manager. E-commerce merchants are required to obtain the transaction manager transaction identifiers from Internet clients prior to confirming payments. The transaction identifier needs to be confirmed by the transaction manager in order to secure payment from a financial institution. The transaction manager will maintain a database of registered e-commerce merchants.

A financial institution, such as a bank 1, provides an approved level of funds that an Internet user has available. This may be, for example, via a charge account or a credit card.

- 5 Each e-commerce merchant requires an account with a financial institution in order to receive payments. The transaction manager is responsible for all payments of transactions to a nominated financial institution of the e-commerce merchant.

Each financial institution may provide to the transaction manager access to a client's
10 financial information including approved funds availability. This will enable a funds transfer aspect of the transaction manager to confirm an Internet user's financial standing. A financial account is issued to a customer on the basis of an understanding between the transaction manager and a financial institution.

- 15 The transaction manager is a trusted intermediary that provides the services between Internet users, e-commerce merchants and financial institutions. In particular, the transaction manager is an intermediary that a user can trust to interact between the merchant and an electronic funds transfer system of a financial institution. The transaction manager provides e-commerce merchants with an approved transaction number in
20 response to a transaction identifier sent to them via a secure network. The transaction manager provides to the financial institution an approved transaction number for each of the transaction identifiers sent by an e-commerce merchant via a secure network. Preferably the transaction manager uses a newly generated account number to replace the original credit card number and/or debit card number account for account transaction
25 processing. This adds another level of security to the process.

The transaction manager is responsible for the security for Internet users carrying out their business to consumer transaction. This is possible through the use of proprietary software, accounting systems, design methodology, data definition and control processes.

30

Referring to Figure 2 the processing of a transaction is shown. The process starts at 5. An

Internet user 4 connects to the Internet at 6 and accesses the transaction manager 2 via the Internet. A user profile password check is conducted for granting access to the transaction manager. The transaction manager also has network security access controls and communication is encrypted. The Internet user is required to register or hold an account
5 with the transaction manager.

The Internet user requests 7 a transaction identifier for his or her shopping needs. That is, the user may request a transaction identifier be provided that will have a record of the limit the user allows to be authorised. This amount must be less than the available credit, but
10 also put an additional limitation on the transaction that can be conducted using transaction identifier. This gives the user control over the maximum value of transaction that may be authorised. The transaction manager checks 8 the Internet user to ensure that he or she is a valid user. The transaction manager confirms the validation process at 9.

15 If, as a result of this decision at 10, the user is not valid then they are rejected from the transaction manager site. If the user is valid the transaction manager issues at 11 a transaction identifier.

The Internet user is then able to request a transaction, such as by selecting an item at e-commerce merchant's site at 12. Upon deciding to purchase the item the user provides the
20 transaction identifier to the e-commerce merchant at 13.

The e-commerce merchant forwards for validation the transaction identifier to the transaction manager at 14. The transaction manager then confirms the validity of the
25 transaction identifier at 15. A security process including a merchant profile password checking is conducted by the transaction manager before access is approved. Further network security access controls such as encryption are provided to prevent security problems.

30 If the transaction identifier is not valid at 16 the transaction rejected. If the identifier is rejected the e-commerce merchant is advised along with the reason for the rejection. If the

transaction identifier is valid the transaction manager allows the transaction to proceed. The transaction manager issues an approved transaction number at 17 to the e-commerce merchant and disables further use of that transaction identifier. Forwarding of the transaction number to the merchant confirms that the transaction identifier was accepted.

5 At 18 the transaction manager issues a credit to the e-commerce merchant's account with the financial institution according to the value of the purchase. The transaction manager undergoes a required security check including a password check before access to the financial institution is approved. Further network security access controls are also provided including encryption of communication. The process then ends at 19.

10

In Figure 3, the system architecture of the transaction manager is shown. An operating system 20 provides an underlayer of the transaction manager system architecture. Sitting on top of the operating system is a relational database management system 21. This is the data collection centre of the system. The relational database management system 21
15 interacts with an application system 22. The application system 22 interacts with an Internet base system 23 that links the transaction manager to the outside world.

Referring to Figure 4, a database structure is shown relating an Internet user's profile to a financial institution and an e-commerce merchant's profile to a financial institution profile.

20 An Internet user's profile 24 is a repository of information concerning a particular Internet user. This is used for validation with a financial institution profile 25. An e-commerce merchant profile 26 or a repository of information concerning particular e-commerce merchant. This is used for validation with financial institution profile 27. Profiles for Internet users will be different to those of e-commerce merchant profiles.

25

Referring to Figure 5, data validation structure and processes are shown. In relation to the Internet user's profile personal details are checked with the relational database management system for accuracy and if accepted account details are then checked with the relational database management system validity. If accepted, credit details are checked
30 with the relational database management system for validity and if accepted transaction details are stored. Audit trials of each check are also recorded.

In relation to the e-commerce merchant profile, corporation details are checked with the relational database management system for accuracy. If accepted, account details are then checked with the relational database management system for validity. If accepted the credit details are checked with the relational database management system for validity. If accepted the transaction details are stored. An audit trail is recorded for each check and changed to the profile.

The present invention provides the following functionality to support e-commerce:

- 10 it provides a true online system, that is a process where all transactions are online;
- it provides a purchasing system where all users are able to make purchases online;
- it provides a payment system that supports other suppliers (merchant and/or financial institution) payment system;
- the system provides password control to validate processes within the system;
- 15 it provides debit and credit card support enable usage of other suppliers (merchant and/or financial institution credit card/debit card as well as an alternative credit card/debit card facility to make purchases and payments);
- it provides support for all financial institution accounts allowing a transaction to be processed by all types of bank accounts (for example, savings and cheques). Internet users
- 20 can use all types of bank accounts to make online purchases and payments provided they are valid users;
- it provides a controlled purchase amount through usage of transaction identifiers with all users able to control the amount of funds for each transaction;
- it provides a user validation system with the system validating the users
- 25 identification;
- it provides a merchant validation system with a system validating the merchants identification;
- it provides protection system through encryption and decryption system and proprietary system architecture.

30

Modifications and variations may be made to the present invention without departing from

the basic inventive concepts. The nature of such modifications and variations are to be determined within the scope of the present invention as defined by the foregoing description and appended claims.

- 5 In the claims of this application and in the description of the invention, except where the context requires otherwise due to express language or necessary implication, the words "comprise" or variations such as "comprises" or "comprising" are used in an inclusive sense, i.e. to specify the presence of the stated features but not to preclude the presence or addition of further features in various embodiments of the invention.

The claims defining the invention are as follows:

1. A method of conducting an online transaction, said method including the steps of:
5 providing a transaction manager;
identifying a registered user to the transaction manager by a login process;
receiving a transaction request from the identified user;
generating a unique identifier and sending the unique identifier to the identified user;
associating the unique identifier with the transaction;
10 providing the unique identifier to the transaction manager;
validating the unique identifier; and
performing the transaction in the event that the unique identifier is valid.
- 2 A method according to claim 1, wherein the transaction is the transfer of money.
15
- 3 A method according to either claim 1 or 2, wherein the transaction is a financial transaction to pay a merchant for the purchase of a product or service.
- 4 A method according to claim 3, wherein the product or service is provided
20 externally to the transaction process.
- 5 A method according to either claim 3 or 4, wherein the provision of the product or service is triggered by the transaction.
- 25 6 A method according to any one of claims 3 to 5, further comprising the step of registering the merchant with the transaction manager, wherein the merchant receives the transaction request from the user and provides the transaction request to the transaction manager.
- 30 7 A method according to any one of claims 3 to 5, further comprising the step of providing the unique identifier to the merchant, wherein the merchant provides

the unique identifier to the transaction manager.

- 8 A method according to claim 1, wherein the transaction is the transfer of money to a third party.
- 5 9 A method according to any one of claims 1 to 8, wherein the transaction is the transfer of money from one bank account to another.
- 10 10 A method according to any one of claims 1 to 9, further comprising the step of registering the user with the transaction manager.
- 15 11 A method according to any one of claims 1 to 10, further comprising the step of requesting the unique identifier, which follows receipting of the transaction request.
- 20 12 A method according to any one of claims 1 to 11, wherein a user making a transaction request comprises requesting the unique identifier from the transaction member.
- 25 13 A method according to any one of claims 1 to 12, wherein the unique identifier is unique to the transaction.
- 30 14 A method according to any one of claims 1 to 13, wherein the login process comprises verifying the identity of the user by providing a password to match a user name, wherein a confirmation password being stored by the transaction manager, wherein the password provided by the user is compared with the confirmation password.
- 15 15 A method according to claim 14, wherein performing the transaction includes the transaction manager providing the merchant with a unique transaction receipt number.

- 16 A method according to any one of claims 1 to 15, wherein the unique identifier is
send to the user via a different communications means to the communications
means over which the user engages in the login process.
- 5 17 A method according to claim 16, wherein the communications means includes a
mobile telephone and other telephone devices including VOIP (Voice Over
Internet Phone) and landline telephone.
- 10 18 A method according to any one of claims 1 to 17, wherein the unique identifier is
send to the user in a different session (at a different time) to the transaction
request.
- 15 19 A method according to claim 3, wherein performing the transaction includes
transaction manager causing the payment to occur.
- 20 20 A method according to claim 19, wherein the payment is made into the
merchant's bank account.
- 20 21 A method according to any one of claims 1 to 20, wherein the transaction is
conducted via an on-line banking service, such that the transaction manager
comprises an on-line banking service computer server.
- 25 22 A method according to claim 21, wherein the transaction is provided by the on-
line banking service.
- 23 23 A method according to claim 21, wherein the transaction is one session with one
or more sub-transactions being provided by the on-line banking service.
- 30 24 A method according to claim 22, wherein a fee is paid to the on-line banking
service provider for each transaction.

- 25 A method according to claim 22, wherein a fee is paid to the on-line banking service provider for each session.
- 5 26 A method according to claim 21, wherein a fee is paid to the on-line banking service provider for the overall provision of the on-line banking service.
- 27 A method according to any one of claims 1 to 26, wherein the transaction manager comprises an user identification component.
- 10 28 A method according to claim 1, wherein the transaction manager comprises a transaction control component.
- 15 29 A method according to any one of claims 1 to 28, wherein the transaction manager comprises a unique identifier generation component and unique identifier validation component.
- 30 A method according to any one of claims 1 to 29, wherein the step of validation of the unique identifiers occurs before the transaction is performed, whereby a second level of verification of the user's identity, which is unique to the transaction, is performed.
- 20 31 A method of identifying a user comprising the steps of:
providing an identification means;
25 providing facilitation means for conducting a transaction;
identifying the user to the identification means;
issuing an identity authenticated code to the identified user;
receiving a request from the user to access an on-line service or purchase of a product by electronic transaction;
30 requesting the user supply the identity authenticated code to the facilitation means;

receiving the identity authenticated code at the facilitation means;
transferring the identity authenticated code from the facilitation means to the
identification means;
validating the identity authenticated code as being that provided to the identified
5 user by the user identification means; and
facilitating the electronic transaction.

- 32 A method according to claim 31, wherein the identity authenticated code to the
user is sent via an different mode of communication;
- 10 33. A method of conducting an online transaction in accordance with any one of
claims 3 to 7, wherein the transaction manager deducts money from a user's
account to cover the money paid to the merchant.
- 15 34. A method of conducting an online transaction in accordance with claim 33,
wherein the transaction manager deducts money at the time of the request of the
unique transaction identifier.
- 20 35. A method of conducting an online transaction in accordance with claim 33,
wherein the transaction manager deducts money at the time of the transfer of
money to the merchant.
- 25 36. A method of conducting an online transaction in accordance with claim 33,
wherein the user's account is with a financial institution.
37. A method of conducting an online transaction in accordance with claim 33,
wherein the user's account is with the transaction manger.
- 30 38. A method of conducting an online transaction in accordance with any one of
claims 3 to 7, wherein the transaction manager issues a new account that
corresponds to an existing account with a financial institution, whereby the new

account details are used by the user and merchant in place of the existing account details.

- 5 39. A method of conducting an online transaction in accordance with claim 38, wherein the transaction manager uses the new account details to look up the existing account details and the existing account details are used by the transaction manager with the financial institution.
- 10 40. A method of conducting an online transaction in accordance with any one of claims 1 to 39, wherein the user requests the unique transaction identifier by an Internet connection.
- 15 41. A method of conducting an online transaction in accordance with claim 10, wherein the user's registration details are stored in a database of the transaction manager.
- 20 42. A method of conducting an online transaction in accordance with claim 41, wherein the user's request for the unique transaction identifier is validated by checking the user's details stored in the database of the transaction manager.
- 25 43. A method of conducting an online transaction in accordance with claim 15, wherein the merchant's registration details are stored in the database including a unique merchant identification.
- 30 44. A method of conducting an online transaction in accordance with claim 43, wherein when the merchant forwards the unique identification number to the transfer manager, and the merchant's unique identifier is sent to the transaction manager, wherein the merchant's identification is validated by the transaction manager before sending the transaction receipt number.
45. A method of conducting an online transaction in accordance with any one of

claims 35 to 37, wherein the transaction manager checks if sufficient funds are available to cover the transaction and the transaction number is only provided to the merchant if sufficient funds are available.

5 46. A method of conducting an online transaction in accordance with any one of claims 35 to 37, wherein the merchant links to the transaction manager by the Internet or a dedicated secure line to provide the unique identifier and receiving the transaction receipt number.

10 47 A transaction manager comprising:
 means for identifying a registered user to the transaction manager by a login process;
 means generating a unique identifier and sending the unique identifier to the identified user when a transaction request is made by the registered user;
15 means for recording an association of the unique identifier with the transaction;
 means for receiving the unique identifier from the registered user;
 means for validating the unique identifier; and
 means for allowing performance of the transaction in the event that the unique identifier is valid.

20