

167167

DESCRIPTION

METHOD OF CONDUCTING TRANSACTIONS OVER A NETWORK

Technical Field

The present invention relates to a method and system for authorizing a transaction between two parties over a network and, more particularly, to authorizing a transaction over the network when an authorization code has been received by an authorizing entity, the authorization code being produced by a fingerprint identification device in response to comparing a fingerprint of one of the parties to a stored fingerprint in the device.

Background Art

As the use of networks, for example the Internet, become more prevalent, an ever expanding quantum of electronic commerce will be conducted between users over these networks. Typically, a consumer of goods and/or services electronically connects to a provider of goods and/or services over a network, for example, by way of a website. Using known website browser software, the consumer may review and select goods or services and request that such goods or services be delivered to a specified address.

The provider of goods or services, of course, expects to be paid for any goods or services requested by the consumer. Typically, this is accomplished by asking the consumer to enter his or her credit card number and expiration date. Sometime thereafter, and most likely after the consumer has disconnected from the provider's website, the provider telephones an authorizing entity (e.g., the originator or managing entity) of the credit card and requests authorization to complete the transaction. In particular, the provider of goods and/or services transmits the credit card number, expiration date, consumer name, and purchase amount to the authorizing entity and awaits authorization. The authorizing entity accesses the consumer's credit card account and verifies that the consumer is in good standing and that the purchase amount will not cause the consumer's credit balance to exceed his or her credit limit. If the authorizing entity's review of the consumer's credit account is favorable, then authorization is transmitted to the provider of goods and/or services to complete the transaction with the consumer.

As the provider of goods and/or services never actually sees the consumer and cannot assess the consumer in terms of whether or not the consumer is attempting to fraudulently utilize the credit card, both the provider of goods and/or services and the



authorizing entity (originator of the credit card) must assume that the consumer is the authorized user of the credit card. It is only when the authorized user of a lost or stolen credit card calls the authorizing entity (or its representative) to report the lost and/or stolen card, that fraudulent uses of the credit card may be avoided.

Similar problems occur when goods and/or services are requested and confirmed by a user of the network simply by connecting with the provider's website. For example, when a provider of goods and/or services requires an initial registration with a particular consumer that authorizes billing the consumer for use of the website, accidental (or fraudulent) use of the website is likely by non-authorized users. More particularly, a parent (authorized user) may contract with a provider of goods and/or services to permit the authorized consumer to utilize the website. The terms of the contract (or registration) may be that the consumer's credit card will be charged for an amount representing use of the website by the authorized consumer (e.g., obtaining information from the website or purchasing goods). Unfortunately, the only way that the provider of goods and/or services knows that a user of the website is an authorized consumer is by way of an identification number (e.g., password etc.) given by the authorized consumer or automatically transmitted by the authorized consumer's personal computer. Thus, any user of the authorized consumer's personal computer who obtains the password (if employed) may access the website and incur charges without the knowledge of the authorized consumer.

Accordingly, there is a need in the art for a new method and system for facilitating and authorizing transactions between parties over a network which provides all parties to the transaction with confidence that the initiator of the transaction is authorized to enter into the transaction.

Summary Of The Invention

In order to overcome the disadvantages of the prior art, the present invention provides a method of conducting a commercial transaction between a customer and a provider of goods or services over a network. The method includes the steps of:

providing the customer with a fingerprint identification device which produces an authentication code when a fingerprint of the customer matches a stored fingerprint within the fingerprint identification device;

maintaining an electronic site on the network over which the customer may request goods or services from the provider of goods or services;

requesting that the customer provide authentication by activating the fingerprint identification device;

receiving at least the authentication code and a account number of the customer at the provider of goods or services over the network from the fingerprint identification device;

transmitting the authentication code and the account number from the provider of goods or services to a managing entity of the account over the network in encrypted form, and requesting authorization to complete the transaction; and

completing the transaction if the managing entity of the account provides the authorization.

Preferably, the stored fingerprint is in an encrypted format and at least one of the authentication code and account number are received over the network in an encrypted form.

The method of the present invention also contemplates permitting the customer to access the account. The steps according to this aspect of the invention include: establishing an electronic connection over the network between the customer and a managing entity of the account; requesting that the user provide authentication to the managing entity of the account by activating the fingerprint identification device; receiving at least the authentication code and the account number of the customer at the managing entity of the account over the network from the fingerprint identification device; and permitting access to the account if the authentication code is valid.

The customer is permitted to at least one of (i) transfer funds from the account; and (ii) deposit funds into the account, when the managing entity of the account has permitted access thereto.

According to another aspect of the invention, the customer is permitted access to an electronic safety deposit box. The steps according to this aspect of the invention further include establishing an electronic connection over the network between the customer and a managing entity of the electronic safety deposit box; requesting that the customer provide authentication to the managing entity of the electronic safety deposit box by activating the

fingerprint identification device; receiving at least the authentication code at the managing entity of the electronic safety deposit box over the network from the fingerprint identification device; and permitting access to the electronic safety deposit box if at least the authentication code is valid.

According to yet another aspect of the invention, the customer is permitted to conduct an investment transaction over the network. The steps according to this aspect of the invention include: establishing an electronic connection over the network between the customer and a settlement bank over which the investor may provide investment instructions; requesting that the customer provide authentication to the settlement bank by activating the fingerprint identification device; receiving at least the authentication code at the settlement bank over the network from the fingerprint identification device; receiving investment instructions at the settlement bank over the network from the customer; and transmitting the investment instructions to a third party if at least the authentication code is valid.

Other objects, features, and advantages will become apparent to those skilled in the art in light of the description herein taken in conjunction with the accompanying drawing.

Brief Description of the Drawings

For the purposes of illustrating the invention, there are shown in the drawings forms which are presented preferred, it being understood, however, that the invention is not limited to the precise arrangements and instrumentalities shown.

FIG. 1 is a block diagram illustrating a preferred system for carrying out the invention.

FIG. 2 is a schematic diagram of a fingerprint identification device which is connectable to a computer in accordance with the present invention.

FIG. 3 is a flow diagram illustrating process steps for authorizing a transaction between a consumer and a provider of goods and/or services over a network in accordance with one aspect of the invention.

FIG. 4 is a flow diagram illustrating a settlement sequence following the transaction process of FIG. 3.

FIG. 5 is a flow diagram illustrating process steps for facilitating an investment transaction over a network in accordance with another aspect of the present invention.

FIG. 6 is a flow diagram illustrating process steps for facilitating access to an electronic account, such as an electronic safety deposit box, in accordance with another aspect of the present invention.

Best Mode of Carrying Out Invention

Reference is now made to FIG. 1 which illustrates a block diagram of a system suitable for carrying out the present invention. The system preferably includes a bank 10, such as a payor bank, settlement bank, originating bank, etc. The payor bank 10 preferably includes a processing unit 22 (such as a central computer, distributed computer, networked computer, etc.) in communication with one or more interface units 20 (for example, network interfaces, wireless interfaces, network servers, etc.). The processing unit 22 is also in communication with a plurality of back office and/or electronic functional units, including, for example, one or more electronic safety deposit boxes 24, bank accounts 26, settlement credit/debit accounts 28, lease accounts 30, and finance accounts 32. Each of the functional units preferably includes one or more databases containing information concerning the accounts thereof and the customers utilizing them.

Preferably, the payor bank 10 issues a plurality of fingerprint identification devices 50 to a plurality of customers 52. The fingerprint identification devices 50 may take any of an number of forms, e.g., a card, a smart card, a cellular phone, and a universal serial bus stick. It is preferred that each fingerprint identification device 50 is associated with one or more of the functional accounts of the payor bank 10. For example, the payor bank 10 may issue a fingerprint identification device 50 to a customer 52 which is associated with a bank account 26. That customer 52 may be issued another fingerprint identification device 50 associated with an electronic safety deposit box 24. It is understood, however, that the payor bank 10 may issue a single fingerprint identification device 50 which is associated with both the bank account 26 and electronic safety deposit box 24 (and any other functional account) without departing from the scope of the invention.

With reference to FIG. 2, the fingerprint identification device 50 is preferably in the form of a card or thin box which contains information about the owner of the device,

the payor bank, the functional account number, etc. The fingerprint identification device 50 includes a microprocessor, memory, and fingerprint sensor 51 which are interconnected and programmed in order to compare a fingerprint of the customer 52 with a stored fingerprint of that customer 52. The card issues an authorization code only when the fingerprint of the customer 52 matches the stored fingerprint. Those skilled in the art will appreciate that any of the known hardware suitable to implement the fingerprint identification device 50 may be employed.

It is most preferred that the stored fingerprint and other information regarding the customer 52 are in encrypted form (e.g., using known PKI Technology) and that this encrypted information remain encrypted when transmitted from the device 50 to any other device. It is preferred that the fingerprint identification device 50 is connectable to a computer 54 (such as a PC) through an interface 56. The fingerprint identification device 50 may include a connector 57 which is matable with a corresponding connector 58 on the interface 56. The interface 56 preferably receives information from the fingerprint identification device 50 through the connectors 57, 58 and transfers at least some of this information to the PC 54 by way of the universal serial bus (USB) interface.

Alternatively, the device 50 may include an integral interface for connecting to the computer 54 by way of the universal serial bus (USB). Thus, the information on the fingerprint identification device 50 may be transmitted over a network (e.g., the Internet) from the computer 54, preferably in encrypted form (e.g., using API data transfer, PKS 11).

Most preferably, the fingerprint identification device 50 is a small, stand alone unit (e.g., measuring about 8.5 cm x 5.4 cm x 0.9 cm and weighting about 35 grams). It is most preferred that the fingerprint sensor 51 include a matrix of pixels formed in a semiconductor chip, a 128 x 192 matrix of pixels being preferred. Any of the known fingerprint matching algorithms may be employed, such as pattern matching. See, for example, U.S. Patent No. 4,582,985, entitled DATA CARRIER, the entire disclosure of which is hereby incorporated by reference.

In an alternative embodiment, the fingerprint identification device may be integral with the interface 56 or the interface 56 may contain separate fingerprint identification circuitry (including sensor 51) such that the device 50 is not required to execute fingerprint recognition and matching. In another alternative embodiment of the invention, the computer 54 may contain fingerprint identification circuitry (including sensor 51) integrally disposed therein such that neither the device 50 nor the interface 56 is required to execute fingerprint recognition and matching.

Referring to FIG. 1, any of the customers 52 may conduct transactions with one or more providers of goods and/or services, such as on-line brokerages 60, on-line goods providers 62, on-line services service providers 64, on-line investment account providers 66, providers of large capital purchases 68, brick and mortar merchants 70 or brick and mortar service providers 72.

Reference is now made to FIG. 3 which is a flow diagram illustrating process steps which are preferably carried out in accordance with the invention. In particular, the process steps illustrated in FIG. 3 relate to a commercial transaction conducted over a network (such as the Internet) between a customer 52 and an on-line provider of goods and/or services, such as the on-line brokerage 60, the on-line goods provider 62, or the on-line services provider 64.

At action 100, the customer 52 connects to the on-line provider of goods and/or services 60, 62 or 64 by way of the network in a manner well known to those skilled in the art. For example, the customer 52 may utilize a personal computer (PC) 54 (FIG. 2) to execute a browser program operable to electronically connect to a website of the provider of goods and/or services. Using the browser program, the customer 52 may view the goods and/or services available from the provider 60, 62 or 64 and select particular goods or services for one or more transactions (action 102).

At action 104, the provider of goods and/or services prompts the customer 52 to authenticate himself or herself as being authorized to use a particular mode for making remittance, for example, debiting a demand deposit account (DDA), debiting a credit card account, etc. In particular, the provider of goods and/or services prompts the customer 52 to authenticate himself by activating the fingerprint identification device 50.

At action 106, the customer 52 activates the fingerprint identification device 50 in a manner consistent with known techniques such that the fingerprint identification device compares the customer's fingerprint with a stored fingerprint (action 108) and produces an authorization code indicating that a match exists between the customer's fingerprint and the stored fingerprint. At action 110, the customer 52 inserts the fingerprint identification device 50 into an interface device 56 (FIG. 2). The customer 52 may alternatively authenticate himself by activating fingerprint identification circuitry in the interface 56 or in the computer 54. Whichever technique is employed, the customer 52 preferably uses the personal computer 54 to access the Internet. Data transfer is then conducted between the fingerprint identification device 50 (or other fingerprint identification circuitry if employed) and the provider of goods and/or services 60, 62 or 64 (action 112). The data transfer preferably includes at least one of the authentication code, payor bank identification number, customer account number, and delivery address. Most preferably, the data of this transfer are in encrypted form.

At action 114, if the customer 52 fails to transfer the authentication code to the provider of goods and/or services 60, 62 or 64, then it is preferred that the provider of goods and/or services rejects the transaction and again requests that the customer authenticate himself (action 104). When at least the authentication code is received by the provider of goods and/or services 60, 62 or 64, then the processing of the transaction is permitted to continue.

At action 116, the provider of good and/or services 60, 62 or 64 preferably transfers data to the payor bank 10, which data preferably includes at least one of the authentication code, payor bank identification number, customer account number, and purchase amount. It is most preferred that at least the authentication code be provided to the payor bank 10. The payor bank 10 then analyzes at least one of the payor bank identification number (action 118), the customer account number (action 120), the purchase amount (action 122) and the authorization code (124) to determine whether one or all of the data are valid. Most preferably, the payor bank 10 analyzes the authentication code (action 124) to verify its validity prior to authorizing the transaction. As illustrated, the queries at actions 118, 120, 122, and 124 are linked serially through the affirmative ("Y") branch of each. It is noted, however, that the queries of actions 118, 120, 122, and 124 may be linked in parallel without

departing from the scope of the invention. It is intended that an affirmative determination at one or more of the queries of actions 118, 120, 122 and 124 tends to advance the process flow toward action 128. If, however, any one or more of the data are not valid and the queries at one or more of actions 118, 120, 122 and 124 are negative ("N"), then the payor bank 10 preferably establishes a negative authorization condition (action 126).

At action 128, the payor bank 10 preferably transmits the authorization condition to the provider of goods and/or services and the provider of goods and/or services determines whether the authorization condition is positive or negative (action 130). When the authorization condition is negative, the provider of goods and/or services refuses to complete the transaction (action 132). Conversely, when the authorization condition is positive, the provider of goods and/or services completes the transaction (action 134).

Those skilled in the art will appreciate that commercial transactions conducted at the point of sale, for example, at brick and mortar stores, 70, 72, may be carried out in accordance with the invention using the steps illustrated in FIG. 3 with the exception of those concerning the transmission of data from the customer 52 to the provider 60, 62 or 64 over the network. Instead, the data (e.g., at least one of the authentication code, payor bank identification number, customer account number, delivery address, etc.) would be provided to, for example, the merchant 70 and/or service provider 72 at the point of sale (action 112).

With reference to FIG. 4, once the commercial transaction has been completed (FIG. 3), the transaction is settled (action 150). Initially, a determination is made as to whether the provider of goods and/or services 70, 72 utilizes the payor bank 10 in settling its transactions (action 152). If it does, a transaction receipt is transmitted from the provider of goods and/or services 70, 72 to the payor bank 10. If not, then the provider of goods and/or services 70, 72 may settle the transaction through its own bank (e.g., a merchant bank 74) by transmitting the transaction receipt to that bank (action 156). The provider's bank would then transmit the transaction receipt to the payor bank 10 (action 154).

At action 158, the payor bank 10 debits the customer's account and at action 160, a determination is again made as to whether the provider of goods and/or services 70, 72 utilizes the same payor bank 10 as the customer 52. If it does, the payor bank 10 directly credits the bank account of the provider of goods and/or services (action 162). If not, the payor bank 10 transmits a credit to the bank of the provider of goods and/or services (action 164) and that bank credits the provider's bank account (action 166).

Reference is now made to FIG. 5 which is a flow diagram illustrating process steps in accordance with another aspect of the present invention. In particular, the process steps represent actions to be taken to facilitate an investment transaction between a customer 52 and an on-line investment service provider 66 (FIG. 1). In accordance with the invention,

the on-line investment provider 66 may be an investment bank, a brokerage, etc., and may be located domestically or off-shore. Preferably, the investment transaction is conducted through the settlement bank 10 (the term settlement being used to indicate that the customer's

bank account within the settlement bank 10 may be debited or credited depending on the investment transaction).

At action 200, the customer 52 preferably accesses the settlement bank 10 via a network, such as the Internet, using any of the known techniques. After the customer 52 has indicated that he or she is interested in conducting an investment transaction, the settlement bank 10 prompts the customer 52 to authenticate himself or herself (action 202). In response, the customer 52 preferably activates the fingerprint identification device 50 (action 204) which causes the device to compare the customer's fingerprint with a stored fingerprint (action 206) and produce an authentication code if a match is obtained.

At action 208, the customer preferably inserts the fingerprint identification device 50 into an interface 56 (FIG. 2) suitable for transmitting data between the fingerprint identification device 50 and the settlement bank 10, for example, via the universal serial bus of the computer 54. Alternatively, the customer 52 may authenticate himself or herself by activating fingerprint identification circuitry in the interface 56 or in the computer 54. Whichever technique is employed, the customer 52 preferably uses the computer 54 to access the Internet. At action 210, data is preferably transmitted from the fingerprint identification device 50 (or other fingerprint identification circuit if employed) to the settlement bank 10, the data including at least one of the authentication code and the customer investment account number (in encrypted form).

At action 212, if the settlement bank 10 receives the authentication code (and, if required, the investment account number), then the investment transaction is permitted to continue. If not, then the process flows back to action 202 where the customer 52 is again prompted to authenticate himself or herself.

At action 214, the customer 52 preferably provides investment instructions to the settlement bank 10 over the network, such as "buy 100 shares of xyz corporation" and, at action 216, the settlement bank 10 transmits the instructions to the on-line investment provider 66 (e.g., an investment bank). It is noted that the investment instructions may be transmitted to the on-line investment provider 66 in a way which maintains the customer's anonymity. Indeed, the customer's name, account number, etc., need not be transmitted to the investment provider 66. The customer 52, however, may instruct the settlement bank 10 as to whether or not he or she wishes to maintain such anonymity.

At action 218, the on-line investment provider 66 executes the investment instructions and does not require authorization because, by previous agreement, the receipt of investment instructions from the settlement bank 10 itself is authorization enough. At action 220, a transaction receipt is transmitted to the settlement bank 10 indicating whether remittance is required or payment is being made. At action 224, the settlement bank 10 credits or debits the customer's investment account in accordance with the transaction receipt and, at action 226, the settlement bank 10 debits and/or credits the on-line investment provider's 66 account.

Reference is now made to FIG. 6 which is a flow diagram illustrating process steps in accordance with yet another aspect of the present invention. In particular, the process steps represent actions to be taken to facilitate access an electronic account within the payor bank 10. Preferably, the electronic bank account is an electronic safety deposit box 24, it being understood that any of the functional accounts (e.g., bank deposit account 26, credit/debit account 28, lease account 30, finance account 32, etc.) may be accessed in a similar way. At action 300, the customer 52 preferably accesses the payor bank 10 via the network using any of the known techniques. After the customer 52 has indicated that he or she is interested in accessing an electronic account (such as an electronic safety deposit box 24), the payor bank 10 then prompts the customer 52 to authenticate himself or herself (action 302). In response, the customer 52 preferably activates the fingerprint identification device 50 (action 304) which causes the device to compare the customer's fingerprint with a stored fingerprint (action 306) and produce an authentication code if a match is obtained.

At action 308, the customer preferably inserts the fingerprint identification device 50 into an interface 56 (FIG. 2) suitable for transmitting data between the fingerprint identification device 50 and the payor bank 10, for example, via the universal serial bus of the computer 54. Alternatively, the customer 52 may authenticate himself or herself by activating fingerprint identification circuitry in the interface 56 or in the computer 54. Whichever technique is employed, the customer 52 preferably uses the computer 54 to access the Internet. At action 310, data is preferably transmitted from the fingerprint identification device 50 (or other fingerprint identification device if employed) to the payor bank 10 (in encrypted form), the data including at least one of the authentication code and the number of the electronic account.

At action 312, if the payor bank 10 receives the authentication code (and, if required, the account number), then the access process continues. If not, the process flows back to action 302 where the customer 52 is again prompted to authenticate himself or herself. At action 314, the customer 52 may again request access to the electronic account, e.g., the electronic safety deposit box 24, and, at action 316, the payor bank 10 grants the customer's request and permits the customer 52 to manipulate, receive, and/or transmit electronic file(s) to the account. Those skilled in the art will appreciate that the files contained in an electronic safety deposit box 24 may include will(s), codicil(s), title to securities or other property, contract(s), certificate(s), insurance policies, etc. These files are represented by the "database" shown in the electronic safety deposit box 24 shown in FIG. 1.

Advantageously, the method and system of the present invention readily provides for authorizing transactions over a network in which all parties to the transaction maintain confidence that the initiator (e.g., the customer) of the transaction is authorized to enter into the transaction. The transactions are not limited to commercial transactions for goods/services, but may include investment transactions, and access to electronic bank accounts, such as electronic safety deposit boxes 24, bank deposit accounts 26, settlement credit/debit accounts 28, etc.

Although the invention herein has been described with reference to particular embodiments, it is to be understood that these embodiments are merely illustrative of the principles and applications of the present invention. It is therefore to be understood that numerous modifications may be made to the illustrative embodiments and that other arrangements may be devised without departing from the spirit and scope of the present invention as defined by the appended claims.

Industrial Applicability

The present invention is useful in a wide range of industrial applications, such as in electronic commerce.

Claims:

1. A method of authorizing a commercial transaction between a customer and a provider of goods or services over a network, wherein the provider of goods or services requests that the customer provide authentication by activating a fingerprint identification device, and the provider of goods or services receives at least an authentication code of the customer over the network from the fingerprint identification device, the method comprising the steps of:

providing the customer with the fingerprint identification device which produces the authentication code when a fingerprint of the customer matches a stored fingerprint within the fingerprint identification device;

receiving at least the authentication code from the provider of goods or services over the network; and

authorizing the transaction if at least the authentication code is valid.

2. The method of claim 1, wherein the stored fingerprint is in an encrypted format.

3. The method of claim 1, wherein the provider of goods or services receives at least an authentication code and an account number of the customer over the network from the fingerprint identification device and the step of receiving at least the authentication code from the provider of goods or services over the network includes receiving an account number of the customer over the network from the fingerprint identification device.

4. The method of claim 3, wherein at least one of the authentication code and account number are received over the network in an encrypted form.

5. The method of claim 1, wherein the network is at least part of the Internet.

6. The method of claim 3, further providing a method of permitting the customer to access the account, comprising the steps of:

establishing an electronic connection over the network between the customer and a managing entity of the account;

requesting that the user provide authentication to the managing entity of the account by activating the fingerprint identification device;

receiving at least the authentication code and the account number of the customer at the managing entity of the account over the network from the fingerprint identification device; and

permitting access to the account if the authentication code is valid.

7. The method of claim 6, wherein the customer is permitted to at least one of (i) transfer funds from the account; and (ii) deposit funds into the account, when the managing entity of the account has permitted access thereto.

8. The method of claim 1, further providing a method of permitting the customer to access an electronic safety deposit box, comprising the steps of:

establishing an electronic connection over the network between the customer and a managing entity of the electronic safety deposit box;

requesting that the customer provide authentication to the managing entity of the electronic safety deposit box by activating the fingerprint identification device;

receiving at least the authentication code at the managing entity of the electronic safety deposit box over the network from the fingerprint identification device; and

permitting access to the electronic safely deposit box if at least the authentication code is valid

9. The method of claim 8, further comprising the step of receiving at least the authentication code and an electronic safety deposit box account number of the customer at the managing entity of the electronic safety deposit box over the network from the fingerprint identification device.

10. The method of claim 8, wherein the electronic safety deposit box is operable to contain at least one of a will, a title to one or more securities, a title to real or personal property, a contract, a certificate, and an insurance policy.

11. The method of claim 1, further providing a method of permitting the customer to conduct an investment transaction over the network, the method comprising the steps of:

establishing an electronic connection over the network between the customer and a settlement bank over which the customer may provide investment instructions;

requesting that the customer provide authentication to the settlement bank by activating the fingerprint identification device;

receiving at least the authentication code at the settlement bank over the network from the fingerprint identification device;

receiving investment instructions at the settlement bank over the network from the customer; and

transmitting the investment instructions to a third party if at least the authentication code is valid.

12. The method of claim 11, further comprising the step of receiving at least the authentication code and an investment account number of the customer at the settlement bank over the network from the fingerprint identification device.

13. The method of claim 11, further comprising the steps of: receiving an instruction from the customer as to whether it wishes to keep its identity anonymous; and transmitting the investment instructions to the third party without identifying the customer if the customer so wishes.

14. The method of claim 11, wherein the third party is at least one of an investment bank, a brokerage, and an off-shore bank.

15. The method of claim 12, further comprising the steps of:

receiving a transaction record from the third party indicating that the investment instructions were carried out; and

settling with the third party by at least one of (i) transferring funds from the customer's investment account to the third party; and (ii) transferring funds into the customer's investment account from the third party.

16. The method of claim 1, wherein the fingerprint identification device is in the form of a card.

17. The method of claim 1, wherein the fingerprint identification device is in the form of a cellular telephone.

18. The method of claim 1, wherein the fingerprint identification device is in the form of a universal serial bus stick.

19. The method of claim 1, wherein the fingerprint identification device is integral with at least one of a computer and an interface device operable to connect to the computer.

20. A method of conducting a commercial transaction between a customer and a provider of goods or services over a network, the method comprising the steps of:

providing the customer with a fingerprint identification device which produces an authentication code when a fingerprint of the customer matches a stored fingerprint within the fingerprint identification device;

maintaining an electronic site on the network over which the customer may request goods or services from the provider of goods or services;

requesting that the customer provide authentication by activating the fingerprint identification device;

receiving at least the authentication code and a account number of the customer at the provider of goods or services over the network from the fingerprint identification device;

transmitting the authentication code and the account number from the provider of goods or services to a managing entity of the account over the network in encrypted form, and requesting authorization to complete the transaction; and

completing the transaction if the managing entity of the account provides the authorization.

21. A method of accessing an electronic safety deposit box over a network, the method comprising the steps of:

providing a user with a fingerprint identification device which produces an authentication code when a fingerprint of the user matches a stored fingerprint within the fingerprint identification device;

establishing an electronic connection over the network between the user and a managing entity of the electronic safety deposit box;

requesting that the user provide authentication to the managing entity of the electronic safety deposit box by activating the fingerprint identification device;

receiving at least the authentication code at the holder of the electronic safety deposit box over the network from the fingerprint identification device; and

permitting access to the electronic safely deposit box if the authentication code is valid.

22. The method of claim 21, wherein the stored fingerprint is in an encrypted format.

23. The method of claim 21, further comprising the step of receiving at least the authentication code and an electronic safety deposit box account number of the user at the managing entity of the electronic safety deposit box over the network from the fingerprint identification device.

24. The method of claim 23, wherein at least one of the authentication code and account number are received over the network in an encrypted form.

25. The method of claim 21, wherein the electronic safety deposit box is operable to contain at least one of a will, a title to one or more securities, a title to real or personal property, a contract, a certificate, and an insurance policy.

26. A method of conducting an investment transaction over a network, the method comprising the steps of:

providing an investor with a fingerprint identification device which produces an authentication code when a fingerprint of the investor matches a stored fingerprint within the fingerprint identification device;

establishing an electronic connection over the network between the investor and a settlement bank over which the investor may provide investment instructions;

requesting that the investor provide authentication to the settlement bank by activating the fingerprint identification device;

receiving at least the authentication code at the settlement bank over the network from the fingerprint identification device;

receiving investment instructions at the settlement bank over the network from the investor; and

transmitting the investment instructions to a third party if at least the authentication code is valid.

27. The method of claim 26, wherein the stored fingerprint is in an encrypted format.

28. The method of claim 26, further comprising the steps of receiving at least the authentication code and an account number of the investor at the settlement bank over the network from the fingerprint identification device.

29. The method of claim 28, wherein at least one of the authentication code and account number are received over the network in an encrypted form.

30. The method of claim 26, further comprising the steps of: receiving an instruction from the investor as to whether it wishes to keep its identity anonymous; and transmitting the investment instructions to the third party without identifying the investor if the investor so wishes.

31. The method of claim 26, wherein the third party is at least one of an investment bank, a brokerage, and an off shore bank.

32. The method of claim 28, further comprising the steps of:

receiving a transaction record from the third party indicating that the investment instructions were carried out; and

settling with the third party by at least one of (i) transferring funds from the investor's account to the third party; and (ii) transferring funds into the investor's account from the third party.

33. An apparatus for authorizing a commercial transaction between a customer and a provider of goods or services over a network, the apparatus comprising:

a fingerprint identification device capable of being in the possession of the customer and being operable to produce an authentication code when the fingerprint of the customer matches a stored fingerprint, the fingerprint identification device being connectable to the network such that the provider of goods or services may receive at least the authentication code over the network; and

a processing unit operable to (i) receive at least the authentication code from the provider of goods or services over the network, and (ii) authorize the transaction if at least the authentication code is valid.

34. The apparatus of claim 33, wherein the stored fingerprint is in an encrypted format.

35. The method of claim 33, wherein the fingerprint identification device is operable to provide at least the authentication code and an account number of the customer over the network to the provider of goods or services.

36. The apparatus of claim 35, wherein at least one of the authentication code and account number are in an encrypted form.

37. The apparatus of claim 33, wherein the network is at least part of the Internet.

38. The apparatus of claim 35, wherein the processing unit is operable to permit the customer to access the account, the processing unit comprising:

a network server operable to (i) establish an electronic connection over the network with the customer; (ii) request that the user provide authentication by activating the fingerprint identification device; (iii) receive at least the authentication code and the account number of the customer over the network from the fingerprint identification device; and (iv) permit access to the account if the authentication code is valid.

39. The apparatus of claim 38, wherein the processing unit is further operable to permit the customer to at least one of (i) transfer funds from the account; and (ii) deposit funds into the account, when access is permitted.

40. The apparatus of claim 33, wherein the processing unit is operable to permit the customer to access an electronic safety deposit box, the processing unit comprising:

a network server operable to (i) establish an electronic connection over the network with the customer; (ii) request that the customer provide authentication by activating the fingerprint identification device; (iii) receive at least the authentication code over the network from the fingerprint identification device; and (iv) permit access to the electronic safety deposit box if at least the authentication code is valid.

41. The apparatus of claim 40, wherein the processing unit is further operable to receive at least the authentication code and an electronic safety deposit box account number of the customer over the network from the fingerprint identification device.

42. The method of claim 40, wherein the electronic safety deposit box is operable to contain at least one of a will, a title to one or more securities, a title to real or personal property, a contract, a certificate, and an insurance policy.

43. The apparatus of claim 33, wherein the processing unit is operable to permit the customer to conduct an investment transaction over the network, the processing unit comprising:

a network server operable to (i) establish an electronic connection over the network with the customer over which the customer may provide investment instructions; (ii) request that the customer provide authentication by activating the fingerprint identification device; (iii) receive at least the authentication code over the network from the fingerprint identification device; (iv) receive investment instructions at the settlement bank over the network from the customer; and (v) transmit the investment instructions to a third party if at least the authentication code is valid.

44. The apparatus of claim 43, wherein the processing unit is further operable to receive at least the authentication code and an investment account number of the customer over the network from the fingerprint identification device.

45. The apparatus of claim 43, wherein the processing unit is further operable to (i) receive an instruction from the customer as to whether it wishes to keep its identity anonymous; and (ii) transmit the investment instructions to the third party without identifying the customer if the customer so wishes.

46. The apparatus of claim 43, wherein the third party is at least one of an investment bank, a brokerage, and an off-shore bank.

47. The apparatus of claim 44, wherein the processing unit is operable to (i) receive a transaction record from the third party indicating that the investment instructions were carried out; and (ii) settle with the third party by at least one of (i) transferring funds from the customer's investment account to the third party; and (ii) transferring funds into the customer's investment account from the third party.

48. The apparatus of claim 33, wherein the fingerprint identification device is in the form of a card.

49. The apparatus of claim 33, wherein the fingerprint identification device is in the form of a cellular telephone.

50. The apparatus of claim 33, wherein the fingerprint identification device is in the form of a universal serial bus stick.