TRANSACTION SYSTEM AND METHOD

Field of the Invention

The present invention relates to a transaction system and method. The system and method are particularly relevant, but not limited to facilitating secure mobile wallet financial transactions and will be described in such context.

Background Art

Each document, reference, patent application or patent cited in this text is expressly incorporated herein in their entirety by reference, which means that it should be read and considered by the reader as part of this text. That the document, reference, patent application, or patent cited in this text is not repeated in this text is merely for reasons of conciseness.

Throughout the specification, unless the context requires otherwise, the word “comprise” or variations such as “comprises” or “comprising”, will be understood to imply the inclusion of a stated integer or group of integers but not the exclusion of any other integer or group of integers.

Furthermore, throughout the specification, unless the context requires otherwise, the word “include” or variations such as “includes” or “including”, will be understood to imply the inclusion of a stated integer or group of integers but not the exclusion of any other integer or group of integers.

The following discussion of the background to the invention is intended to facilitate an understanding of the present invention only. It should be appreciated that the discussion is not an acknowledgement or admission that any of the material referred to was published, known or part of the common general knowledge of the person skilled in the art in any jurisdiction as at the priority date of the invention.

Rapid advancement in the development of mobile devices and related applications (hereinafter ‘apps’) has resulted in increasing e-commerce transactions performed because such advancement in technology offers

users the convenience of 'on the go' transactions as long as any type of connection (GSM, GPRS, 3G, Wi-Fi etc.) can be established to the Internet. In particular, credit card users or fund source owners now enjoy unprecedented e-shopping experience as they may now choose from a variety of transaction channels/modes instead of the traditional point of sale (POS) or related electronic transfers requiring the use of dedicated end terminals which typically are located only at designated locations where the sale takes place.

The availability of increasing transaction channels/modes inadvertently lead to the increasing occurrences of fraud/security breach, where information of credit card users such as PAN, CVC2, Expiry Date, etc. are exposed due to insecure websites or hacking activity. Despite of the efforts of card issuers and acquirer in the financial industry encouraging the implementation of a variety of financial security standards (SSL, EMV Chips and 3D secure) etc., such security standards would secure the transaction channel and/or the transaction device to certain extent but are not an effective fool proof way of preventing scheming, theft and internal fraud. Moreover, not all electronic merchants are mandated to implement those security compliance/standards, and unaware credit card users may inadvertently subject themselves to such 'insecure' transaction channels.

As an example, a credit card holder wishes to reserve an airline ticket and thus access the online booking website. To pay the online reservation the standard process is to provide the cardholder information like Card Name, PAN (Primary Account Number or card number), CVC2 and Expiry Date. If these transaction data are not properly protected and obtained by an unauthorized entity, the unauthorized entity may use the data for other unauthorized payment transaction or may even fabricate a card and use the fabricated card for transaction just like a legitimate card transaction.

To overcome the potential breach in security, prior art transaction systems that provides additional security by allowing a holder of a financial account card, such as a credit card or debit card, to disable and re-enable use of the card by locking and unlocking the card repeatedly has been disclosed.

However, such a system adopts an “all or nothing” approach to the security problem in that no transactions at all can be made when the associated card is in the locked state, and the holder has to unlock the card prior to making any transactions.

The system as described in PCT publication WO2010/147559 describes a system and method that allows a user or provider of a 'smart card', such as a credit card, to change the state of a transaction channel, in particular allowing a user or provider to 'lock' and/or 'unlock' certain transaction channels/modes such as web purchasing, point of sale purchasing, etc. with respect to other transaction modes. The system allows a user or provider the flexibility to 'choose' the types of transaction channels that may be used to effect transactions. So, for example, a user may decide that, for security reasons, he/she will 'lock' his card to prevent the card from being used for web-based purchases, but will leave the card unlocked for traditional point of sale (POS) purchases. If the user's card is stolen, an unauthorized user would not be able to use the card to effect any web-based purchases, thereby providing an extra level of security while according certain level of flexibility.

The system was further improved as described in PCT publication WO 2013/103323 where card issuers are given the option of the locking/unlocking feature.

While the above systems provide a level of flexibility to a user to disable certain transaction channels instead of the whole account, there exist limitations faced by the user in particular when he wishes to make authorized batch payment to online merchants.

The present invention seeks to improve the transaction systems and methods that reduces or prevents the occurrence of transaction fraud to at least some extent while allowing greater flexibility for the user to perform transaction and greater customization of the lock/unlock feature.

Disclosure of the Invention

In accordance with an aspect of the present invention, there is provided a transaction system comprising:

a transaction facilitator operable to receive and process a transaction request from a user device; a transaction channel controller operable to change the state of the transaction channel between a first and a second state; and a fund provider operable to receive processed transaction request and determine if the transaction channel is in the first or second state; and provide or not provide the funds accordingly.

Preferably, the first state corresponds to a state where the transaction channel is locked and forbidden for any transaction.

Preferably, the default state is the first state.

Preferably, the instruction to change the transaction channel from the first to second state and vice versa is initiated by the user device.

Preferably, the fund provider comprises a user profile database operable to automate the instruction to change the transaction channel from the first to second state and vice versa.

Preferably, the user profile database is operable to capture one or more of the following transaction parameters from the transaction request in order to determine whether the transaction channel should be in the first or second state:- Transaction Datetime stamp; Merchant Category Code; Merchant Name; Merchant Address; Transaction Amount; Country Code; or Currency Code.

Preferably, the user profile database is operable to determine the location of the user device sending the transaction request in order to determine whether the transaction channel should be in the first or second state.

Preferably, the transaction channel is one of the following:- point of sale (POS) terminal; Internet transaction; ATM.

In accordance with a second aspect of the present invention, there is provided a transaction method comprising:

receiving and processing from a transaction facilitator a transaction request from a user device;

receiving from a transaction channel controller a request to change the state of the transaction channel between a first and a second state;

wherein the processed transaction request is successful or not successful depending on whether the transaction channel is in the first or second state.

In accordance with a third aspect of the present invention, there is provided a transaction engine for use in a transaction system of the first aspect.

Brief Description of the Drawings

The present invention will now be described, by way of example only, with reference to the accompanying drawings, in which:

Fig. 1 shows a user requesting the change of state of his fund source between a lock and a unlock state via a transaction state controller (Lock/Unlock Controller) according with an embodiment of the invention;

Fig. 2 illustrates a user performing a transaction with the transaction state controller and fund source system;

Fig. 3 illustrates an unauthorized user performing an unauthorized transaction via the Internet while the fund source system is in the lock state;

Fig. 4 illustrates an unauthorized user performing an unauthorized transaction via a Point of Sale terminal while the fund source system is in the lock state;

Fig. 5 shows the transaction system with different transaction channels and/or devices;

Fig. 6 shows the transaction system wherein the transaction state controller comprises an electronic wallet operable to receive and process registration requests;

Fig. 7 illustrates the system of Fig. 6 being used for self-registrations for personalization of the electronic wallet and generation of a personalized transaction medium such as a credit/debit card; and

Fig. 8 illustrates the system of Fig. 6 being used for multiple linking of fund sources.

Other arrangements of the invention are possible and, consequently, the accompanying drawings are not to be understood as superseding the generality of the description of the invention.

Description of Embodiments of the Invention

In accordance with an embodiment of the invention there is a transaction system 10 comprising a user device 12 operable to send a transaction request 14 via a transaction channel 16. The transaction channel 16 may be chosen from a plurality of transaction channels 16.

The system further comprises a transaction facilitator 18 operable to receive and process the transaction request from the user device 12.

In addition, the system 10 comprises a transaction channel controller 20 operable to change the transactional state of the transaction channel and/or transaction device 12 between a first and a second state.

The system 10 also includes a fund provider 22 operable to receive processed transaction request and determine if the transaction channel is in the first or second state; and notify the user device 12 accordingly.

Referring to Fig. 1, the user device 12 sends a request to transaction channel controller 20 (Lock/Unlock controller) to change the transaction channel 16 from a first state (lock) to a second state (unlock), and vice versa. It is to be appreciated that the terms ‘first’ and ‘second’ are used for illustration purpose only and may be interchangeable.

The transaction device 12 is a personal computer, smart phone or any device capable of displaying and interacting with a payment portal. The user interface for displaying and interacting with the payment portal is typically in the form of a website of a payment gateway of a merchant. The website is accessible by a user via a web browser of a personal computer 12 operably

connected to be in data communication with other components of the transaction system 10 via a communication network comprising a plurality of transaction channels. The plurality of transaction channels includes (but is not limited to) 3G/4G, Wi-Fi connection to the Internet; direct LAN connection to the Internet; point of sale terminal; or Automated Teller Machines (ATM).

The merchant offers good and services for sale, which may be purchased on-line by a customer accessing the website.

The use and operation of the Internet, computers and servers using software applications and payment portals are well known to persons skilled in the art and need not be described in any further detail herein except as is relevant to the present invention.

In the embodiment described and with reference to both Fig. 1 and Fig. 2, the user of transaction device 12 is the fund source owner and wishes to reserve as well as make payment for one or more air tickets. Before making any reservation, he accesses the transaction mode/channel controller 20 (via an authentication procedure) to enable (unlock) the particular transaction channel 16, in this case Internet transaction for access to his source fund 22. The authentication procedure is in the form of a PIN authentication for example.

Once Internet transaction channel is enabled, the user may then access the airline reservation website for performing his necessary reservation. Once the reservation is made, the user would be prompted to make payment by choosing his transaction payment preference. If he chooses online electronic payment mode, he will be prompted to key in his preferred credit card number and details such as Card Name, PAN (Primary Account Number or card number), CVC2 and Expiry Date.

Upon keying in the transaction details, the airline reservation website will access the fund source system 22, for example MasterCard™ Worldwide, where the user has an account with.

As the transaction channel 'Internet transaction' has earlier been enabled, payment would successfully be debited from the fund source 22 once the credit card number and details are verified to be correct. The successful

payment notification will be sent to transaction channel controller 20. The transaction channel controller 20 will then send an electronic transaction receipt in the form of an SMS or an email to notify the user of the transaction device 12 of the successful transaction. Upon successful payment notification, the transaction is then deemed completed.

If 'Internet transaction' was not previously enabled, then the fund source 22 rejects the payment request even though the provided credit card details may be valid. An 'unsuccessful' notification will then be sent to the transaction channel controller 20. The transaction channel controller 20 will send a SMS or email to the transaction device 12 notifying the user of the unsuccessful transaction.

Fig. 3 illustrates the scenario where an unauthorized person 120 snipes credit card information of the user of the transaction device 12 and attempts to use the credit card information to make unauthorized airline reservations. As 'Internet transaction' as a mode of transaction to access the fund source 22 was not previously enabled by the user, the fund source will reject any payment request sent to it, regardless of the validity of the credit card details provided.

Fig. 4 illustrates the scenario where an unauthorized person 120 snipes credit card information of the user of the transaction device 12 and fabricate a fake credit card based on the sniped credit card information. The unauthorized person then attempts to use the credit card information to make unauthorized purchase with a merchant at a physical store using a Point of Sale terminal 16. If 'POS transaction' as a mode of transaction to access the fund source 22 was not previously enabled by the user, the fund source will reject any payment request sent to it, regardless of the validity of the credit card details provided.

In another embodiment, the fund source 22 is coupled with one or more user profile databases. The user profile databases may include location based services and are used to capture usage patterns, locations, favourite merchants, transaction amount, countries where most transaction take place, currency of transactions etc. The captured user profile data may be used to

automate the change of transaction states between 'lock' and 'unlock' without the need for a user's manual input provided the user chooses to effect such a feature known as 'enhanced lock-unlock'. It is to be appreciated that the enhanced lock-unlock feature may be used in conjunction with the manual lock/unlock or as an alternative. In the latter, where there is a conflict between manual and automatic instructions to lock/unlock the fund source, the manual instruction prevails and the automatic lock/unlock instruction is overrided.

Referring to Fig. 1, the enhanced lock-unlock feature may be sent via one of the request to 'turn on' the automatic lock-unlock feature. The enhanced lock-unlock feature is customized for a user/fund source owner by taking into account the 'risk appetite' of the user/fund source owner. The customization process is described as follows.

Prior to activating the enhanced lock unlock feature, a user will be prompted by the fund source system 22 to input the number of transaction parameters he wishes to use for customizing the 'lock-unlock' feature. The lower the risk appetite of the user, the more transaction parameters could be used for customization.

Using an example, a user may be presented a list of transaction parameters as a basis for an automatic lock if there is a match in the value/parameter

1. Transaction date time stamp — for prohibiting transactions if the transactions takes place at certain date and time (for example, when the user is overseas/ or during hours when the probability of the user making a purchase is low)
2. Merchant category code – for prohibiting transactions with merchants belonging to certain categories which the user has a low probability of making any purchase
3. Merchant name – for prohibiting transactions with blacklisted merchants

4. Merchant address – for prohibiting transactions with blacklisted merchants

5. Transaction amount – for prohibiting transactions above a certain upper limit

6. Country code – for prohibiting transactions in certain countries

7. Currency code – for prohibiting transactions made in certain currencies

In addition to the defined transaction parameters, location based services may be used to enable the risk alert management for the auto-lock feature.

Compared to the current auto-lock facility which is based on the global system settings of minute interval and triggered unlock timestamp, the customization of the 'lock-unlock' feature provides a 'fine-tune' adjustments depending on users' preference and are not limited by a predetermined period of time as disclosed in PCT WO2010/147559.

The feature affords the flexibility for authorization of batch payment to online merchants for example if the merchant name and address are not in the blacklist.

Variants

- The capability to lock/unlock accessibility to the fund source may be extended to the transaction device 12 in addition to the transaction channels.

The use and operation of transactions facilitated by credit card companies, such as MasterCard Worldwide is well known to persons skilled in the art and need not be described in any further detail herein except as is relevant to the present invention. Mechanisms and elements required to implement the 'lock' and 'unlock' such as specific processors, Unicard Gateway, Acquirer/Issuer system are found in PCT publication WO2010/147559 and the details of which are incorporated herein by reference.

In another embodiment, the system may incorporate the further feature where card issuers are given the option of locking/unlocking as described in PCT

publication WO 2013/103323. The feature as disclosed may be used in combination or in conjunction with the enhanced lock/unlock feature.

The various embodiments described above involve certain level of integration process such as the re-routing of transaction channels to the lock-unlock module, rule modification of the card management system; and the activation/linking with the user device 12 via transaction channels such as SMS, STK, Mobile-Apps, and Web-Portal. The embodiments above may be further improved by having features to:-

manage, monitor and maintain different fund sources account; remembering different PIN security of each fund sources;

manage and maintain different identification information that is required during the pre-authentication process like login-credentials which can also be used for pre-authorization.

In addition, the above embodiments may be further improved by having a simpler and " seamless" integration options with issuer banks or fund source system.

In accordance with another embodiment of the invention and with reference to Fig. 6, wherein like numerals reference like parts, the lock-unlock controller 20 is improvised to include a Proxy Wallet 200. The proxy wallet 200 is suited to issue physical transaction cards (e.g. credit or debit cards) that is capable for Point of Sale, Near Field Communication (NFC) and RFC devices for Face to face (F2F) transaction. The user 12 may register for proxy wallet 200 by initiating a sign-up via any transaction channel 16 such as Web portal, mobile apps, or USSD as illustrated in Fig. 7.

The sign up and registration capability allows a user to personalize the proxy wallet card generated and define a security PIN authentication. It also allows a user to register basic information as compliance for KYC (know-your-customer) and compliance with regulatory requirement such as the Anti-Money Laundering Act (AMLA) which requires certain level of declaration and transparency.

If the card user has multiple fund sources, he may link his various fund sources as illustrated in Fig. 8. The multiple linking of fund sources (via OAuth protocol verification process if available) during sign-up and/or linking process includes white-label cards with available commercial integration to a financial suite system, such as an e-Money Financial Suite (eFS) eco-system. The Proxy wallet owner can select the default/hierarchy fund source for authorization process.

In addition to the multiple linking of fund sources, the user may link all his identifications used for different fund sources via a Multiple Linking of Identification feature. This multiple linking feature links the different or associated identification of cardholder (as the proxy wallet owner) for instant pre-authentication and the acquiring of payment authorization process. This different identification used may include Mobile Number, Email Account, Social-media Account, Government-ID, Plate-number, Transponder ID, Biometric-Scan Data, NFC device ID/sticker, including those ID's that can associate to specific Merchant or Biller Account.

For instance, if the proxy wallet owner is a regular customer of AMAZON e-shopping then he/she can register his log-in account such that upon check-out and he chooses the system acquiring service for payment the system will automatically detect the corresponding Proxy Wallet Card since the log-in credential from AMAZON was already registered as one of wallet owner's ID.

Single PIN Authentication – this capability feature provide single PIN authentication not only for online transaction but also for card presence transaction devices that requires security PIN entry.

Permeability Transaction Security – this feature provide additional security layer to proxy wallet card by accessing user-defined security configuration to allow or restrict specific channel or transaction scenario for financial transaction. This feature uses the combination of account lock-unlock status, available parameters in transactions request (like PAN, Merchant Code, Merchant Name, Currency code, Country code, threshold Amount, Datetime, etc), specified/default fund source (for charging) and Card holders ID's which are all linked and/or associated to Proxy Wallet Card.

Cardholder Management Module – This capability feature provide self-care User-Interface to allow the following

- Fund source management such as linking, delinking, amount limits per transaction, aggregated transaction limits, account lock-unlock status, including other obvious feature for fund source management
- ID Management such as linking, delinking, amount limits per transaction, aggregated transaction limits, account lock-unlock status, including other obvious feature for fund source management
- Quick Transaction Search to verify and validate the details of authorized transaction
- Online Transaction Statement to retrieved and view statement of account history per fund sources associated or linked to Smart Wallet Proxy Card
- Summary of history transaction to provide reports of usage graphs patterns
- Security PIN Management such as change PIN and PIN Reset

Bank Module - This capability feature will provide standard API (pre-activation & activation, check lock-unlock status, transaction notification via SMS, Apps, email, etc) gateway for easy integration with participating issuing banks partner who are more comfortable for direct integration instead of usual acquiring channel. The module can be deployed as part of Proxy Wallet Lock-unlock Control or co-located with bankcard management system (just like MIP of Mastercard™) to provide close-loop and reliable network integration.

The invention provides the Physical Card as proxy wallet (Pseudo PAN) to link different fund sources and provides single PIN for pre-authorization security process. This will address the difficulties of managing and maintaining different fund sources account and difficulties to remember different PIN security of each fund sources.

The invention allows Multiple Linking of card holders (Proxy wallet owner's) ID to address the difficulties of managing and maintaining different identification information that is required during the pre-authentication process such as Mobile Number, Email Account, Social-media Account, Government-ID, Plate-number, Transponder ID, Biometric-Scan Data, NFC device ID/sticker, including those ID's that can associate to specific Merchant or Biller Account for online payment or purchase transaction.

The invention offers alternative integration using bank module for direction integration with issuing bank partners.

The invention also address the limitation of Paypal proxy virtual account that is not applicable for POS, NFC and RCF face-to-face (F2F) transaction and limited for safe online shopping only.

It should be further appreciated by the person skilled in the art that variations and combinations of features described above, not being alternatives or substitutes, may be combined to form yet further embodiments falling within the intended scope of the invention.

The Claims Defining the Invention are as Follows

1. A transaction system comprising

a transaction facilitator operable to receive and process a transaction request from a user device;

a transaction channel controller operable to change the state of the transaction channel between a first and a second state; and

a fund provider operable to receive processed transaction request and determine if the transaction channel is in the first or second state; and provide or not provide the funds accordingly.

2. A transaction system according to claim 1, wherein the first state corresponds to a state where the transaction channel is locked and forbidden for any transaction.

3. A transaction system according to claim 2, wherein the default state is the first state.

4. A transaction system according to claim 2 or 3, wherein the instruction to change the transaction channel from the first to second state and vice versa is initiated by the user device.

5. A transaction system according to claim 2 or 3, wherein the fund provider comprises a user profile database operable to automate the instruction to change the transaction channel from the first to second state and vice versa.

6. A transaction system according to claim 5, wherein the user profile database is operable to capture one or more of the following transaction parameters from the transaction request in order to determine whether the transaction channel should be in the first or second state:- Transaction Datetime stamp; Merchant Category Code; Merchant Name; Merchant Address; Transaction Amount; Country Code; or Currency Code.

7. A transaction system according to claim 5, wherein the user profile database is operable to determine the location of the user device sending the transaction request in order to determine whether the transaction channel should be in the first or second state.

8. A transaction system according to any one of the preceding claims, wherein the transaction channel is one of the following:-

point of sale terminal; Internet transaction; ATM.

9. A transaction system according to claim 1, wherein the transaction channel controller comprises an electronic wallet operable to create a transaction medium for the user, the transaction medium comprising an identifier of the user.

10. A transaction system according to claim 9, wherein the transaction medium is a credit/debit card.

11. A transaction system according to claim 9, wherein the electronic wallet comprises an authorization module operable to verify the legitimacy of fund source information.

12. A transaction system according to any one of claims 9 to 11, wherein the electronic wallet is operable to process and validate the request for linking of multiple fund sources.