SYSTEMS AND METHODS FOR FACILITATING A SECURE TRANSACTION AT A NON-FINANCIAL INSTITUTION SYSTEM

TECHNICAL FIELD

[0001] The technical field relates to systems and methods for transferring funds over an electronic money transfer network, and more particularly to systems and methods for securely transferring funds over an electronic money transfer network to individuals who have access to a physical payment terminal or online payment processes maintained by an entity other than a financial institution.

BACKGROUND

[0002] Many existing systems of transferring money over electronic money transfer networks, such as Automatic Clearing House (ACH) networks, have limitations. Traditional wire transfers, for instance, typically require both a sender of money and recipient of money to be physically present at a financial institution or have direct access (e.g., online access) to an account at a financial institution. Requiring a sender and a recipient to have accounts at financial institution(s) may make it difficult to transfer money from/to some people, such as underbanked segments of the population and/or people who lack ready access to financial institutions. Moreover, traditional wire transfers that involve transferring money between financial institutions or exchange of currency is heavily regulated and generally requires additional fees. These fees may form the basis of transaction costs that make transfer of money between individuals inefficient, impractical or otherwise difficult.

[0003] Many existing systems of transferring money to individuals do not accommodate otherwise possible money transfer scenarios. As an example, existing systems of transferring money may not make funds available to people who want to send or receive money at a physical payment terminal of a retail store or other non-financial institution that is not a financial institution. Existing systems of transferring money may not make funds available to people who want to send or receive money using online payment processes of non-financial institutions. Debit transfer systems and other systems of transferring money to people at retail establishments and/or retail websites may be cost-prohibitive and/or may not facilitate transfers of money between people. Many existing systems of transferring money to individuals may not make fund available soon after a request to transfer funds has been made (e.g., substantially in "real-time"). As a result, it has often proven difficult to cost-effectively

transfer money over electronic money transfer networks to individuals, particularly those individuals who lack access to the payment systems of financial institutions.

SUMMARY

[0004] The systems, methods, and computer-readable media discussed herein relate to securely transferring funds over an electronic money transfer network, such as an Automatic Clearing House (ACH) network, to individuals who have access to a second (e.g., public) network. An example method may include receiving transaction data related to a fund transfer, the transaction data specifying a transfer amount of the fund transfer, a sender public identifier to identify a sender of the fund transfer, a recipient public identifier to identify a recipient of the fund transfer, a financial institution identifier for a sender financial institution, a financial institution identifier for a recipient financial institution, and a tokenized financial instrument of the sender, determining, using the financial institution identifier for the sender financial institution, the sender financial institution, the sender financial institution being a member of a payment network, providing to the sender financial institution the tokenized financial instrument of the sender to enable the sender financial institution to de-tokenize the tokenized financial instrument of the sender and identify an account of the sender financial institution associated with the sender, receiving, from the sender financial institution, a sender private identifier generated by the sender financial institution, the sender financial institution generating the sender private identifier upon confirming the account of the sender financial institution associated with the sender, associating the sender private identifier with the sender public identifier, providing to the sender financial institution the transfer amount of the fund transfer, the recipient public identifier, and the recipient financial institution identifier to enable the sender financial institution to determine availability of money in the account associated with the sender to satisfy the transfer amount of the fund transfer, generating a transaction identifier associated with the fund transfer, and providing the transaction identifier and a recipient private identifier to the recipient financial institution to enable the recipient financial institution to identify an account associated with the recipient to enable the recipient financial institution to receive an ACH message over the ACH network, the ACH message indicating payment from the sender financial institution to the recipient financial institution, the ACH message being generated by the sender financial institution and including the transaction identifier to identify the fund transfer between a sender and a recipient, the ACH message allowing the recipient financial institution to retrieve money from an ACH batch transfer and deposit money into the account associated with the recipient.

[0005] In some embodiments, the method further comprises validating that the sender has authorization to use the public identifier to perform the fund transfer. The method may further comprises receiving a tokenized financial instrument of the recipient and a recipient FI identifier associated with the recipient financial institution, determining, using the recipient FI identifier, the recipient financial institution, the recipient financial institution being a member of the payment network, providing to the recipient financial institution the tokenized financial instrument of the recipient to enable the recipient financial institution to de-tokenize the tokenized financial instrument of the recipient and identify an account of the recipient financial institution associated with the recipient, and receiving, from the recipient financial institution, the recipient private identifier generated by the recipient financial institution, the recipient financial institution generating the recipient private identifier upon confirming the account of the recipient financial institution associated with the sender.

[0006] The method may further comprise receiving the transfer amount of the fund transfer, the sender public identifier to identify the sender of the fund transfer, the recipient public identifier to identify the recipient of the fund transfer, the financial institution identifier for the sender financial institution, the financial institution identifier for the recipient financial institution, and the tokenized financial instrument of the sender from an first online reseller of goods. The first online reseller of goods may tokenize a financial instrument of the sender to create the tokenized financial instrument of the sender. The financial instrument may be issued by the sender financial institution.

[0007] In some implementations, the method may further comprise receiving a tokenized financial instrument of the recipient from a second online reseller of goods different than the first online reseller of goods. The second online reseller of goods may tokenize a financial instrument of the recipient to create the tokenized financial instrument of the recipient. The recipient financial institution may transfer funds to the account associated with the recipient before the recipient financial institution receives the ACH message. The method may further comprise providing a notification a request to a sender system requesting if the sender will accept the fund transfer from the sender.

[0008] An example system comprises one or more processors and a memory coupled to the one or more processors. The memory may be configured to instruct the one or more processors to perform a method. The method may comprise receiving transaction data related

to a fund transfer, the transaction data specifying a transfer amount of the fund transfer, a sender public identifier to identify a sender of the fund transfer, a recipient public identifier to identify a recipient of the fund transfer, a financial institution identifier for a sender financial institution, a financial institution identifier for a recipient financial institution, and a tokenized financial instrument of the sender, determining, using the financial institution identifier for the sender financial institution, the sender financial institution, the sender financial institution being a member of a payment network, providing to the sender financial institution the tokenized financial instrument of the sender to enable the sender financial institution to de-tokenize the tokenized financial instrument of the sender and identify an account of the sender financial institution associated with the sender, receiving, from the sender financial institution, a sender private identifier generated by the sender financial institution, the sender financial institution generating the sender private identifier upon confirming the account of the sender financial institution associated with the sender, associating the sender private identifier with the sender public identifier, providing to the sender financial institution the transfer amount of the fund transfer, the recipient public identifier, and the recipient financial institution identifier to enable the sender financial institution to determine availability of money in the account associated with the sender to satisfy the transfer amount of the fund transfer, generating a transaction identifier associated with the fund transfer, and providing the transaction identifier and a recipient private identifier to the recipient financial institution to enable the recipient financial institution to identify an account associated with the recipient to enable the recipient financial institution to receive an ACH message over the ACH network, the ACH message indicating payment from the sender financial institution to the recipient financial institution, the ACH message being generated by the sender financial institution and including the transaction identifier to identify the fund transfer between a sender and a recipient, the ACH message allowing the recipient financial institution to retrieve money from an ACH batch transfer and deposit money into the account associated with the recipient.

[0009] A nontransitive computer readable media system may comprise executable instructions, the executable instructions being executable by a processor to perform a method. The method may comprise receiving transaction data related to a fund transfer, the transaction data specifying a transfer amount of the fund transfer, a sender public identifier to identify a sender of the fund transfer, a recipient public identifier to identify a recipient of the fund transfer, a financial institution identifier for a sender financial institution, a financial institution

identifier for a recipient financial institution, and a tokenized financial instrument of the sender, determining, using the financial institution identifier for the sender financial institution, the sender financial institution, the sender financial institution being a member of a payment network, providing to the sender financial institution the tokenized financial instrument of the sender to enable the sender financial institution to de-tokenize the tokenized financial instrument of the sender and identify an account of the sender financial institution associated with the sender, receiving, from the sender financial institution, a sender private identifier generated by the sender financial institution, the sender financial institution generating the sender private identifier upon confirming the account of the sender financial institution associated with the sender, associating the sender private identifier with the sender public identifier, providing to the sender financial institution the transfer amount of the fund transfer, the recipient public identifier, and the recipient financial institution identifier to enable the sender financial institution to determine availability of money in the account associated with the sender to satisfy the transfer amount of the fund transfer, generating a transaction identifier associated with the fund transfer, and providing the transaction identifier and a recipient private identifier to the recipient financial institution to enable the recipient financial institution to identify an account associated with the recipient to enable the recipient financial institution to receive an ACH message over the ACH network, the ACH message indicating payment from the sender financial institution to the recipient financial institution, the ACH message being generated by the sender financial institution and including the transaction identifier to identify the fund transfer between a sender and a recipient, the ACH message allowing the recipient financial institution to retrieve money from an ACH batch transfer and deposit money into the account associated with the recipient.

[0010] These and other advantages will become apparent to those skilled in the relevant art upon a reading of the following descriptions and a study of the several examples of the drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] FIG. 1 depicts a schematic diagram of a funds transfer system in which a sender and a recipient use different banking institutions according to an example implementation.

[0012] FIG. 2 depicts a schematic diagram of token management logic that may manage tokens for fund transfer requests according to an example implementation.

[0013] FIG. 3A depicts a process in which a fund transfer request results in the funds being received by a registered or unregistered recipient according to an example implementation.

[0014] FIG. 3B depicts a process in which a fund transfer request results in the funds being received by a registered or unregistered recipient according to an example implementation.

[0015] FIG. 4 depicts a screen shot of a web page that may be presented to a user to configure user preferences and manage connections with other users.

[0016] FIG. 5 depicts a screen shot of a web page that may be presented to a user to configure notification settings.

[0017] FIG. 6 depicts a screen shot of a web page that may be presented to a user to send money to a recipient.

[0018] FIG. 7 depicts a screen shot of a web page that may be presented to an out-of-network user when an out-of-network user is sent a payment.

[0019] FIG. 8 depicts a schematic diagram of a funds transfer system in which a sender and a recipient use different banking institutions according to an example implementation.

[0020] FIG. 9 depicts a flow diagram illustrating an example process for facilitating transfer of funds to an out-of-network recipient according to an example implementation.

[0021] FIG. 10 depicts a flow diagram illustrating an example process for facilitating transfer of funds from an out-of-network sender to an in-network recipient according to an example implementation.

[0022] FIG. 11 depicts a flow diagram illustrating an example process for facilitating expedited transfer of funds from an in-network sender to an in-network recipient according to an example implementation.

[0023] FIG. 12 depicts a diagram of a funds transfer system for securely transferring funds from a sender non-financial institution system to a recipient non-financial institution system, according to some implementations.

[0024] FIG. 13 depicts a diagram of transfer logic, according to some implementations.

[0025] FIG. 14 depicts a diagram of registration logic, according to some implementations.

[0026] FIG. 15 depicts a diagram of a data flow for securely transferring funds from a sender to a recipient in a funds transfer system, according to some implementations.

[0027] FIG. 16A depicts a diagram of a flowchart of a method for securely transferring funds from a sender to a recipient in a funds transfer system, according to some implementations.

[0028] FIG. 16B depicts a diagram of a flowchart of a method for securely transferring funds from a sender to a recipient in a funds transfer system, according to some implementations.

[0029] FIG. 17 depicts a diagram of a data flow for securely transferring funds from a sender to an unregistered recipient in a funds transfer system, according to some implementations.

[0030] FIG. 18A depicts a diagram of a flowchart of a method for securely transferring funds from a sender to an unregistered recipient in a funds transfer system, according to some implementations.

[0031] FIG. 18B depicts a diagram of a flowchart of a method for securely transferring funds from a sender to an unregistered recipient in a funds transfer system, according to some implementations.

[0032] FIG. 19 depicts a diagram of a data flow for registering a participant in a funds transfer system, according to some implementations.

[0033] FIG. 20 depicts a diagram of a flowchart of a method for registering a participant in a funds transfer system, according to some implementations.

[0034] FIG. 21 depicts an example of a digital device, according to some implementations.

DETAILED DESCRIPTION

[0035] Referring to FIG. 1, a funds transfer system 100 that implements a payment network, or a "funds transfer payment network," is shown. The funds transfer system 100 may be utilized by senders to send funds to recipients and by recipients to receive the funds. The funds transfer system 100 may facilitate the transfer of funds from senders to receivers (e.g., recipients) without either party disclosing any financial account information to each other. The senders and recipients may be individuals or business entities. In the example implementation, the sender uses a bank account as the source of funds. In other implementations, the sender may use credit cards, debit cards, business credit cards or check cards as the source of funds. The funds transfer system 100 may be used for both intrabank transfers (i.e., transfers in which the sender and the recipient both have accounts at the same bank and the funds are transferred between the accounts within the same bank) and interbank transfers (i.e., transfers in which the sender and the recipient have accounts at different banks and the funds are transferred between the accounts at different banks).

[0036] The funds transfer system 100 may include, among other systems, a sender computer system 110, a bank computer system 120, a recipient computer system 130, a bank computer system 150, a payment service computer system 160, and an automated clearing house computer system 170. Each of the above described systems may communicate through a network 140, which may include one or more of the Internet, Cellular network, Wi-Fi, Wi-Max, a proprietary banking network, and so on. In FIG. 1 and throughout the remaining description, for sake of providing an example, it is assumed that the sender performs a funds transfer from an account maintained by the bank computer system 120 and the receiver receives the funds using an account maintained by the bank computer system 150. Hence, the computer system 120 is sometimes referred to herein as the sender bank computer system and the computer system 150 is sometimes referred to herein as the receiver bank computer system. It will be appreciated of course that any given bank computer system may operate in different capacities in the context of different fund transfer transactions. Additionally, while the examples provided herein are primarily in the context of a sender requesting a funds transfer to a recipient, it will also be appreciated that a recipient may request a funds transfer from a sender.

[0037] The sender computer system 110 may be used by an individual user (e.g., a business owner or employee, a consumer, and so on) to create transactions and interact with

banking functions provided through an online banking area of a website provided by the sender bank computer system 120 or through a website provided by a payment service 160. The sender computer system 110 may, for example, comprise a user computer (e.g., desktop or laptop computer), a cellular telephone, smart phone, a mobile handheld wireless e-mail device, a personal digital assistant, a portable gaming device, or other suitable device. The sender computer system 110 may also comprise one or more servers each with one or more processors configured to execute instructions stored in memory. For example, such an arrangement may be utilized if the sender is a merchant or other business.

[0038] The sender computer system 110 may comprise network interface logic 112, a display device 114, an input device 116, and client application 118. Network interface logic 112 may include, for example, program logic that connects the sender computer system 110 to the network 140. As described in greater detail below, for example, the sender computer system 110 may receive and display screens on the display device 114 including account information, transaction instructions, and so on. In an example implementation, such screens may be used to request a username and password information. Such screens may also be used to prompt the user to provide information regarding the amount of the funds and the identity of the merchant or individual that is to receive the funds. Such information may comprise, for example, a name, an address, a phone number, an e-mail address, a selection of a recipient from an electronic directory, and/or other information. Such screens may also include screens displaying information regarding past transactions. Such screens are presented to the user via the display device 114. The input device 116 may be used to permit the user to initiate account access and to facilitate receiving fund transfer request information from the user.

[0039] The client application 118 may comprise program logic (i.e., stored executable instructions) configured to implement at least some of the functions described herein. As will be appreciated, the level of functionality that resides on the sender computer system 110 as compared to other components of the funds transfer system 100 may vary depending on the implementation. The client application 118 may simply be a web browser (e.g., Internet Explorer®, Mozilla Firefox®, Chrome®, Safari®, and so on) configured to receive and display web pages received from the banking computer system 120. The client application may also comprise a mobile web browser, text message (SMS) interface, a dedicated application, or other program suitable for sending and receiving information over the network 140.

[0040] The bank computer system 120 is operated by a bank institution that maintains accounts held by customers, such as demand deposit accounts, credit card accounts, home mortgage loans, student loans, and so on. The bank computer system 120 may, for example, comprise one or more servers each with one or more processors configured to execute instructions stored in memory, send and receive data stored in memory, and perform other operations to implement the operations described herein associated with logic or processes shown in FIGS. 1-7.

[0041] The bank computer system 120 may include network interface logic 122, account processing logic 124, an account database 126, and an information directory 128. The network interface logic 122 may include, for example, program logic that connects the bank computer system 120 to the network 140. The network interface logic 122 may facilitate secure communications between the bank and the sender and/or the recipient. The network interface logic 122 may also facilitate communication with other entities, such as other banks, settlement systems, and so on. The network interface logic 122 may include user interface program logic configured to generate and present web pages to users accessing the bank computer system 120 over the network 140.

[0042] The account processing logic 124 performs account processing to process transactions in connection with the account(s) of the account holder, such as account credits and debits to checking and savings accounts, credits and debits to home mortgage and home equity accounts, credits and debits to student loan accounts, and so on. Thus, whenever funds are transferred into or out of an account of an account holder (e.g., a sender or recipient of funds), the account processing logic 124 reflects an appropriate debit or credit in the account database 126, which stores account information (e.g., transactions, information about the account holder, and so on) for accounts that are maintained by the bank on behalf of its customers. The account processing logic 124 may also process fund transfer requests to transfer funds from a sender using the sender computer system 110 to a recipient using the recipient computer system 130.

[0043] The information directory 128 may be used when an identifier other than a bank account/routing number is used (e.g. an e-mail address, phone number, Universal Payment Identification Code (UPIC), randomly generated number, and so on) to identify a recipient of a funds transfer. The information directory 128 may be a database that is maintained to allow

the financial institution to convert/correlate the recipient's cell phone number (or e-mail address, or other identifier) to a bank account number/routing number of the recipient's bank account. This arrangement allows the sender to uniquely identify the recipient (e.g., with an e-mail address or other identifier), without necessarily having private/personal information regarding the recipient (i.e., the recipient's bank account/routing number).

[0044] Users may register their information with the information directory 128 prior to any financial transaction. A user may be added to the information directory 128 upon registering for the funds transfer system 100 through the bank computer system 120. Upon registration, a new entry may be created for the newly registered user in a database that implements the information directory 128. The user may provide one or more identifiers (e.g., phone numbers, e-mail addresses, and so on) that the user may share with other individuals with whom the user interacts (for example, in the same way that people selectively or freely share phone numbers and e-mail addresses with other individuals for purposes of communicating with such other individuals). Herein, such identifiers are referred to as "public identifiers" or "public tokens." (The terms "identifier" and "token" are used interchangeably herein to refer to a code (e.g., an e-mail address, a phone number, a user generated or system generated character string, etc.) that identifies a user.) The information directory 128 may also generate or otherwise associate an identifier that is securely maintained and that is used to identify the user in the information directory 128. Herein, such identifiers are referred to as "private identifiers." The private identifier may, for example, be a unique ID of the database entry for the user in the information directory 128. While the private identifier is known by the information directory 128, it need not be known by the user with whom it is associated or by other users. However, it may be known by banks and other entities that are members of the funds transfer payment network. In addition to the public identifier(s) (e.g., phone numbers, e-mail addresses, and so on), the private identifier (e.g., database UID), other information may also be stored in the database entry, such as account information (account numbers, routing numbers, etc.) for accounts held by the user at the bank and user preferences. At least some of this information may be populated automatically, e.g., if the user registers for the funds transfer system 100 during a secure on line banking session on the bank computer system 120.

[0045] Additionally, the database entry for each user may also store a registry of other users connected to that user. That is, for each user, a registry may be stored that includes a listing of each other user with whom the user has an established connection. Such connection

may be established, for example, the first time that the user sends or receives funds from the other user. A connection may also be established by way of a user interface that permits a user to add connections with other users through a lookup service in the information directory 128 and/or another information directory. An example of such a user interface is discussed below in connection with FIG. 4. The users may include not only users that are registered in the funds transfer payment network, but also other affiliated payment networks, as discussed in greater detail below. For each user in the registry, additional information may be stored, such as their unique ID and/or other information. As another example, the information for the other users may be stored in separate database entries in the information directory 128.

[0046] In various implementations, a plurality of information directories may exist, each directory maintained by a different institution or entity. For example, users that maintain accounts at the bank associated with bank computer system 120 may register through bank computer system 120, users that maintain accounts at the bank associated with bank computer system 150 may register through bank computer system 150, and so on for other users that maintain accounts at other entities. Such entities may also include non-bank entities (e.g., payment processing companies, credit agencies, credit card network providers, and so on), and users may also register through such non-bank entities.

[0047] In addition to the public and private identifiers that have already been described herein, additional identifiers may also be used. For example, such additional identifiers may be handled with varying levels of security. As another example, variations of existing public identifiers may be used to implement special purpose public tokens, public tokens with customized functionality, and so on, as discussed in greater detail below.

[0048] The token management logic 129 manages tokens. For example, the token management logic 129 may be configured to register tokens, authenticate tokens, generate tokens and so on. The token management logic 129 may also facilitate identification of the recipient when a token is not recognized. The token management logic 129 may also be used to customize attributes of tokens, such that particular accounts are used, particular methods of notification are used, and so on. The token management logic 129 is discussed in greater detail below in connection with FIG. 2.

[0049] The recipient computer system 130 may be configured in generally the same manner as the other computer systems described herein. For example, if the fund recipient is

an individual, the computer system 130 may be a mobile device, such as a cellular phone, smart phone, mobile handheld wireless e-mail device, personal digital assistant, portable gaming device, a desktop computer or other suitable device. The computer system 130 may also comprise one or more servers each with one or more processors configured to execute instructions stored in memory. For example, such an arrangement may be utilized if the recipient is a merchant or other business.

[0050] In one implementation (e.g., where the recipient is a bricks-and-mortar merchant), the recipient computer system 130 may include point of sale devices (e.g., cash register systems) that are equipped to electronically obtain public token information from customers. For example, the cash register systems may be equipped with a near field communication (NFC) reader device that is capable of reading a public token (e.g., cell phone number) from an NFC equipped cell phone. As another example, the cell phone may include an application that is configured to generate a bar code or other image on a display screen that contains the public token, and the cash register system may be equipped with a bar code reader configured to read the bar code. The recipient computer system 130 may then request payment from the sender via the funds transfer system 100 using the public token obtained at the point of sale.

[0051] The recipient bank computer system 150 may be configured in a similar manner as the sender bank computer system 120. Thus, the bank computer system 150 comprises network interface logic 152, account processing logic 154, account database 156, and information directory 158 corresponding to the network interface logic 122, account processing logic 124, account database 126 and information directory 128 of the bank computer system 120.

[0052] The payment service computer system 160 may be associated with a payment service that is configured to facilitate interbank fund transfers, e.g., a payment service provided by a non-bank entity as previously mentioned. The payment service may, for example, be an entity that is formed as a joint venture between banks and/or other entities that send and receive funds using the funds transfer system 100. As another example, the payment service may be a third party vendor. As another example, the payment service may be a web portal provided for an online community of individuals where such individuals obtain user names/login IDs or otherwise become registered members. The individuals may, for example,

use the web portal to interact with each other and/or to interact with a service provided by the online community. Examples of online communities include MSN®, iPhone® users, Facebook®, LinkedIn®, and so on. The payment service may, for example, be an additional service that is offered by the web portal to the members of the online community. As another example, the payment service may be provided by one of the banks, i.e., such that the bank performs both the operations described herein as being performed by the bank computer system 120/150 and the operations described herein as being performed by the payment service computer system 160.

[0053] Herein, the banks associated with computer systems 120 and 150 are assumed to be "member banks" That is, the banks associated with computer systems 120 and 150 are assumed to follow established protocols for transferring funds using the funds transfer system 100. For example, in the context of a payment service that is created as a joint venture, the member banks may include at least the banks that are part owners of the joint venture, as well as potentially other banks. While two member banks are shown in FIG. 1, it will be appreciated that there may be additional member banks. Additionally, as previously indicated, non-bank entities may also be members. The payment service may also be used by senders and recipients that have bank accounts at non-member banks, for example, by permitting such users to register directly with the payment service computer system 160. Hence, users do not need to be customers of any particular bank in order to be able to use the funds transfer system 100.

[0054] The payment service computer system 160 may, for example, comprise one or more servers each with one or more processors configured to execute instructions stored in memory, send and receive data stored in memory, and perform other operations to implement the operations described herein associated with logic or processes shown in FIGS. 1-6. The payment service computer system 160 includes network interface logic 162 and an information directory 168. Although not specifically shown, it will be appreciated that the payment service computer system 160 may include account processing logic and an account database in the same or similar manner to the account processing logic 124, 155 and the account databases 126, 156. The network interface logic 162 may include user interface program logic configured to generate and present web pages to users accessing the payment service computer system 160 over the network 140.

[0055] The information directory 168 may be used when an identifier other than a bank account/routing number is used (e.g. an e-mail address, phone number, Universal Payment Identification Code (UPIC), randomly generated number, and so on). As described above in connection with the information directory 128 and 158, the information directory 168 is a database that is maintained to allow the payment service to convert/correlate the recipient's cell phone number (or e-mail address, or other token) to a bank account number/routing number of the recipient's bank account for users that registered through the payment computer service system 160. This arrangement allows the sender to uniquely identify the recipient (e.g., with an e-mail address or other identifier), without necessarily having private/personal information regarding the recipient (i.e., the recipient's bank account/routing number).

[0056] Users including senders and recipients may register their information with the information directory 168 in advance, e.g., where such users do not bank or have accounts with any of the other member entities. Additionally, the payment service computer system 160 may be configured such that users that only wish to send funds may do so without registering. For example, the payment service computer service system 160 may be configured to generate web pages that receive credit card information from a sender to complete a transaction each time a sender wishes to send funds, without requiring that the sender ever register with the payment service computer service system 160.

[0057] As will be appreciated, the information that is stored in the information directory 168 may vary depending on the implementation, including the extent to which information is also stored in the information directories 128 and 158. For example, in one implementation, when a user registers at the bank computer system 120 (or at the bank computer system 150, or at the computer system of another member entity), information may be stored in both the information directory 128 and the information directory 158. The information directory 128 may store a complete identification of the user's bank accounts and other information collected during registration. Conversely, the information directory 168 may store a reduced amount of information, such as the registered public token(s), the financial institution with it is associated, and the private token (e.g., unique ID) associated with each token. More detailed bank account number/routing number, or other sensitive information need not be stored at the information directory 168. In another implementation, instead of using a payment service computer system 160 to maintain the information directory 168, such information may be stored entirely in the information directories 128, 158 maintained by

individual member banks. As will also be appreciated, the extent to which transaction details are tracked and maintained in the account processing logic 124, 154 as compared to the extent to which transaction details are tracked and maintained by the payment service computer system 160 may vary depending on the implementation.

[0058] The Automatic Clearing House (ACH) system 170 is used to transmit funds to and from bank accounts of the senders and recipients. As is known, the ACH Network is a nationwide batch oriented electronic funds transfer system which provides for interbank clearing of electronic payments for participating depository financial institutions. An ACH entry may start with an account holder (known as the Receiver in ACH terminology) authorizing an Originator (e.g., a person or a company) to issue ACH debit or credit to an account. Depending on the ACH transaction, the Originator must receive authorization from the Receiver. In accordance with the rules and regulations of ACH, no financial institution may issue an ACH transaction (whether it is debit or credit) towards an account without prior authorization from the Receiver. Once authorization is received, the Originator then creates an ACH entry to be given to an Originating Depository Financial Institution (ODFI), which may be any financial institution that does ACH origination. This ACH entry is then sent to an ACH Operator (i.e., central clearing facilities through which financial institutions transmit or receive ACH entries, e.g., the Federal Reserve or the Electronic Payments Network) and is passed on to the Receiving Depository Financial Institution (RDFI), where the Receiver's account is issued either a credit or debit, depending on the ACH transaction. The RDFI may, however, reject the ACH transaction and return it to the ODFI with the appropriate reason, such as that there were insufficient funds in the account or that the account holder indicated that the transaction was unauthorized. An RDFI has a prescribed amount of time in which to perform returns (e.g., two to sixty days from the receipt of the ACH transaction). An ODFI receiving a return of an ACH entry may re-present the ACH entry two more times, or up to three total times, for settlement. Again, the RDFI may reject the transaction, after which the ODFI may no longer represent the transaction via ACH. The above description of ACH system is one in use currently, the implementations of the current invention will continue to function similarly even if some methods and steps in the ACH system are modified.

[0059] Referring to FIG. 2, FIG. 2 shows the token management logic 169 in greater detail. As shown in FIG. 2, the token management logic 169 includes sponsor identification or sponsor searching logic 182, registration logic 184, token authentication logic 186, rules

engine 188, and token generation logic 190. Although the token management logic 169 is shown, it will be appreciated that the token management logic 129 and 159 may be configured in the same or similar manner.

[0060] The sponsor identification logic 182 may be configured to identify a sponsor of a token. For example, if the sender uses a token to identify a recipient that is unrecognized at the information directory 128 of the sender bank computer system 120 (i.e., because the recipient is not a customer of the sender bank), the sponsor identification logic 182 may be configured to receive the token from the sender bank computer system 120 and access the information directory 168 to provide an identification of the unique ID and financial institution associated with that token.

[0061] As will be appreciated, the extent to which the bank computer systems 120, 150 have sponsor identification logic that operates in the same manner as the sponsor identification logic 182 may depend, in part, on the extent to which the information is stored in the information directory 168 as compared to the extent to which information is also stored in the information directories 128 and 158. In various implementations, greater or lesser degrees of reliance may be placed on the information directory 168 to perform user identification functions in a centralized fashion in connection with the transfer of funds between entities. Herein, for sake providing an example, it is assumed that the information directory 168 is used to perform user identification functions in a centralized fashion in connection with the transfer of funds between entities. In such implementations, it may be possible to avoid replicating all the functions of the sponsor identification logic 182 and the bank computer systems 120, 150.

[0062] In one implementation, the funds transfer payment network is configured to interact with other affiliated payment networks (e.g., PayPal, CashEdge, and so on). In such an arrangement, if the token provided by the sender bank computer system 120 is not recognized in the information directory 168, the sponsor identification logic 182 is configured to transmit inquiries to the other affiliated payment networks (e.g., in a predetermined sequence) to determine if the token is recognized at any of the other affiliated payment networks. If the recipient is registered with another payment network, then the funds may be transferred to the recipient by routing the funds through the other payment network. In an implementation where a user lookup service is provided by the information directory 168, the look up service may operate in the same manner to identify users registered at remote entities. Information may

also be stored in the information directory 168 identifying the payment network determined to be associated with that token, thereby facilitating additional funds transfers to that token in the future. Hence, in such an arrangement, funds may be pushed to a recipient that is not registered with the funds transfer payment network but rather that is registered with another payment system. Additionally, such funds may be pushed to the recipient without the sender having to know or be concerned about whether the recipient is registered with the funds transfer payment network.

[0063] The registration logic 184 is configured to facilitate the process of registering new users. For example, in the preceding discussion, if the token is not recognized at the information directory 168, and is not registered at any other affiliated payment network, then the registration logic may be configured to send the recipient an e-mail or other communication inviting the recipient to register with the payment network. Such an e-mail may include a link to the website provided by the payment service computer system 160. The registration logic 184 may be configured to generate web pages for presentation to the user at the website to facilitate the registration process. If, based on information provided by the user when registering at the website, it is determined that the user is a customer of one of the member entities, then the user may be forwarded to the website of the member entity to complete the registration process. As will be appreciated, the registration logic 184 may also present web pages to the user in other scenarios (e.g., where the user has arrived at the website as a result of a search engine query, where the user has arrived at the website via another website (e.g., such as an online community website or merchant website), and so on). The registration logic 184 may create new database entries in the information directory 168 responsive to inputs received from the user.

[0064] The token authentication logic 186 is configured to authenticate tokens. For example, when a user registers a new token, the token authentication logic 186 may be configured to confirm that the user is associated with that token (e.g., that the user who is attempting to register a cell phone number as a token is indeed the owner of that cell phone number). (Herein, the term "own" in the context of telephone numbers refers to the telephone number being assigned to one particular user as opposed to being assigned to other users, and is not being used to refer to ownership as between the user and the phone carrier that provides the telephone number to the user. The term is used analogously in the context of e-mail addresses.) As another example, when a user attempts to register a new e-mail address, the

authentication logic 186 may perform an authentication operation such as sending the user an e-mail at the new e-mail address. The e-mail may, for example, contain a link that must be accessed by the user in order to successfully complete the registration process.

[0065] Additionally, the token authentication logic 186 may be configured to perform authentication operations on previously-registered tokens. For example, a user that registers a cell phone number may ultimately switch cell phone numbers and/or cell phone carriers. The token authentication logic 186 may be configured to process disconnect directories that are published by cell phone carriers and that list cell phone numbers that have been disconnected by that carrier. For example, if a registered cell phone number is listed as having been disconnected, the token authentication logic 186 may send an e-mail to the user at a registered e-mail address to determine whether the cell phone number is no longer a valid token for that user or whether the user has merely changed cell phone carriers but has retained the cell phone number.

[0066] The token authentication logic 186 may also be configured to send follow up communications to the user trying to use a token to send/receive money from another user if there is uncertainty regarding whether the other user is correct owner of the token. For example, the token authentication logic 186 may be configured to notify the sender that such uncertainty exists, request that the sender provide confirm information that was provided regarding the recipient, provide additional information regarding the recipient, and so on. For example, if a user attempts to send funds using the token jsmith@abc-company.com, an e-mail may be sent to the user if there is uncertainty whether ownership of the token jsmith@abc-company.com has changed (e.g., due to a change in employees at ABC Company). The authentication logic 186 may also be configured to access other networks or online communities (e.g., Facebook, LinkedIn, etc.) to obtain additional information that may be used to authenticate the token. The token authentication logic 186 may also be configured to track the changing public tokens by date and time of use and the date and time that a particular recipient ceases to use a particular public token.

[0067] Hence, the registration logic 182 and the authentication logic 184 cooperate to facilitate the registration of tokens and to ensure that the tokens are associated with their correct owners. In one implementation, the entity that registers a token is responsible for warranting the validity of the registration. For example, if the recipient bank registers a token

415-555-1226, and subsequently accepts a payment to the user that registered the token 415-555-1226, then the recipient bank is responsible for refunding money to the sender if the user that registered the token 415-555-1226 is not actually the owner of that cell phone number at the time of the funds transfer (e.g., because the previous owner changed cell phone numbers, and the new owner is on a different payment network). Hence, the recipient bank undertakes responsibility for correctly authenticating the user at the time of registration and for routinely processing disconnect directories to ensure that the authentication remains valid.

[0068] In one implementation, the warranty (and/or limited access to the information directory 168) may be provided as a service to third parties. For example, an on line retailer that is refunding money to a customer may wish to verify that a token previously provided by the customer (e.g., "415-555-1226") remains accurate. If funds are refunded to the customer at the "415-555-1226" token, but the customer no longer owns that token, then the payment service would be responsible for refunding the funds to the correct customer. The fee charged for the service may, for example, be based on the dollar value of liability accepted by the payment service for providing incorrect information. As another example, a service may be provided in which a per token fee is charged for identifying a user based on a token and/or for identifying a token (e.g., e-mail address, cell phone number, etc.) based on an identification of a user.

[0069] The rules engine 188 is configured to permit users to configure different attributes for different tokens. The attributes may be specified in rules that are configured based on user specified preferences. In various implementations, the rules engine 188 may provide a user with default settings that are used until the user decides to customize the rules. For example, the rules engine 188 may be used to configure the manner in which funds are directed to various accounts held by the user at the bank (e.g., to forward at least a portion of the funds or transfer funds into a particular type of account), and so on. As another example, the funds may be split between a plurality of accounts according to the rules specified by the user, e.g., the funds may also be transferred into at least one of a retirement account, savings account, PayPal® account, or a certificate of deposit. As another example, portion of the received funds may be forwarded to a different user that is registered with the payment network. As another example, the rules engine 188 may be used to configure the manner in which a notification is sent to a recipient informing the recipient that a fund transfer request has been made by a sender. For example, according to one implementation, the rules may be

configured to specify the channel(s) by which notifications are sent (e-mail, text message, voicemail, and so on), the e-mail account(s) and/or phone number(s) to which notifications are sent, and so on. As another example, if the fund transfer amount is greater than a threshold value, the user may receive an automated telephone call instead of an e-mail message or may receive an e-mail/telephone call instead of no message. As another example, if the fund transfer request originated from a particular sender, then the user may specify the mode of the notification (e.g., e-mail, voicemail, or text message). As another example, the rules engine 188 may be used to configure the payment channel used to send funds to a recipient (e.g., ACH transfer, credit card network, PayPal network, printed and mailed check, and so on). As another example, the rules engine 188 may be used to configure the speed with which funds are transferred to the recipient (e.g., instantaneous, same day, overnight, 2-day payment, and so on). As another example, the rules engine 188 may be used to configure transaction limits (e.g., to ensure that no more than $500 can be charged to a particular token during a predetermined time period such as one day, one week, one month, etc.).

[0070] The token generation logic 190 may be configured to generate additional public tokens for a user. The token generation logic 190 may cooperate with the rules engine 188 to create different tokens that are configured with different attributes. For example, a business may wish to use different individual tokens depending on whom within the business is responsible for processing a particular transaction. For example, a recipient that is a landlord that owns several apartment buildings may wish to create different tokens for each apartment building. For example, the additional tokens may be based on user provided alphanumeric character strings, may be system generated based on pseudo random character strings, or may be generated in another fashion. For example, if the landlord recipient already uses an e-mail address as a public token (e.g., landlord@mail.com), the additional public tokens may be variants of the public token already used by the recipient (e.g., landlord@mail.com/building1, landlord@mail.com/building2, landlord@mail.com/building3 and so on). Such tokens may then be configured with different attributes using rules engine 188. For example, if each of the different buildings has a different building manager, then an e-mail may be sent to an e-mail address of the respective building manager for a particular apartment building when a tenant of that apartment building pays rent.

[0071] As another example, the landlord recipient may provide each tenant with a different public token for use by the tenants to pay rent. Again, for example, the additional

tokens may be variants of the public token already used by the recipient (e.g., landlord@mail.com/unit101, landlord@mail.com/unit102, landlord@mail.com/unit103 and so on). The bank computer system 150 may then receive funds from each tenant and all the funds may be transferred to one or more accounts belonging to the landlord. The account processing logic 154 may be configured to generate a report showing the funds received in connection with each token (thereby showing, for example, which tenants have paid in a given month and which tenants have not paid in a given month). Tokens may also be programmed with additional information, for example, the amount of the expected monthly payment. The account processing logic 154 may then be configured to compare the amount actually received with the expected monthly payment to ensure that the tenant has paid completely and to track overall account status of the tenant.

[0072] As another example, a recipient may also configure single use tokens. For example, a recipient may be organizing an event in which other users are expected to financially contribute to the event. The recipient may then configure a token (e.g., johnsmith@mail.com/moms-birthday-party) which may be provided to the other users. The account processing logic 154 may then generate a report showing the funds that have been received from various ones of the other users in connection with that token.

[0073] As another example, senders may also configure different tokens. For example, a sender may use a first token as their default token (e.g., johnsmith@mail.com), and create additional special purpose tokens where payment is to be made from other accounts (e.g., johnsmith@mail.com/collegesavings to make a tuition payment from a college savings fund).

[0074] As another example, as previously indicated, the information directories 128, 158, 168 may provide a lookup service that may be used by users to establish connections with other users. In such an implementation, users may be able to configure aspects of their tokens that are displayed to other users. For example, if an individual is operating a business under another name (e.g., Joseph Smith DBA "Joe's Lawn Service"), it may be desirable to permit the user to configure the token such that the business name is displayed to other users, even though the name on the account is actually the individual's name. In this manner, it may be easier for customers of the business to establish a connection with the business.

[0075] Referring to FIGS. 3A and 3B, FIGS. 3A and 3B illustrate a process in which the funds may be received by a registered or unregistered recipient according to an example

implementation. In FIGS. 3A and 3B, a fund transfer message is received from a sender at the sender bank computer system 120 and propagates to the recipient bank computer system, where it causes funds to be deposited in to the account of a recipient. Specifically, at step 301 in FIG. 3A, the sender bank computer system 120 receives a fund transfer request from a sender which identifies the recipient using a token. At step 311, the bank computer system 120 searches the information directory 128 to determine whether the token is associated with a user that is registered with the sender bank (i.e., a transfer within the same bank). If the token is associated with a user registered with the sender bank then, at step 313, the recipient's account information is retrieved from the information directory 128. Subsequently, at step 315, the funds are transferred to the recipient's account. The funds may be transferred to the recipient's financial account based on preferences of the sender and the recipient, as discussed in greater detail below in connection with FIGS. 4 to 6.

[0076] If, at step 311, the recipient is not registered with the sender bank, then the process proceeds to step 321. At step 321, the bank computer system 120 transmits an inquiry to the payment service computer system 160, and it is determined if the token is associated with a user that is registered at another member entity of the funds transfer payment network. For example, if it is the first time that the sender has transferred funds to this particular recipient, then the bank computer system 120 may transfer the public token of the recipient as provided by the sender. In this scenario, the sponsor identification logic 182 may perform a search of the information directory 168 to determine if the token is associated with a user that is registered with another member entity. If the public token is located in the directory, then the payment service computer system 160 may return the unique ID associated with the public token along with an identification of the financial institution or other member entity with which it is associated to the sender bank computer system 120. The sender bank computer system 120 may then create another registry entry for the sender, and store the public token and the unique 1D of the recipient as part of the registry entry. The sender bank computer system 120 may also prompt the sender to provide other information about the recipient (e.g., a nickname or other name by which the sender wishes to identify the recipient).

[0077] As another example, if the sender has transferred funds to this recipient previously, then the bank computer system 120 may transfer the unique ID of the recipient to the payment service computer system 160. In this scenario, the sponsor identification logic 182 may use the unique ID as an index to the database that implements the information

directory 168 to locate the recipient in the information directory 168. Assuming the unique ID is still valid and is still located in the information directory 168, then the payment service computer system 160 may return the financial institution or other member entity with which it is associated to the sender bank computer system 120. As another example, if the sender has transferred funds to this recipient previously, then the bank computer system 120 identifies the member entity with which it is associated based on the unique ID itself (e.g., where the unique ID is embedded with information that identifies the financial institution). At step 323, the sender's registry is updated to include an entry for the recipient, including the unique identifier of the recipient. At step, 325 the funds are transferred to the member entity (e.g., the recipient bank in the example of FIG. 1) for deposit along with the unique ID of the recipient. Based on the unique ID, the information directory 158 may be accessed by the recipient bank computer system 150 to identify the account number of the recipient. The funds may then be deposited in the bank account of the recipient.

[0078] If, at step 321, the recipient is not a user that is registered at another member entity of the funds transfer payment network, then the process proceeds to step 331 illustrated in FIG. 3B. At step 331, the sponsor identification logic 182 of the payment service computer system 160 transmits inquiries to other payment networks (e.g., PayPal®, Star, Blink, Interlink, Plus, etc.), and it is determined if the token is associated with a user that is registered at another payment network. For example, the sponsor identification logic 182 may transmit an inquiry to a first payment network to inquire whether the recipient is registered at that payment network. If not, the sponsor identification logic 182 may continue to transmitting additional inquiries to other affiliated payment networks until the payment network at which the recipient has registered an account is identified. At step 333, if the recipient is registered with another payment network, information may also be stored in the information directory 168 identifying the payment network determined to be associated with that token, thereby facilitating additional funds transfers to that token in the future. Next, at step 335 the funds may be transferred to the recipient by routing the funds through the other payment network. Hence, in such an arrangement, funds may be pushed to a recipient that is not registered with the funds transfer payment network without the sender having to know or be concerned about whether the recipient is registered with the funds transfer payment network.

[0079] If, after the search of other payment networks is completed, no other payment network is identified at which the recipient is registered, then the recipient is presumed to not

be a registered user of any payment network. Accordingly, at step 341, an invitation is sent to the recipient to invite the recipient to join the payment network. For example, if the token used by the sender is an e-mail address, then an e-mail is sent to the recipient informing that another user is attempting to transfer funds to the recipient and inviting the recipient to join the payment network. A link in the e-mail may, for example, deliver the recipient to the website provided by the bank computer system 120. As another example, if the token used by the sender is a cell phone number, the recipient may be sent a text message containing a URL inviting the recipient to join the payment network. As will be appreciated, the recipient may be sent such an invitation in other situations, e.g., if the recipient is not a registered user of the funds transfer payment network, even if the user is a registered user of another payment network.

[0080] At step 343, the recipient may be prompted to provide account information. At step 351, based on the account information, it may be determined whether the user is a customer of one of the member entities. For example, a bank routing number for a demand deposit account may be used to determine whether the user is a customer of one of the member entities. If the recipient is a customer of a member entity, then at step 353 the recipient may be transferred to the member entity for registration (e.g., the recipient bank in the example of FIG. 1). A unique ID is associated with the recipient in the information directory 158 of the recipient bank computer system 150 and in the information directory 168 of the payment service computer system 160. At step 355, the sender's registry is updated to include the recipient, including the unique identifier of the recipient. At step 357, the funds are transferred to the recipient.

[0081] If the recipient is not a customer of a member entity, then at step 363 the recipient is registered by the payment service computer system 160. At step 365, the sender's registry is updated to include an entry for the recipient, including the unique identifier of the recipient. At step 367, the funds are transferred to the recipient. As will be appreciated, if the recipient has customized fund transfer preferences, the fund transfer may be processed by the rules engine 188 according to the recipient preferences. Examples of token customization to reflect such preferences were previously described above in connection with rules engine 188 and token generation logic 190.

[0082] FIG. 4 is a screen shot of a web page 400 that may be provided to a user when the user selects a preferences tab. The web page 400 may be used to configure preferences in connection with the token management logic 129, 159 or 169 (depending on where the user registered for the payment network). Web page 400 includes a plurality of fields including a default notification settings field 401, a manage connections field 411, and a manage recipients field 431. The default notification settings field 401 presents the user with information regarding the current default notification settings for a funds transfer event. As shown in the screen shot in FIG. 4, notification settings field 401 may include settings to specify a telephone number to which automated telephone call notifications or text message notifications should be sent (field 403) and an e-mail address to which e-mail notifications should be sent (field 405). The user may also be permitted to specify the name on the account (field 407) as it should appear to other users when the other users receive a funds transfer notification. The information specified in field 407 may also be used in other situations, for example, when other users are searching for connections through a lookup service in information directory 128, 156, 168. The user may configure the rules engine 188 to notify the user regarding transactions based on the user preferences received from the user prior to the occurrence of the transactions. If the user fails to configure customized notification settings, default notification settings may be used. In various implementations, a user may choose different/custom notification settings for each token that the user has registered.

[0083] In the example shown in FIG. 4, the telephone number that may receive a call, text message or voice message, upon the occurrence of a predetermined event is 949-555-7878. Additionally, the e-mail address that may be used to notify the user that a fund transfer has occurred from or to the user's accounts is pat@mail.com. The user may choose to be notified by e-mail or telephone or both.

[0084] The token field 413 may display a particular token that the user has registered or is in the process of registering. The status field 415 may display whether the token has been verified/unverified or is active/inactive. The receiving money field 417 is derived in part on the information in the status field and indicating whether a particular token is currently available for sending/receiving money. For example, for the inactive phone number (i.e., 650-555-5555), the user may send/receive funds using this token for connections established prior to the token becoming inactive. However, the user cannot establish new connections with other users based on this token. For example, this may be a mobile number that was

previously owned by the user. Because a unique ID serves as the basis for funds transfers after a connection has been established, previously established connections are still valid (because they are based on the unique ID and not the mobile number), however, new connections are not permitted to be established (because another user may now be using the token).

[0085] The account number field 419 may display the type of account and a partial account number of an account that is associated with the token in field 413. Hence, funds sent/received using the token specified in field 413 are withdrawn from/deposited to the account specified in field 419. If an account number is not associated with the e-mail address or the mobile number in field 413, then the account number field 419 may display a message such as "account is not specified." The notification field 421 may indicate whether the default notification settings specified in field 701 are to be used for notifications or whether other/customized settings are to be used.

[0086] Actions field 423 may include various links that allow the user to take various actions. For example, links may include, edit, remove, and verify. If the status of a token is verified, then the edit field allows the user to edit attributes of the token as specified in the rules engine 188. For example, the accounts and notification preferences (fields 719 and 721) may be edited in greater detail. If the account number is verified, then the remove link may also be displayed. if the account is unverified or inactive, a verify link that sends an e-mail or a SMS and displays a verification code may be displayed. An edit and remove link may also be displayed for unverified or in active e-mail or telephone numbers. The user may also add new tokens using new connections link 425.

[0087] As will be apparent from fields 401 and 411, separate payment and notification channels may be used for funds transfers. For example, for the 415-555-4001 token, the payment channel occurs through the 415-555-4001 token, however, the notification channel occurs through the 949-555-7878 and pat@mail.com tokens. Additionally, if the user decides to set a custom notification channel for the 415-555-4001 token, the user can do so without disrupting connections that have already been established using the 415-555-4001 token. Disrupting one channel (e.g., by changing the token) does not impact the other channel.

[0088] The manage connections field 431 allows a user to perform various functions related to managing the user's connections with other users. Field 431 shows a registry of connections that have been established by a user. Within field 431 various information may be

displayed regarding each other user, for example, name (field 433), nickname (field 435), e-mail/mobile (field 437), status (field 439), and actions (field 441) and a link that allows a user to add new recipients 443. Although not specifically shown, it will be appreciated that a unique ID may also be stored for each of the users in the registry shown in field 431. As previously indicated, the unique ID need not be known by the user and is maintained more securely.

[0089] The name field 433 may be the name of the recipient as it appears on the account associated with the other user (e.g., as specified by the other user). The nickname field 435 may be a nickname assigned to the other user (e.g., as specified by the user). The e-mail/mobile field 437 may display the public tokens that are being used by the recipient. The status field 437 may display whether a permanent connection has been established for a particular contact. Actions field 441 may be determined based on the status field. For example, if a link has been established, then the actions field 441 may display a link that allows a user to send money to the recipient. If a link has not been established, then the actions field may display a send money link, but the actions field 441 may also display a view details link. The view details link may display another screen to the user where the user may provide further details to establish a connection with a recipient. Other actions that may be displayed are edit and remove. Edit may allow the user to edit each field discussed above and remove may allow a user to remove a recipient and related information from the user's registry. A link 443 may be used to add additional users to the registry, e.g., via a search of information directories 128, 158 and/or 168.

[0090] In an example implementation, the manage connections field 431 may present a message to the user that informs the user when another user is no longer the owner of a token. The message may include a link that allows the user to update the token information. In other implementations, if the other user's information has changed, then the message presented by the manage connections field 431 may allow the user to update the outdated information.

[0091] FIG. 5 is a screen shot of a form that allows a user to update default or custom notification settings. In FIG. 5, the user is provided with a list of e-mail addresses associated with the user's account. The user may use a checkbox to indicate which e-mail address should receive a notification. For example, the user in the screen shot shown in FIG. 5 has chosen e-mail address "psmith@google.com" by placing a check mark 505 in the appropriate field. In

other implementations, a user may choose multiple e-mail addresses instead of choosing a single e-mail address. Also shown on the screen shot are telephone numbers associated with the user accounts. The user may use a check mark 509 to select a phone number that receives a notification. In other implementations, the user may choose multiple telephone numbers and multiple e-mail addresses for notification. A link 511 may allow the user to add e-mail addresses or telephone numbers to the account information maintained by the bank. In one implementation, the user may select the link and the user may be automatically taken to a web portal provided by a banking institution. The user may click on save button 513 to save the notification changes implemented by the user.

[0092] FIG. 6 shows a screen shot of a web page 600 that may be presented to a user when the user selects the send money tab. The web page 600 may include a send money field 601 that the user may fill out to send money to a chosen recipient. The web page 600 may include a display of various payment channels 619 that are available to the user. The web page 600 may also include a field 630 showing details regarding recent transactions that are pending, returned or completed.

[0093] The send money form 601 may prompt the user to choose a recipient from a pull down menu 603. The list of recipients presented using menu 603 may be populated using the list of recipients contained in field 431 discussed in FIG. 4. The list of recipients menu 603 may contain the names of users that the user has sent funds to or received funds from in the past or that have been added in another manner. In one implementation, the recipients may be identified by the nicknames assigned to each recipient. Since the nicknames may be directly correlated with the unique ID within the token management logic 129, the account information may be derived from the nicknames via the unique ID. Hence, as previously indicated, the connection between the two users is not disrupted when a cell phone number or e-mail address becomes obsolete. After choosing the recipient, the user may choose an account from which funds may be sent to the recipient using a drop down menu 605. The drop down menu may be pre-populated with a list of all accounts that are held by the user. The user may enter a dollar amount that the user would like to transfer to the recipient in the amount field 607. The user's name may be presented with an optional field description 609 that may allow the user to ascertain that the payment was for a particular product or service provided by the recipient. Another field may be auto-populated with the user's name as the sender of the funds. A nickname field 611 is also displayed if the recipient knows the user by a name that is different

than the user's name as it appears on the user's account. The send money form 601 also displays links that allow the user to add recipients 615, manage recipients 617 and edit the current notification preferences 613.

[0094] The payment channels form 619 presented to the user may allow the user to choose various payment channels such as, credit card, ACH or PayPal®. Also displayed with each payment channel may be the funds available to recipient field 623. For example, the credit card method may make the funds available to the recipient within 2-days of processing the send request. However, the user may be charged a fee as indicated by field 625, for example, $5.00. In other examples, a user may choose ACH in field 621, however the funds may be available to the recipient in 4 days with no fee. Other payment channels, such as PayPal®, Star, Blink, Interlink, and Plus may also be presented to the user.

[0095] Field 630 shows a few of the most recent transactions that the user has performed. Additional recent transactions may be displayed via selection of a link to view more transfers and/or by selecting the transfer activity tab. Field 630 may display various fields that include information regarding the transactions. For example, such fields may include a date sent field 633, from account field 635, recipient field 637, amount field 639, description field 641, status field 643 and actions field 645. The date sent field 633 lists the date when the user initiated the send request. The from account field 635 may display the type of account (i.e. checking, savings, or money market) and a partial account number. The recipient field 637 may display the full name of the recipient. The amount field 639 displays the dollar amount sent to the recipient. The description field 641 displays the description that was entered by the user while processing the request. The status field 643 may inform the user whether the fund transfer is pending, returned or not processed, or has been completed. The actions field 645 may display a link that allows a user to view more details regarding the current status of the fund transfer.

Out-Of-Network Payments

[0096] In an alternative implementation to FIGS. 3A and 3B, a sender may be able to send funds to a recipient who is not a registered user of any member of any payment network—either the funds transfer payment network or other existing payment networks. For example, a user at a participating bank (i.e., sending bank) through the sending bank's online interface, enters a token (e.g., cell phone number or email address) for a desired recipient and a

dollar amount desired to be sent to the recipient. The dollar amount and the token are then sent to the funds transfer payment network for matching services. Because the recipient is either out of the funds transfer payment network or not part of any known payment network, or both, the funds transfer payment network fails to match the token in the payment network's directory. In response, the funds transfer payment network sends a message to the sending bank indicating that the token is unknown. The funds transfer payment network also creates a pending payment, which may include some or all of the following fields: unknown token, sending bank, dollar amount, user name, and recipient name.

[0097] The sending bank then sends a message to the recipient using the token. For example, the sending bank may send a message to the recipient that the sender wants to send the recipient money. Alternatively, the funds transfer payment network sends the message to the recipient. If the recipient is not a registered user of any member of any payment network, the recipient is directed to a link to the website of the funds transfer payment network to begin the process of registering to receive the pending payment. If the token entered by the sender is the recipient's email address, the recipient receives the link at his or her email address. If the token entered by the sender is the recipient's cell phone number, the recipient receives the link at his or her cell phone number.

[0098] FIG. 7 shows a screen shot of an example web page 700 that may be presented to a recipient upon accepting an invitation in a link. As indicated in FIG. 7, the recipient is prompted to enter the token where the recipient was notified about the pending payment. The user enters the token in the field in web page 700. The funds transfer payment network matches the entered token to a pending payment. In one implementation, the recipient can only proceed if the entered token matches an unknown token for a pending payment.

[0099] In one implementation, a recipient who is not registered with any member of the funds transfer payment network can only join the funds transfer payment network and receive funds if a registered sender invites that non-registered recipient. The information and account ownership of the recipient may be validated and collected before the recipient can even join the funds transfer payment network. Thus, it should be appreciated that the funds transfer payment network may verify that a payment is pending before a non-registered out-of-network recipient can join the funds transfer payment network. Herein, "out-of-network" refers to users of financial institutions that are not members of the funds transfer payment network.

Alternatively, "out-of-network" may also refer to financial institutions that are not members of the funds transfer payment network. An in-network user must send an out-of-network user a payment before the out-of-network user can join the funds transfer payment network. This may prevent fraud by ensuring that all users or entities involved in a transaction can be verified. Additionally, because out-of-network users must be invited to the funds transfer payment network by in-network users, fraud and fraudulent transactions are further reduced or eliminated.

[00100] Once the recipient is registered with the funds transfer payment network, the funds transfer payment network may send the recipient's bank account information to the sending bank to complete the initiation transaction. The transaction may be completed via ACH, for example. As is known in the art, ACH transactions may be a "pull" transaction or a "push" transaction. When an in-network user sends money to an out-of-network user, the sending bank may use a push transaction.

[00101] Once the recipient is a registered user of the funds transfer payment network, the funds transfer payment network and funds transfer system 100 may maintain information about the recipient in an out-of-network database. FIG. 8 illustrates an example funds transfer system 800. Funds transfer system 800 is similar to funds transfer system 100, except that the payment service computer system includes an out-of-network database 167. The out-of-network database 167 may store information collected during a financial transaction involving out-of-network users. For example, the funds transfer payment network may perform a funds transfer to an out-of-network user and may store bank information about the out-of-network recipient in the out-of-network database 167. In one implementation, the funds transfer system 800 may store token and bank account information for out-of-network users in the out-of-network database 167.

[00102] In an alternative implementation, the funds transfer system 800 stores bank account information for out-of-network users in the out-of-network database 167, but does not store token information for out-of-network users in the out-of-network database 167. Instead, the funds transfer payment network associates the recipient with a private identifier as described above. The private identifier may be stored in information directory 168. Alternatively, the private identifier may be stored in information directory 128, or information directory 158. Thus, the user's token information is stored in a separate directory, e.g.,

information directory 168, from the out-of-network database 167, and a user's bank account information is stored in the out-of-network database 167. It should be appreciated that this alternative implementation increases user security by not storing a user's token and a user's bank information in the same database. It should also be appreciated that no publicly available information is stored with a user's bank information, thereby reducing the risk of fraud or theft. Thus, the funds transfer payment network can securely process payments and transactions for out-of-network recipients by using a private identifier to match a recipient's token to the recipient's bank information.

[00103] In one implementation, information directory 168 does not store bank account information. Although the out-of-network database 167 is shown outside of payment service computer system 160 in FIG. 8, in one implementation, the out-of-network database 167 may reside inside payment service computer system 160.

[00104] In future transactions involving the recipient, the funds transfer payment network utilizes the out-of-network database 167 to facilitate the transfer funds of funds from a member. FIG. 9 is a flow diagram illustrating an example process 900 for facilitating payment or transfer of funds to an out-of-network recipient, according to an example implementation of the present invention. Although the process 900 is described with reference to the flow diagram illustrated in FIG. 9, it will be appreciated that many other methods of performing the acts associated with the process 900 may be used. For example, the order of many of the blocks may be changed, certain blocks may be combined with other blocks, and many of the blocks described are optional.

[00105] To pay funds to an out-of-network recipient whose information is already stored in out-of-network database 167, data may flow between a sender computer system 110, a funds transfer payment network that uses or implements payment service computer system 160, including out-of-network database 167, and recipient computer system 130. A sender may wish to send funds to a recipient using a token, as shown in block 902. The sending bank sends the token and dollar amount to the funds transfer payment network. The funds transfer payment network notes that the token is for an out-of-network recipient, as shown in block 904, and sends a message to the sending bank indicating the recipient is an out-of-network recipient, as shown in block 906. The sending bank may send a confirmation to the funds transfer payment network to continue the transaction, as shown in block 908. Upon receiving

confirmation, the funds transfer payment network accesses the separate out-of-network database 167, as shown in block 910. The funds transfer payment network matches the token to the recipient's bank information stored in out-of-network database 167, as shown in block 912. The funds transfer payment network encrypts the receiving bank account information and opaquely sends the recipient's bank account information to the sending back, as shown in block 914. The sending bank decrypts and sends the recipient's bank account information and any other information required to complete the transaction to ACH 170.

[00106] The funds transfer system 100 also allows communications to non-customers of a financial institution. For example, once a bank is a member of the funds transfer payment network, that bank may be able to send messages to users who are not customers of that bank. Thus, the funds transfer payment network can behave as a communications intermediary. For example, when a new user is prompted to sign up to register with a member entity, that user may be presented a screen that expressly gains approval to send that user messages. In other words, the user must agree in one implementation to receive messages from members as a condition of joining the funds transfer payment network and the funds transfer system 100. Therefore, once a user is signed up, that user can be contacted by other members.

[00107] In one implementation, financial institutions who are members of the funds transfer payment network are able to send, receive and request funds on behalf of their customers to non-customers. Thus, it should be appreciated that a financial institution that is a member of the funds transfer payment network can help its customers do business with other entities who are not customers of that financial institution.

[00108] In one implementation, the funds transfer system 100 may track the status of payments and provide notifications to a sender and recipient as to the status of payments.

[00109] In one implementation, information is encrypted by a sender bank and decrypted by a receiver bank so that the payment network does not have access to any of the sender or receiver information. For example, the sender bank may use an encryption algorithm that is known by the receiver bank but is not known by a funds transfer payment network. In this case, the sending bank encrypts the account information before any information is given to the payment network. The payment network processes the information, including transferring encrypted sender and receiver information to the receiving bank. The receiving bank knows how to decrypt the encrypted information. In this manner the payment network cannot access

any information being communicated by one bank to another bank. The entire transfer of funds is thus opaque to the funds transfer payment network.

[00110] In one implementation, the funds transfer system 100 relies on the banks' existing fraud systems to manage risks. In one implementation, the payment system does not actually move any money from one entity to another or one bank to another. There is no account owned by the payment service that can even hold money, even for a temporary period of time. The payment system in one implementation only facilitates the transfer of money from one bank to another bank.

[00111] In one implementation, the funds transfer system 100 or funds transfer payment network may send a payment from an out-of-network user to an in-network user. The funds transfer payment network may create a separate out-of-network database for storing information about the out-of-network sender or utilize an existing database.

[00112] In one implementation, a user of a member bank may be able to present a bill or invoice using the funds transfer system 100. The bill may be presented to a consumer of a product or service provided by the user of the member bank. The consumer may be an in-network user or an out-of-network user. A bill presentment may include an electronic file, e.g., an Adobe PDF® document, a Microsoft Word® document, a text file, an image file or any other suitable document that displays a bill to the consumer. The electronic file, e.g., an Adobe PDF® document, may include terms for payment provided by the biller. In one implementation, the funds transfer system 100 may present other items besides bills, such as mortgage documents, business documents, subpoenas, or patent filings or applications, for example.

[00113] The funds transfer system 100 may also be used to securely present documents where the bank verifies the identity of the consumer receiving the documents. The sender can also use the bank to verify receipt of the documents. In one implementation, the biller can track whether the consumer has received the bill. For example, the biller may receive a notification from the funds transfer system 100 that the consumer received the bill. The sender may also be able to confirm that the consumer viewed the bill, e.g., opened or accessed the electronic file on a computer or mobile phone. It should be appreciated that receipt verification or tracking is useful because the biller can confirm, and the consumer cannot deny, that the consumer received the bill.

[00114] For an in-network bill presentment, the biller sends a request for money, or a bill or invoice, to the funds transfer payment network. The request or the bill includes a token identifying the recipient of the bill, or the consumer. The biller appends a request ID to the payment ID and sends the bill to the funds transfer payment network. The biller may also be able to add payment instructions to the bill. The funds transfer payment network routes the bill or invoice to the consumer based upon the token. The consumer responds by paying. The funds transfer payment network then notifies the biller of payment. A payment ID is sent to the bank and is then matched to the account. It should be appreciated that the biller or the biller's bank does not need to have the routing and account number of the consumer, thereby increasing security and convenience for the consumer and the biller.

[00115] For out-of-network consumers, instead of sending a payment ID with a request ID, the funds transfer payment network provides instructions to the billing bank to debit an account. The funds transfer payment network also provides the consumer's ACH information plus the payment ID, plus the request ID to the biller's bank to debit.

[00116] In one implementation, an out-of-network user may be able to send payments to a member bank customer even if the member bank customer did not send a payment request to the out-of-network user. Thus, registered out-of-network users, i.e., users who appear in the out-of-network database 167, can send money to a customer of a member bank. The member bank customers can receive money using that member bank customer's channel of choice. It should be appreciated that the member bank customer does not have to provide perceived confidential information, such as bank account numbers, to out-of-network users from whom they want to receive money. The funds transfer system 100 may be used for debit accounts, electronic funds transfers, credit card transactions, Amazon® payments, payments that are facilitated simply via electronic mail, business to business or merchant payments, expedited payments and scheduled payments, such as for rent, a housekeeper, or a weekly babysitter. In one implementation, the funds transfer payment network verifies account access via trial deposits. The sender gives amounts of transactions and the funds transfer system 100 verifies that the out-of-network sender has access to an account and has authorized the debit transaction.

[00117] In one implementation, the out-of-network users sending money may be subject to send limits. The send limit amounts may be for per day, per rolling seven-day or per rolling

30-day time periods. The send limits may be enforced for each out-of-network user regardless of the destination of the payments. If an out-of-network user attempts to send a payment exceeding a send limit, the funds transfer system 100 may inform the out-of-network user that the payment exceeds the send limit. In one implementation, the funds transfer payment network can impose transaction fees when an out-of-network user sends money to a customer of a member bank.

[00118] The decision to accept and execute a money transfer from an out-of-network consumer who wishes to send money may be managed by the member bank, i.e., the bank of the in-network user receiving the money. As described above with respect to the out-of-network database 167, out-of-network users must enroll for the out-of-network service before being able to send money to a member bank customer. Thus, it should be appreciated that an out-of-network user who is registered may be able to both initiate a payment to a registered customer of a member bank and respond to a request for money (e.g., a bill) from a customer of a member bank.

[00119] The debit transactions from an out-of-network user's bank account may be originated via ACH rails by the member banks. In one implementation, the member bank requires at least one of the following to process a transaction via ACH rails: sender name, transaction amount, transaction fee, recipient profile ID, recipient name as provided by the sender, payment memo, initiation date, bank account number, routing number, and an account type, e.g., checking or savings. When an out-of-network user sends money to an in-network user, the sending bank may use a pull transaction.

[00120] For security purposes, in one implementation, out-of-network users may not be allowed to initiate requests for payments and may also not be allowed to send payments to other out-of-network users. It should be appreciated that these features prevent fraud and also encourage financial institutions to join the funds transfer payment network.

[00121] FIG. 10 is a flow diagram illustrating an example process 1000 for facilitating payment or transfer of funds from an out-of-network sender to an in-network recipient, according to an example implementation of the present invention. Although the process 1000 is described with reference to the flow diagram illustrated in FIG. 10, it will be appreciated that many other methods of performing the acts associated with the process 1000 may be used. For

example, the order of many of the blocks may be changed, certain blocks may be combined with other blocks, and many of the blocks described are optional.

[00122] To send funds from an out-of-network sender whose information is already stored in out-of-network database 167 to an in-network recipient, data may flow between a sender computer system 110, a funds transfer payment network that uses or implements payment service computer system 160, including out-of-network database 167, and recipient computer system 130. A sender may wish to send funds to a recipient using a token, as shown in block 1002. The sending bank sends the token and dollar amount to the funds transfer payment network. The funds transfer payment network notes that the request is from an out-of-network sender as shown in block 1004. The funds transfer payment network may verify account access using trial deposits, as shown in block 1006. The funds transfer payment network sends a message to the receiving bank indicating the sender is an out-of-network sender, as shown in block 1008. The receiving bank may send a confirmation to the funds transfer payment network to continue the transaction, as shown in block 1010. Upon receiving confirmation, the funds transfer payment network accesses the separate out-of-network database 167, as shown in block 1012. The funds transfer payment network matches the sender to the sender's bank information stored in out-of-network database 167, as shown in block 1014. The funds transfer payment network encrypts the sending bank account information and opaquely sends the sending bank's account information to the receiving back, as shown in block 1016. The receiving bank decrypts and sends the sender's account information and any other information required to complete the transaction to ACH 170.

Expedited Payments

[00123] In one implementation, a sender may be able to make a "real time" or expedited payment of funds to a recipient. It should be appreciated that a payment may be considered to be "real time" if the paid funds are made available to the recipient much quicker than payments are typically made available. For example, a payment may be considered to be near real time if the funds are deposited in the recipient's account within a few minutes. In one implementation, a payment may be considered to be real time if funds from a sender to a recipient are deposited in the recipient's account in the amount of time required to send a message from the sender's bank to the recipient's bank. Messages may be sent between the

sending bank, the funds transfer payment network and the recipient bank via a messaging service, such as, IBM® WebSphere MQ.

[00124] Some systems attempt to provide real time payments, however they require leveraging debit card systems, which can be inconvenient. Other systems utilize the ACH system, which may take several days to process and does not provide the speed of the real time or expedited payments presently disclosed. Other systems require that the sender create an account with some alternative payment provider. Yet other systems require having a direct connection to a financial institution's core processing platform.

[00125] Still other systems allow making quick payments from the sender's credit card. The funds transfer payment network allows sending funds in real time from the sender's financial institution, such as the sender's primary financial institution, to the recipient. It should be appreciated that sending funds from the sender's primary financial institution may allow the sender to centralize his or her financial transactions and more easily and conveniently manage his or her money. A sender could use any number of financial institutions, and could send/receive money from any of them as long as each financial institution is a member of the funds transfer payment network and the sender uses a different token (e.g., email address, phone) at each financial institution.

[00126] Other systems allow quick payments when the sending bank is the same as the recipient bank. The funds transfer payment network enables real time payments from a sender to a recipient even when the sender and recipient use different banks. The funds transfer payment network can work with any core financial institution's system through a system of APIs, and does not require a direct connection to a financial institution's core processing platform. The funds transfer payment network could alternatively work with non-bank financial institutions such as, for example, brokerage houses or investment companies.

[00127] In one implementation, the sending and recipient banks are both in-network banks. The sending bank and the receiving bank may be required to agree to offer real time payments to each other before a real time payment can be made. For example, the funds transfer payment network may provide a real time payment service to the sending bank and the recipient bank, in which the banks agree to facilitate real time payments to each other. The funds transfer payment network may additionally or alternatively require that before becoming a member bank, a bank must agree to send and receive real time payments from other member

banks. Individual users may also sign up with their respective financial institutions to be able to send and/or receive expedited payments for a service fee.

[00128] FIG. 11 is a flow diagram illustrating an example process 1100 for facilitating payment or transfer of funds in real time from an in-network sender to an in-network recipient, according to an example implementation of the present invention. Although the process 1100 is described with reference to the flow diagram illustrated in FIG. 11, it will be appreciated that many other methods of performing the acts associated with the process 1100 may be used. For example, the order of many of the blocks may be changed, certain blocks may be combined with other blocks, and many of the blocks described are optional.

[00129] To pay funds in real time from an in-network sender to an in-network recipient, data may flow between a sender computer system 110, a funds transfer payment network that uses or implements payment service computer system 160, and recipient computer system 130. A sender may wish to send funds in real time to a recipient, as shown in block 1102. In one implementation, the recipient must be eligible to receive a real time payment, such as, for example, by signing up with a service with the recipient's financial institution. The sending bank may query the funds transfer payment network as to whether the recipient is eligible to receive real time payments. The funds transfer payment network checks whether the recipient is eligible to receive real time payments, as shown in block 1104, and if so, sends a confirmation message to the sending financial institution, as shown in block 1106. Upon receiving confirmation that the recipient is eligible, the sending bank removes the funds from the sender's account, as shown in block 1108. Thus, at this stage in the process 1100, the funds have been removed from the sender's bank account.

[00130] The sending bank then sends an expedited payment message to the funds transfer payment network, as shown in block 1110. The funds transfer payment network in turn sends an expedited payment message to the recipient bank indicating a real time payment, as shown in block 1112. The recipient bank then funds the recipient's account, as shown in block 1114. It should be appreciated that at this stage in the process 1100, the funds have been deposited into the recipient's bank account. It should also be appreciated that at this stage in the process 1100, the recipient bank has funded the recipient's bank account from its own funds, but the sending bank has not yet funded the money to the recipient bank.

[00131] The reconciliation or settlement between the sending bank and the recipient bank may occur at some time after the recipient's account has been funded. The settlement or reconciliation between the sending and recipient banks may not occur for several hours or even days after a payment is made to a recipient. The amount of time between the funds being deposited in the recipient's account and the reconciliation between the sending and recipient banks may be referred to as a reconciliation delay. It should be appreciated that the funds transfer payment network substantially avoids the recipient having to wait for the reconciliation delay before receiving the funds. In some cases, the funds transfer payment network may provide a maximum number of time, e.g., two hours, for the money to become available to the recipient. It should be appreciated that the money could become available to the recipient in substantially the amount of time required to send an electronic message to the recipient bank.

[00132] Referring back to FIG. 1100, after the recipient's account has been funded, the recipient bank notifies the funds transfer payment network that the recipient's account has been funded, as shown in block 1116. The funds transfer payment network then notifies the sending bank that the recipient's account has been funded, as shown in block 1118. The sending bank may send payment confirmation message to the sender indicating that the recipient's account has been funded. The sending bank then settles the funds with the recipient bank via, for example, an ACH payment, as shown in block 1120.

[00133] In one implementation, to make the payment even quicker, the sending bank may not withdraw funds from the sender's account until after the recipient's account has been funded. The sending bank may however restrict a sender from choosing to send more money than available in the sender's account. This way, the sending back is assured that the sender's account has enough funds to pay back the sending bank.

[00134] In one implementation, instead of the receiving bank immediately funding the recipient's account, the recipient must accept the payment before the funds are transferred to the recipient's account. Upon the recipient accepting the payment, the receiving bank transfers the requisite amount to the recipient's account.

[00135] In one implementation, the funds transfer payment network may require an unregistered recipient to register at an in-network financial institution before being able to receive the funds in an expedited manner.

[00136] The implementations of the present invention have been described with reference to drawings. The drawings illustrate certain details of specific implementations that implement the systems and methods and programs of the present invention. However, describing the invention with drawings should not be construed as imposing on the invention any limitations that may be present in the drawings. The present invention contemplates methods, systems and program products on any machine-readable media for accomplishing its operations. The implementations of the present invention may be implemented using an existing computer processor, or by a special purpose computer processor incorporated for this or another purpose or by a hardwired system.

[00137] As noted above, implementations within the scope of the present invention include program products comprising machine-readable media for carrying or having machine-executable instructions or data structures stored thereon. Such machine-readable media can be any available media that can be accessed by a general purpose or special purpose computer or other machine with a processor. By way of example, such machine-readable media can comprise RAM, ROM, EPROM, EEPROM, CD-ROM or other optical disk storage, magnetic disk storage or other magnetic storage devices, or any other non-transitory medium which can be used to store desired program code in the form of machine-executable instructions or data structures and which can be accessed by a general purpose or special purpose computer or other machine with a processor. Combinations of the above are also included within the scope of machine-readable media. Machine-executable instructions comprise, for example, instructions and data which cause a general purpose computer, special purpose computer, or special purpose processing machines to perform a certain function or group of functions.

[00138] Implementations of the present invention have been described in the general context of method steps which may be implemented in one implementation by a program product including machine-executable instructions, such as program code, for example in the form of program modules executed by machines in networked environments. Generally, program modules include routines, programs, objects, components, data structures, etc. that perform particular tasks or implement particular abstract data types. Machine-executable instructions, associated data structures, and program modules represent examples of program code for executing steps of the methods disclosed herein. The particular sequence of such executable instructions or associated data structures represent examples of corresponding acts for implementing the functions described in such steps.

[00139] As previously indicated, implementations of the present invention may be practiced in a networked environment using logical connections to one or more remote computers having processors. Those skilled in the art will appreciate that such network computing environments may encompass many types of computers, including personal computers, hand held devices, multi processor systems, microprocessor-based or programmable consumer electronics, network PCs, minicomputers, mainframe computers, and so on. Implementations of the invention may also be practiced in distributed computing environments where tasks are performed by local and remote processing devices that are linked (either by hardwired links, wireless links, or by a combination of hardwired or wireless links) through a communications network. In a distributed computing environment, program modules may be located in both local and remote memory storage devices.

[00140] An exemplary system for implementing the overall system or portions of the invention might include a general purpose computing computers in the form of computers, including a processing unit, a system memory, and a system bus that couples various system components including the system memory to the processing unit. The system memory may include read only memory (ROM) and random access memory (RAM). The computer may also include a magnetic hard disk drive for reading from and writing to a magnetic hard disk, a magnetic disk drive for reading from or writing to a removable magnetic disk, and an optical disk drive for reading from or writing to a removable optical disk such as a CD ROM or other optical media. The drives and their associated machine-readable media provide nonvolatile storage of machine-executable instructions, data structures, program modules and other data for the computer. It should also be noted that the word "terminal" as used herein is intended to encompass computer input and output devices. Input devices, as described herein, include a keyboard, a keypad, a mouse, joystick or other input devices performing a similar function. The output devices, as described herein, include a computer monitor, printer, facsimile machine, or other output devices performing a similar function.

[00141] It should be noted that although the diagrams herein may show a specific order and composition of method steps, it is understood that the order of these steps may differ from what is depicted. For example, two or more steps may be performed concurrently or with partial concurrence. Also, some method steps that are performed as discrete steps may be combined, steps being performed as a combined step may be separated into discrete steps, the sequence of certain processes may be reversed or otherwise varied, and the nature or number of

discrete processes may be altered or varied. The order or sequence of any element or apparatus may be varied or substituted according to alternative implementations. Accordingly, all such modifications are intended to be included within the scope of the present invention as defined in the appended claims. Such variations will depend on the software and hardware systems chosen and on designer choice. It is understood that all such variations are within the scope of the invention. Likewise, software and web implementations of the present invention could be accomplished with standard programming techniques with rule based logic and other logic to accomplish the various database searching steps, correlation steps, comparison steps and decision steps. The foregoing description of implementations of the invention has been presented for purposes of illustration and description. It is not intended to be exhaustive or to limit the invention to the precise form disclosed, and modifications and variations are possible in light of the above teachings or may be acquired from practice of the invention. The implementations were chosen and described in order to explain the principals of the invention and its practical application to enable one skilled in the art to utilize the invention in various implementations and with various modifications as are suited to the particular use contemplated. Other substitutions, modifications, changes and omissions may be made in the design, operating conditions and arrangement of the implementations without departing from the scope of the present invention as expressed in the appended claims.

Secure Transfer of Funds through Non-Financial Institutions

[00142] In various implementations, senders and/or recipients may have access to an online payment processes or a physical payment terminal maintained by a non-financial institution (e.g., service provider). A "sender" of funds, as used herein, may comprise an entity (individual, company, corporation, etc.) that provides instructions to transfer an amount of funds from the sender's financial institution to a recipient. A "recipient" of funds, as used herein, may refer to the intended recipient of the funds from the sender (e.g., the recipient of funds may receive funds at a recipient account at the recipient's financial institution). A "participant of a funds transfer," as used herein, may refer to either sender of funds or a recipient of funds.

[00143] A "financial institution" or FI is an entity that primarily deals with financial transactions such as investments, loans, and/or deposits. Example financial institutions include organizations such as commercial banks, investment banks, insurance companies, brokerages,

investment companies, money transmitting entities, trust companies, savings and loans entities, credit unions, shadow banks, or the like.

[00144] A "non-financial institution," or "non-FI" as used herein, may refer to an entity that does not provide financial services as part of its primary functions. A non-financial institution may comprise a business entity that facilitates sale or exchange of goods and services. Examples of such business entities include service entities and retail entities (e.g., brick-and-mortar retail stores and an online retailers). In some implementations, non-financial institutions comprise social networking entities that provide social networking services to users and/or other individuals. Examples of such social networking entities include Facebook®, LinkedIn®, social networks provided by Alphabet®, Inc., and Snapchat®.

[00145] Non-financial institutions may support online payment system. An "online payment system," as used herein, may refer to a website or networked application as well as a server system that enables goods/services to be browsed, reviewed, and/or paid for by an individual (e.g., a sender or recipient) using the individual's digital device. For example, the non-financial institution may provide a physical device and/or online service for payment of services rendered or payment of past bills to the non-financial institution. In another example, an online retailer (e.g., the GAP) may provide a payment processing server in communication over a public network such as the Internet. An individual may interact with the payment processing server through a webpage (accessible by a browser on any number of digital devices) or an application such as an application on a smartphone.

[00146] In various implementations, non-financial institutions may include physical payment terminals that accept funds from individuals for payment of goods and/or services. The physical payment terminals at non-financial institutions may also allow individuals to obtain funds (e.g., physical currency, digital currency, or the like).

[00147] Financial institutions may act as financial intermediaries between senders and recipients and may facilitate transfer of funds. Financial institutions may be regulated by government(s) and/or other regulatory bodies. A "sender financial institution" may refer to a financial institution that provides financial services to an entity that attempts to transfer funds to another. For example, a sender financial institution may be the sender's bank. The sender's bank may include any number of bank accounts associated with the sender. Each account of the sender may include one or more sender account numbers (e.g., an account number that

identifies account of the sender). The sender financial institution may provide access to funds (physical currencies, digital currencies, line(s) of credit, etc.) that the sender may use to transfer funds to a recipient.

[00148] A "recipient financial institution" may refer to a financial institution that provides financial services to an entity that receives funds from another. For example, a recipient financial institution may be the recipient's bank. The recipient's bank may include any number of bank accounts associated with the recipient. Each account of the recipient may include one or more recipient account numbers (e.g., an account number that identifies account of the recipient). The recipient financial institution may provide access to funds (physical currencies, digital currencies, line(s) of credit, etc.) that the recipient may use to receive funds from a sender.

[00149] FIG. 12 depicts a diagram of a funds transfer system 1200 for securely transferring funds from a sender non-financial institution system to a recipient non-financial institution system, according to some implementations. The funds transfer system 1200 may include a sender system 1202, a recipient system 1204, a first non-FI system 1206, a second non-FI system 1208, a sender FI system 1210, a recipient FI system 1212, a payment service system 1218, an automatic clearing house (ACH) system 1220, a public network 1214 and an ACH network (e.g., private network) 1216.

[00150] The sender system 1202 may include one or more digital devices associated with a sender (e.g., a user). As an example, the sender may be a person who transfers funds to a third-party recipient using a website of a non-financial institution or a physical payment terminal of the non-financial institution (e.g. using a credit card, debit card, or smart device with a terminal provided by the non-financial institution). As an example, the sender may be a person who has access to a networked application or web page that is managed by a retailer (e.g., the first non-FI system 1206). A transfer of funds by the sender may be backed by a sender financial institution, discussed further herein. As an example, the sender may maintain a sender account at a sender financial institution that provides access to funds that the sender wishes to transfer to a recipient.

[00151] The sender system 1202 may have some or all of the components of a digital device, an example of which is shown in FIG. 19 and discussed further herein. For example, the sender system 1202 may be computer (e.g., desktop or laptop computer), a cellular

telephone, a smart phone, a mobile handheld wireless e-mail device, a personal digital assistant, a portable gaming device, or other suitable digital device. The sender system 1202 may also include one or more processors configured to execute instructions stored in memory.

[00152] The sender system 1202 may include network interface logic 1222, a display device 1224, an input device 1226, and a client application 1228. The network interface logic 1222 may include program logic that enables a connection between the sender system 1202 with the public network 1214 (or any network). The display device 1224 may include a display configured to display content, such as a graphical user interface (GUI) of an online payment system or information from the payment server system 1218 and/or information from the sender FI system 1210. The input device 1226 may be used to permit the sender to initiate account access and to facilitate receiving fund transfer request information from the user.

[00153] In some implementations, the sender system 1202 may enable sending funds to the recipient system 1204. For example, the sender system 1202 may include a browser or application configured to interact with online payment processes (e.g., online payment system) supported by the first non-FI system 1206.

[00154] The client application 1228 may include program logic configured to implement one or more of the functions of the sender system 1202. In some implementations, the client application 1228 may include or be an application configured to receive and display content (e.g., to the display device 1224) or may include or be a web browser configured to receive and display web pages from the sender FI system 1210. For example, the client application 1228 may include a mobile web browser, a Short Messaging Service (SMS) or other text messaging application, a dedicated application, or other computer program configured to send/receive information over the network 1214.

[00155] Though FIG. 12 shows the sender system 1202 within the funds transfer system 1200, it is noted that in some implementations, the sender system 1202 may not reside within the funds transfer system 1200 or some or all of the functions of the sender system 1202 may be performed by the first non-FI system 1206. For example, in some implementations where the first non-FI system 1206 incorporates a physical payment terminal, the funds transfer system 1200 may not include the sender system 1202, and/or the first non-FI system 1206 may perform some or all of the functions ascribed to the sender system 1202.

[00156] The recipient system 1204 may include a digital device associated with a recipient. For instance, a recipient may be a person who receives funds proved by the sender (e.g., from the sender system 1202) via online payment processes of a non-financial institution (e.g., first non-FI system 1206). Transfers of funds to the recipient may include transfers to an account held by the recipient at a recipient financial institution. In some implementations, funds are transferred into a recipient account held by the recipient at the recipient financial institution (e.g., recipient FI system 1212) before these funds are made available to the recipient. In various implementations, the recipient FI system 1212 may provide funds to the recipient before a transfer of the funds is made from the sender's account at the sender FI system 1210 (e.g., via the ACH network 1216).

[00157] The recipient system 1204 may have some or all of the components of a digital device, an example of which is shown in FIG. 19 and discussed further herein. Like the sender system 1202, the recipient system 1204 may be computer (e.g., desktop or laptop computer), a cellular telephone, a smart phone, a mobile handheld wireless e-mail device, a personal digital assistant, a portable gaming device, or other suitable digital device. The recipient system 1204 may also include one or more processors configured to execute instructions stored in memory.

[00158] The recipient system 1204 may include network interface logic 1230, a display device 1232, an input device 1234, and a client application 1236. The network interface logic 1230, the display device 1232, and the input device 1234 may be configured similarly to their counterparts in the sender system 1202. The client application 1236 may include program logic configured to implement one or more of the functions of the recipient system 1204. In various implementations, the client application 1236 may include an application configured to receive and display content or a web browser configured to receive and display web pages from the first non-FI system 1206, the second non-FI system 1208, the sender FI system 1210, the payment service system 1218, the recipient FI system 1212, or any combination. The client application 1236 may include a mobile web browser, a Short Messaging Service (SMS) or other text messaging application, a dedicated application, or other computer program configured to send/receive information over the network 1214.

[00159] In various implementations, the recipient system 1204 may receive a notification request that requests permission to receive funds from the sender, a notification request that requests approval of a transaction, a notification indicating a status of a transfer of

funds, and/or a notification of successful transfer of funds from a sender. The recipient system 1204 may be configured to interact with online payment processes supported by the first non-FI system 1206, the second non-FI system 1208, or both.

[00160] Though FIG. 12 shows the recipient system 1204 within the funds transfer system 1200, it is noted that in some implementations, the recipient system 1204 may not reside within the funds transfer system 1200 or some or all of the functions of the recipient system 1204 may be performed by the second non-FI system 1208. For example, in some implementations where the second non-FI system 1208 incorporates a physical payment terminal, the funds transfer system 1200 may not include the recipient system 1204, and/or the second non-FI system 1208 may perform some or all of the functions ascribed to the recipient system 1204.

[00161] The first non-FI system 1206 may include any number of digital devices configured to support the functions of the first non-financial institution. For example, the first non-FI system 1206 may be a server that hosts a website of a retailer. The website may allow users (e.g., sender or receiver) to browse goods and/or services. The website may also allow users to make purchases of the goods and/or services. In some implementations, the first non-FI system 1206 may be a server for interacting with an application (e.g., client application 1228 or client application 1236) on any number of digital devices. The application may allow users to make payments for the goods and/or services.

[00162] In various implementations, the first non-FI system 1206 may provide services to assist users to direct funds to other users. For example, the first non-FI system 1206 may provide an interface or devcie that allows the sender or recipient to register with the payment service system 1218. The interface may also enable the sender system 1202 to identify the recipient and indicate an amount to transfer to the recipient. The first non-FI system 1206 may provide all or part of the information to the payment service system 1218, the sender FI system 1210, or any other system as further described herein. In such implementations, the first non-FI system 1206 may include one or more servers each with one or more processors configured to execute instructions stored in memory. The servers may be configured to process payment information provided by the client application 1228 on the sender system 1202.

[00163] The first non-FI system 1206 may have some or all of the components of a digital device, an example of which is shown in FIG. 19 and discussed further herein. In some

implementations, the first non-FI system 1206 includes a physical payment terminal that is configured to manage payments for a sender non-financial institution. In these implementations, the physical payment terminal may comprise circuitry, other hardware, and/or software configured to process payment information from the sender (e.g., a credit card at the physical terminal) or from the sender system 1202.

[00164] The first non-FI system 1206 may include network interface logic 1238, an optional display device 1240, an input device 1242, and a non-FI application 1244. The network interface logic 1238, the display device 1240, and the input device 1242 may be configured similarly to counterparts described herein.

[00165] The non-FI application 1244 may be configured to manage payments for a sender non-financial institution. For example, the non-FI application 1244 may provide a physical device, web pages, or information to applications (e.g., including client application 1228). The non-FI application 1244 may, in some implementations, allow for users to pay for goods/services previously purchased, browse goods/services, purchase goods/services, and/or provide requests to transfer money to others. In some implementations, the sender non-FI application 1244 may include program logic to process payment information provided to a physical payment terminal supported by the first non-FI system 1206. The sender non-FI application 1244 may include program logic to support online payment processes managed by the first non-FI system 1206.

[00166] In some embodiments, the non-FI application 1244 or a financial services provider (e.g., the MasterCard neetwork) may tokenize (e.g., encrypt) a number of other identifying information associated with a financial instrument of a sender or recipient (e.g., a credit card or debit card number) to create a token for the sender or recipient. The issuing or backing financial institution for the financial instrument may be capable of de-tokenizing the token to recover the information as disclosed herein. The non-FI institution 1244 may store the tokenized financial instrument of the sender or recipient for future transactions. The non-FI application 1244 may also retrieve or identify a financial identifier that identifies a financial institution associated with the financial instrument (e.g., the financial institution that issued the financial instrument).

[00167] The second non-FI system 1208 may be similar to the first non-FI system 1206. For example, both systems may be owned by the same entity or related entities (e.g., both

systems provide services for the same entity). Alternately, each system may be operated, owned, or controlled by different entities.

[00168] Like the first non-FI system 1206, the second non-FI system 1208 may include any number of digital devices configured to support the functions of the second non-financial institution. For example, the second non-FI system 1208 may provide a physical interface to receive public identifiers and/or account numbers of senders or recipients to transfer funds to any number of individuals. In another example, the second non-FI system 1208 may be a server that hosts a website of a retailer. The website may allow users (e.g., sender or recipient) to browse past purchases and/or future purchases for goods or services. The website may also allow users to make purchases of the goods and/or services. In some implementations, the second non-FI system 1208 may be a server for interacting with an application (e.g., client application 1228 or client application 1236) on any number of digital devices. The application may allow users to make payments for the goods and/or services.

[00169] In various implementations, the second non-FI system 1208 may provide services to assist users to direct funds to other users. For example, the second non-FI system 1208 may provide an interface (e.g., of a physical device) that that allows the sender or recipient to register with the payment service system 1218. The interface may also enable the sender system 1202 to identify the recipient and indicate an amount to transfer to the recipient. The second non-FI system 1208 may provide all or part of the information to the payment service system 1218, the first FI system 1206, or any other system as further described herein. In such implementations, the second non-FI system 1208 may include one or more servers each with one or more processors configured to execute instructions stored in memory. The servers may be configured to process payment information provided by the client application 1236 on the recipient system 1204.

[00170] The second non-FI system 1208 may have some or all of the components of a digital device, an example of which is shown in FIG. 19 and discussed further herein. The second non-FI system 1208 may have some or all of the components of a digital device, an example of which is shown in FIG. 19 and discussed further herein. In some implementations, the second non-FI system 1208 includes servers and/or a physical payment terminal that is configured to manage payments for a recipient non-financial institution. The physical payment

terminal may comprise circuitry, other hardware, and/or software configured to process payment information in payment hardware on the recipient system 1204.

[00171] In some implementations, the second non-FI system 1208 may be configured to support online payment processes for a recipient non-financial institution. In such implementations, the second non-FI system 1208 may include one or more servers each with one or more processors configured to execute instructions stored in memory. The servers may be configured to process payment information provided by the client application 1236 on the recipient system 1204.

[00172] The second non-FI system 1208 may include network interface logic 1246, a display device 1248, an input device 1250, and a non-FI application 1252. The network interface logic 1246, the display device 1248, and the input device 1250 may be configured similarly to counterparts described herein. The non-FI application 1252 may be configured to manage payments. The recipient non-FI application 1252 may include program logic to process payment information provided to a website or a physical payment terminal supported by the second non-FI system 1208. In some implementations, the recipient non-FI application 1252 comprises program logic to support online payment processes managed by the second non-FI system 1208, as well as logic to tokenize a sender or receiver's financial instrument(s).

[00173] The sender FI system 1210 may be any digital device operated by or providing services to a financial institution (e.g., a sender financial institution). The sender FI system 1210 may have some or all of the components of a digital device, an example of which is shown in FIG. 19 and discussed further herein. The sender FI system 1210 may hold one or accounts on behalf of a sender. The sender financial institution may maintain accounts held by customers, such as demand deposit accounts, credit card accounts, home mortgage loans, student loans, or the like. The sender FI system 1210 may include one or more servers each with one or more processors configured to execute instructions stored in memory, send and receive data stored in memory, and perform one or more operations. The sender FI system 1210 may include network interface logic 1254, account processing logic 1256, an account database 1258, an information directory 1260, and token management logic 1262. The network interface logic 1254 may include program logic that connects the sender FI system 1210 to the network 1214. The network interface logic 1254 may facilitate secure communications between the sender FI system 1210 and other elements in FIG. 12.

[00174] The account processing logic 1256 may be configured to process transactions in connection with the account(s) of the account holder, such as account credits and debits to checking and savings accounts, credits and debits to home mortgage and home equity accounts, credits and debits to student loan accounts, or the like. In some implementations, when funds are transferred into or out of an account of an account holder (e.g., an account of a participant), the account processing logic 1256 may reflect an appropriate debit or credit in the account database 1258. The account processing logic 1256 may also process fund transfer requests to transfer funds from a sender to a recipient. The funds may be transferred using the techniques described herein.

[00175] The account database 1258 may be configured to store account information (e.g., transactions, information about the account holder, and so on) for accounts that are maintained by the bank on behalf of its customers.

[00176] The information directory 1260 may be configured to store tables that correlate user identifiers with account information used to effect a transfer of funds. The information directory 1260 may be used when a user identifier not specifying account information is used to effect a transfer of funds. In some implementations, the information directory 1260 may associate a sender's private identifier with a sender's account in the account database 1258. The information directory 1260 is further described herein.

[00177] "Account information," as used herein, may refer to information used to effect a transfer of funds to or from a participant of a funds transfer. Account information may include, for instance, account numbers, routing numbers, credit card numbers, digital currency codes that effect transfer of funds, or the like.

[00178] A "user identifier" or interchangeably, "user token," as used herein, may refer to information that identifies a participant of a funds transfer for the purpose of transferring funds. User identifiers may include or be associated with public identifiers/public tokens and private identifiers/private tokens.

[00179] A "public identifier" or interchangeably a "public token," may refer to information that identifies a participant of a funds transfer but that does not identify account information related to the participant. In some implementations, public identifiers may be configured to be shared by participants with one another. As an example, a participant may

wish to share a public identifier with other participants who wish to send him funds or receive funds from him. Public identifiers may be, for example, email addresses or other information that may be used to identify a participant (e.g., a sender or recipient) such as a phone number.

[00180] A "private identifier" or interchangeably, a "private token," as used herein, may refer to information that identifies a user (e.g., a user with an account at the FI system) and/or may be associated with account information (e.g., an account number) related to the participant. Private identifiers may be generated by the sender FI system 1210 and may be used by the sender FI system 1210 to identify account information, such as account numbers, routing numbers, credit card information, or the like. In some implementations, the private identifier does not include a bank account number, routing number, credit card numbers, or the like.

[00181] Private identifiers may be known by one or more financial institutions and entities that are members of a payment network that effect transfers of funds to participants. In one example, the sender FI system 1210 may generate a private identifier associated with the sender. The private identifier, however, may not indicate to any other entity any private information. The sender FI system 1210 may share the sender's private identifier with the payment service system 1218. The sender's private identifier may not be provided to the sender system 1202, sender, recipient's system 1204, recipient, first non-FI system 1206, or the second non-FI system 1208. Neither the payment service system 1218 nor the recipient FI system 1212 may be able to identify any account numbers or other private information from the sender's private identifier.

[00182] The FI system (e.g., sender FI system 1210 and the recipient FI system 1212 may not share private identifiers with any entity other than FI systems (e.g., each other), the automatic clearing house system 1220 discussed herein, and/or the payment service system 1218. Similarly, the payment service system 1218 may not share the private identifiers received from FI systems with any entities other than FI systems. As described herein, participants to funds transfers between non-financial institutions may transfer funds to one another using public identifiers that the participants may provide one another, using the techniques described herein. This arrangement, in some implementations, allows the sender to uniquely identify the recipient (e.g., with an e-mail address or other identifier), without necessarily having private/personal information regarding the recipient (i.e., the recipient's

bank account/routing number). In addition to the public and private identifiers that have already been described herein, additional identifiers may also be used. For example, such additional identifiers may be handled with varying levels of security. As another example, variations of existing public identifiers may be used to implement special purpose public tokens, public tokens with customized functionality, and so on, as discussed in greater detail below.

[00183] The sender FI system 1210 may include an account database 1258 and an information directory 1260. Once a user is registered with the payment service system 1218 described herein, the sender FI system 1210 may generate a private identifier associated with a user's public identifier. The private identifier of the user may be associated with both the user's public identifier (e.g., the user's email address, phone number, or other contact information) as well as a user's account at the sender FI system 1210. The account database 1258 may include the user's account and the information directory 1260 may associate the public identifier, private identifier, and account information (e.g., account number). The account database 1258 may include any number of accounts for any number of users. The information directory 1260 may include information for any number of private identifiers and public identifiers for any number of users.

[00184] The token management logic 1262 may be configured to manage tokens (e.g., public identifiers and/or private identifiers). In various implementations, the token management logic 1262 may be configured to register tokens, authenticate tokens, generate tokens, or the like. The token management logic 1262 may also facilitate identification of the recipient when a token is not recognized. The token management logic 1262 may also be used to customize attributes of tokens, such that particular accounts are used, particular methods of notification are used, and so on. The token management logic 1262 may have some or all of the attributes of the token management logic 129 shown in FIG. 2 and discussed in relation thereto.

[00185] In some implementations, the token management logic 1262 may be configured to recognize, identify, authenticate, and de-tokenize tokens of financial instruments (e.g., that were tokenized by the first non-FI system 1206). Once de-tokenized, the token management logic 1262 may recover financial information such as an account number or routing number associated with a financial instrument as discussed herein.

[00186] The recipient FI system 1212 may comprise a digital device operated by a financial institution that provides financial services to the recipient system 1204. The recipient FI system 1212 may have some or all of the components of a digital device, an example of which is shown in FIG. 19 and discussed further herein. The recipient financial institution may maintain accounts held by customers, such as demand deposit accounts, credit card accounts, home mortgage loans, student loans, or the like. The recipient FI system 1212 may include one or more servers each with one or more processors configured to execute instructions stored in memory, send and receive data stored in memory, and perform one or more operations. The recipient FI system 1212 may include network interface logic 1264, account processing logic 1266, an account database 1268, an information directory 1270, and token management logic 1272. The network interface logic 1264, the account processing logic 1266, the account database 1268, the information directory 1270, and the token management logic 1272 may be configured similarly to counterparts in the sender FI system 1210.

[00187] The payment service system 1218 may include a digital device configured to enable or facilitate payment services that allow secure transfer of funds from the sender to the recipient (e.g., from a sender account at the sender FI system 1210 to a recipient account at the recipient FI system 1212 as instructed by the sender system 1202 via the first non-FI system 1206). The payment service system 1218 may have some or all of the components of a digital device, an example of which is shown in FIG. 19 and discussed further herein. The payment service system 1218 may comprise one or more servers each with one or more processors configured to execute instructions stored in memory, send and receive data stored in memory, and perform one or more operations.

[00188] In some implementations, the payment service system 1218 assists in the transfer of funds between one or more of the sender FI system 1210, the recipient FI system 1212, the sender non-FI bank system 1214, and the recipient non-FI bank system 1216.

[00189] The payment service system 1218 may provide payment services to participants that have accounts at member banks. More particularly, in some implementations, the financial institutions associated with the sender FI system 1210 and the recipient FI system 1212 may comprise member banks. "Member banks," as used herein, may refer to financial institutions that are members of the payment service system 1218 and that follow protocols established by government agencies, regulatory bodies, or the like for transferring funds to one

another. In various implementations, the payment service system 1218 provides payment services to participants that have accounts at financial institutions that are not member banks.

[00190] The payment service system 1218 may include network interface logic 1295, account processing logic 1276, an account database 1278, an information directory 1280, token management logic 1282, fund transfer logic 1284, and registration logic 1286. The network interface logic 1274, the account processing logic 1276, the account database 1278, the information directory 1280, and the token management logic 1282 may be configured similarly to counterparts in the sender FI system 1210.

[00191] In various implementations, participants to a funds transfer may share their information with the information directory 1280 using the network 1214. Network interface logic 1274 may be configured to receive information over the network 1214. The account processing logic 1276 may determine if a public identifier of a participant is registered by determining if there is an account associated with the public identifier in the account database 1278. A participant may be added to the information directory 1280 upon registering for the funds transfer system 1200 through the sender FI system 1210 or through the first non-FI system 1206. Upon registration, a new entry may be created for the newly registered user in a database that implements the information directory 1280. In some implementations, the information directory 1280 is populated automatically with public identifiers and private identifiers during a secure online banking session that includes the sender FI system 1210.

[00192] In some implementations, the information directory 1280 stores registries of other participants connected to a specific participant. For instance, for each user, the information directory 1280 may store a registry that includes a listing of each other user with whom the user has an established connection. Such connection may be established, for example, the first time that the user sends or receives funds from the other user. A connection may also be established by way of a user interface that permits a user to add connections with other users through a lookup service in the information directory 1280 and/or another information directory. An example of such a user interface is discussed in connection with FIG. 4 and further herein. The users may include not only users that are registered in the funds transfer payment network, but also other affiliated payment networks, as discussed in greater detail below. For each user in the registry, additional information may be stored, such as their

unique ID and/or other information. As another example, the information for the other users may be stored in separate database entries in the information directory 1280.

[00193] In various implementations, the information directory 1280 may comprise one of a plurality of information directories, each maintained by a different institution or entity. Each information directory may store information about participants relevant to the digital device containing it. Each information directory may allow relevant participants to register with it.

[00194] The fund transfer logic 1284 may be configured to assist with the transfer of funds between two participants. The fund transfer logic 1284 is further described with regard to FIG. 13. Fund transfers may involve transfers of funds from a sender to a recipient. In various implementations, all participants to a transfer may have registered for fund transfer services provided by the payment service system 1218. However, in some implementations, at least one participant may be registered only for financial services of a financial institution and/or registered to use the purchase processes (physical purchase terminal, online purchase processes, etc.) of a non-financial institution. As noted herein, registration for fund transfer services provided by the payment service system 1218 may include registering public identifiers for participant accounts and/or receipt of participant redemption tools (e.g., financial instruments), both of which are further discussed herein. In various implementations, a recipient of a funds transfer may need not take any action to accept a payment (e.g., the recipient may have an "auto-accept" status that allows transfer to the recipient's participant account without further action by the recipient). It is noted in some implementations, the recipient may have to manually accept at least some or all fund transfers.

[00195] In some implementations, the payment service system 1218 may provide a web portal provided for an online community of individuals where such individuals obtain user names/login IDs or otherwise become registered members. The individuals may, for example, use the web portal to interact with each other and/or to interact with a service provided by the online community. Examples of online communities include MSN®, iPhone® users, Facebook®, LinkedIn®, etc. The payment service may, for example, be an additional service that is offered by the web portal to the members of the online community. As another example, the payment service may be provided by one of the financial institutions, e.g., such that a financial institution performs both the operations described herein as being performed by

the sender FI system 1210, the recipient FI system 1212, the sender non-FI bank system 1214, and the recipient non-FI bank system 1216.

[00196] In implementations where the second non-FI system 1208 corresponds to a physical purchase terminal, the transfer logic 1284 may manage transfers of funds from the sender FI system 1210 to the second non-FI system 1208. Funds obtained at the second non-FI system 1208 may take the form of physical currency, digital currencies, etc. a recipient may obtain from the physical purchase terminal. In implementations where the second non-FI system 1208 supports online payment processes, the transfer logic 1284 may manage transfers of funds from the sender FI system 1210 to the second non-FI system 1208 and/or the recipient system 1204. Funds obtained at the second non-FI system 1208 and/or the recipient system 1204 may take the form of digital currencies, etc. that can be deposited into online accounts maintained by the recipient FI system 1212 and/or accessed by the second non-FI system 1208 and/or the recipient system 1204. In some implementations, the transfer logic 1284 may facilitate fund transfers to unregistered participants. In some implementations, the transfer logic 1284 may instruct the sender FI system 1210 and the recipient FI system 1212 to extract public identifiers from the transaction data. The transfer logic 1284 may further instruct the sender FI system 1210 and/or the recipient FI system 1212 to look up DDAs after the public identifiers have been extracted.

[00197] The registration logic 1286 may be configured to manage registration of unregistered participants for fund transfers. The registration logic 1286 is further described with regard to FIG. 14. In some implementations, the registration logic 1286 may issue participant accounts to access those participant accounts. A "participant account," as used herein, may refer to a registration account managed by the payment service system 1218 to assist in the transfer of funds between financial institutions. A participant account may be linked to and/or backed by funds in financial accounts provided by a financial institution. Participant accounts may be identified by account numbers and/or other account identifiers.

[00198] The registration logic 1286 may create tokenized account data for those participant accounts when a participant seeks to register user identifiers for those participant accounts. "Tokenized account data," as used herein, may comprise a representation of account information that makes the account information secure from outside discovery. In some implementations, tokenized account data may comprise a proxy number or encrypted version

of account information. The tokenized account data may further include the names/identifiers/etc. of financial institutions that are associated with the account information. In various implementations, the registration logic 1286 may allow users to register user identifiers for participant accounts.

[00199] The Automatic Clearing House (ACH) system 1220 may include one or more digital devices used to transmit funds to and from bank accounts of the senders and recipients. The Automatic Clearing House (ACH) system 1220 may be used to transmit funds to and from bank accounts of the senders and recipients. In some implementations, the ACH system 1220 may facilitate secure transfer of funds and/or information between the sender FI computer system 1210 and the recipient FI computer system 1212. The ACH system 1220 may include a computer system configured similarly to the ACH system 170 shown in FIG. 1.

[00200] In some implementations, the ACH system 1220 may enable a batch processing system. A "batch processing system," as used herein, may include a system that allows financial institutions to accumulate transactions over a specified period of time. In some implementations, financial institutions that transfer funds to one another over a batch processing system may accumulate transactions over a specified period of time (hourly, daily, weekly, etc.) or until a specified event has occurred. After the specified period of time or specified event, the financial institutions may settle amounts owed to one another using a private network (e.g., ACH network 1216) and/or the ACH system 1220. In some implementations, a batch transfer system may allow financial institutions to transfer funds to one another as needed and to settle amounts owed to one another at a specified time each day, week, etc. Settlement times may be supported by regulations. As an example, National Automated Clearing House Association (NACHA) rules may require financial institutions that use a batch processing system to settle credits to one another before the end of the next business day after a specific fund transfer.

[00201] In various implementations, the ACH network 1220 may allow the sender FI system 1210 and the recipient FI system 1212 to transfer funds electronically. Instead of using paper to carry necessary transaction information, such as with checks, transactions over the ACH network 1220 may be transmitted electronically over a private network, allowing for faster and more secure processing times and cost savings. The ACH network 1220 may process different types of transactions, including but not limited to Direct Deposit transactions

and Direct Payments transactions. Direct Deposit transactions may comprise the deposit of funds for payroll, employee expense reimbursement, government benefits, tax and other refunds, and annuities and interest payments. Direct Deposit transactions may include ACH credit payment from a business or government to a consumer. Direct Payment transactions may comprise the use of funds to make a payment. In some implementations, individuals and/or organizations can make a Direct Payment via ACH as either an ACH credit or ACH debit. Direct Payment transactions may be processed as ACH debit transactions, ACH credit transactions, or some combination thereof. A Direct Payment transaction processed as an ACH credit transaction pushes funds into an account. An example of this is when a consumer initiates a payment through his/her bank or credit union to pay a bill. A Direct Payment processed as an ACH debit transaction may pull funds from an account. An example of this is when a consumer establishes a recurring monthly payment for a mortgage or utility bill, and his/her account is debited automatically.

[00202] While FIG. 12 describes a sender system 1202 and a recipient system 1204, it will be appreciated that the sender system 1202 and the recipient system 1204 may be optional. For example, a sender may interact directly with the first non-FI system 1206 which may include, for example, a physical device configured to receive a credit or debit card number from the sender. The physical device may further receive a public identifier of the sender. In some implementations, the physical device or another part of the sender system 1202 may further receive an amount to transfer to a recipient as well as a recipient public identifier. In this example, the physical device, sender system 1202, or a financial services provider (e.g., MasterCard or Visa) may tokenize the credit or debit card number and/or provide an identifier of the financial institution that backs or issued the financial instrument. The non-FI system 1206 and/or the financial services provider may provide the sender public identifier, identifier of the financial institution (e.g., that identifies the sender FI system 1210), amount to be transferred, and/or the recipient identifier to the payment service system 1218 and/or the sender FI system 1210.

[00203] FIG. 13 depicts a diagram of fund transfer logic 1284, according to some implementations. The fund transfer logic 1284 may include transaction data management logic 1302, payment validation logic 1304, information directory management logic 1306, payment notification logic 1308, and payment status management logic 1310. One or more of the transaction data management logic 1302, the payment validation logic 1304, the information

directory management logic 1306, the payment notification logic 1308, and the payment status management logic 1310 may be implemented using physical computer processor(s) and memory stored in the fund transfer logic 1284. The memory may store computer program instructions to instruct the physical processor(s) to implement one or more of the transaction data management logic 1302, the payment validation logic 1304, the information directory management logic 1306, the payment notification logic 1308, and the payment status management logic 1310.

[00204] The transaction data management logic 1302 may be configured to manage transaction data, including transaction data to and from participant systems (e.g., the sender system 1202, the recipient system 1204, the first non-FI system 1206, and the second non-FI system 1208) as well as transaction data to and from the payment service system 1218. "Transaction data," as used herein, may refer to data related to a transaction, including a request to perform a fund transfer from one participant to another (e.g., from a sender to a recipient received from the first non-FI system 1206), public identifier of the sender, public identifier of the recipient, a transaction identifier identifying the transaction to transfer funds, a private identifier of the sender, a private identifier of the recipient, an financial institution (FI) identifier associated with the sender, an FI identifier associated with the recipient, or any combination. In some implementations, transaction data includes an amount of funds to be transferred.

[00205] The transaction data management logic 1302 may, in some implementations, receive transaction data (e.g., from the sender system 1202, the first non-FI system 1206, the sender FI system 1210, and/or financial services provider) indicating a sender is attempting to provide funds to a recipient. The transaction data may, in this example, include a public identifier of the sender, a public identifier of the recipient, a sender FI system identifier, and an amount to transfer. The transaction data management logic 1302 may determine if the sender is registered by comparing the public identifier of the sender to a list of registered users (e.g., to information in the account database 1278, the information directory 1280, or the like). If registered, the transaction data management logic 1302 may provide a success message that the sender is registered to the first non-FI system 1206 and/or the sender system 1202. Further, the transaction data management logic 1302 may provide a private identifier of the sender and the amount to be transferred to the sender FI system 1210. The transaction data management logic 1302 may also provide a public identifier of the recipient, a private identifier of the recipient, a

recipient FI identifier, a public identifier of the sender and/or any other information to the sender FI system 1210.

[00206] The transaction data management logic 1302 may receive authorization from the sender FI system 1210 indicating that the sender FI system 1210 has identified the account of the sender and that the sender has sufficient funds for the transaction. At any time, the transaction data management logic 1302 may generate and share a transaction identifier with the sender FI system 1210 and/or the recipient FI system 1212 identifying the transaction to transfer funds from the sender to the recipient.

[00207] In some implementations, the transaction data management logic 1302 may provide logic and/or instruction to the first non-FI system 1206 to enable the first non-FI system 1206 to provide fund transfer options to users of the system. For example, the transaction data management logic 1302 may provide logic (e.g., code or software) to the first non-FI system 1206 to be placed or embedded within a physical device, web page or code provided by the first non-FI system 1206 to the sender or sender system 1202. The logic may allow the sender to see options to transfer money, allow the sender to input or select a recipient's public identifier, allow the sender to input or select their own public identifier, indicate an amount of funds to transfer, receive a debit or credit card number of the sender, and/or any other information.

[00208] The validation logic 1304 may be configured to validate payment details related to transaction data. Validation may involve determining if the sender public identifier is registered, determining if the recipient public identifier is registered, or determination of the FI identifier is associated with a known financial institution (or a member financial institution). It will be appreciated that the FI identifier may be generated as part of the tokenization of the debit or credit card number of the sender or in any number of ways (e.g., retrieved based on the debit or credit card of the sender, or information provided by the sender).

[00209] In various implementations, the validation logic 1304 implements one or more validation protocols (e.g., validation interfaces) that request confirmation from financial institutions whether or not a sender has authorization to provide the funds requested. The validation logic 1304 may further implement one or more checks to see if public identifiers provided in association with transaction data are valid.

[00210] The information directory management logic 1306 may be configured to provide instructions to add the transaction data to the information directory 1280. In various implementations, the information directory management logic 1306 may add, delete and/or otherwise modify or manage the information directory 1280.

[00211] The payment notification logic 1308 may be configured to provide support payment notifications, e.g., notifications to the sender FI system 1210 indicating success or failure of the fund transfer to the recipient and/or sender.

[00212] The payment status management logic 1310 may be configured to manage status updates indicating if the fund transfer is possible or if there is an error. In some implementations, the payment status management logic 1310 may request additional information to assist in the process of the fund transfer.

[00213] FIG. 14 depicts a diagram of registration logic 1286, according to some implementations. It will be appreciated that, in some implementations, the registration logic 1286 may register a sender and/or a recipient once. The registration logic 1286 may include participant account issuing logic 1402, user identification verification logic 1404, tokenization logic 1406, financial institution identification logic 1408, and account confirmation logic 1410. One or more of the participant account issuing logic 1402, the user identification verification logic 1404, the tokenization logic 1406, the financial institution identification logic 1408, and the account confirmation logic 1410 may be implemented using physical computer processor(s) and memory stored in the registration logic 1286. The memory may store computer program instructions to instruct the physical processor(s) to implement one or more of the participant account issuing logic 1402, the user identification verification logic 1404, the tokenization logic 1406, the financial institution identification logic 1408, and the account confirmation logic 1410.

[00214] The participant account issuing logic 1402 may be configured to facilitate issuance of participant accounts. In some implementations, the participant account issuing logic 1402 may create account numbers and/or other account identifiers that participants can use as the basis of participant accounts (e.g., which may assist in the transfer of funds between financial institutions).

[00215] The user identification verification logic 1404 may be configured to verify user identifiers when the user identifiers are provided for registering a participant account. In various implementations, the user identification verification logic 1404 is configured to assess whether a participant has the right to register a specific participant account. The user identification verification logic 1404 may further be configured to determine whether or not a user identifier and/or participant account information provided by a participant are associated with accounts at a financial institution or if the financial institution may be identified.

[00216] Verification of a public identifier may involve one or more verification techniques, such as verifying the public identifier is in appropriate format (e.g., appropriate alphanumeric format), verifying the public identifier has not been previously assigned to another participant, and verifying the public identifier does not include account information.

[00217] The tokenization logic 1406 may be configured to tokenize participant account information. In various implementations, the tokenization logic 1406 may encrypt participant account information or assign proxy numbers to participant account information to keep the participant account information secure from discovery by outside entities, including non-financial institutions.

[00218] The financial institution identification logic 1408 may be configured to identify a financial institution associated with participant account information. The financial institution identification logic 1408 may identify a participant financial institution that provides financial services to the participant system. In some implementations, the financial institution identification logic 1408 may use names/identifiers/etc. of financial institutions included in tokenized account data to identify the appropriate participant financial institution. As examples, in implementations where the participant system corresponds to the sender system 1202, the financial institution identification logic 1408 may identify the sender FI system 1210. In implementations where the participant system corresponds to the recipient system 1204, the financial institution identification logic 1408 may identify the recipient FI system 1212.

[00219] The account confirmation logic 1410 may provide status updates and/or other information to indicate whether or not a participant account has been successfully registered. The account confirmation logic 1410 may instruct the participant system to confirm ownership of the public identifier and send the public identifier and the account information to a non-FI system that corresponds to the participant system. As an example, the account confirmation

logic 1410 may instruct the sender system 1202 to confirm ownership of the public identifier and send the public identifier and the account information to the first non-FI system 1206. As another example, the account confirmation logic 1410 may instruct the recipient system 1204 to confirm ownership of the public identifier and send the public identifier and the account information to the second non-FI system 1208.

[00220] The account confirmation logic 1410 may instruct the non-FI system that corresponds to the participant system to send the public identifier and the tokenized account data to the payment service system 1218. In some implementations, the public identifier and the tokenized account data is sent directly to the payment service system 1218, while in other implementations, the public identifier and the tokenized account data is sent to the payment service system 1218 through the sender non-FI bank system 1214. The account confirmation logic 1410 may instruct the relevant participant FI system to obtain an identifier of the financial institution associated with the participant using the tokenized account data. The account confirmation logic 1410 may instruct the participant FI system to perform DDA lookups, map DDA numbers to the public identifier, and associate the public identifier with the relevant user account. In various implementations, the account confirmation logic 1410 may provide confirmation of whether or not the participant was successfully registered for fund transfers at non-financial institutions.

[00221] FIG. 15 depicts a diagram of a data flow 1500 for securely transferring funds from a sender to a recipient in a funds transfer system, according to some implementations. The data flow 1500 depicted in FIG. 15 may be an example, for example, where both the sender and the recipient are already registered with the payment service system 1218. The data flow 1500 includes components of the funds transfer system 1200, shown in FIG. 12, and discussed further herein. More particularly, the data flow 1500 includes operations one or more of the sender system 1202, the recipient system 1204, the first non-FI system 1206, the sender FI system 1210, the recipient FI system 1212, and the payment service system 1218. It is noted that the elements of the data flow 1500 are by way of example only, and that various implementations may employ a greater number of elements or a lesser number of elements without departing from the scope and substance of the inventive concepts described herein.

[00222] At an operation 1502, the sender system 1202 may receive transaction data related to a fund transfer from the sender system 1202. The transaction data may specify an

amount of funds to be transferred, a public identifier of a sender (e.g., a participant associated with the sender system 1202), and a public identifier of a recipient (e.g., a participant associated with the second non-FI system 1208). As further noted herein, the public identifiers of the sender and the recipient may facilitate routing the fund transfer to the recipient and facilitate reconciliation between sender and recipient financial accounts without requiring account information to be provided outside financial institutions.

[00223] At an operation 1504, the sender system 1202 may provide the transaction data to the first non-FI system 1206 over the public network 1214 (or any network). In various implementations, the sender system 1202 may provide the transaction data to a physical purchase terminal or to an application, website, or the like sourced by online purchase processes supported by the first non-FI system 1206. The transaction data may comprise the amount of funds for the transfer, as well as the public identifiers of the sender and the recipient.

[00224] It will be appreciated that operations 1502 and 1504 may be optional. For example, as discussed herein, the non-FI system 1206 may include a physical device configured to receive fund transfer information (e.g., sender public identifier, credit or debit card number, amount to be transferred or the like) from the sender without a sender system 1202.

[00225] At an operation 1506, the first non-FI system 1206 may route the transaction data to the payment service system 1218. The first non-FI system 1206 may recognize that the public identifiers of the sender and recipient are in a format that corresponds to a fund transfer managed by the payment service system 1218. At an operation 1508, the first non-FI system 1206 may provide the transaction data to the payment service system 1218 over the public network 1214 (or any other network).

[00226] At an operation 1510, the payment service system 1218 may validate payment details for the transaction data. As noted herein, validation may involve determining whether the public identifier of the sender is valid, whether the public identifier of the recipient is valid, whether the sender has authorization to provide the funds requested, and/or the like. In some implementations, the payment service system 1218 confirms that the public identifier of the sender is associated with a sender private identifier and an FI system (e.g., sender FI system 1210). Similarly, the payment service system 1218 may confirm that the public identifier of

the recipient is associated with a recipient private identifier and an FI system (e.g., recipient FI system 1212). The payment validation logic 1304 may perform operation 1510.

[00227] At an operation 1512, the payment service system 1218 may add some or all of the transaction data to the information directory 1280. For example, the payment service system 1218 may log fund transfer information (e.g., time, amount to transfer, recipient public identifier, sender FI identifier, recipient FI identifier, transaction identifier, and/or the like). In some embodiments, the payment service system 1218 may store additional information, such as additional sender public identifiers, with a recipient account. In various implementations, if the fund transfer request was successfully added to the information directory 1280, the payment service system 1218 may send a notification to the first non-FI system 1206 to that effect. The information directory management logic may perform operation 1512.

[00228] At an operation 1514, the information directory management logic 1306 may gather sender private identifier and recipient private identifier from the information directory 1280. As discussed herein, the sender private identifier may have been previously generated by the sender FI system 1210 and provided to the payment services system 1218. Similarly, the recipient private identifier may have been previously generated by the recipient FI system 1212.

[00229] At an operation 1516, the payment service system 1218 may provide a payment notification to the sender FI system 1210 over the public network 1214 (or any network). The payment notification may inform the sender FI system 1210 that the fund transfer request was successfully added to the information directory 1280. The payment notification may include at least some of the transaction data, including the amount of the funds transfer request, the private identifier of the sender, and the private identifier of the recipient. The payment notification may include instructions or information to the sender FI system 1210 to assist with the transfer funds to the recipient FI system 1212. The payment notification logic 1308 may perform operation 1516.

[00230] At an operation 1518, the sender FI system 1210 may look up one or more accounts (e.g., DDAs) associated with the sender's private identifier. In various implementations, the sender FI system 1210 may use the private identifier of the sender to look up DDAs in the information directory 1260. The sender FI system 1210 may identify any number of accounts and/or other information relevant to the sender system 1206.

[00231] At an operation 1520, the sender FI system 1210 may determine if the sender account has sufficient finds to perform the fund transfer. At an operation 1522, the sender FI system 1210 may perform internal checks, such as checks related to whether or not a sender account has sufficient funds, whether or not the transaction data is likely to be fraudulent/suspicious, or any other checks which may be based on regulation compliance.

[00232] At an operation 1524, the sender FI system 1210 may provide instructions to the payment service system 1218 to update any relevant status related to whether or not funds for the fund transfer is approved and/or will be conducted. At any time the payment service system 1218 may generate a transaction identifier that identifies the transaction. The transaction identifier may be shared by the payment service system 1218 with the sender FI system 1210 and the recipient FI system 1204. The payment service system 1218 may provide to the first non-FI system 1206 a first notification of the updated status, including whether or not the funds for the transfer are to be transferred.

[00233] At an operation 1526, the payment service system 1218 may provide to the sender system 1202 (or the first non-FI system 1206) a second notification of the updated status, including whether or not the funds will be transferred. In various implementations, the payment status management logic 1310 may perform the operations 1524 and 1526.

[00234] At an operation 1528, the sender FI system 1210 may provide the recipient FI system 1212 with a batch transfer to settle fund transfer between the two financial institutions using the ACH network 1216. In various implementations, the request to settle the payment may include or be associated with an ACH message that specifies a transaction identifier (e.g., identifying the transaction and may be linked to the amount to be transferred, an identifier of the sender FI system 1210, and any other information) and/or the amount of the funds transfer. In some implementations, the batch transfer may accompany the sender private identifier, the sender public identifier, the recipient private identifier, the recipient public identifier, the FI identifier of the sender FI system 1210, and/or any other information. Alternately, the sender private identifier, the sender public identifier, the recipient private identifier, the recipient public identifier, the FI identifier of the sender FI system 1210, and/or any other information may be provided at a later time. In some implementations, the payment status management logic 1310 may perform the operation 1528.

[00235] At an operation 1530, the recipient FI system 1212 may identify the transaction identifier and retrieve information related to the transfer including, for example, the recipient and the amount of money to transfer. For example, the recipient FI system 1212 may use the transaction identifier to identify the recipient and retrieve one or more accounts (e.g., DDAs) associated with the recipient.

[00236] At an operation 1532, the recipient FI system 1212 may deposit funds in the amount of the funds transfer into the recipient account of the recipient. For example, the funds may be deposited into the recipient's DDA by the recipient FI system 1212 from the amount received in the ACH transfer.

[00237] At an operation 1534, the recipient FI system 1212 may provide the second non-FI system 1208 and/or the recipient system 1204 with an updated status indicating funds were transferred into the recipient account.

[00238] At an operation 1536, the recipient FI system 1212 may provide the payment service system 1218 with an updated status indicating funds were transferred into the recipient account. At an operation 1538, the payment service system 1218 may provide the first non-FI system 1206 or the sender system 1202 with an updated status indicating funds were transferred into the recipient account.

[00239] FIG. 16A and FIG. 16B depict diagrams of flowchart of methods 1600A and 1600B for securely transferring funds from a sender to a recipient in a funds transfer system, according to some implementations. The flowchart of methods 1600A and 1600B may include similar operations as that of FIG. 15. The methods 1600A and 1600B may be performed by one or more of the systems or system components shown in FIGS. 12-14. It is noted that the methods 1600A and 1600B may include more or less operations than those explicitly shown.

[00240] At an operation 1602, the transaction data management logic 1302 may receive transaction data from the first non-FI system 1206 over the public network 1214. The transaction data may specify a transfer amount of a fund transfer between a sender and a recipient (e.g., between the sender system 1202 and the second non-FI system 1208 or the recipient system 1204). In some implementations, the transaction data may include a sender public identifier to identify a sender of the fund transfer. The sender public identifier may include information that may be used to contact the sender such as an email address, a

username, a phone number, an alphanumeric string or the like that uniquely identifies the sender but does not include financial information of the sender to secure from outside discovery. The transaction data may include a recipient public identifier to identify a recipient of the fund transfer. The recipient public identifier may similarly include an email address, a username, a phone number, an alphanumeric string or the like. The recipient public identifier may also uniquely identifies the recipient but keeps financial information of the recipient secure from outside discovery.

[00241] At an operation 1604, the transaction data management logic 1302 of the payment service system 1218 may determine that the sender and recipient are registered to respectively use the sender public identifier and the recipient public identifier to perform the fund transfer. In various implementations, the transaction data management logic 1302 may determine that the sender and the recipient are registered with the information directory 1280. The transaction data management logic 1302 may determine, e.g., that public and/or private identifiers of senders and/or recipients have been registered in the information directory 1280.

[00242] At an operation 1606, the transaction data management logic 1302 may gather, using the sender public identifier, an identifier of a sender financial institution having a sender financial account and a sender private identifier. At an operation 1608, the transaction data management logic 1302 may gather, using the recipient public identifier, an identifier of a recipient financial institution having a recipient financial account and a recipient private identifier. The transaction data management logic 1302 may obtain the sender financial institution and/or the recipient financial institution using names, identifiers, etc. incorporated in the transaction data to identify the sender financial institution and the recipient financial institution.

[00243] At an operation 1610, the payment notification logic 1308 may send at least some of the transaction data and retrieved information to the sender financial institution to effectuate the fund transfer. In various implementations, the sender private identifier, the recipient public identifier, the recipient FI system 1212, and the transfer amount may be sent by the payment notification logic 1308 to the sender FI system 1210. The portions of the transaction data may comprise data sufficient to identify the sender of the fund transfer, the recipient of the fund transfer, and the transfer amount of the fund transfer.

[00244] At an operation 1612, the sender FI system 1210 may retrieve a sender account using the sender private identifier. In some implementations, the sender FI system 1210 may identify the sender account by using the sender private identifier to query the information directory 1260. The resulting response may form the basis of retrieving the sender account. As discussed herein, during registration, the sender private identifier is generated by the sender FI system 1210 during registration and may be used to link the sender with one or more account numbers of accounts of the sender maintained or managed by the sender FI system 1210. The sender private identifier may not be an account number or an encrypted account number. For example, although the sender private identifier is not provided to the sender system 1202, the recipient system 1204, or the first non-FI system 1206, the sender private identifier may have not be reverse engineerable (e.g., an account number cannot be obtained from the sender private identifier). The sender private identifier may only be an identifier that can be used by the sender FI system 1210 because of an association with other account information. At an operation 1614, the sender FI system 1210 may evaluate whether or not the sender financial account has sufficient funds to perform the fund transfer. In some implementations, the sender FI system 1210 may send one or more instructions to the sender FI system 1210 to ensure the sender has account access, sufficient funds, and other information needed to use the public identifier to perform the fund transfer.

[00245] At an operation 1616, the sender FI system 1210 may evaluate whether the fund transfer is likely to be fraudulent based on the transaction data. In some implementations, the payment validation logic 1304 may determine whether circumstances of the sender's transfer make it appear like the sender is not who the sender claims to be. The sender FI system 1210 may evaluate whether the sender's Internet Protocol (IP) addresses, etc. are valid and/or if the sender has attempted the fund transfer from an authorized system or system the sender has used before, repeated fund transfers in a short time, or the like. If the transfer passes approval, the sender FI system 1210 may provide a notification that it is capable of performing the fund transfer. At an operation 1618, the payment service system 1218 may receive a notification that the sender FI system 1210 is capable of performing the fund transfer.

[00246] In some implementations, the payment service system 1218 may generate a transaction identifier associated with the fund transfer and provide the transaction identifier to the sender FI system 1210 and the recipient FI system 1212. The transaction identifier may be

used in the ACH batch transfer between the sender FI system 1210 and the recipient FI system 1212.

[00247] At an operation 1620, the payment notification logic 1308 may provide to one or more of the sender system 1202 and the first non-FI system 1206 a status of the fund transfer that indicates the fund transfer will occur.

[00248] At an operation 1622, the sender FI system 1210 or the payment service system 1218 may provide to the recipient FI system 1212 transaction data that identifies the transaction identifier, the recipient private identifier, the transfer amount, the identifier of the sender financial institution, and/or the sender private identifier to the recipient financial institution. In various implementations, the private identifiers are provided so that account information need not be transmitted over the public network 1214 (or other network).

[00249] At an operation 1624, the sender FI system 1210 may provide funds (including funds for the funds transfer) to the recipient FI system 1212 through the ACH system 1220 and/or the ACH network 1216 as part of a batch fund transfer process. At an operation 1628, the payment status management logic 1310 may receive a notification of a deposit of the fund transfer into a recipient financial account at the recipient financial institution.

[00250] FIG. 17 depicts a diagram of a data flow 1700 for securely transferring funds from a sender to a recipient in a funds transfer system, according to some implementations. The data flow 1700 may be, for example, where one participant, such as the sender, is not previously registered with the payment service system 1208. The data flow 1700 includes components of the funds transfer system 1200, shown in FIG. 12, and discussed further herein. More particularly, the data flow 1700 includes operations of one or more of the sender system 1202, the first non-FI system 1206, the second non-FI system 1208, the sender FI system 1210, the payment service system 1218, and the recipient FI system 1212 may provide. It is noted that the elements of the data flow 1700 are by way of example only, and that various implementations may employ a greater number of elements or a lesser number of elements without departing from the scope and substance of the inventive concepts described herein.

[00251] At an operation 1702, the sender system 1202 may receive transaction data related to a fund transfer. The transaction data may specify an amount of funds to be

transferred. The transaction data may specify a public identifier of a sender (e.g., a participant associated with the sender system 1202) and a public identifier of a recipient. As further noted herein, the public identifiers of the sender and the recipient may facilitate routing the fund transfer to the recipient and facilitate reconciliation between sender and recipient financial accounts without requiring account information to be provided outside financial institutions. It will be appreciated that the recipient system 1204 may also receive transaction data related to a fund transfer.

[00252] At an operation 1704, the sender system 1202 (and the recipient system 1204) may provide the transaction data to the first non-FI system 1206 over the public network 1214. In various implementations, the sender system 1202 may provide the transaction data to a physical purchase terminal or to an application, website, or the like sourced by payment processes supported by the first non-FI system 1206. Similarly, the recipient system 1204 may provide transaction details to the second non-FI system 1208 or the first non-FI system 1206. In some embodiments, the first non-FI system 1206 and the second non-FI system 1208 are owned by the same entity. In some embodiments, the sender system 1202 provides a first financial instrument of a sender or a tokenized financial instrument of a sender (to generate a sender token) to the first non-FI system 1206 and the recipient system 1204 provides second financial instrument of the recipient or a tokenized financial instrument of the recipient (to generate a recipient token) to the first non-FI system 1206 or second non-FI system 1208.

[00253] It will be appreciated that operations 1702 and 1704 may be optional. For example, as discussed herein, the non-FI system 1206 may include a physical device configured to receive fund transfer information (e.g., sender public identifier, credit or debit card number, amount to be transferred or the like) from the sender without a sender system 1202.

[00254] It will be appreciated that the first and second non-FI system may not be necessary. For example, the sender system 1202 and the recipient system 1204 may each be smartphones configured to share transaction information (e.g., funds to be transferred, tokenized financial instruments to create tokens from the recipient and sender, and public identifiers of the sender and recipient). The transaction information may be provided to the payment services system 1218.

[00255] At an operation 1706, the first non-FI system 1206 may route the transaction data to the payment service system 1218. At an operation 1708, the first non-FI system 1206 may provide the transaction data to the payment service system 1218 over the public network 1214 (or any network). The transaction data may include a sender public identifier, a recipient public identifier, an amount to be transferred, the recipient token, and the sender token. In some implementations, the first non-FI system 1206 may receive an account number associated with any number of financial instruments. The first non-FI system 1206 may tokenize the account number of a financial instrument or provide the account number to a financial service provider associated with the financial instrument to tokenize the account number. Subsequently, the first non-FI system 1206 or the financial service provider associated with the financial instrument may provide the token(s) of the account number(s) to the payment services system 1218.

[00256] At an operation 1710, the payment service system 1218 may confirm if the sender is registered with the payment services system 1218 using the sender's public identifier. If the sender is already registered, the sender may not need to be re-registered. If the sender is not recognized, the payment services system 1218 may request additional information from the sender, sender system 1202, or the first non-FI system 1206 to identify the sender.

[00257] Similarly, the payment service system 1218 may confirm if the recipient is registered with the payment services system 1218 using the recipient's public identifier. If the recipient is already registered, the recipient may not need to be re-registered. If the recipient is not recognized, the payment services system 1218 may request additional information from the recipient, recipient system 1204, the first non-FI system 1206, or the second non-FI system 1208, to identify the sender.

[00258] In some implementations, the first non-FI system 1206 or an entity associated with the sender's financial instrument may tokenize the sender's financial instrument and/or the recipient's financial instrument (to generate the sender token and/or the recipient token). The first non-FI system 1206 may also send an FI identifier associated with the sender's financial instrument (e.g., the bank that issued the financial instrument) and the FI identifier associated with the recipient's financial instrument to the payment services system 1218. If the payment services system 1218 determines to register the sender (e.g., upon request of the sender for registration), the payment services system 1218 may identify the sender FI system

1210 with the FI identifier and may provide the sender's token and sender public identifier to the sender FI system 1210.

[00259] At an operation 1712, the payment service system 1218 may add the transaction data to the information directory 1280 to tentatively log the transaction. It will be appreciated that the non-FI system 1210 may log or store information related to the fund transfer including, for example, the sender public identifier, the funds to be transferred, the recipient public identifier, the financial identifier associated with the financial instrument, the tokenized account number of the financial instrument (e.g., the sender's token and/or the recipient's token), or any combination.

[00260] At an operation 1714, the payment service system 1218 may provide a notification including the sender public identifier, recipient public identifier, sender's token, funds to be transferred, or any other information to the sender FI system 1210 over the public network 1214 (or any network). The payment service system 1218 may also provide a notification including the sender public identifier, recipient public identifier, recipient's token, funds to be transferred, or any other information to the recipient FI system 1212 over the public network 1214 (or any network).

[00261] At an operation 1716, the sender FI system 1210 may de-tokenize the sender's token to identify the financial instrument number (e.g., the credit or debit card number). At an operation 1718, the sender FI system 1210 may look up one or more de-tokenized numbers to identify the sender and any number of accounts (e.g., DDAs) associated with the sender. In various implementations, the sender FI system 1210 may use the public identifier of the sender to further confirm accounts. The sender FI system 1210 may identify, e.g., account and/or other information relevant to the sender system 1206. If the sender and the sender's account(s) at the sender FI system 1210 are identified, in operation 1720 the sender FI system 1210 may generate a sender private identifier and share the private identifier with the payment services system 1218 which may then store the information in an information directory.

[00262] At an operation 1722, the sender FI system 1210 may determine if the sender account has sufficient finds to perform the fund transfer. The sender FI system 1210 may also perform internal checks, such as checks related to whether or not the transaction data is likely to be fraudulent/suspicious, etc. At an operation 1724, the sender FI system 1210 may provide instructions to the payment service system 1218 to update status of the transaction.

[00263] At an operation 1726, the payment service system 1218 may provide to the first non-FI system 1206 a first notification of the updated status, including whether or not the funds for the transfer may be transferred. At an operation 1728, the payment service system 1218 may provide to the first Non-FI system 1206 or the sender system 1202 a second notification of the updated status, including whether or not the funds for the transfer may be transferred. In various implementations, the payment status management logic 1310 may perform the operations 1726 and 1728.

[00264] At any time, the payment services system 1218 may generate a transaction identifier associated with the transaction. In one example, the payment services system 1218 may generate the transaction identifier once the sender private identifier is received from the sender FI system 1210 and the recipient private identifier is received from the recipient FI system 1212. The payment services system 1218 may provide transaction identifier and any other information to the recipient FI system 1212 and the sender FI system 1210.

[00265] At an operation 1730, the recipient FI system 1212 may de-tokenize the recipient token. At an operation 1734, the recipient FI system 1212 may look up one or more DDAs associated with the recipient's public identifier. The recipient FI system 1212 may use the public identifier of the recipient to look up DDAs associated with the sender system 1202 in the information directory 1270.

[00266] At an operation 1734, the sender FI system 1210 may provide the recipient FI system 1212 with a batch payment to settle the payment for the funds transfer over the ACH network 1216. In various implementations, the request to settle the payment may include a both transfer over the ACH network 1216 and may accompany the transaction identifier and the amount of the funds transfer.

[00267] At an operation 1736, the recipient FI system 1212, using the transaction identifier, may identify funds from the ACH batch processing and deposit funds in the amount of the transfer into a recipient account of the recipient. The funds may be deposited into the recipient's DDA by the recipient FI system 1212. At an operation 1738, the recipient FI system 1212 may update the status of the recipient account to indicate funds were transferred into the recipient account. At an operation 1740, the recipient FI system 1212 may provide the recipient non-FI system 1208 and/or the recipient system 1204 with an updated status indicating funds were transferred into the recipient account.

[00268] At an operation 1742, the recipient FI system 1212 may provide the payment service system 1218 with an updated status indicating funds were transferred into the recipient account. At an operation 1744, the payment service system 1218 may provide the first non-FI system 1206 with an updated status indicating funds were transferred into the recipient account. At an operation 1746, the first non-FI system 1206 may provide the sender system 1202 with an updated status indicating funds were transferred into the recipient account. At an operation 1748, the sender FI system 1210 and the recipient FI system 1212 may settle amounts of the fund transfer over the ACH system 1220 and/or the ACH network 1216. Operation 1748 may occur as part of batch transfer process between the two institutions.

[00269] In some embodiments, the recipient FI system 1212 may place funds within the recipient's account before funds are received through the ACH network from the sender FI system 1210. The recipient FI system 1212 may then be reimbursed when the batch payment is received.

[00270] FIG. 18A and FIG. 18B depict diagrams of flowchart of a methods 1800A and 1800B for securely transferring funds from a sender to a recipient in a funds transfer system, according to some implementations. The flowchart in 1800A and 1800B may be similar to the flow discussed in FIG. 17. The methods 1800A and 1800B may be performed by one or more of the systems or system components shown in FIGS. 12-14. It is noted that the methods 1800A and 1800B may include more or less operations than those explicitly shown.

[00271] At an operation 1802, the transaction data management logic 1302 of the payment services system 1218 may receive transaction data from the first non-FI system 1206 over the public network 1214. The transaction data may specify a transfer amount of a fund transfer between a sender and a recipient (e.g., between the sender system 1202 and the second non-FI system 1208 or the recipient system 1204), a sender public identifier to identify a sender of the fund transfer, a recipient public identifier to identify the recipient of the fund transfer, a sender token of a tokenized financial instrument of the sender, a recipient token of a tokenized financial instrument of the recipient, a sender FI identifier associated with the sender's financial instrument (e.g., issuing bank of the sender's financial instrument), and/or a recipient's FI identifier associated with the recipient's financial instrument. It will be appreciated that transaction data may be received from any number of sources. For example, the transaction data management logic 1302 may receive some of the transaction data from the

first non-FI ssytem 1206 and receive the sender token of a tokenized financial instrument of the sender, the recipient token of a tokenized financial instrument of the recipient, or both, from any number of entities.

[00272] At an operation 1804, the transaction data management logic 1302 may determine that the sender and recipient are not registered to respectively use the sender public identifier and the recipient public identifier to perform the fund transfer. In various implementations, the transaction data management logic 1302 may determine that the sender and the recipient are registered through non-financial institutions. In various implementations, the sender, the recipient, or both may not be registered.

[00273] At an operation 1806, the transaction data management logic 1302 may identify the sender FI system 1210 and the recipient FI system 1212 using the financial institution identifiers from the transaction data received in operation 1804.

[00274] At an operation 1808, the payment notification logic 1308 may send at least some of the transaction data to the sender financial institution to effectuate the fund transfer. In various implementations, the sender public identifier, the recipient public identifier, the transfer amount, recipient FI identifier, and/or the sender's token may be sent by the payment notification logic 1308 to the sender FI system 1210. The portions of the transaction data may comprise data sufficient to identify the sender of the fund transfer, the recipient of the fund transfer, and the transfer amount of the fund transfer.

[00275] At an operation 1810, the payment notification logic 1308 may send at least some of the transaction data to the recipient financial institution to effectuate the fund transfer. In various implementations, the recipient public identifier, the sender public identifier, the transfer amount, sender FI identifier, and/or the recipient's token may be sent by the payment notification logic 1308 to the recipient FI system 1212. The portions of the transaction data may comprise data sufficient to identify the sender of the fund transfer, the recipient of the fund transfer, and the transfer amount of the fund transfer.

[00276] At an operation 1812, the sender FI system 1210 may de-tokenize the sender private identifier. At an operation 1814, the sender FI system 1210 may retrieve a sender account using information from the de-tokenized sender private identifier (e.g., using the sender's credit card number or debit card number).

[00277] At an operation 1816, the sender FI system 1210 may evaluate whether or not the sender financial account has sufficient funds to perform the fund transfer. In some implementations, the sender FI system 1210 may ensure the sender has account access, sufficient funds, and other information needed to use the public identifier to perform the fund transfer.

[00278] At an operation 1818, the sender FI system 1210 may evaluate whether the fund transfer is likely to be fraudulent based on the transaction data. The sender FI system 1210 may provide a notification that it is capable of performing the fund transfer. At an operation 1820, the payment service system 1218 may receive a notification that the sender FI system 1210 is capable of performing the fund transfer.

[00279] At an operation 1822, the recipient FI system 1212 may de-tokenize the recipient's token. At an operation 1824, the recipient FI system 1212 may identify one or more of the recipient's accounts at the recipient FI system 1212 using the de-tokenized recipient's token (e.g., using the credit card number or debit card number of the recipient). If successful, may recipient FI system 1212 may provide a notification that the recipient's account has been determined to the payment service system 1218 in operation 1826. The payment services system 1218 may provide a transaction identifier for the transfer and a notification to recipient FI system 1212 and/or the sender FI system 1210 indicating that the one or both financial institutions are ready to perform the transfer.

[00280] In operation 1828, the sender FI system 1210 may provide funds for the funds transfer to the recipient FI system 1212 through the ACH system 1220 and/or the ACH network 1216 as part of a batch fund transfer process including an indication of the transaction identifier. At an operation 1830, the payment status management logic 1310 may receive a notification of a deposit of the fund transfer into a recipient financial account at the recipient financial institution.

[00281] FIG. 19 depicts a diagram of a data flow 1900 for registering a participant in a funds transfer system, according to some implementations. The data flow 1900 includes the components of the funds transfer system 1200, shown in FIG. 12, and discussed further herein. The data flow may include the payment service system 1218, and a participant system 1902, a participant non-FI system 1904, and a participant FI system 1906. In some implementations, the participant system 1902 corresponds to the sender system 1202, the participant non-FI

system 1904 corresponds to the first non-FI system 1206, and the participant FI system corresponds to the sender FI system 1210. In various implementations, the participant system 1902 corresponds to the recipient system 1204, the participant non-FI system 1904 corresponds to the second non-FI system 1208, and the participant FI system 1906 corresponds to the recipient FI system 1212. The data flow 1900 further includes a plurality of operations that correspond to instructions the registration logic 1286 may provide the components of the funds transfer system 1200. It is noted that the elements of the data flow 1900 are by way of example only, and that various implementations may employ a greater number of elements or a lesser number of elements without departing from the scope and substance of the inventive concepts described herein.

[00282] At an operation 1908, the participant FI system 1906 may create a participant account. The participant account may be linked to a financial account at a financial institution. In various implementations, the participant account may comprise an account number and/or other account identifier that can be used to identify the account when a participant seeks to register a public identifier for the account. The participant account may be linked to a financial account at a financial institution that comprises financial data, such as debit/credit card information, routing numbers, account numbers, etc. The financial data may comprise identifiers (names, routing numbers, etc.) of financial institutions that provide financial services to the participant system 1902. At an operation 1910, the participant FI system 1906 may create of a financial instrument (e.g., debit/credit cards may be printed and/or online accounts created for the participant account).

[00283] At an operation 1912, the participant FI system 1906 may share the financial instrument with the participant (user of the participant system 1902), the participant system 1902, and/or the payment service system 1218. The participant FI system 1906 may share the financial instrument in conjunction with a financial services provider (e.g., MasterCard). In some implementations, a code may be mailed and/or electronically sent to a participant or the participant system 1902 so that a participant may register user identifier(s) for the participant account.

[00284] In some implementations, a participant system 1902 may interact with the participant non-FI system 1904. In other implementations, the participant may interact with the participant non-FI system 1904 (e.g., using a credit card and a physical devcie of the

participant non-FI). Operations 1914-1920 are described herein from using the participant system 1902 although it will be appreciated that other implementations do not require all or any of the operations.

[00285] At an operation 1914, the participant system 1902 may receive a request from the participant to register a participant account using the financial instrument. At an operation 1916, the participant system 1902 may provide the participant with one or more participant registration screens. At an operation 1918, the participant system 1902 may receive a public identifier of a participant. In some implementations, the public identifier and the account information may be provided into an input device of the participant system 1902. The public identifier may comprise an alphanumeric or other string that can identify the participant. The participant system 1902 may receive passwords, biometric authentication techniques, other authentication techniques or the like that allow verification of the public identifier.

[00286] At an operation 1920, the participant system 1902 may send the public identifier and the participant account information to the participant non-FI system 1904. In some embodiments, the participant system 1902 or participant (e.g., a user) may provide the financial instrument (e.g., an account number, routing number or the like related to a financial instrument) to the participant non-FI system 1904 or may tokenize the financial instrument to generate a token of the financial instrument and provide the token to the participant non-FI system 1904 or a financial services provider. The participant system 1902 may also send a FI identifier that issued the financial instrument to the participant non-FI system 1904.

[00287] At an operation 1922, the participant non-FI system 1904 or a financial services provider associated with the account data may identify tokenized account data representative of participant account information. The tokenized account data may comprise an encrypted version of the participant account information. In some implementations, the tokenized account data may comprise a proxy number that is representative of debit/credit/etc. card numbers in the participant account information. At an operation 1926, the participant non-FI system 1904 (or the financial services provider) may identify tokenized account data representative of the participant account information.

[00288] At an operation 1924, the participant non-FI system 1904 and/or the financial services provider may send the public identifier and the tokenized account data to the payment service system 1218. At an operation 1926, the participant non-FI system 1904 may optionally

send the public identifier and/or the tokenized account data to the participant FI system 1906. In some implementations, the participant non-FI system 1904 may provide the information to the participant FI system 1906, the payment service system 1218, or both.

[00289] At an operation 1928, the participant FI system 1906 may optionally send the public identifier and/or the tokenized account data to the payment service system 1218. In one example, the information is shared by the participant non-FI system 1904 with the participant FI system 1906 which, in turn, optionally shares all or some of the information with the payment service system 1218.

[00290] At an operation 1930, the payment service system 1218 may verify the public identifier is not in use. Verification of the public identifier may include reviewing an information directory to determine whether another user has already registered the public identifier in association with another account. In some implementations, the payment service system 1218 may return a failure message if the public identifier is already in use. The user identification verification logic 1404 may perform operation 1930.

[00291] At an operation 1932, the payment service system 1218 may identify a participant financial institution using the tokenized account data or a financial institution identifier from the participant system 1902 and/or the participant non-FI system 1904. In some embodiments, the payment service system 1218 may evaluate the tokenized account data for names, identifiers, or the like that correspond to financial institutions. In various implementations, the payment service system 1218 may de-tokenize the tokenized account data to extract information to identify a participant financial institution (e.g., the financial institution that manages the participant FI system 1906).

[00292] At an operation 1934, the payment service system 1218 may send the public identifier and the tokenized account data (e.g., the participant's token) to the participant FI system 1906. The account confirmation logic 1410 may perform the operations 1932 and 1934.

[00293] At an operation 1936, the participant FI system 1906 may de-tokenize the tokenized account data. The participant FI system 1906 may decrypt, translate any proxy numbers, etc. to obtain account information for the participant account. At an operation 1938, the participant FI system 1906 may perform a DDA lookup using, e.g., the account information

for the participant's account. At an operation 1940, the participant FI system 1906 may map the DDA to the user's public identifier. The participant FI system 1906 may generate a private identifier associated with an account number of the participant at the participant's FI system 1906. In some implementations, the participant FI system 1906 may write the account number (e.g., DDA), the public identifier, and the private identifier into an information directory stored in the participant FI system 1906. At an operation 1942, the participant FI system 1906 may update the public identifier status to reflect the fact that the public identifier can be used for future funds transfers and other transactions involving the participant.

[00294] At an operation 1944, the participant FI system 1906 may provide the payment service system 1218 with a confirmation that the public identifier can be used for future fund transfers and other transactions involving the participant. The participant FI system 1906 may also share the private identifier of the participant with the payment service system 1218.

[00295] At an operation 1946, the information directory management logic 1306 may associate the participant private identifier with the participant public identifier. At an operation 1948, the payment service system 1218 may provide the participant non-FI system 1904 with a success message that the public identifier can be used for future funds transfers and other transactions involving the participant. The account confirmation logic 1410 may perform operation 1948.

[00296] At an operation 1950, the participant non-FI system 1904 may provide configure the participant system 1902 to show a success message indicating that the participant successfully registered. At an operation 1952, the participant non-FI system 1904 may provide the participant system 1902 with a success message that the public identifier can be used for future funds transfers and other transactions involving the participant. At an operation 1954, the success message may be shown on the participant system 1902.

[00297] FIG. 20 depicts a diagram of a flowchart of a method 2000 for registering a participant in a funds transfer system, according to some implementations. The method 2000 may be performed by one or more of the modules shown in FIGS. 12-14. It is noted that the method 2000 may include more or less operations than those explicitly shown.

[00298] At an operation 2002, the participant account issuing logic 1402 creates a participant financial account. The participant account issuing logic 1402 may create a sender

financial account corresponding to a specific sender or a recipient account corresponding to a specific recipient. The participant account issuing logic 1402 may link the participant account to a financial account maintained/backed by a financial institution. In some implementations, the participant account may be linked to collateral, cash, etc. The participant account issuing logic 1402 may store information about the participant account in the information directory 1280.

[00299] At an operation 2004, the user identification verification logic 1404 receives a proposed public identifier from the participant. The proposed public identifier may or may not comprise email addresses, alphanumerical usernames, Universal Payment Identification Codes (UPICs), phone numbers, user-generated or system-generated numbers or character strings, etc. The proposed public identifier may provide a basis to identify a participant and/or a participant system.

[00300] At an operation 2006, the user identification verification logic 1404 verifies whether the proposed public identifier is associated with any participants. The user identification verification logic 1404 may verify whether or not the proposed public identifier comprises appropriate email addresses, alphanumerical usernames, Universal Payment Identification Codes (UPICs), phone numbers, user-generated or system-generated numbers or character strings, etc. The user identification verification logic 1404 may verify whether or not the proposed public identifier corresponds to a public identifier used to identify another participant.

[00301] At an operation 2008, the user identification verification logic 1404 registers the proposed public identifier as the participant public identifier if the proposed public identifier is not associated with any participants. As discussed herein, the participant public identifier and any other financial information (e.g., tokens, financial instrument numbers and the like) may be shared with the participant's financial institution. Alternately, the participant may interact with the financial institution (e.g., log onto the participant's account) and the financial institution may confirm the participant's account. The financial institution may generate a participant private identifier associated with the participant and the participant's account number at the financial institution and private the participant private identifier with the payment services system.

[00302] The user identification verification logic 1404 may store the proposed public identifier along with the private identifier and associated account information in the information directory 1280.

[00303] FIG. 21 depicts an example of a digital device 2100, according to some implementations. The digital device 2100 comprises a processor 2105, a memory system 2110, a storage system 2115, a communication network interface 2120, an Input/output (I/O) interface 2125, a display interface 2130, and a bus 2135. The bus 2135 may be communicatively coupled to the processor 2105, the memory system 2110, the storage system 2115, the communication network interface 2120, the I/O interface 2125, and the display interface 2130.

[00304] In some implementations, the processor 2105 comprises circuitry or any processor capable of processing the executable instructions. The memory system 2110 comprises any memory configured to store data. Some examples of the memory system 2110 are storage devices, such as RAM or ROM. The memory system 2110 may comprise the RAM cache. In various implementations, data is stored within the memory system 2110. The data within the memory system 2110 may be cleared or ultimately transferred to the storage system 2115.

[00305] The storage system 2115 comprises any storage configured to retrieve and store data. Some examples of the storage system 2115 are flash drives, hard drives, optical drives, and/or magnetic tape. In some implementations, the digital device 2100 includes a memory system 2110 in the form of RAM and a storage system 2115 in the form of flash data. Both the memory system 2110 and the storage system 2115 comprise computer readable media which may store instructions or programs that are executable by a computer processor including the processor 2105.

[00306] The communication network interface (com. network interface) 2120 may be coupled to a data network. The communication network interface 2120 may support communication over an Ethernet connection, a serial connection, a parallel connection, or an ATA connection, for example. The communication network interface 2120 may also support wireless communication (e.g., 802.1 a/b/g/n, WiMAX, LTE, 3G, 2G). It will be apparent to those skilled in the art that the communication network interface 2120 may support many wired and wireless standards.

[00307] The optional input/output (I/O) interface 2125 is any device that receives input from the user and output data. The display interface 2130 is any device that may be configured to output graphics and data to a display. In one example, the display interface 2130 is a graphics adapter.

[00308] It will be appreciated by those skilled in the art that the hardware elements of the digital device 2100 are not limited to those depicted in FIG. 21. A digital device 2100 may comprise more or less hardware elements than those depicted. Further, hardware elements may share functionality and still be within various implementations described herein. In one example, encoding and/or decoding may be performed by the processor 2105 and/or a co-processor located on a GPU.

[00309] The above-described functions and components may be comprised of instructions that are stored on a storage medium such as a computer readable medium. The instructions may be retrieved and executed by a processor. Some examples of instructions are software, program code, and firmware. Some examples of storage medium are memory devices, tape, disks, integrated circuits, and servers. The instructions are operational when executed by the processor to direct the processor to operate in accord with some implementations. Those skilled in the art are familiar with instructions, processor(s), and storage medium.

[00310] For purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the description. It will be apparent, however, to one skilled in the art that implementations of the disclosure can be practiced without these specific details. In some instances, modules, structures, processes, features, and devices are shown in block diagram form in order to avoid obscuring the description. In other instances, functional block diagrams and flow diagrams are shown to represent data and logic flows. The components of block diagrams and flow diagrams (e.g., modules, blocks, structures, devices, features, etc.) may be variously combined, separated, removed, reordered, and replaced in a manner other than as expressly described and depicted herein.

[00311] Reference in this specification to "one implementation", "an implementation", "some implementations", "various implementations", "certain implementations", "other implementations", "one series of implementations", or the like means that a particular feature, design, structure, or characteristic described in connection with the implementation is included

in at least one implementation of the disclosure. The appearances of, for example, the phrase "in one implementation" or "in an implementation" in various places in the specification are not necessarily all referring to the same implementation, nor are separate or alternative implementations mutually exclusive of other implementations. Moreover, whether or not there is express reference to an "implementation" or the like, various features are described, which may be variously combined and included in some implementations, but also variously omitted in other implementations. Similarly, various features are described that may be preferences or requirements for some implementations, but not other implementations.

[00312] The language used herein has been principally selected for readability and instructional purposes, and it may not have been selected to delineate or circumscribe the inventive subject matter. It is therefore intended that the scope be limited not by this detailed description, but rather by any claims that issue on an application based hereon. Accordingly, the disclosure of the implementations is intended to be illustrative, but not limiting, of the scope, which is set forth in the following claims.

CLAIMS

1. A method being implemented via execution of computing instructions configured to run at one or more processors and stored at one or more non-transitory computer-readable media, the method comprising:

receiving, at a payment service computer system, transaction data related to a fund transfer, the transaction data specifying a transfer amount of the fund transfer, a sender public identifier to identify a sender of the fund transfer, a recipient public identifier to identify a recipient of the fund transfer, a sender financial institution identifier for a sender financial institution, a recipient financial institution identifier for a recipient financial institution, and a tokenized financial instrument of the sender;

determining, at the payment service computer system, the sender financial institution, using the sender financial institution identifier, the sender financial institution being a member of a payment network associated with the payment service computer system;

providing, from the payment service computer system to the sender financial institution, the tokenized financial instrument of the sender to enable the sender financial institution to de-tokenize the tokenized financial instrument of the sender and identify a sender account of the sender financial institution associated with the sender;

providing, from the payment service computer system to the sender financial institution, the transfer amount of the fund transfer, the recipient public identifier, and the recipient financial institution identifier to enable the sender financial institution to determine availability of money in the sender account to satisfy the transfer amount of the fund transfer;

determining, at the payment service computer system, a recipient private identifier based on the recipient public identifier;

generating, at the payment service computer system, a transaction identifier associated with the fund transfer;

sending the transaction identifier from the payment service computer system to the sender financial institution; and

providing the transaction identifier and a recipient private identifier from the payment service computer system to the recipient financial institution to enable the recipient financial institution to identify a recipient account of the recipient financial institution associated with the recipient to enable the recipient financial institution to receive an ACH message over an ACH network, the ACH message indicating payment from the sender financial institution to the recipient financial institution, the ACH message being generated by the sender financial institution and including the transaction identifier to identify the fund transfer between the sender and the recipient, and the ACH message allowing the recipient financial institution to retrieve funds from an ACH batch transfer and deposit the funds into the recipient account.

2. The method of claim 1, further comprising validating that the sender has authorization to use the sender public identifier to perform the fund transfer.

3. The method of claim 1, further comprising:

receiving, at the payment service computer system, a tokenized financial instrument of the recipient and the recipient financial institution identifier associated with the recipient financial institution;

determining, at the payment service computer system, using the recipient financial institution identifier, the recipient financial institution, the recipient financial institution being a member of the payment network associated with the payment service computer system; and

providing, from the payment service computer system to the recipient financial institution, the tokenized financial instrument of the recipient to enable the recipient financial institution to de-tokenize the tokenized financial instrument of the recipient and identify the recipient account.

4. The method of claim 1, wherein the transaction data related to the fund transfer are received from a first online reseller of goods.

5. The method of claim 4, wherein the first online reseller of goods tokenizes a financial instrument of the sender to create the tokenized financial instrument of the sender.

6. The method of claim 5 wherein the financial instrument of the sender is issued by the sender financial institution.

7. The method of claim 4, further comprising:

receiving, at the payment service computer system, a tokenized financial instrument of the recipient from a second online reseller of goods different than the first online reseller of goods.

8. The method of claim 7, wherein the second online reseller of goods tokenizes a financial instrument of the recipient to create the tokenized financial instrument of the recipient.

9. The method of claim 1, wherein the recipient financial institution transfers the funds to the recipient account before the recipient financial institution receives the ACH message.

10. The method of claim 1, further comprising:

providing a request from the payment service computer system to a recipient system associated with the recipient requesting if the recipient will accept the fund transfer from the sender.

11. A system comprising:

one or more processors;

one or more non-transitory computer-readable media storing computer instructions configured to run on the one or more processors to perform:

receiving, at a payment service computer system, transaction data related to a fund transfer, the transaction data specifying a transfer amount of the fund transfer, a sender public identifier to identify a sender of the fund transfer, a recipient public identifier to identify a recipient of the fund transfer, a

sender financial institution identifier for a sender financial institution, a recipient financial institution identifier for a recipient financial institution, and a tokenized financial instrument of the sender;

determining, at the payment service computer system, the sender financial institution, using the sender financial institution identifier, the sender financial institution being a member of a payment network associated with the payment service computer system;

providing, from the payment service computer system to the sender financial institution, the tokenized financial instrument of the sender to enable the sender financial institution to de-tokenize the tokenized financial instrument of the sender and identify a sender account of the sender financial institution associated with the sender;

providing, from the payment service computer system to the sender financial institution, the transfer amount of the fund transfer, the recipient public identifier, and the recipient financial institution identifier to enable the sender financial institution to determine availability of money in the sender account to satisfy the transfer amount of the fund transfer;

determining, at the payment service computer system, a recipient private identifier based on the recipient public identifier;

generating, at the payment service computer system, a transaction identifier associated with the fund transfer;

sending the transaction identifier from the payment service computer system to the sender financial institution; and

providing the transaction identifier and a recipient private identifier from the payment service computer system to the recipient financial institution to enable the recipient financial institution to identify a recipient account of the recipient financial institution associated with the recipient to enable the recipient financial institution to receive an ACH message over an ACH network, the ACH message indicating payment from the sender financial institution to the recipient financial institution, the ACH message being generated by the sender financial institution and including the transaction identifier to identify the fund transfer between the sender and the recipient,

and the ACH message allowing the recipient financial institution to retrieve funds from an ACH batch transfer and deposit the funds into the recipient account.

12. The system of claim 11, wherein the method further comprises validating that the sender has authorization to use the sender public identifier to perform the fund transfer.

13. The system of claim 11, wherein the method further comprises:

receiving, at the payment service computer system, a tokenized financial instrument of the recipient and the recipient financial institution identifier associated with the recipient financial institution;

determining, at the payment service computer system, using the recipient financial institution identifier, the recipient financial institution, the recipient financial institution being a member of the payment network associated with the payment service computer system; and

providing, from the payment service computer system to the recipient financial institution, the tokenized financial instrument of the recipient to enable the recipient financial institution to de-tokenize the tokenized financial instrument of the recipient and identify the recipient account.

14. The system of claim 11, wherein the transaction data related to the fund transfer are received from a first online reseller of goods.

15. The system of claim 14, wherein the first online reseller of goods tokenizes a financial instrument of the sender to create the tokenized financial instrument of the sender.

16. The system of claim 15 wherein the financial instrument of the sender is issued by the sender financial institution.

17. The system of claim 14, wherein the computing instructions are further configured to perform:

receiving, at the payment service computer system, a tokenized financial instrument of the recipient from a second online reseller of goods different than the first online reseller of goods.

18. The system of claim 17, wherein the second online reseller of goods tokenizes a financial instrument of the recipient to create the tokenized financial instrument of the recipient.

19. The system of claim 1, wherein the recipient financial institution transfers funds to the recipient account before the recipient financial institution receives the ACH message.

20. One or more non-transitory computer-readable media comprising executable instructions, the executable instructions being executable by a processor to perform:

receiving, at a payment service computer system, transaction data related to a fund transfer, the transaction data specifying a transfer amount of the fund transfer, a sender public identifier to identify a sender of the fund transfer, a recipient public identifier to identify a recipient of the fund transfer, a sender financial institution identifier for a sender financial institution, a recipient financial institution identifier for a recipient financial institution, and a tokenized financial instrument of the sender;

determining, at the payment service computer system, the sender financial institution, using the sender financial institution identifier, the sender financial institution being a member of a payment network associated with the payment service computer system;

providing, from the payment service computer system to the sender financial institution, the tokenized financial instrument of the sender to enable the sender financial institution to de-tokenize the tokenized financial instrument of the sender and identify a sender account of the sender financial institution associated with the sender;

providing, from the payment service computer system to the sender financial institution, the transfer amount of the fund transfer, the recipient public

identifier, and the recipient financial institution identifier to enable the sender financial institution to determine availability of money in the sender account to satisfy the transfer amount of the fund transfer;

determining, at the payment service computer system, a recipient private identifier based on the recipient public identifier;

generating, at the payment service computer system, a transaction identifier associated with the fund transfer;

sending the transaction identifier from the payment service computer system to the sender financial institution; and

providing the transaction identifier and a recipient private identifier from the payment service computer system to the recipient financial institution to enable the recipient financial institution to identify a recipient account of the recipient financial institution associated with the recipient to enable the recipient financial institution to receive an ACH message over an ACH network, the ACH message indicating payment from the sender financial institution to the recipient financial institution, the ACH message being generated by the sender financial institution and including the transaction identifier to identify the fund transfer between the sender and the recipient, and the ACH message allowing the recipient financial institution to retrieve funds from an ACH batch transfer and deposit the funds into the recipient account.