US 20070094151A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2007/0094151 A1

Moenickheim et al. (43) Pub. Date: Apr. 26, 2007

(54) SYSTEMS AND METHODS OF RULES-BASED DATABASE ACCESS FOR ACCOUNT AUTHENTICATION

(76) Inventors: **Peter Moenickheim**, Dublin, OH (US); **Paul J. Lyda**, Powell, OH (US)

Correspondence Address:
SUTHERLAND ASBILL & BRENNAN LLP
999 PEACHTREE STREET, N.E.
ATLANTA, GA 30309 (US)

(21) Appl. No.: **11/612,254**

(22) Filed: **Dec. 18, 2006**

Related U.S. Application Data

(63) Continuation of application No. 10/206,239, filed on Jul. 29, 2002, now Pat. No. 7,177,846.

Publication Classification

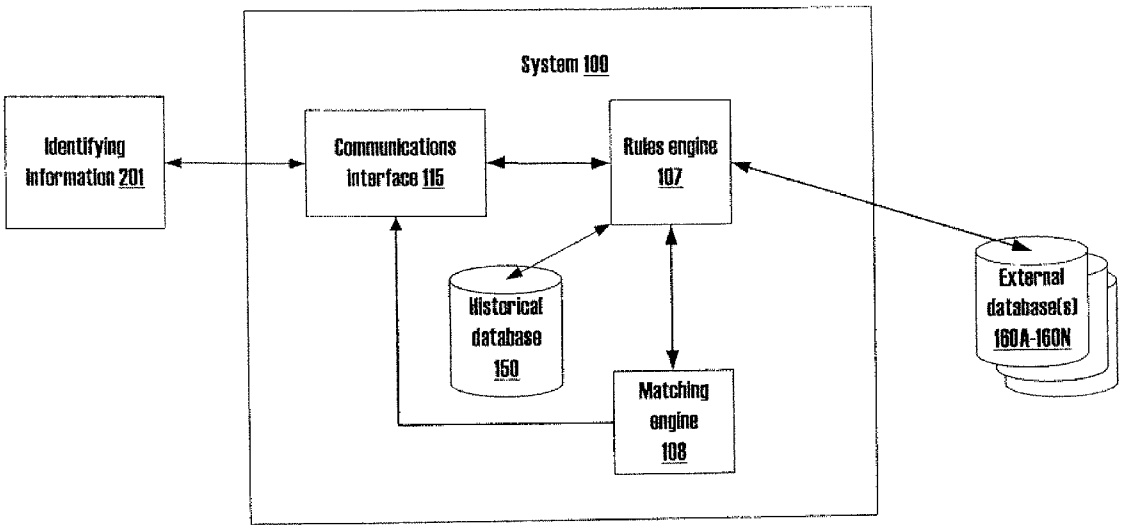
(51) **Int. Cl.**

G06Q	*99/00*	(2006.01)
H04L	*9/00*	(2006.01)
H04K	*1/00*	(2006.01)

(52) **U.S. Cl.** **705/64**

(57) **ABSTRACT**

Systems and methods for authenticating a customer association with a particular deposit account used when conducting financial transactions on behalf of the customer. The system receives identity information and routing and transit number or account number (RTN/DDA) information, where at least a portion of identity information identifies an account holder and at least a portion of the RTN/DDA information identifies a deposit account. A selection of numerous databases used to authenticate an association between the deposit account and the account holder is made based on one or more criteria. A database is then accessed according to the selection; and an association between the deposit account and the account holder is authenticated using the received identity information and RTN/DDA information and the selected database.



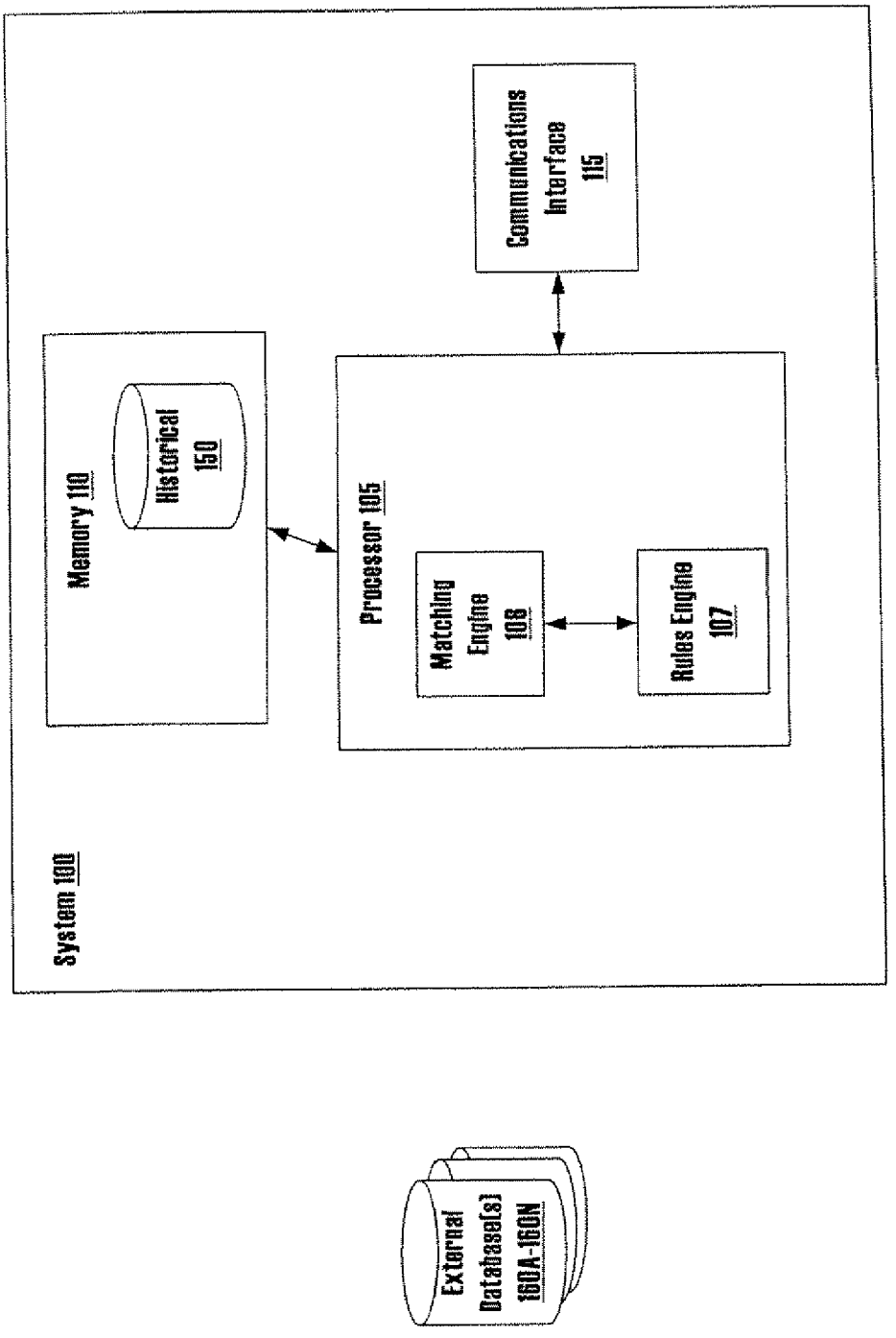

System 100
Memory 110
Historical 150
Processor 105
Matching Engine 108
Rules Engine 107
Communications Interface 115
External Database(s) 160A-160N

FIG. 1

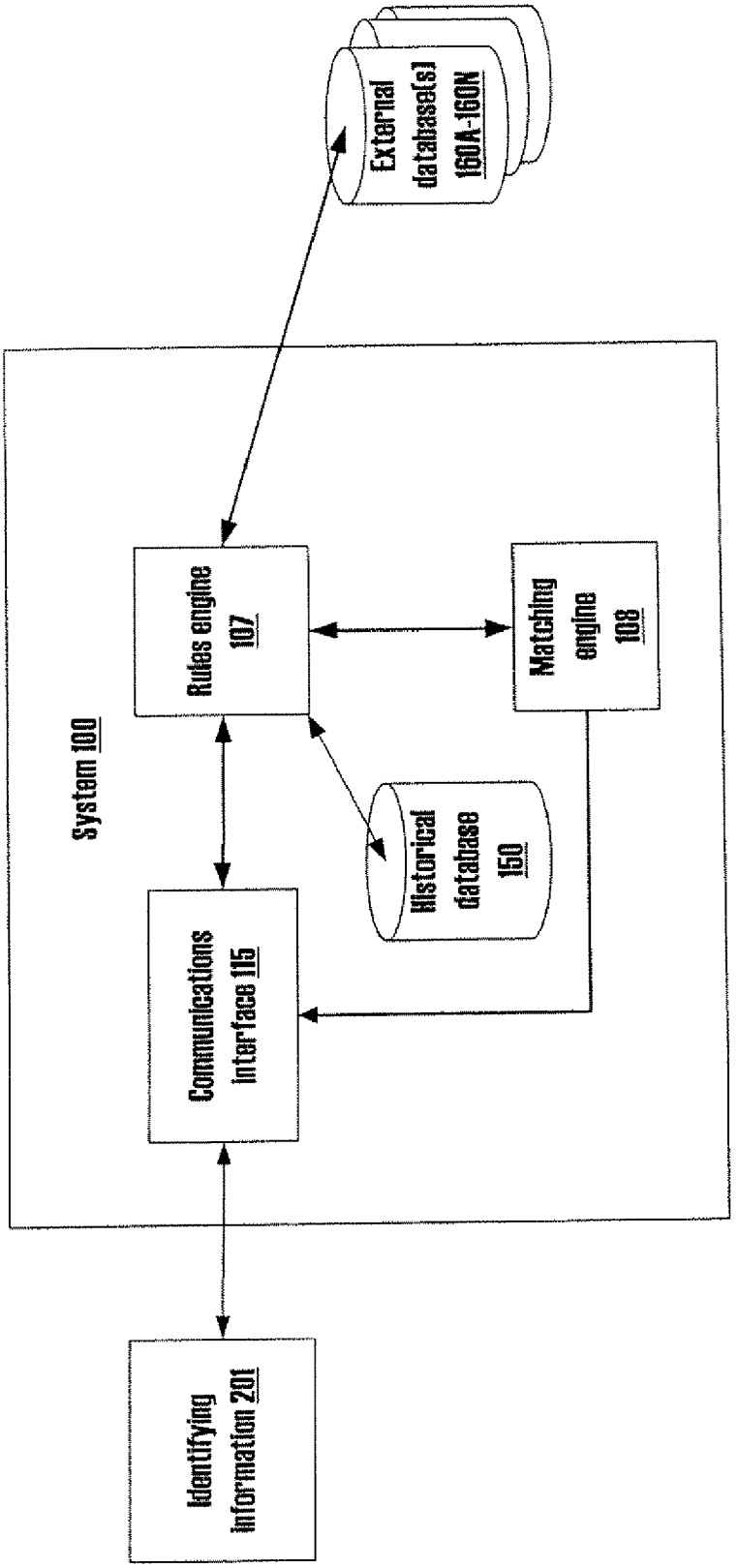

External database(s) 160A-160N
System 100
Rules engine 107
Matching engine 108
Historical database 150
Communications interface 115
Identifying information 201

FIG. 2

SYSTEMS AND METHODS OF RULES-BASED DATABASE ACCESS FOR ACCOUNT AUTHENTICATION

CROSS REFERENCE TO A RELATED APPLICATION

[0001] This application is a continuation of pending U.S. application Ser. No. 10/206,239, filed Jul. 29, 2002, entitled "Technique For Account Authentication," the disclosure of which is incorporated by reference herein in its entirety.

FIELD OF THE INVENTION

[0002] The present invention relates to electronic commerce, and more particularly to authentication of deposit account information.

BACKGROUND OF THE INVENTION

[0003] On-line payment service providers make payments on behalf of payors to payees. In making a payment on behalf of a payor, an on-line payment service provider debits a deposit account belonging to the payor and issues a credit to the payee, either electronically, by check drawn on an account belonging to the on-line service provider, or by draft drawn from the payor's deposit account. It will be understood by one skilled in the art that drafts serve as both the debit and the credit vehicle.

[0004] A payor must register with an on-line payment service provider to access services offered by the on-line payment service provider. The registration process, which can be either on-line, typically via the World Wide Web, or by paper forms, includes the payor (registering customer) providing information identifying a demand deposit account, such as a checking account, belonging to the payor to the on-line payment service provider. This identifying information includes a unique routing and transit number (RTN), which identifies the financial institution at which the deposit account is maintained, as well as a unique account number (DDA) identifying the payor's deposit account maintained at the financial institution. Together, this information is known as RTN/DDA information, and alternatively RT/DDA information.

[0005] For both on-line and paper registration, the registering customer has conventionally been required to supply the on-line payment service provider a voided check from the deposit account. This voided check is used as a fraud prevention measure to authenticate the association between the registering customer and the deposit account. Thus, in conventional enrollment, a registering customer has not been able to immediately direct an on-line payment service provider to make payments on his or her behalf, as the voided check must physically be delivered to the on-line payment service provider, and then the voided check must be authenticated by a customer service representative of the on-line payment service provider.

[0006] Recently, new completely on-line and real-time registration techniques have been introduced. In one, a trusted agent, typically a consumer service provider (CSP), guarantees to indemnify an on-line payment service provider against fraud committed by a registering customer that the CSP represents. No attempt is made by the on-line service provider to authenticate the association between the registering customer and that registering customer's deposit account.

[0007] In another completely on-line and real-time registration technique, the registering customer's identity is verified, by leveraging one or more commercial databases, while the registering customer is participating in an on-line registration session. While the registering customer's identity is verified, an association between the registering customers deposit account and the registering customer is not authenticated. At most, the on-line payment service provider can be assured that the registering customer is who he or she purports to be. Based upon a verified identity, on-line payment service providers have found that there is less chance of the registering customer providing fraudulent information identifying a deposit account. These two techniques each allow a registering customer the convenience of immediately directing payments.

[0008] In both of these completely on-line and real-time techniques, a registering customer is required to enter RTN/DDA information. As the registering customer is not required to supply a voided check, the sole source of this information is the registering customer. On-line payment services have found that registering customers often make mistakes in entering these numbers. On-line payment services, in rectifying these unintentional mistakes, incur customer service costs. In addition, fraudulent deposit account identifying information is also still received under both completely online registration techniques. Even when a CSP indemnifies an on-line payment service, costs are still associated with the fraud.

[0009] Other new registration techniques have also been introduced. These techniques are not completely on-line or real-time. In one technique, a financial institution at which a customer's account is maintained supplies RTN/DDA information. While an association between a customer and an account is authenticated because the financial institution itself supplies RTN/DDA information, this does not occur during an on-line and real-time enrollment session with a customer. In another technique, a registering customer provides RTN/DDA information during an on-line session. Subsequent to the session, a service provider makes one or more small debits and/or credits, via electronic funds transfer, from/to the customer's account. The customer then determines the amount(s) and initiates another on-line session with the service provider and identifies the amount(s) to the service provider. If the customer supplied amount(s) is/are correct, the service provider has a high level of confidence that the account is actually associated with the registering customer. However, the enrollment process can not be completed fully in a single session, as the consumer must take some action (determining the amount(s)) subsequent to an initial registration session.

[0010] Accordingly, a need exists for an on-line and real-time technique to authenticate an association between a registering customer and a demand deposit account which mitigates occurrence of both incorrect entry of RTN/DDA information and fraud.

[0011] Some on-line payment services access more than one commercial database in the registration process in attempting to locate information used to authenticate a registering customer's identity (not to authenticate an association between a customer and a deposit account). Often an on-line service provider must access multiple commercial

databases before useful information is found. These commercial databases charge for access, making this an expensive process.

[0012] Accordingly a need exists for a technique for registration for electronic commerce service which minimizes costs associated with utilizing information belonging to an entity other than an electronic commerce service provider.

BRIEF DESCRIPTION OF THE DRAWINGS

[0013] In order to facilitate a fuller understanding of the present invention, reference is now made to the appended drawings. These drawings should not be construed as limiting the present invention, but are intended to be exemplary only.

[0014] FIG. **1** depicts a computing system maintained by an electronic commerce service provider.

[0015] FIG. **2** depicts the processing to authenticate an association between a deposit account and a registering customer.

DETAILED DESCRIPTION OF AN EXEMPLARY EMBODIMENT

[0016] FIG. **1** shows an electronic commerce service system **100** maintained by an electronic commerce service provider (hereinafter, service provider). Included in system **100** is a processor **105** which is driven by instructions stored in memory **110**. Processor **105** could be multiple processors working either in concert or independently to provide the functionality described herein. Likewise, memory **110** could be multiple memories. Processor **105** includes a rules engine **107** and a matching engine **108**, which will be discussed below. Also shown is a communications interface **115** for communicating with registering customers and other entities. Though only one communications interface **115** is depicted, it should be understood that multiple communications interfaces could be included in system **100**. Memory **110**, in addition to storing the above described instructions, also stores a historical database **150** which stores information associated with registrations of each of multiple registering customers, data accumulated during provision of electronic commerce services, as well as other information used to determine which external databases (described below) to access during an on-line and real-time registration session. It will be appreciated that registration processing could be performed as a batch process. That is, not in real-time.

[0017] Also depicted in FIG. **1**, though not necessarily a part of system **100**, are multiple external databases **160**A-**160**N. These external databases store information gathered by entities other than the service provider. Information stored in these external databases **160**A-**160**N is utilized to authenticate an association between a registering customer and a deposit account.

[0018] These external databases **160**A-**160**N belong to any one of, or any combination of, check printing services, check verification services, check guarantee services, and financial institutions. Examples of check printing services are Deluxe, Harland, and Clark American, though other check printing services' databases could also be accessed. Examples of check verification and/or guarantee services are Telecheck and Equifax Check Services, though other check verification and/or guarantee services' databases could also be accessed. A financial institution maintains deposit accounts on behalf of depositors, in addition to providing other financial services. A financial institution, obviously, has knowledge of associations between accounts that financial institution maintains and depositors (customers). A financial institution may have knowledge about associations between accounts and depositors for accounts that are maintained at other financial institutions. Information stored in external database **160**A-**160**N is associated with deposit accounts. Check printing services retain information associated with each check order printed for an account holder. This information is typically retained so that a subsequent check order for the account holder can be printed without all account holder identifying and account identifying information being supplied a second time in order to print the second order. Thus, check printing services maintain information that authenticates an association between an account holder and an account.

[0019] It should be noted that one or more of the external databases **160**A-**160**N, though belonging to an entity other than the service provider, could be hosted by the service provider. In such a case, a third party such as a check printing, verification, or guarantee service, would provide information to be stored to the service provider. The service provider would then access the service provider hosted external database(s) as necessary.

[0020] As shown in FIG. **2**, a registering customer provides, during an on-line enrollment session, preferably via a World Wide Web interface **201**, identifying information **105** such as one or more of name, drivers license number, and social security number to system **100**. This information is received by communications interface **115**. Any or all of this identifying information could be provided, in addition to other forms of identifying information. The registering customer also provides RTN/DDA information identifying a deposit account which they are authorizing the service provider to access. It should be noted that identifying information could be received from an entity other than a registering customer, such as a sponsor. Sponsors provide access to electronic commerce services on behalf of customers.

[0021] This received information is then processed by the rules engine **107** while the registering customer is still participating in the on-line enrollment session. The rules engine **107** first determines if historical database **150** contains information upon which a positive authentication between the registering customer and the customer's deposit account can be based. If so, the on-line registration session can be successfully completed without accessing commercial databases.

[0022] If the historical database **150** does not contain information which leads to a successful registration, then based upon logic derived from historical registration experience and other information contained in the historical database **150**, the rules engine **107** determines which of external databases **160**A-**160**N to access to authenticate an association between the registering customer and a deposit account. Criteria that can be used by the rules engine **107** in determining which external database to access includes the registering customer's financial institution's RTN (ABA)

number. This information can be used because, based upon the historical information stored in the historical database **150**, it is known that certain financial institutions utilize certain check printing services.

[**0023**] Other criteria that can be utilized to determine which of the external databases **160**A-**160**N to access includes geographic criteria, such as the location of the registering customer and/or his or her financial institution. Yet another criteria is cost. That is, fees charged by entities maintaining external databases **160**A-**160**N for accessing different ones of the external databases **160**A-**160**N vary among the external databases. Still another criteria is a success rate of particular ones of the external databases **160**A-**160**N in providing information useful in the registration process.

[**0024**] The rules engine **107** determines an order in which to access the external databases **160**A-**160**N. Once the rules engine **107** determines the order in which the external databases **160**A-**160**N should be accessed, the first determined external database is accessed in an attempt to locate information upon which to base an authentication determination.

[**0025**] If information upon which to base an authentication determination is not found in the first determined external database, the second determined external database is accessed. This process continues until information is found. It should be noted that if information for successful authentication information is not found in any database or other data store, the registering customer could be given the opportunity, on-line and in-session, to resubmit account identifying information, in view of the chance that the registering customer may have provided incorrect identifying information beforehand.

[**0026**] Once information is found in an external database, all or a portion of the information gathered via the web interface from the registering customer is used by the matching engine **108** in authenticating the RTN/DDA information received from the registering customer. That is, the matching engine **108** compares the RTN/DDA information and the identity information received from the registering customer with data stored in the external database. If the received data matches that supplied by the registering customer, the association is successfully authenticated.

[**0027**] Upon successful authentication, the registering customer is informed, via the on-line registration session, that registration is successful. The registering customer becomes a registered customer. The service provider can immediately and in-session provide services to the registered customer with confidence that an authentic association between the registered customer and a deposit account identified by that customer is in fact authentic.

[**0028**] In the event that on-line authentication of customer supplied information is unsuccessful, the registering customer would be required to complete the registration process by traditional techniques. This could include, for instance, requiring the registering customer to supply a voided check to the service provider, as well as any other known registration technique.

[**0029**] In a variation of the above-described process, instead of accessing the external databases **160**A-**160**N in a determined order to determine if each database includes information which can be used in the authentication process, each of external databases **160**A-**160**N are accessed, in the same determined order as above, and an authentication attempt is made against data stored in each external database. Thus, the first determined external database is accessed, and based upon data stored in that database an authentication attempt is made. If that authentication attempt is unsuccessful, the second determined external database is accessed and another authentication attempt is made. This process continues until a successful authentication is made, or until each database has been accessed. As above, if on-line authentication is unsuccessful, the registering customer would have to complete the registration process in an off-line fashion. In another variation, external databases **160**A-**160**N could be accessed in a random order.

[**0030**] In yet another variation of the above-described process, an entity to whom an external database belongs might not offer direct access to the information stored in the database. In such a case, the service provider transmits at least a portion of the received identifying information as well as the RTN/DDA information to the entity to whom the external database belongs. That entity then compares this received information with information contained in the database.

[**0031**] That entity then returns a match key to the service provider. The match key could be one of four types: Account Found-Full Match, Account Found-No Match, Account Not Found, and Account Found-Possible Match. If the match key is of the Account Found-Full Match type, the authentication is successful. If the match key is of either the Account Found-No Match or Account Not Found types, the authentication is not successful and conventional, off-line, authentication techniques could be utilized. If the match key is of the Account Found-Possible Match type, further on-line activity can be performed to complete the authentication. This further activity could include the service provider providing further received identifying information to the entity to whom the database belongs, and could include the service provider querying the registering customer, via the still active on-line session, for additional identifying information, which would then be transmitted to the entity to whom the database belongs for further processing. It will be appreciated that the returned Match Key could be processed with other information to make the determination that authentication is successful or not. This other information could belong to the entity receiving the Match Key, or another entity. Also, instead of being processed with other information, a returned Match Key could be just one factor considered when making a determination as to a successful or unsuccessful authentication.

[**0032**] It should be noted that the inventive technique of on-line authentication of RTN/DDA information could be performed by the service provider on behalf of an entity other than the service provider. This authentication process could be performed in real-time, via perhaps a Web-based interface or a direct connection between another entity and the service provider, or could be performed as an asynchronous (e.g. batch file based or messaging-based) process for another entity. Further, it will be appreciated that the account authentication technique disclosed herein can be performed in a batch mode,

[**0033**] The present invention is not to be limited in scope by the specific embodiments described herein. Indeed, vari-

ous modifications of the present invention in addition to those described herein, will be apparent to those of skill in the art from the foregoing description and accompanying drawings. Thus, such modifications are intended to fall within the scope of the appended claims.

That which is claimed:

1. A method comprising:

receiving identity information and routing and transit number or account number (RTN/DDA) information, wherein at least a portion of identity information identifies an account holder and at least a portion of the RTN/DDA information identifies a deposit account;

selecting at least one database of a plurality of databases to authenticate an association between the deposit account and the account holder, wherein the selection is based on at least one criterion;

accessing the at least one database of the plurality of databases; and

authenticating an association between the deposit account and the account holder using the received identity information and RTN/DDA information and the at least one database.

2. The method of claim 1, wherein the identity information includes identifying information selected from the group consisting of a name, drivers license number, and social security number.

3. The method of claim 1, wherein the at least one criterion is selected from a group consisting of (i) the RTN portion of the RTN/DDA information, (ii) a geographic location associated with the account holder, (iii) a geographic location associated with the financial institution associated with the first deposit account, (iv) a cost associated with accessing the at least one database, (v) a success rate associated with using the at least one database to authenticate associations between deposit accounts and account holders and (vi) historical information stored in a historical database.

4. The method of claim 1, wherein one or more of the plurality of databases is an external database.

5. The method of claim 1 wherein authenticating an association between the deposit account and the account holder is conducted in real time during an on-line enrollment session.

6. The method of claim 1, further comprising:

prior to selecting at least one database of a plurality of databases to authenticate an association between the deposit account and the account holder, processing the identifying information to determine whether a historical database contains historical information upon which a positive authentication between the deposit account and the account holder may be based; and

wherein the at least one database of the plurality of databases is selected to authenticate an association between the deposit account and the account holder if the historical database cannot be used to positively authenticate the association between the first deposit account and the account holder.

7. The method of claim 6, wherein the historical database is an internal database.

8. The method of claim 1, further comprising:

subsequent to authenticating an association between the deposit account and the account holder, registering the account holder to use a service.

9. The method of claim 8, wherein registering the account holder includes informing the account holder that registration has been successful.

10. The method of claim 1, further comprising, prior to accessing the at least one database, determining an order to access more than one of the plurality of databases to authenticate an association between the deposit account and the account holder.

11. The method of claim 10, further comprising:

processing the received identity information and RTN/DDA information to identify a first database and a second database of the plurality of databases; and

wherein determining an order to access more than one of the plurality of databases to authenticate an association between the deposit account and the account holder includes determining an order in which to access the first database and the second database.

12. The method of claim 1, wherein the order identifies the first database as the first to be accessed.

13. The method of claim 12, further comprising:

upon failing to authenticate the association between the deposit account and the account holder using the first database, accessing the second database using the received identity information and RTN/DDA information for authentication.

14. A system comprising:

at least one communication interface, wherein the at least one communication interface receives at least one of identity information and routing and transit number or account number (RTN/DDA) information, wherein at least a portion of identity information identifies an account holder and at least a portion of the RTN/DDA information identifies a deposit account; and

a processor, in communication with the at least one communication interface, wherein the processor contains programmed logic to execute software instructions for:

receiving the at least one identity information and RTN/DDA information from the communication interface,

selecting at least one database of a plurality of databases to authenticate an association between the deposit account and the account holder, wherein the selection is based on at least one criterion;

accessing the at least one database of the plurality of databases; and

authenticating an association between the deposit account and the account holder using the received identity information and RTN/DDA information and the at least one database.

15. The system of claim 14, wherein the identity information includes identifying information selected from the group consisting of a name, drivers license number, and social security number.

16. The system of claim 14, wherein the at least one criterion is selected from a group consisting of (i) the RTN portion of the RTN/DDA information, (ii) a geographic location associated with the account holder, (iii) a geographic location associated with the financial institution associated with the first deposit account, (iv) a cost associated with accessing the at least one database, (v) a success rate associated with using the at least one database to authenticate associations between deposit accounts and account holders and (vi) historical information stored in a historical database.

17. The system of claim 14, wherein one or more of the plurality of databases is an external database.

18. The system of claim 14, wherein the external database belongs to one or more entities selected from the group consisting of check printing services, check verification services, check guarantee services, and financial institutions.

19. The system of claim 14, wherein the processor contains programmed logic to execute software instructions for authenticating an association between the deposit account and the account holder in real time during an on-line enrollment session.

20. The system of claim 14, wherein the processor contains programmed logic to execute software instructions for:

prior to selecting at least one database of a plurality of databases to authenticate an association between the deposit account and the account holders processing the identifying information to determine whether a historical database contains historical information upon which a positive authentication between the deposit account and the account holder may be based; and

wherein the at least one database of the plurality of databases is selected to authenticate an association between the deposit account and the account holder if the historical database cannot be used to positively authenticate the association between the first deposit account and the account holder.

21. The system of claim 20, wherein the historical database is an internal database.

22. The system of claim 14, wherein the processor contains programmed logic to execute software instructions for:

subsequent to authenticating an association between the deposit account and the account holder, registering the account holder to use a service.

23. The system of claim 22, wherein the software instructions for registering the account holder include software instruction for informing the account holder that registration has been successful.

24. The system of claim 14, wherein the processor contains programmed logic to execute software instructions for:

prior to accessing the at least one database, determining an order to access more than one of the plurality of databases to authenticate an association between the deposit account and the account holder.

25. The system of claim 24, wherein the processor contains programmed logic to execute software instructions for:

processing the received identity information and RTN/DDA information to identify a first database and a second database of the plurality of databases; and

wherein determining an order to access more than one of the plurality of databases to authenticate an association between the deposit account and the account holder includes determining an order in which to access the first database and the second database.

26. The system of claim 25, wherein the order identifies the first database as the first to be accessed.

27. The system of claim 26, wherein the processor contains programmed logic to execute software instructions for:

upon failing to authenticate the association between the deposit account and the account holder using the first database, accessing the second database using the received identity information and RTN/DDA information for authentication.

28. A system comprising:

means for receiving identity information and routing and transit number or account number (RTN/DDA) information, wherein at least a portion of identity information identifies an account holder and at least a portion of the RTN/DDA information identifies a deposit account;

means for selecting at least one database of a plurality of databases to authenticate an association between the deposit account and the account holder, wherein the selection is based on at least one criterion;

means for accessing the at least one database of the plurality of databases; and

means for authenticating an association between the deposit account and the account holder using the received identity information and RTN/DDA information and the at least one database.

* * * * *