System and Method for Facilitating a Transaction with a Social Network Account Identifier

Technical Field

[0001] The present invention relates broadly, but not exclusively, to systems and methods for facilitating a transaction with social network account identifier.

Background Art

[0002] Social networks have become one of the dominant forms of user interaction with the Internet in the recent years. Extension adoption of social networking services has led to increasing use of social login – a form of single sign-on system leveraging on existing information such as account identifiers (or social network account identifiers) and passwords from social network services to sign into third party services, rather than creating a new specific account for the third party services. Social login can simplify third party account registration and subsequent account access for users while providing pre-registration validation for the third party services.

[0003] However, social login is generally unavailable to pre-existing users of third party services. In other words, if current users of the third party services wish to leverage on their social network account identifiers, it may be necessary to create new separate accounts with the third party services. Moreover, implementation and use of social login can generally increase the attack surface of the third party services i.e. the totality of different entry points from which unauthorised users can extract and/or modify information within the third party services. Particularly, unauthorised users can potentially use data breaches on social networks to obtain credentials of the social network accounts without the legitimate users' permissions and in turn use such compromised credentials to access the linked third party services. The compromised social network accounts may also be used to create new fraudulent accounts with other third party services. Importantly, reliance on social network accounts for social login can create a single failure point which would considerably exacerbate the damage caused to the users if the social network accounts were to be compromised.

[0004] In view of the security concerns associated with social login, service providers, particularly those associated with financial and/or payment services, have been generally reluctant to implement social login for users. Users, likewise, are also reluctant to adopt

social login for financial and/or payment services, particularly in light of multiple high-profile data and privacy breaches. Hence, for financial and/or payment services, particularly with regard to transactions involving goods and/or services, the users are likely to adhere to traditional transaction and authentication methods, such as payment cards with “chip and personal identification number (PIN)” authentication method, where users provide a confidential numerical PIN code of 4-6 digits together with the payment card at the time of initiating the transaction. However, the methods of authentication for payment cards are not impervious to fraud. Vulnerabilities exist and attacks exploiting such vulnerabilities have been used against such authentication methods. More importantly, the method requires the users to remember their PIN code. If the users forget the correct PIN code, the PIN code either has to be retrieved or reset at the request of the users.

[0005] Accordingly, what is needed is a system and method for facilitating a transaction with a social network account identifier that seeks to address one or more of the above-mentioned problems. Furthermore, other desirable features and characteristics will become apparent from the subsequent detailed description and the appended claims, taken in conjunction with the accompanying drawings and this background of the disclosure.

Summary

[0006] A first aspect provides a system configured to facilitate a transaction with a social network account identifier, the system comprising:

at least one processor; and

at least one memory including computer program code;

the at least one memory and the computer program code configured to, with the at least one processor, cause the system at least to:

receive, from a device, a transaction request comprising the social network account identifier and an authentication input;

compare the received authentication input with an authentication code associated with the social network account identifier;

determine one or more payment account information that is associated with the social network account identifier, on the condition that the received authentication input corresponds to the authentication code; and

forward, to a payment processing server, the transaction request and the one or more determined payment account information.

[0007] A second aspect provides a method for facilitating a transaction with a social network account identifier, the method comprising,

receiving, from a device, a transaction request comprising the social network account identifier and an authentication input;

comparing the received authentication input with an authentication code associated with the social network account identifier;

determining one or more payment account information that is associated with the social network account identifier, on the condition that the received authentication input corresponds to the authentication code; and

forwarding, to a payment processing server, the transaction request and the one or more determined payment account information.

Brief Description of Drawings

[0008] Embodiments of the disclosure will be better understood and readily apparent to one of ordinary skill in the art from the following written description, by way of example only, and in conjunction with the drawings, in which:

Fig.1

[0009] Fig. 1 shows a schematic diagram of a system configured to associate a social network account identifier with one or more payment account information, in accordance with embodiments of the disclosure.

Fig.2

[0010] Figs. 2A and 2B show schematic diagrams of a system configured to facilitate a transaction with a social network account identifier, in accordance with embodiments of the disclosure.

Fig.3

[0011] Fig. 3 shows a flowchart illustrating a method for associating a social network account identifier with one or more payment account information, in accordance with embodiments of the disclosure.

Fig.4

[0012] Fig. 4 shows a flowchart illustrating a method for facilitating a transaction, in accordance with embodiments of the disclosure.

Fig.5

[0013] Fig. 5 shows an exemplary server including modules for facilitating a transaction with a social network account identifier, in accordance with embodiments of the disclosure.

Fig.6

[0014] Fig. 6 shows a schematic diagram of a computing device used to realise the systems of Figs. 1 and 2.

[0015] Skilled artisans will appreciate that elements in the figures are illustrated for simplicity and clarity and have not necessarily been depicted to scale. For example, the dimensions of some of the elements in the illustrations, block diagrams or flowcharts may be exaggerated in respect to other elements to help to improve understanding of the present embodiments.

Detailed Description

Overview

[0016] Various embodiments of the present disclosure provide a system and a method for facilitating a transaction with a social network account identifier. More specifically, embodiments of the present disclosure provide an alternative user identification and/or authentication system which can advantageously allow users to perform transactions using the social network account identifier, while addressing and/or mitigating one or more of the aforementioned drawbacks. Advantageously, any increase in attack surface of the system and method can be mitigated and/or addressed with an authentication method which include an out-of-band authentication message channelled through a server that is associated with the social network account identifier (i.e. a social network service server) and a user device. The authentication can be performed during the registration, and can also be beneficially implemented during the transaction process as a form of continuous authentication.

[0017] In various embodiments, the social network account identifier can be associated with a payment account of a user, registered by the user with an entity party to the payment network (e.g. a payment facilitator or an issuer) and used in lieu of the payment account details for a transaction. That is, the social network account identifier can be used as a reference that maps back to one or more payment account information of the payment account. The social network account identifier is used as a substitute for one or more payment account information that may be sensitive in at least a part of the transaction process, thereby minimising exposure of the one or more payment account information and lowering risk of compromise and/or unauthorised access to the payment account

information. As will be described in further details, the social network account identifier, together with an appropriate authentication input can be appropriately used as an identification and/or authentication for user access to transaction services. These transaction services include, but is not limited to transactions online (e.g. online banking and e-commerce) and in-person transactions (e.g. transactions at retail locations, at payment terminals such as automated teller machines (ATMs) and retail banking).

Registration

[0018] In various embodiments of the present disclosure, the user can first register a social network account identifier to be associated with the payment account. The registration can be performed via an application program that is installed on a user device, through an online portal (e.g. HTML website) associated with the entity party to the payment network, or at payment terminals (e.g. ATMs associated with an issuer of the payment account). A registration request that is submitted by the user through the application program or online portal can include (i) the social network account identifier and (ii) one or more payment account information of the payment account that is to be associated with the social network account identifier. In embodiments of the disclosure, the entity to which the registration request is sent can be a payment facilitator (e.g. Mastercard) or the issuer of the payment account. The payment facilitator is an entity (e.g. a company or organisation) which operates to process transactions, clear and settle funds for payments between two other entities (e.g. two banks). The issuer of the payment account is an entity (e.g. a company or organisation) typically issues (e.g. establishes, manages, administers) a payment account (e.g. a credit card account, a stored value card, or a debit card account linked to a bank account).

[0019] The registration request is routed to a server associated with the entity that is responsible for association of the social network account identifier with the payment account. As will be described in the following description, the entity can be the payment facilitator or the issuer. The server is configured to receive and process the registration request, and can, on receiving the registration request, validate the request and authenticate the user by generating and transmitting a verification code to a server that is associated with the social network account identifier (i.e. a social network service server). The social network service server can, in turn, forward the verification code to the user via communication means indicated by the user on the social network service, to authenticate the user. For example, the verification code can be sent via communication means such as short message service (SMS), email, or a private message on the social network platform. The verification code can be received by the user and entered into a verification input field on the application program

that is installed on the user device, or through the online portal associated with the entity. The verification input is then transmitted by the user device to the registration server. The registration server is configured to receive the verification input from the user device and compare the received verification input with the verification code that is transmitted to the social network service server. If the received verification input corresponds to the transmitted verification code, the one or more payment account information can be associated with the social network account identifier.

[0020] In various embodiments of the present disclosure, the server is further configured to transmit a confirmation message (i.e. an association success message) to the user device, in response to association of the one or more payment account information with the social network account identifier. In embodiments where the server is associated with the issuer of the payment account rather than the payment facilitator, the server can be further configured to transmit a copy of a mapping file including the association to a server of the payment facilitator.

[0021] In various embodiments of the present disclosure, the registration request can further include a user-determined identification number. The user-determined identification number can be recorded by the server and can serve as the authentication code associated with the social network account identifier. That is, user-determined identification number can be used to authenticate transaction requests including the social network account identifier. In alternate embodiments of the present disclosure, the authentication code can be a card verification code associated with the payment account or a one-time password that is transmitted to the user device.

Transaction Process

[0022] In various embodiments, the social network account identifier can be presented in lieu of payment account information to a device (e.g. in lieu of a payment card at a transaction terminal or in lieu of an user identifier at an online portal or application program) to initiate a transaction. That is, the social network account identifier can be used as an identification and/or authentication method for user access to transaction services once the social network account identifier is associated with the one or more payment account information.

[0023] The transaction process is initiated when a system configured to facilitate a transaction that is received from the device. The transaction request includes the social network account identifier and an authentication input. The system can, upon receiving the

transaction request, compare the received authentication input with the authentication code associated with the social network account identifier. On condition that the received authentication input corresponds to the authentication code, the system can be configured to determine the one or more payment account information that is associated (i.e. registered) with the social network account identifier and forward the transaction request together with the one or more determined payment account information to a payment processing server for further processing. The system can also be configured to modify the transaction request to include the one or more determined payment account information prior to forwarding the transaction request.

[0024] Accordingly, embodiments of the present disclosure can advantageously provide a simplified, streamlined system and method for facilitating a transaction with a social network account identifier. Various embodiments provide a system and method that can receive, determine and communicate authenticity and payment card information in a safe and efficient manner.

Terms Description (in Addition to Plain and Dictionary Meaning of Terms)

[0025] Unless context dictates otherwise, the following terms will be given the meaning provided here:

[0026] An payment account refers to one that is suitable for a transaction. The payment account can be used for the purpose of purchasing goods and/or services. The payment account can be a deposit account, a credit card account, a current account, or any other type of account offered by a financial institution, and represents the funds that an account holder has entrusted to the financial institution and from which the account holder can make withdrawals. Alternatively, an payment account can be a loan account in which case the account holder owes money to the financial institution. Moreover, the payment account may be a payment card or a digital wallet. A payment card is a card that can be used by an account holder for a transaction with a merchant. In the following disclosure, the term “payment cards” refer to any suitable transaction cards, such as credit cards, debit cards, prepaid cards, charge cards, membership cards, promotional cards, frequent flyer cards, identification cards, gift cards, and/or any other device that may hold payment account information, such as mobile phones, smartphones, smartwatches, tablets, personal digital assistants (PDAs), and/or computers. Each type of payment card can be used as a method of payment for performing a transaction. A digital wallet refers to an account that can be used by a digital wallet user for a transaction with a merchant. The digital wallet is usually linked to a digital wallet user’s bank account or a digital wallet user’s payment card.

Typically, the payments by digital wallets are facilitated by a different entity such as Google®, Apple® or Paypal®. Additionally or alternatively, the payments by digital wallets are facilitated by an entity who also manages the payment cards such as Mastercard®. Such transactions that are made using the digital wallets are also known as wallet-based transactions.

[0027] An acquirer refers to a bank or financial institution that processes credit or debit payments on behalf of the merchant. The acquirer may manage a corresponding acquirer server which may allow merchants to accept payments using a payment account (e.g. debit or credit cards) from the card-issuing banks (i.e. issuers). The acquiring bank may enter into a contract or arrangement with the merchant and may offer the merchant a corresponding merchant account. This arrangement provides the merchant with a line of credit. Under the agreement, the acquiring bank exchanges funds with issuers on behalf of the merchant, and pays the merchant for its daily payment-card activity's net balance, that is, gross sales minus reversals, interchange fees, and acquirer fees. The acquirer may impose acquirer fees for an additional cost mark-up added to an association of interchange fees and may vary according to the acquirer's discretion. The acquirer may also maintain an acquiring channel that drives a network for a transaction terminal. The transaction terminal may be provided by the acquirer and the network may have the capability of accepting transactions from the transaction terminal connected to the acquirer’s interface.

[0028] A database, or databases refer to any databases located within a computing system or remote server such as a computer in a cloud server. The database or databases may each be a cloud database running on a cloud computing platform.

[0029] An issuer refers to a bank or credit union who offers credit means to consumers (or users), such as credit cards. The issuer makes the credit limit available to cardholders (i.e. users) and is responsible for sending payments to the acquirer or merchants for purchases made with credit cards from that bank. The issuer may manage a corresponding issuer server which interlinks the user and the acquirer by contracting with the cardholders for the terms of the repayment of transactions. The issuer server is generally associated with the payment account issuer, i.e. the issuer of the account associated with the payment account information and used to fund the transaction. The issuer server may include one or more computing devices that are used to process funding of the transaction. The issuer may be an entity (e.g. a company or organisation) which issues (e.g. establishes, manages, administers) a payment account (e.g. a credit card account, a stored value card, or a debit card account linked to a bank account) and payment account information. The issuer server

may include one or more computing devices that are used to establish communication with another server by exchanging messages with and/or passing information to the other server. Further, in various embodiments, the issuer server can also establish communication with the other server to complete a process or step that may be external to the transaction process. For example, the other server may be associated with a service, and the issuer server can be configured to communicate with the server to register a user to the service, or to verify and/or authenticate the user to the service.

[0030] A payment device refers to a device on which transactions can be made. In the following disclosure, the payment device can belong to the user (i.e. a user device) and may be a portable computing device on which the user is able to install and view the application program. That is, the user may register as a registered user of the application program executing on the payment device. Examples of a payment device include but not limited to mobile phones, smartphones, smartwatches, tablets, personal digital assistants (PDAs), and/or computers. Importantly, a payment device can also include a transaction terminal (see below).

[0031] A payment network server is used to settle financial transactions through the transfer of monetary value, and include the institutions, instruments, people, rules, procedures, standards, and technologies that make such an exchange possible. The payment network server may be managed by a payment network facilitator which is an intermediary that links the different parties involved in a financial transaction. For example, when a user uses his payment card at the payment device to initiate a transaction request, the payment network server (or payment network facilitator) may route the transaction request from the transaction terminal to the issuer and may route an approval from the issuer to the acquirer. A further example of the payment network server is one that manages rules for accounts that may be issued by issuers and facilitates funds exchange between accounts. Therefore, the payment network server may connect the issuer associated to an account of the user and the merchant for the transfer of funds between the issuer and the merchant. The payment network server (or payment network facilitator) may also generate programming codes and instructions relating to the transaction. Further, in embodiments, the payment network server can be configured to route information to a social network service server to register, verify and/or authenticate the user.

[0032] A transaction generally includes a financial transaction, and can effect a change in the balance of financial accounts of two or more parties. A financial transaction can also include an agreement, or communication, carried out between a buyer (e.g. a user or

account holder) and a seller (e.g. a merchant) to exchange goods and/or services for payment. Accordingly, a transaction request includes information that is exchanged or provided to facilitate the transaction. A typical transaction request can include the user's payment account information (e.g. user's payment card details). The user's payment account information can include an issuer's identifier identifying the issuer managing the user's payment account. The transaction request can also include the value of the goods and/or services, a description of the goods and/or services and details of the merchant involved in the transaction. The transaction request can also include information relating to the merchant, e.g. a merchant's account identifying an acquirer managing the merchant's account. The transaction can also include an electronic funds transfer (i.e. the electronic transfer of money from one financial account to another, either within a single financial institution or across multiple institutions via computer-based systems). In embodiments of the disclosure, a social network account identifier can be included in the transaction request.

[0033] A transaction terminal refers to a device which interfaces with payment cards to facilitate a transaction. In the following disclosure, the transaction terminal may be a device located at the merchant's store, a portable computing device or a payment gateway in the merchant's website. Examples of such a terminal include but not limited to a point-of sale (POS) terminal, an automated teller machine, a mobile phone, a laptop or a tablet.

Exemplary Embodiments

[0034] Embodiments of the present disclosure will be described, by way of example only, with reference to the drawings. Like reference numerals and characters in the drawings refer to like elements or equivalents.

[0035] Some portions of the description which follows are explicitly or implicitly presented in terms of algorithms and functional or symbolic representations of operations on data within a computer memory. These algorithmic descriptions and functional or symbolic representations are the means used by those skilled in the data processing arts to convey most effectively the substance of their work to others skilled in the art. An algorithm is here, and generally, conceived to be a self-consistent sequence of steps leading to a desired result. The steps are those requiring physical manipulations of physical quantities, such as electrical, magnetic or optical signals capable of being stored, transferred, combined, compared, and otherwise manipulated.

[0036] Unless specifically stated otherwise, and as apparent from the following, it will be appreciated that throughout the present specification, discussions utilizing terms such as

“associating”, “calculating”, “comparing”, “determining”, “forwarding”, “generating”, “identifying”, “including”, “inserting”, “modifying”, “receiving”, “replacing”, “scanning”, “transmitting” or the like, refer to the action and processes of a computer system, or similar electronic device, that manipulates and transforms data represented as physical quantities within the computer system into other data similarly represented as physical quantities within the computer system or other information storage, transmission or display devices.

[0037] The present specification also discloses apparatus for performing the operations of the methods. Such apparatus may be specially constructed for the required purposes, or may include a computer or other computing device selectively activated or reconfigured by a computer program stored therein. The algorithms and displays presented herein are not inherently related to any particular computer or other apparatus. Various machines may be used with programs in accordance with the teachings herein. Alternatively, the construction of more specialized apparatus to perform the required method steps may be appropriate. The structure of a computer will appear from the description below.

[0038] In addition, the present specification also implicitly discloses a computer program, in that it would be apparent to the person skilled in the art that the individual steps of the method described herein may be put into effect by computer code. The computer program is not intended to be limited to any particular programming language and implementation thereof. It will be appreciated that a variety of programming languages and coding thereof may be used to implement the teachings of the disclosure contained herein. Moreover, the computer program is not intended to be limited to any particular control flow. There are many other variants of the computer program, which can use different control flows without departing from the spirit or scope of the disclosure.

[0039] Furthermore, one or more of the steps of the computer program may be performed in parallel rather than sequentially. Such a computer program may be stored on any computer readable medium. The computer readable medium may include storage devices such as magnetic or optical disks, memory chips, or other storage devices suitable for interfacing with a computer. The computer readable medium may also include a hard-wired medium such as exemplified in the Internet system, or wireless medium such as exemplified in the GSM mobile telephone system. The computer program when loaded and executed on a computer effectively results in an apparatus that implements the steps of the preferred method.

[0040] In embodiments of the present disclosure, use of the term ‘server’ may mean a single computing device or at least a computer network of interconnected computing devices

which operate together to perform a particular function. In other words, the server may be contained within a single hardware unit or be distributed among several or many different hardware units.

[0041] Fig. 1 shows a schematic diagram of a system 100 configured to associate a social network account identifier with one or more payment account information, in accordance with embodiments of the disclosure. The system 100 includes a device 101, a registration server 102, a mapping server 208, and a social networking service server 212. In embodiments of the disclosure, the mapping server 208 and the social networking service server 212 can be part of system 200 (as shown in Figs. 2A and 2B) which is configured to facilitate a transaction with the social network account identifier. The device 101 can be a payment device (e.g. device 202) or a user device 214 as shown in shown in Figs. 2A and 2B.

[0042] The system 100 can be used to implement method 300 as shown in Fig. 3. Fig 3 shows a flowchart illustrating the method 300 for associating a social network account identifier with one or more payment account information, in accordance with embodiments of the disclosure. The method 300 broadly includes:

step 302: receiving, from a device, a registration request comprising the social network account identifier and the one or more payment account information prior to receiving the transaction request;

step 304: transmitting, to a server associated with the social network account identifier, a verification code that is generated in response to the registration request;

step 306: receiving, from the device, a verification input;

step 308: comparing the received verification input with the transmitted verification code; and

step 310: associating the one or more payment account information with the social network account identifier, on the condition that the received verification input corresponds to the transmitted verification code.

[0043] At step 302, the registration request 104 is received by the registration server 102. The registration request 104 is generated by the device 101, and can include the social network account identifier and the one or more payment account information. The

registration request can be generated with an application program that is installed on a user device (e.g. a digital wallet application running on the user device, the device 101 being the user device), or through an online portal (e.g. a website) associated with the entity party to the payment network (e.g. the issuer, in which case the device 101 can be the issuer server). For example, a user may navigate to the online banking website of the issuer, access a registration request generation page and input the social network account identifier and the one or more payment account information to be associated with the social network account identifier. In embodiments of the present disclosure, the registration server 102 can be a server associated with the payment facilitator (e.g. payment network server 206 as shown in Figs. 2A and 2B, or a server of the issuer that is configured to process the registration request, e.g. issuer server 210). The registration server 102 is in direct communication with mapping server 208, which can store more mapping tables containing the association between the social network account identifier and the one or more payment account information.

[0044] At step 304, a verification code 106 is generated and subsequently transmitted to the social networking server 212, in response to receipt of the registration request 104. In an embodiment of the present disclosure, the verification code 106 can be transmitted via a dedicated HTTPS channel. It can be appreciated that the generated verification code 106 can be encrypted with asymmetric cryptography prior to transmission. For example, the verification code 106 can be first signed (i.e. encrypted) by a private key of a first key pair and then encrypted by a public key of a second key pair. Alternatively, the verification code 106 can be first encrypted by a public key of a first key pair and then signed (i.e. encrypted) by a private key of a second key pair. The first key pair can be associated with the registration server 102 and the second key pair can be associated with the social networking service server 212.

[0045] In embodiments of the present disclosure, the social networking server 212 to which the verification code 106 is sent can be determined based on the social network account identifier in the registration request 104. For example, the registration server 102 can be configured to identify the related social network service (and the server 212) based on the format of the social network account identifier. Alternatively, the social network service (and consequently the server 212) can be identified by the user on the application program, or through the online portal prior to transmission of the registration request 104. For example a list of social networking service providers can be presented to the user and the user can

select the relevant social network service to which the registration request 104 is sent from the list.

[0046] In embodiments of the disclosure, the verification code 106 can be a one-time password. The one-time password can be generated by the registration server 106 using at least one or more payment account information. For example, the one-time password (OTP) can be a random number generated using a pseudorandom number generator, with the at least one or more payment account information used as a random seed. The one or more payment account information can include one or more of a group consisting of (i) a name of payment account holder, a payment account identifier, a primary account number (PAN) of a payment card associated with the payment account and expiration date of the payment card. It can also be appreciated that the one-time password can be generated with a true random number generator (e.g. a hardware random number generator).

[0047] The verification code 106 can be in turn routed to the device 101 by the social networking server 212 via communication means predefined by the user, or via means available on the social network service. For example, the verification code can be sent via a short message service (SMS), an email, or a private message on the social network platform. In other words, the verification code 106 used to authenticate the user is sent out-of-band. That is, the out-of-band message can make use of two separate networks which work simultaneously to authenticate a user. For example, a fraudulent user may initiate a registration request via the application program, or through the online portal and the owner of the social networking service account can be informed of such an attempt through the aforementioned communication means. This advantageously provides an opportunity to the user of the social networking service account to stop the registration request. The verification code 106 can be received by the user and entered into a verification input field on the device 101. A verification input 110 is then transmitted by the device 101 to the registration server 102.

[0048] At step 306, the verification input 110 is received by the registration server 102. At step 308, the received verification input 110 is compared by the registration server 102 with the verification code 106 that was transmitted to the social networking service server 212. At step 310, the one or more payment account information is associated with the social network account identifier by the registration server 102, on the condition that the received verification input 110 corresponds to the transmitted verification code 106. In various embodiments, the registration server 102 can be further configured to record the association

in a mapping file 112 and transmit the mapping file 112 to a mapping server 208. The mapping server 208 can be configured to store the mapping file 112 and can also transmit the mapping file 112 securely to servers associated with other entities party to the payment network if required. The mapping server 208 can be managed by either the payment facilitator and/or the issuer.

[0049] In various embodiments of the present disclosure, the registration server 102 can be further configured to transmit a confirmation message 114 to the device 101, in response to successful association of the one or more payment account information with the social network account identifier.

[0050] In embodiments of the present disclosure, the registration request 104 can further include a user-determined identification number. If the received verification input 110 corresponds to the transmitted verification code 106, the user-determined identification number can be recorded by the registration server 102 as an authentication code (e.g. personal identification number) associated with the social network account identifier. That is, the authentication code can be used to authenticate transaction requests including the social network account identifier. The user-determined identification number can be stored on the mapping file 112 by the registration server 102 and transmitted to the mapping server 208. In alternate embodiments, the authentication code can be a card verification code associated with the payment account.

[0051] Figs. 2A and 2B shows a schematic diagram of a system 200 configured to facilitate a transaction with a social network account identifier, in accordance with embodiments of the disclosure. The system 200 includes a device 202, an acquirer server 204, a payment network server 206, a mapping server 208 and an issuer server 210. In various embodiments of the present disclosure (as shown in Fig. 2A), the system 100 can further include a social network service server 212 and a user device 214. Further, the mapping server 208 in system 200 can be administered by the payment facilitator or the issuer.

[0052] The device 202 is in direct communication with the acquirer server 204, which is in turn in direct communication with the payment network server 206. The payment network server 206 is in direct communication with the mapping server 208 and the issuer server 210. In embodiments of the disclosure, the payment network server 206 can also directly communicate with the social network service server 212 and the user device 214 (as shown in Fig. 1). The system 200 is used to implement method 400 shown in Fig. 4. Fig. 4 shows a

flowchart illustrating the method 400 for facilitating a transaction, in accordance with embodiments of the disclosure. The method 400 broadly includes:

step 402: receiving, from a device, a transaction request comprising the social network account identifier and an authentication input;

step 404: comparing the received authentication input with an authentication code associated with the social network account identifier;

step 406: determining one or more payment account information that is associated with the social network account identifier, on the condition that the received authentication input corresponds to the authentication code;

step 508: forwarding, to a payment processing server, the transaction request and the one or more determined payment account information

[0053] At step 402, a transaction request 216 can be received from the device 202. The transaction request 216 can include a social network account identifier and an authentication input. The device 202 is typically a payment device which can serve as a main conduit for transmitting the transaction request 216 and for receiving an authorisation/failure response 224 of the transaction request 216. In embodiments of the present disclosure, the device 202 can be a device of the user that is configured to function as a payment device. In other embodiments, the device 202 can be transaction terminal. Examples of a transaction terminal include point-of-sale (POS) terminal, an automated teller machine (ATM) and the like. The device 202 can also be a laptop computer, smartphone, smartwatch or a tablet with an operating system can which host an application configured to generate and transmit the transaction request 216. It can be appreciated that the social network account identifier and the authentication input can be inputted into the device 102 by the user, or presented to the device 102 by means known in the art (e.g. voice input).

[0054] In various embodiments, the transaction request 216 can include an ISO 8583 formatted message. ISO 8583 is an international standard for systems that exchange electronic transactions initiated using payment card information. ISO 8583 defines a message format and a communication flow so that different systems can exchange such transaction requests and authorisation messages. An ISO 8583 formatted message can comprise a message type indicator (MTI), one or more bitmaps indicating which data elements are present and data elements representing the fields of the message. In

embodiments of the present disclosure, the ISO 8583 formatted message can include data element field entries storing at least the social network account identifier and the authentication input. In other words, the transaction request 216 can be compliant with the ISO 8583 standard and includes data elements which carry transaction information generated by the device 202.

[0055] Notably, as payment account information is not included at the time of generating the transaction request 216, it can be appreciated that data element fields relating to payment account information can either be blank, or filled with dummy values (i.e. placeholder values). Further, the ISO 8583 formatted message can further include a data element field entry indicating that the transaction request 216 is generated with a social network account identifier, rather than a typical transaction request which includes payment account information such as a payment card number (PAN) of the payment account. That is, the ISO 8583 formatted message can include an identifier indicating that the transaction request 216 includes a social network account identifier, and the identifier can be advantageously used to allow the payment network to differentiate between the transaction request 216 and a typical transaction request. For example, the identifier may be stored a predetermined binary format data element entry field, and the device 202 can be configured to populate the identifier with a binary value of “1” if a transaction request includes a social network account identifier. Consequently, the device 202 can be configured to populate the identifier with a binary value of “0” if a transaction request does not include a social network account identifier (e.g. the transaction request is a typical request including payment account information).

[0056] The transaction request 216 can be received by the acquirer server 204 at step 402. The acquirer server 204 is typically associated with an acquirer. Examples of the acquirer include a bank and/or other financial institution. The acquirer server 204 may include one or more computing devices that are used to establish communication with another server by exchanging messages with and/or passing information to the other server. In embodiments of the disclosure, the acquirer server 204 is configured to record the transaction request 216, process the transaction request 216 in a manner similar to a typical transaction request and subsequently transmit the transaction request 216 to the payment network server 206.

[0057] The payment network server 206 is configured to receive the transaction request 216. The payment network server 206 can be operated by a payment facilitator. For example, the payment network server 206 may be a Banknet network operated by the payment facilitator (e.g. MASTERCARD®). In embodiments of the disclosure, the payment

network server 206 is configured to route information between the acquirer server 204 and the issuer server 210. The network server 206 is also configured to communicate with the mapping server 208 and the social networking service server 212.

[0058] In embodiments where the aforementioned user-determined identification number is recorded by the registration server 102 as the authentication code associated with the social network account identifier and stored on the mapping server 208, the network server 206 can be configured to retrieve the authentication code from the mapping server 208 and compare the received authentication input with the retrieved authentication code. In alternate embodiments, where the authentication code is recorded as a card verification code associated with the payment account, the network server 206 can similarly be configured to retrieve the card verification code from a linked database (e.g. the issuer server 210) and compare the received authentication input with the retrieved authentication code.

[0059] In other embodiments of the disclosure, where an authentication code is not recorded by the registration server 102, the payment network server 206 can be configured to generate an authentication code 228 prior to step 402 (receipt of the transaction request 216 as shown in Fig. 2A) The authentication code 228 can be generated in response to receipt of an authentication request 226 from the user device 214. The authentication request 226 can include the one or more payment account information. Upon receipt of the authentication request 226, the payment network server 206 can retrieve, from the mapping server 208, the corresponding social network account identifier based on the received one or more payment account information. The payment network server 206 can then transmit based on the social network account identifier, the authentication code 228 to the appropriate social networking service server 212. The authentication code 228 can be in turn routed to the user device 214 by the social networking server 212 via communication means available on the social network service. For example, the authentication code 228 can be sent via short message service (SMS), email, or a private message on the social network platform. In other words, the authentication code 228 used to authenticate the user is sent out-of-band. As the authentication code 228 is sent with each new transaction request 216, security of the transaction method can be advantageously enhanced as the user can be authenticated with each new transaction request 216, and the authentication code 228 is valid only for one transaction request. The authentication code 228 can be inputted into the device 202 as the authentication input 230. The device 202 can then generate and transmit the transaction request 216 including the social network account identifier and the authentication input 230 to the acquirer server 204.

[0060] In alternate embodiments of the disclosure, where the aforementioned user-determined identification number is stored on the mapping server 208 as the authentication code associated with the social network account identifier, the payment network server 206 can be configured to generate a transaction and authentication request 238 prior to step 402 (receipt of the transaction request 216 as shown in Fig. 2B). The transaction and authentication request 238 is generated in response to receipt of message 236 from the device 202. The message 236 is generated by the device 202, and routed through the acquirer server 204. The message 236 includes the social network account identifier, but excludes the authentication input. In various embodiments, the message 236 can be an ISO 8583 formatted message. The payment network server 206, upon receipt of the message 236, generates the transaction and authentication request 238 requesting at least the authentication input and transaction information. The transaction and authentication request 238 is routed back to the device 202 via the acquirer server 204. The device 202 is configured to request for an authentication input and transaction details upon receipt of the transaction and authentication request 238. Upon receiving the required information, the device 202 can then generate and transmit the transaction request 216 including the social network account identifier and an authentication input to the acquirer server 204.

[0061] In various embodiments, the transaction request 216 can be complaint with ISO 8583 standard and can include data elements (DE) which carry the transaction information. The transaction request 216 would be similar to normal transaction requests, except that the data element fields relating to payment account information would either be blank, or filled with dummy values (i.e. placeholder values). Further, in various embodiments, a DE 52 (data field no. 52) can include the authentication input, rather than a verification code e.g. PIN conventionally used to authenticate payment account information in a normal transaction request. Thus, the embodiments in the present disclosure may be advantageously implemented on existing payment systems without modification to existing software and/or hardware, provided that the device 202 additionally supports alphanumeric entry of the social network account identifier and the authentication input. The transaction request 216 can be received by the acquirer server 204, processed similarly to normal transaction requests and subsequently transmitted to the payment network server 206..

[0062] At step 406, the one or more payment account information that is associated with the social network account identifier can be determined with the payment network server 206, on the condition that the received authentication code 228 corresponds to the authentication code. The payment network server 206 can determine the one or more

payment account information by accessing the mapping file 112 stored on the mapping server 208.

[0063] At step 408, the transaction request 216 and the one or more determined payment account information can be forwarded to a payment processing server (e.g. the issuer server 210) in a transaction request 222 for further processing. The transaction request 222 includes the transaction request 216 and the one or more determined payment account information. For example, in embodiments where the transaction request 216 is presented in an ISO 8583 format, the payment network server 206 can be configured to include the one or more determined payment account information in one or more reserved data element fields of the ISO 8583 message.

[0064] Moreover, in various embodiments, the payment network server 206 can be further configured to modify the transaction request 216 to include the one or more determined payment account information prior to forwarding the transaction request 216 as the modified transaction request 222. For example, in embodiments where the transaction request 216 is presented in an ISO 8583 format, the payment network server 206 can be configured to replace the dummy data (i.e. placeholder values) present in the element fields relating to payment account information with the one or more determined payment account information and transmit the modified transaction request 222 to the issuer server 210.

[0065] The issuer server 210 is configured to receive the modified transaction request 222. The issuer server 210 can process the modified transaction request 222, and in turn generate and transmit a response 224 back to the payment network server 206. The response 224 can include data indicative of an authorisation of transfer of funds from the user or a transaction failure message including a response code indicating a reason for the transaction failure. The payment network server 206 then transmits the response 224 back to the acquirer server 204 which in turn routes the message to device 202.

[0066] Fig. 5 shows a server 500 including modules for facilitating a transaction with a social network account identifier, in accordance with embodiments of the disclosure. In implementations, the registration server 102 and the payment network server 206 can be generally described as one or more physical devices (i.e. servers) including at least one processor 502 and at least one memory 504 including computer program code. The at least one memory 504 and the computer program code are configured to, with the at least one processor 502, cause the server to perform the operations described in Figs. 3 and 4. Examples of the registration server 102 and the payment network server 206 are shown in Fig. 5. The server 500 can include a receiver module 506, a comparison module 508, an

update module 510 and a transmitter module 512. With reference to Fig. 2 and Fig. 4, the receiver module 506 is configured to receive, from a device, the transaction request comprising the social network account identifier and the authentication input. The comparison module 508 is configured to compare the received authentication input with the authentication code associated with the social network account identifier. The update module 510 is configured to determine the one or more payment account information that is associated with the social network account identifier, on the condition that the received authentication input corresponds to the authentication code. The transmitter module 512 is configured to forward the transaction request and the one or more determined payment account information to a payment processing server.

[0067] In various embodiments, the server 500 can additionally include a modifier module 514, an generator module 516, and an association module 518. The modifier module 514 is configured to modify the transaction request to include the one or more determined payment account information prior to forwarding of the transaction request by the transmitter module 512. The receiver module 506 can be further configured to receive, from the device, a registration request comprising the social network account identifier and the one or more payment account information prior to the receipt of the transaction request. The transmitter module 512 can be further configured to transmit, to a server associated with the social network account identifier, a verification code that is generated by the generator module 516 in response to the registration request. The receiver module 506 can also be configured to receive a verification input from the device, and the comparison module 508 can be configured to compare the received verification input with the transmitted verification code. The association module 518 can be configured to associate the one or more payment account information with the social network account identifier, on the condition that the received verification input corresponds to the transmitted verification code.

[0068] Fig. 6 depicts an exemplary computing device 600, hereinafter interchangeably referred to as a computer system 600, where one or more such computing devices 600 may be used to execute the methods 300, 400 of Figs. 3 and 4. One or more components of the exemplary computing device 600 can also be used to implement the systems 100, 200 as well as the device 101, the registration server 102, the device 202, the acquirer server 204, the payment network server 206, the mapping server 208, the issuer server 210, the social network service server 212 and the user device 214. The computing device 600 can also be used to implement the exemplary server 500. The following description of the computing device 600 is provided by way of example only and is not intended to be limiting.

[0069] As shown in Fig. 6, the example computing device 600 includes a processor 607 for executing software routines. Although a single processor is shown for the sake of clarity, the computing device 600 may also include a multi-processor system. The processor 607 is connected to a communication infrastructure 606 for communication with other components of the computing device 600. The communication infrastructure 506 may include, for example, a communications bus, cross-bar, or network.

[0070] The computing device 600 further includes a main memory 608, such as a random access memory (RAM), and a secondary memory 610. The secondary memory 610 may include, for example, a storage drive 612, which may be a hard disk drive, a solid state drive or a hybrid drive and/or a removable storage drive 617, which may include a magnetic tape drive, an optical disk drive, a solid state storage drive (such as a USB flash drive, a flash memory device, a solid state drive or a memory card), or the like. The removable storage drive 617 reads from and/or writes to a removable storage medium 677 in a well-known manner. The removable storage medium 677 may include magnetic tape, optical disk, non-volatile memory storage medium, or the like, which is read by and written to by removable storage drive 617. As will be appreciated by persons skilled in the relevant art(s), the removable storage medium 677 includes a computer readable storage medium having stored therein computer executable program code instructions and/or data.

[0071] In an alternative implementation, the secondary memory 610 may additionally or alternatively include other similar means for allowing computer programs or other instructions to be loaded into the computing device 600. Such means can include, for example, a removable storage unit 622 and an interface 650. Examples of a removable storage unit 622 and interface 650 include a program cartridge and cartridge interface (such as that found in video game console devices), a removable memory chip (such as an EPROM or PROM) and associated socket, a removable solid state storage drive (such as a USB flash drive, a flash memory device, a solid state drive or a memory card), and other removable storage units 622 and interfaces 650 which allow software and data to be transferred from the removable storage unit 622 to the computer system 600.

[0072] The computing device 600 also includes at least one communication interface 627. The communication interface 627 allows software and data to be transferred between computing device 600 and external devices via a communication path 626. In various embodiments of the disclosure, the communication interface 627 permits data to be transferred between the computing device 600 and a data communication network, such as a public data or private data communication network. The communication interface 627 may

be used to exchange data between different computing devices 600 which such computing devices 600 form part an interconnected computer network. Examples of a communication interface 627 can include a modem, a network interface (such as an Ethernet card), a communication port (such as a serial, parallel, printer, GPIB, IEEE 1394, RJ45, USB), an antenna with associated circuitry and the like. The communication interface 627 may be wired or may be wireless. Software and data transferred via the communication interface 627 are in the form of signals which can be electronic, electromagnetic, optical or other signals capable of being received by communication interface 627. These signals are provided to the communication interface via the communication path 626.

[0073] As shown in Fig. 6, the computing device 600 further includes a display interface 602 which performs operations for rendering images to an associated display 655 and an audio interface 652 for performing operations for playing audio content via associated speaker(s) 657.

[0074] As used herein, the term "computer program product" may refer, in part, to removable storage medium 677, removable storage unit 622, a hard disk installed in storage drive 612, or a carrier wave carrying software over communication path 626 (wireless link or cable) to communication interface 627. Computer readable storage media refers to any non-transitory, non-volatile tangible storage medium that provides recorded instructions and/or data to the computing device 600 for execution and/or processing. Examples of such storage media include magnetic tape, CD-ROM, DVD, Blu-ray™ Disc, a hard disk drive, a ROM or integrated circuit, a solid state storage drive (such as a USB flash drive, a flash memory device, a solid state drive or a memory card), a hybrid drive, a magneto-optical disk, or a computer readable card such as a PCMCIA card and the like, whether or not such devices are internal or external of the computing device 600. Examples of transitory or non-tangible computer readable transmission media that may also participate in the provision of software, application programs, instructions and/or data to the computing device 600 include radio or infra-red transmission channels as well as a network connection to another computer or networked device, and the Internet or Intranets including e-mail transmissions and information recorded on Websites and the like.

[0075] The computer programs (also called computer program code) are stored in main memory 608 and/or secondary memory 610. Computer programs can also be received via the communication interface 627. Such computer programs, when executed, enable the computing device 600 to perform one or more features of embodiments discussed herein. In various embodiments, the computer programs, when executed, enable the processor 607 to

perform features of the above-described embodiments. Accordingly, such computer programs represent controllers of the computer system 600.

[0076] Software may be stored in a computer program product and loaded into the computing device 600 using the removable storage drive 617, the storage drive 612, or the interface 650. The computer program product may be a non-transitory computer readable medium. Alternatively, the computer program product may be downloaded to the computer system 600 over the communication path 626. The software, when executed by the processor 607, causes the computing device 600 to perform the necessary operations to execute the methods 300, 400 as shown in Figs. 3 and 4.

[0077] It is to be understood that the embodiment of Fig. 6 is presented merely by way of example to explain the operation and structure of the system 600. Therefore, in some embodiments one or more features of the computing device 600 may be omitted. Also, in some embodiments, one or more features of the computing device 600 may be combined together. Additionally, in some embodiments, one or more features of the computing device 600 may be split into one or more component parts.

[0078] It will be appreciated that the elements illustrated in Fig. 6 function to provide means for performing the various functions and operations of the system as described in the above embodiments.

[0079] When the computing device 600 is configured to realise the system 200 to facilitate a transaction with a social network account identifier, the system 200 will have a non-transitory computer readable medium having stored thereon an application which when executed causes the system 200 to perform steps comprising: (i) receiving, from a device, a transaction request comprising a social network account identifier and an authentication input and (ii) comparing the received authentication input with an authentication code associated with the social network account identifier. The system 200 can also perform the steps comprising (iii) determining one or more payment account information that is associated with the social network account identifier, on the condition that the received authentication input corresponds to the authentication code and (iv) forwarding, to a payment processing server, the transaction request and the one or more determined payment account information.

[0080] It will be appreciated by a person skilled in the art that numerous variations and/or modifications may be made to the present disclosure as shown in the specific embodiments without departing from the spirit or scope of the disclosure as broadly described. The present

embodiments are, therefore, to be considered in all respects to be illustrative and not restrictive.

Claims

1. A system configured to facilitate a transaction with a social network account identifier, the system comprising:

at least one processor; and

at least one memory including computer program code;

the at least one memory and the computer program code configured to, with the at least one processor, cause the system at least to:

receive, from a device, a transaction request comprising the social network account identifier and an authentication input;

compare the received authentication input with an authentication code associated with the social network account identifier;

determine one or more payment account information that is associated with the social network account identifier, on the condition that the received authentication input corresponds to the authentication code; and

forward, to a payment processing server, the transaction request and the one or more determined payment account information.

2. The system of claim 1, wherein the at least one memory and the computer program code are configured to, with the at least one processor, cause the system further to:

modify the transaction request to include the one or more determined payment account information prior to forwarding the transaction request.

3. The system of claim 1 or 2, wherein the at least one memory and the computer program code are configured to, with the at least one processor, cause the system further to:

receive, from the device, a registration request comprising the social network account identifier and the one or more payment account information prior to the receipt of the transaction request;

transmit, to a server associated with the social network account identifier, a verification code that is generated in response to the registration request;

receive, from the device, a verification input;

compare the received verification input with the transmitted verification code; and

associate the one or more payment account information with the social network account identifier, on the condition that the received verification input corresponds to the transmitted verification code.

4. The system as claimed in claim 3, wherein the at least one memory and the computer program code are configured to, with the at least one processor, cause the system to generate a one-time password using at least the one or more payment account information as the verification code.

5. The system as claimed in claim 3 or 4, wherein the registration request comprises a user-determined identification code; and

wherein associating the one or more payment account information with the social network account identifier, the system is configured to register the user-determined identification number as the authentication code associated with the social network account identifier.

6. The system as claimed in any one of claims 1 to 4, wherein the at least one memory and the computer program code are configured to, with the at least one processor, cause the system to:

receive, from an user device, an authentication request requesting the authentication code, the authentication request comprising the one or more payment account information;

generate the authentication code; and

transmit, based on the one or more payment account information, the authentication code to the server associated with the social network account identifier.

7. The system as claimed in any one of claims 1 to 4, wherein the authentication code comprises a card verification code associated with the payment account.

8. The system as claimed in any one of claims 1 to 7, wherein the one or more payment account information comprises one or more of a group consisting of: name of payment account holder, payment account identifier, primary account number (PAN) of a payment card associated with the payment account , and expiration date of the payment card.

9. The system as claimed in any one of claims 3 to 8, wherein the at least one memory and the computer program code are configured to, with the at least one processor, cause the system further to transmit, to the device, a confirmation message in

response to an association of the one or more payment account information with the social network account identifier.

10. A method for facilitating a transaction with a social network account identifier, the method comprising,

receiving, from a device, a transaction request comprising the social network account identifier and an authentication input;

comparing the received authentication input with an authentication code associated with the social network account identifier;

determining one or more payment account information that is associated with the social network account identifier, on the condition that the received authentication input corresponds to the authentication code; and

forwarding, to a payment processing server, the transaction request and the one or more determined payment account information.

11. The method as claimed in claim 10, further comprising modifying the transaction request to include the determined one or more payment account information prior to forwarding the transaction request.

12. The method as claimed in claim 10 or 11, further comprising:

receiving, from the device, a registration request comprising the social network account identifier and the one or more payment account information prior to receiving the transaction request;

transmitting, to a server associated with the social network account identifier, a verification code that is generated in response to the registration request;

receiving, from the device, a verification input;

comparing the received verification input with the transmitted verification code; and

associating the one or more payment account information with the social network account identifier, on the condition that the received verification input corresponds to the transmitted verification code.

13. The method as claimed in claim 12, further comprising transmitting with the server associated with the social network account identifier, the verification code to the device.

14. The method as claimed in claim 12 or 13, wherein transmitting the verification code comprises generating a one-time password using at least the one or more payment account information as the verification code.

15. The method as claimed in any one of claims 12 to 14, wherein receiving the registration request comprises receiving a user-determined identification code; and

wherein associating the one or more payment account information with the social network account identifier comprises registering the user-determined identification number as the authentication code associated with the social network account identifier.

16. The method as claimed in any one of claims 10 to 14, wherein the method comprises:

receiving, from an user device, an authentication request requesting the authentication code, the authentication request comprising the one or more payment account information;

generating the authentication code; and

transmitting, based on the one or more payment account information, the authentication code to the server associated with the social network account identifier.

17. The method as claimed in claim 16, further comprising transmitting with the server associated with the social network account identifier, the authentication code to the user device.

18. The method as claimed in any one of claims 10 to 14, wherein the authentication code comprises a card verification code associated with the payment account.

19. The method as claimed in any one of claims 10 to 18, wherein the one or more payment account information comprises one or more of a group consisting of: name of payment account holder, payment account identifier, primary account number (PAN) of a payment card associated with the payment account , and expiration date of the payment card.

20. The method as claimed in any one of claims 12 to 19, further comprising transmitting, to the device, a confirmation message in response to an association of

the one or more payment account information with the social network account identifier.