US 20130332364A1

(19) United States

(12) Patent Application Publication

(10) Pub. No.: US 2013/0332364 A1

(43) Pub. Date: Dec. 12, 2013

Templeton et al.

(54) **AUTHORIZING USE OF A FINANCIAL INSTRUMENT**

(71) Applicants: **James Templeton**, San Jose, CA (US); **Sanjay Bhargava**, San Carlos, CA (US)

(72) Inventors: **James Templeton**, San Jose, CA (US); **Sanjay Bhargava**, San Carlos, CA (US)

(73) Assignee: **PayPal Inc.**, San Jose, CA (US)

(21) Appl. No.: **13/965,017**

(22) Filed: **Aug. 12, 2013**

Related U.S. Application Data

(63) Continuation of application No. 13/291,398, filed on Nov. 8, 2011, now Pat. No. 8,515,871, which is a continuation of application No. 12/198,575, filed on Aug. 26, 2008, now Pat. No. 8,296,204, which is a continuation of application No. 09/901,594, filed on Jul. 11, 2001, now Pat. No. 6,461,110.

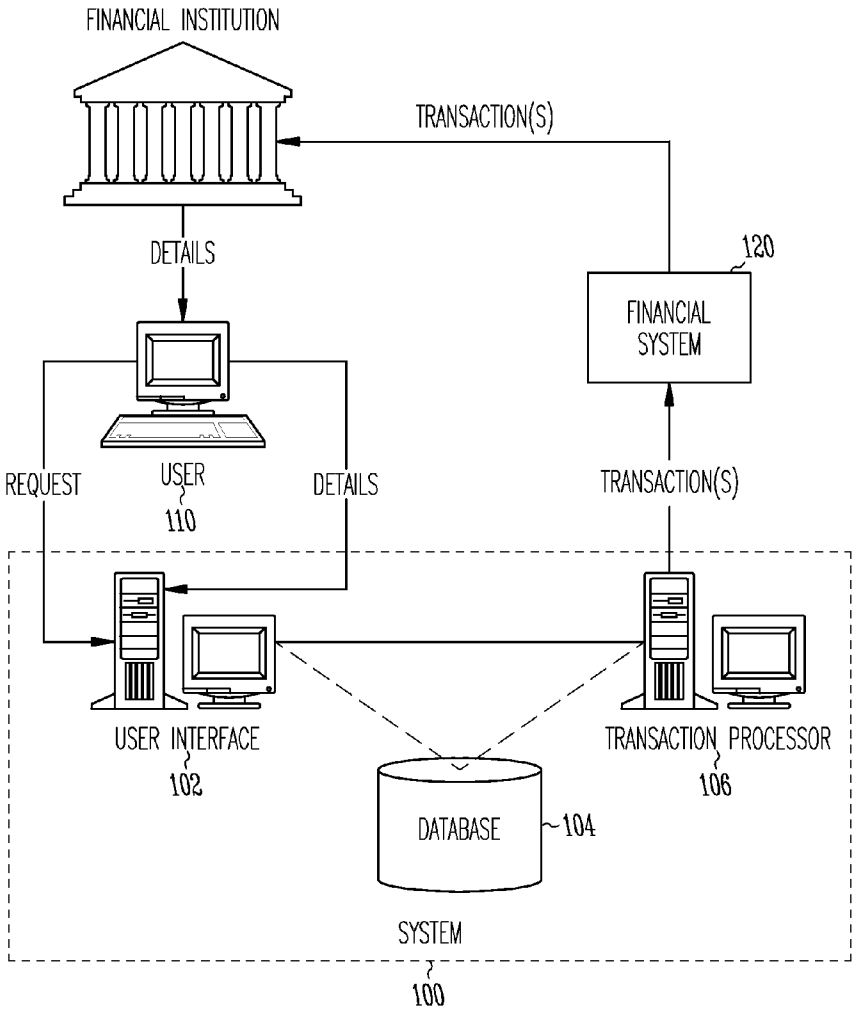
Publication Classification

(51) **Int. Cl.**
G06Q 20/40 (2006.01)

(52) **U.S. Cl.**
CPC *G06Q 20/4016* (2013.01)
USPC **705/44**

(57) **ABSTRACT**

Computer-implemented method and system are provided for verifying a financial instrument. The method comprises receiving, via a user interface, a request to use a financial instrument. A transaction processor initiates at least one transaction having a variable detail, using the financial instrument, and saves the variable detail. A requested detail relating to the at least one transaction is received via the user interface and the transaction processor compares the stored detail with the requested detail. The transaction processor authorizes the use of the financial instrument in response to receiving the correct input that matches the saved variable detail.



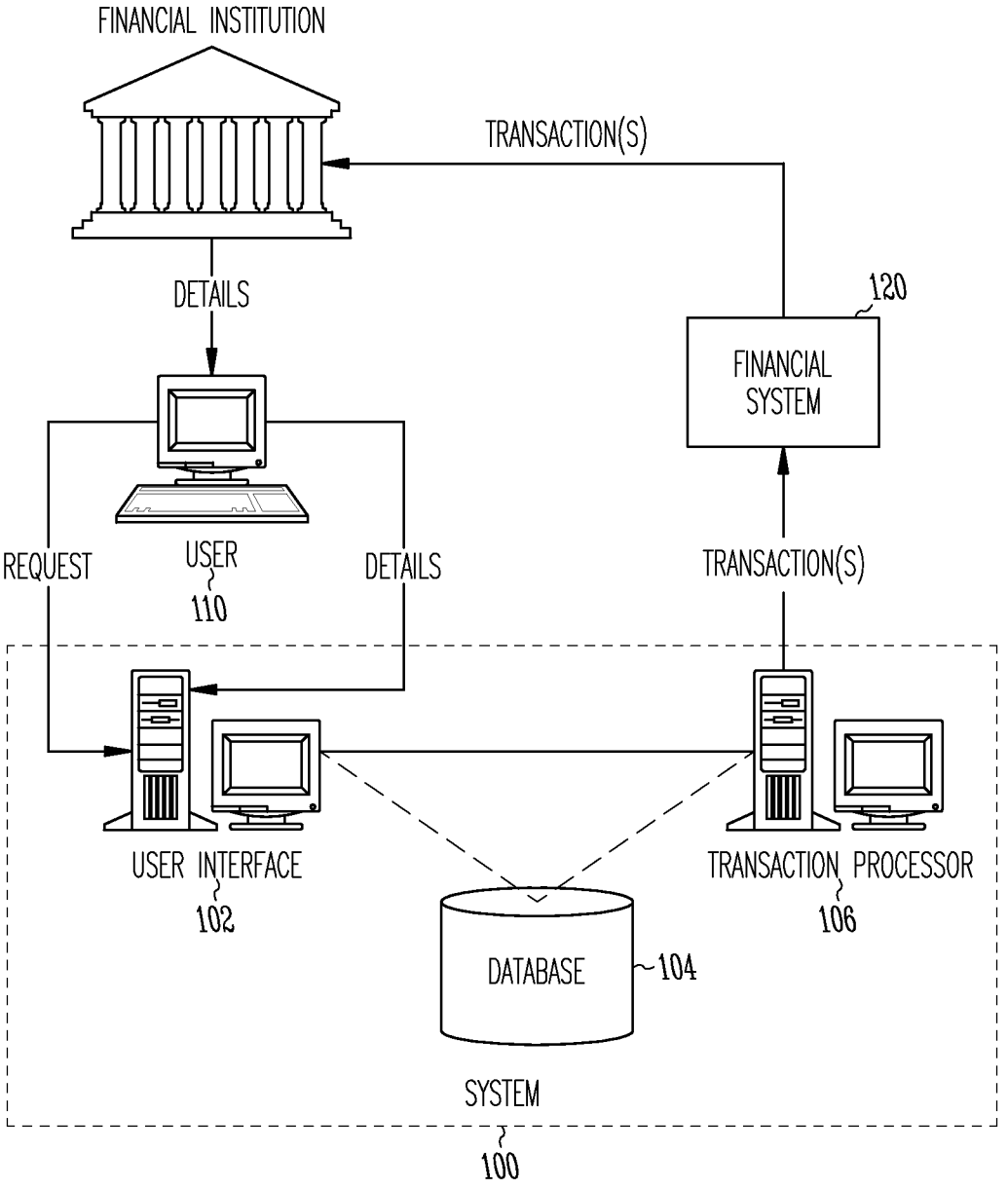

FINANCIAL INSTITUTION
TRANSACTION(S)
DETAILS
120
FINANCIAL SYSTEM
REQUEST
USER
110
DETAILS
TRANSACTION(S)
USER INTERFACE
102
DATABASE
104
TRANSACTION PROCESSOR
106
SYSTEM
100

FIG. 1

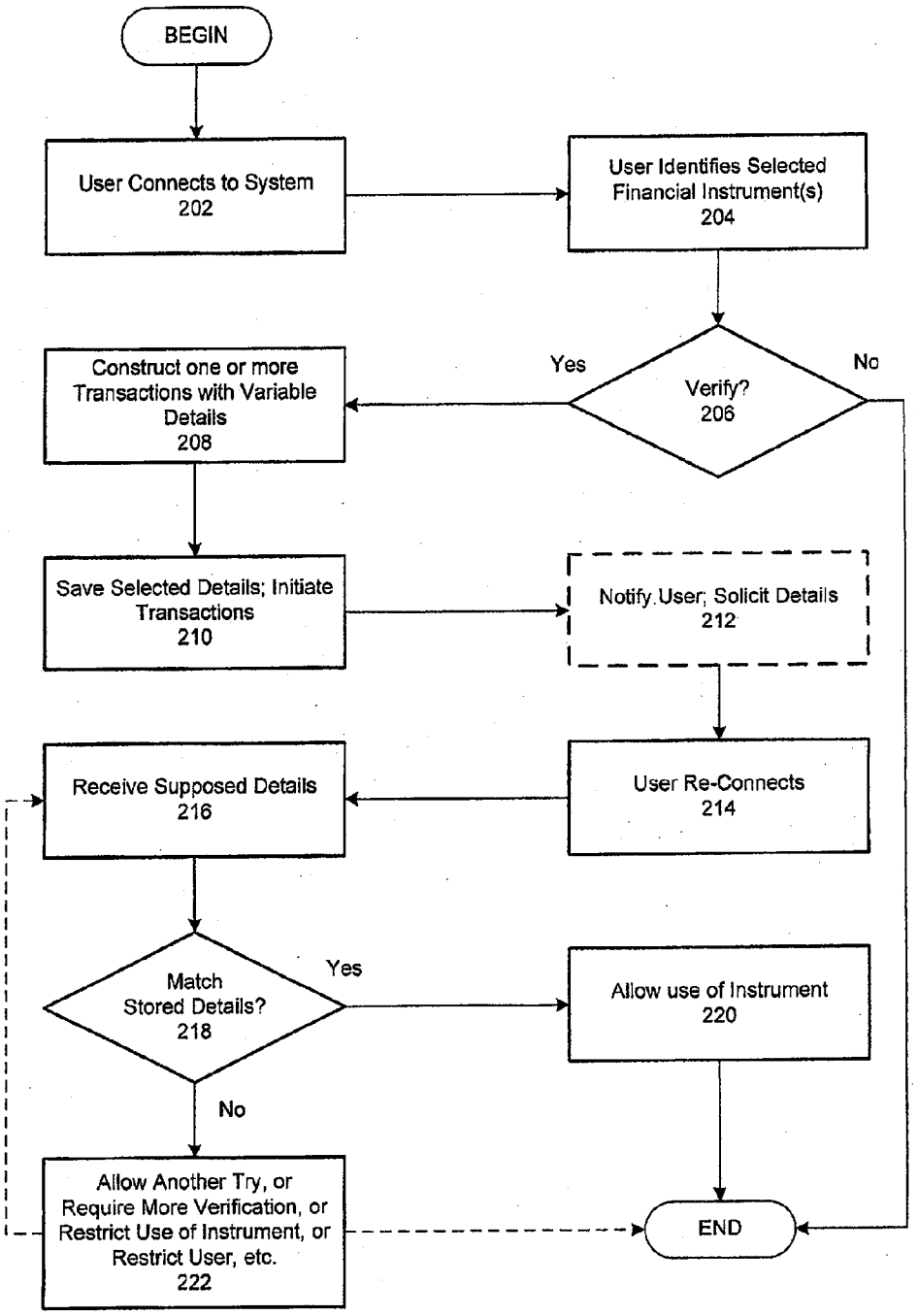

BEGIN
User Connects to System
202
User Identifies Selected Financial Instrument(s)
204
Verify?
206
Yes
No
Construct one or more Transactions with Variable Details
208
Save Selected Details; Initiate Transactions
210
Notify User; Solicit Details
212
User Re-Connects
214
Receive Supposed Details
216
Match Stored Details?
218
Yes
No
Allow use of Instrument
220
Allow Another Try, or Require More Verification, or Restrict Use of Instrument, or Restrict User, etc.
222
END

FIG. 2

AUTHORIZING USE OF A FINANCIAL INSTRUMENT

RELATED APPLICATIONS

[0001] This patent application is a Continuation of U.S. patent application Ser. No. 13/291,398, filed Nov. 8, 2011, which is a Continuation of U.S. patent application Ser. No. 12/198,575 filed Aug. 26, 2008, which is a Continuation of U.S. patent application Ser. No. 09/901,594, filed Jul. 10, 2001 ("SYSTEM AND METHOD FOR VERIFYING A FINANCIAL INSTRUMENT"), which claims the benefit of the filing date of U.S. Provisional Application Ser. No. 60/217,202, filed Jul. 10, 2000 ("RANDOM ACCOUNT ACTIVITY TO VERIFY A CREDIT CARD"), the contents of which are incorporated by reference herein in their entirety.

BACKGROUND

[0002] This invention relates to the fields of computer systems and data communications. More particularly, a system and method are provided for verifying financial instruments or accounts, such as credit cards, debit cards, bank accounts, etc.

[0003] Modern financial systems make it easy to perform financial transactions without using physical currency. For example, credit cards and ACH (Automated Clearing House) transactions (i.e., electronic checks) are increasingly used in place of cash to make purchases, transfer money, or engage in other financial transactions.

[0004] These convenient instruments are, however, subject to theft and fraudulent use. A thief may obtain all the information needed to use a stolen credit card from the card itself, while all that is needed to conduct an ACH transaction (e.g., to withdraw money from a checking account) are the bank account and routing numbers from a check. It is then a simple matter for the thief or fraud artist to pose as the rightful owner or holder of a credit card or bank account. Existing safeguards against fraud (e.g., checking a credit card against a list of stolen cards, checking the name on a checking account before completing an ACH transaction) are often insufficient. It is typically the merchant, vendor, bank or other entity that accepts a credit card or electronic check transaction that is liable for the amount of money that is stolen or misappropriated if the rightful owner or holder is not at fault.

DESCRIPTION OF THE FIGURES

[0005] FIG. **1** is a block diagram of a system for verifying a potential user's authorization to use a financial instrument, in accordance with an embodiment of the present invention.

[0006] FIG. **2** is a flowchart illustrating one method of verifying a person's authorization to use a financial instrument, in accordance with an embodiment of the invention.

DETAILED DESCRIPTION

[0007] The following description is presented to enable any person skilled in the art to make and use the invention, and is provided in the context of particular applications of the invention and their requirements. Various modifications to the disclosed embodiments will be readily apparent to those skilled in the art and the general principles defined herein may be applied to other embodiments and applications without departing from the scope of the present invention. Thus, the present invention is not intended to be limited to the embodiments shown, but is to be accorded the widest scope consistent with the principles and features disclosed herein.

[0008] The program environment in which a present embodiment of the invention is executed illustratively incorporates a general-purpose computer or a special purpose device such as a hand-held computer. Details of such devices (e.g., processor, memory, data storage, display) may be omitted for the sake of clarity.

[0009] It should also be understood that the techniques of the present invention might be implemented using a variety of technologies. For example, the methods described herein may be implemented in software executing on a computer system, or implemented in hardware utilizing either a combination of microprocessors or other specially designed application specific integrated circuits, programmable logic devices, or various combinations thereof. In particular, the methods described herein may be implemented by a series of computer-executable instructions residing on a suitable computer-readable medium. Suitable computer-readable media may include volatile (e.g., RAM) and/or non-volatile (e.g., ROM, disk) memory, carrier waves and transmission media (e.g., copper wire, coaxial cable, fiber optic media). Exemplary carrier waves may take the form of electrical, electromagnetic or optical signals conveying digital data streams along a local network or a publicly accessible network such as the Internet.

[0010] In one embodiment of the invention, a system and method are provided for verifying a financial instrument or account or verifying a user's authorization to use a financial instrument or account. A financial instrument or account may be defined to include credit cards, debit cards, bank accounts, brokerage accounts, money market accounts, and so on—virtually any entity that may be used as a source or destination of electronically exchanged value.

[0011] More particularly, a system and method of the invention may be applied to ensure that a financial instrument identified by a user (e.g., as a source of funds) is actually owned or controlled by the user. The likelihood or risk that the user has stolen the instrument, and is now attempting to use it fraudulently, may therefore be determined to be lower than if the verification was not performed.

[0012] In an embodiment of the invention, a series of transactions are performed using the instrument identified by the user. The transactions may include debits or credits to a credit card, deposits or withdrawals from a bank account, etc. Certain details of the transactions are recorded (e.g., amount, type of transaction, merchant identity, date or time of a transaction) and the user is invited to retrieve specified details (e.g., from an account statement, by calling the holder or issuer of the instrument) and identify them to the system. If the user correctly identifies the specified details, the verification process is successful. If the user is unsuccessful, he or she may be given a limited number of additional opportunities to input the correct details and, if still unsuccessful, may be barred from using the instrument. In this embodiment, the user is required to pass his or her financial institution's own verification/authentication process in order to obtain the necessary details of the transactions, thereby making it even less likely that he or she is a fraudulent user.

[0013] An embodiment of the invention may be used or applied for various reasons or in various situations. For example, a merchant may initiate or implement a verification process when a customer wishes to make a purchase (e.g., if the customer is new or if the cost of the purchase is relatively

large). The customer may be able to rapidly retrieve the necessary details of the verification transactions by accessing them on-line (e.g., through a web site of her credit card issuer or bank) or by telephone.

[0014] Another embodiment of the invention may be applied to prospectively verify a user's authority to use a financial instrument. For example, an on-line system may allow users to make fund transfers and/or purchases on-line. A user may identify a financial instrument that he would like to use but the on-line system may require the financial instrument, or the user's authorization to use the instrument, to be verified before allowing the user to use it in the system.

[0015] FIG. **1** depicts a system for verifying a user's control of or authorization to use a financial instrument, according to one embodiment of the invention. In this embodiment, system **100** includes user interface **102**, database **104** and transaction processor **106**. User interface **102** may operate on a web server, application server, data server or other computing device. In an alternative embodiment of the invention a user may interact with the system via a human agent or representative of the system, an interactive voice recorder or other means, in addition to or instead of user interface **102**. Database **104** may be separate from or integrated with user interface **102** or the computer system on which the user interface executes. Transaction processor **106** may be configured for initiating transactions for one or more different types of financial instruments or, alternatively, system **100** may include multiple transaction processors, in which case the capabilities of each may or may not overlap.

[0016] User interface **102** is configured to receive user connections, such as from user **110**, and may operate differently (e.g., display different web pages, forms or menus) depending on a user's status. For example, for a connection from a new user, interface **102** may present the user with a registration form, information about services offered by the system (e.g., electronic commerce, fund transfers), etc. A registration form may require the user to identify one or more financial instruments, any of which may then be verified according to an embodiment of the invention. For registered or other experienced users, interface **102** may present customized pages or displays, electronic commerce opportunities, etc. Such a user may be invited to identify a financial instrument or account for immediate or future use as a source or destination of funds. User interface **102** may be configured to accept connections via publicly available networks (e.g., the Internet), private networks and other dedicated or shared links, which may be wired or wireless.

[0017] Transaction processor **106** is coupled to one or more financial systems or entities for processing financial transactions. Thus, financial system **120** may comprise an ACH (Automated Clearing House) vendor (e.g., a Treasury Management Service configured to handle ACH transactions such as electronic checks and deposits), a merchant acquirer or Treasury Management Service that handles credit card and/or debit card transactions, or some other entity. As specified above, system **100** may include multiple transaction processors. Each transaction processor may be configured for a different type of financial instrument and may interact with a different financial system or entity. Transaction processor **106** may be a separate or specialized element of system **100** (e.g., a computer server) or may be incorporated into another element of the system (e.g., a data server, web server).

[0018] Financial system **120** is coupled to the user's financial institution corresponding to the financial instrument being verified. Financial institution **130** may therefore be the user's bank, credit card issuer, brokerage, investment manager, etc. Financial system **120** may, in an embodiment of the invention, represent a collection of financial institutions and entities that communicate with each other by specified formats (e.g., for credit card, debit card and/or ACH transactions). Thus, financial system **120** may comprise financial institution **130**.

[0019] In one method of verifying a user's financial instrument or account through system **100**, user **110** connects to system **100** and identifies an instrument or account that he or she would like to use (e.g., as a source of funds for purchases or money transfers). User interface **102**, or the server operating the user interface, passes the identifying information to transaction processor **106**. Transaction processor **106** initiates one or more transactions, using variable details such as an amount of the transaction, type of transaction (e.g., deposit, withdrawal, debit, credit), different vendor names or identities, or other details that may be reported to or retrieved by a valid user or owner of the instrument. The transaction may be generated or constructed by user interface **102**, transaction processor **106** or some other entity within system **100** (e.g., an application or data server). The generating entity also saves selected details of the transaction(s) to database **104**.

[0020] Transaction processor **106** then initiates the series of transactions through appropriate financial systems or entities (e.g., financial system **120**), which execute the transaction(s) in conjunction with the user's financial institution **130**. Thus, the transaction processor takes information regarding the transactions(s), changes it into a form that financial system **120** can understand or use, and then interacts with or otherwise passes it to the financial system.

[0021] User **110** obtains details of the transaction(s) from a statement from institution **130**, from an on-line system provided by the institution, by calling the institution, etc. User **110** then re-connects to system **100** (e.g., through user interface **102**) and provides the requested details. The system compares the details provided by user **110** with the stored details and, if they match, authorizes or allows the user to use the instrument or take other desired action that may otherwise be prevented or denied. A more comprehensive method of the invention is described below in conjunction with FIG. **2**.

[0022] One result of implementing an embodiment of the invention may be to reduce fraud rates, charge-backs, rejections, etc., in order to reduce the cost of business for merchants and other entities. A merchant that accepts credit cards, debit cards, electronic checks or other instruments that can be verified through a method of the invention may perform such verification for all users, just for users deemed high risk, or for some other group of users. For example, if the merchant calculates or otherwise obtains a level of risk presented by a user, that level may determine whether the user presents a low enough risk that verification is unnecessary, high enough to warrant verification, or so high that the user should be rejected without even attempting to verify the user's selected instrument.

[0023] Because the identity of a vendor (e.g., merchant) involved in a financial transaction is typically reported to a user, the specific vendor account or name used to perform a verifying transaction may be one of the details required of a user in order to verify a financial instrument. Thus, the entity (e.g., merchant, vendor, on-line service) performing or implementing a method of the invention may establish a number of vendor accounts with its merchant acquirer, credit card issuer

or the bank or other institution through which it will initiate ACH and/or other transactions. Alternatively, instead of requiring separate accounts, the entity's bank, merchant acquirer or other financial system partner may allow the entity to specify a merchant name, account, or other detail to be part of the transaction.

[0024] Advantageously, the use of variable or different merchant names facilitates the use of an embodiment of the invention internationally. In particular, even if the verifying transactions are initiated in one currency and, at the user's end are converted into another currency, the merchant name or other variable identity can still be used as a verifying detail.

[0025] If the manner in which verification transactions are handled causes some of the transaction information to be truncated or excised, the verification system (e.g., system **100** of FIG. **1**) may structure transactions accordingly or take that handling into account when comparing stored transaction details against the details offered by a user. For example, if it is likely that part of a vendor name or account will be truncated, then that portion of a transaction may be reported in a way that prevents truncation of disambiguating information (e.g., by using a vendor name of "2468AcmeCorporation" instead of "AcmeCorporation2468"). Then, as long as the user can provide the "2468Acme" portion, this may be considered to match the account name.

[0026] FIG. **2** demonstrates one method of verifying a user's specified financial instrument or verifying the user's authority to use the instrument, according to one embodiment of the invention. In this embodiment, a user selects a credit card, debit card, bank account or other account that offers electronic checking or deposits, to be the source of funds for purchases, money transfers or other transactions at a merchant (or other entity).

[0027] In order to use variable or different merchant or vendor names/accounts for verifying transactions (as described above), the merchant may, prior to the illustrated method, establish multiple accounts with its credit card issuer or ACH vendor.

[0028] In state **202** of the method of FIG. **2**, a user (or a user's agent) connects to the verification system, which may be implemented as part of an on-line or traditional merchant or, another entity that accepts payment in forms other than physical currency. This connection may be the user's initial contact with the system, in which case he or she may (or may be required to) verify a source of funds as part of a registration process. Or, this may be just one of many visits, but the user may be requesting a transaction (e.g., a purchase or fund transfer) that requires verification.

[0029] In state **204**, the user identifies one or more financial instruments (e.g., credit cards, debit cards, bank accounts, charge cards) or other sources of funds. Such an instrument or source may not be the one that the user is attempting, or desires, to use for a particular transaction. In particular, verifying any financial instrument or source of funds associated with the user may reduce the risk that he or she is a fraudulent user. Illustratively, the user may be required to provide (where applicable) an account name or number, the name of the registered owner/user, a physical (e.g., street) address associated with the instrument or account, a telephone number, a password or PIN, etc. In this embodiment of the invention, some or all of the electronic communications involving the system that contain financial or private data may be encrypted or otherwise protected.

[0030] In state **206** the system determines whether verification is required before the user may use an identified financial instrument. This determination may be made on the basis of various risk factors and fraud profiles, which may differ in different embodiments of the invention. For example, if any of the information provided by the user does not correspond with the identified instrument, this may indicate higher risk and the need for verification. Some other risk factors may include: a recently changed address or telephone number associated with the instrument, the time of day during which the user has connected, the number or amount of transactions the user wants to perform, the user's electronic address (e.g., IP—Internet Protocol) and whether it corresponds with his or her asserted physical address, and virtually any other activity that may be indicative of a risky or fraudulent user. Illustratively, domestic (i.e., United States) credit card users may not be subjected, in one embodiment of the invention, to verification of their credit cards, whereas all international users may require verification. Similarly, all bank accounts or other sources of electronic checks or debits may be deemed to require verification. If verification is required, the illustrated method continues at state **208**; otherwise, the method ends.

[0031] In state **208**, the system (e.g., a user interface, web or application server, transaction processor) generates a series of one or more verifying transactions involving the identified financial instrument. Certain details may vary from one transaction to another, thereby decreasing the likelihood that the user could guess them. Illustrative variable details include the number of transactions, type of transaction (e.g., deposit or withdrawal, debit or credit), amount of the transaction, merchant name or account used in the transaction, etc.

[0032] In one embodiment of the invention, a typical series of verifying transactions may include two deposits (to a bank account) or credits (to a credit card), each of which is between $0.01 and $0.99 in value, and may involve different merchant identities (e.g., 1234XYZCorporation, 5160XYZCorporation). To decrease the cost of performing transactions in this embodiment, one or both of the deposit/credit amounts may be biased toward the lower end of the value range.

[0033] In state **210**, selected details (e.g., all or a subset of the variable details) of the transactions are saved (e.g., stored in a database) and the transactions are initiated (e.g., through transaction processors coupled to the appropriate financial systems or entities). The verifying transactions may be initiated all at the same time, may be separated in time or sent through different financial systems or entities. Also, the verifying transactions may be joined with other transactions (e.g., a verifying deposit may be merged with a subscription fee being charged to the user), in which case details of the merged transactions would be saved for comparison with the details reported by the user.

[0034] In optional state **212**, the user may be notified (e.g., via electronic mail) that he or she should wait for or retrieve evidence of the transactions. The user may be notified when, or shortly after, the transaction is initiated. Or, the user may be notified after enough time has passed for the transaction to be completed.

[0035] The user's evidence of the transaction(s), which should include all or a subset of the details of the transaction (s), may be in the form of a monthly statement mailed to the user from his or her financial institution. Or, the user may take a more proactive approach and access his or her instrument or account status on-line or via telephone. In some manner, the user obtains information regarding the transaction(s).

[0036] In state **214** the user (or an agent of the user) connects to the system and, in state **216**, proffers or provides supposed details of the verifying transaction(s). Illustratively, the system (e.g., a user interface) may prompt the user to enter the amount of each transaction, the merchant name (or the variable part thereof), the type of transaction, and/or any other detail that was stored.

[0037] In this embodiment, the system is configured to communicate with the user through a user interface. However, in alternative embodiments the user may be able to interact with human operators for all or any part of the verification process.

[0038] In state **218** the system compares the stored details to the details proffered by the user. If they match (e.g., if the stored details include the proffered details) the illustrated method continues at state **220**. Otherwise, the method proceeds to state **222**.

[0039] In state **220**, the system approves the user's use of the identified financial instrument, or allows some action that was previously disallowed due to questionable risk levels, and the method ends.

[0040] In state **222**, verification failed, in which case the user may be allowed to re-enter supposed details (e.g., up to some maximum number of times) or may have to provide different verification (e.g., by submitting a copy of a statement regarding the instrument—such as a monthly statement from the user's financial institution). Or, the system may restart the verification process, restrict the user's activity or use of the instrument, etc. the method may therefore end or return to a previous state.

[0041] In one embodiment of the invention, if a user for whom a series of verifying transactions have been initiated does not return to the system to submit details of the transactions within a predetermined period of time (e.g., five days, two weeks, one month), he or she may be contacted (e.g., via electronic mail and/or telephone) and prompted to complete the process.

[0042] The foregoing descriptions of embodiments of the invention have been presented for purposes of illustration and description only. They are not intended to be exhaustive or to limit the invention to the forms disclosed. Accordingly, the above disclosure is not intended to limit the invention; the scope of the invention is defined by the appended claims.

1. A method comprising:

receiving, from a user, via a user interface, a request to use a financial instrument in response to the request to use the financial instrument, initiating, in real time, at least one transaction having a variable detail, using the financial instrument;

in response to the initiating the at least one transaction notifying the user in real time of the initiation of the transaction;

saving the variable detail; and

using at least one processor, authorizing use of the financial instrument in response to receiving matching input from the user, the matching input matching the saved variable detail.

2. The method of claim **1**, wherein the financial instrument is suitable for use as a source or destination of electronically exchanged value.

3. The method of claim **1**, comprising obtaining identification of the financial instrument by presenting to the user a registration form via the user interface.

4. The method of claim **1**, comprising initiating the one or more transactions through a financial system.

5. The method of claim **1**, comprising:

in response to determining that input from the user does not match the variable detail, providing the user with a limited number of additional opportunities to input correct details.

6. The method of claim **1**, wherein the variable detail includes one or more of a type of a transaction of the one or more transactions and a number of transactions in the one or more transactions.

7. The method of claim **1**, wherein:

the one or more transactions are initiated on behalf of a vendor; and

the variable detail includes a vendor identifier, the vendor identifier identifying the vendor.

8. The method of claim **1**, comprising:

determining a status of the user; and

selecting a presentation for the user, based on the status of the user.

9. The method of claim **1**, wherein said authorizing comprises:

receiving a subsequent transaction, the subsequent transaction identifying a source; and

transferring funds to the financial instrument from the one for more financial instruments from the source.

10. The method of claim **1**, wherein a financial instrument from the one for more financial instruments is associated with at least one of a credit card account, a debit card account, and a checking account.

11. A system comprising:

at least one processor coupled to the memory;

a user interface to receive, from a user, a request to use a financial instrument, using the at least one processor;

a transaction processor to, using the at least one processor:

in response to the request to use the financial instrument, initiate, in real time, at least one transaction having a variable detail, using the financial instrument, in response to the initiating the at least one transaction notify the user in real time of the initiation of the transaction,

save the variable detail, and

authorize use of the financial instrument in response to receiving matching input from the user, the matching input matching the saved variable detail.

12. The system of claim **11**, wherein the financial instrument is suitable for use as a source or destination of electronically exchanged value.

13. The system of claim **11**, wherein the user interface is to obtain identification of the financial instrument by presenting to the user a registration form via the user interface.

14. The system of claim **11**, wherein the transaction processor is to initiate the one or more transactions through a financial system.

15. The system of claim **11**, c wherein the transaction processor is to:

in response to determining that input from the user does not match the variable detail, provide the user with a limited number of additional opportunities to input correct details.

16. The system of claim **11**, wherein the variable detail includes one or more of a type of a transaction of the one or more transactions and a number of transactions in the one or more transactions.

17. The system of claim **11**, wherein the transaction processor is to initiate the one or more transactions are initiated on behalf of a vendor, the variable detail includes a vendor identifier, the vendor identifier identifying the vendor.

18. The system of claim **11**, wherein the user interface is to:

determine a status of the user; and

select a presentation for the user, based on the status of the user.

19. The system of claim **11**, wherein the transaction processor is to:

receive a subsequent transaction, the subsequent transaction identifying a source; and

transfer funds to the financial instrument from the one for more financial instruments from the source.

20. A machine-readable non-transitory storage medium having instruction data to cause a machine to:

receive a request to use a financial instrument;

in response to the request to use the financial instrument, initiate, in real time, at least one transaction having a variable detail, using the financial instrument;

in response to the initiating the at least one transaction notify the user in real time of the initiation of the transaction;

save the variable detail; and

authorize use of the financial instrument in response to receiving matching input from the user, the matching input matching the saved variable detail.

* * * * *