(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 July 2017 (20.07.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/123157 A1

(51) International Patent Classification:
G06Q 20/40 (2012.01)

(21) International Application Number:
PCT/SG2017/050017

(22) International Filing Date:
13 January 2017 (13.01.2017)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10201600285Q 14 January 2016 (14.01.2016) SG

(71) Applicant: **VOXP PTE LTD** [SG/SG]; 24 Raffles Place, #27-01 Clifford Centre, Singapore 048621 (SG).

(72) Inventors: **MENDIOLA, Dennis**; 77 Seventh Avenue Apt 2T, New York, New York 10011 (US). **FETALVERO, Melvin Ryan Lopez**; 10 Road 5, Project 6, Quezon City (PH).

(74) Agent: **YUSARN AUDREY**; 24 Raffles Place, #27-01 Clifford Centre, Singapore 048621 (SG).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *of inventorship (Rule 4.17(iv))*

Published:

— *with international search report (Art. 21(3))*

WO 2017/123157 A1

(54) Title: SYSTEM AND METHOD FOR RESPONDING TO A FRAUDULENT EVENT

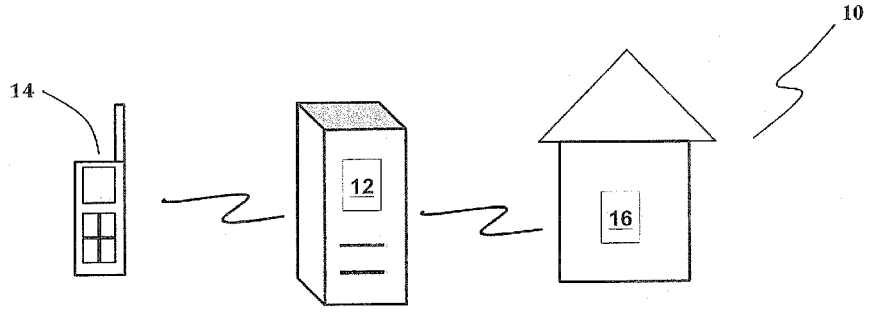

Fig. 1

(57) Abstract: A system for reporting an event comprising a communication facilitator associated with at least one network destination address, the at least one network destination address associated with an alphanumeric identifier; a user device having a user identifier, the user identifier associated with a transaction account; and an account database maintaining a state of the transaction account, the account database arranged in data communication with the communication facilitator; wherein when the user device sends a request to establish a connection with the communication facilitator via the alphanumeric identifier, the user identifier is sent to the communication facilitator, and the communication facilitator is then operable to match the user identifier with the associated transaction account and electronically instruct the account database to change the state of the transaction account from a first state to a second state.

SYSTEM AND METHOD FOR RESPONDING TO A FRAUDULENT EVENT

FIELD OF THE INVENTION

The present invention relates to a system and method for reporting and/or responding to one or more events. In particular, the system and method are suited for responding to a fraudulent or suspected fraudulent event such as ATM frauds.

BACKGROUND ART

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.

Financial fraud in the form of ATM fraud is growing at an increasing rate over the past few years. For example, in the Philippines, hundreds of millions was lost in 2900 cases of Bank Fraud in the time period of 2012-2013. As of late 2014, ATM fraud is at its highest and growing and result in $2 billion or more in losses (and rising) at ATMs around the world.

Smart Chips & EMV Compliant chip cards are existing solutions to minimize fraud occurrences but these are imperfect solutions. E-Commerce are typically dominated by Cash on Delivery (COD) transactions. Such increase in fraudulent activities result in the lack of trust of consumers in financial institutions.

In addition, most financial institutions such as banks rely on paper receipts for an account holder who withdraw cash from the ATM machine and there is no way to inform a user if someone makes a duplicate card to hack into the system.

While some financial institutions issue electronic receipts in the form of simple text message such as electronic short messages (i.e. SMS), with steps to follow

when a user suspect that a fraudulent event had taken place, the steps to report such fraudulent activities often include steps that are cumbersome, slow and may require many sub-steps of authentication of the user's identity before his/her account can be locked. Precious time is lost in the process of responding or reporting fraudulent activities, where the fraudster could have already made a few additional fraudulent transactions before the user account is finally locked.

It is an object of the invention to mitigate the above problem and provide an improved technical solution for responding to such fraudulent event(s).

SUMMARY OF THE INVENTION

Throughout the document, 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 invention is built upon existing electronic receipts (typically in the form of SMS) sent to a user informing him/her that a debit on his transaction account, such as a financial account (e.g. bank account) has taken place. This is due in part because the financial account is linked to the user's unique identifier such as a mobile identification number (MIN). Where the user suspects or know that the debit or withdrawal is a fraudulent event, he is required to initiate a call (which is regarded as an electronic trigger) to certain alphanumeric number(s) tied to the financial institution to lock his account. Such a process is cumbersome and precious time is wasted.

In according with an aspect of the invention there is a system for responding to an event comprises the provisioning of a communication facilitator for interfacing between a computer device and at least one financial institution. The communication facilitator is associated with at least one destination address which may be in the form of network address. Each of the at least one

destination address may in turn be associated with one or more toll-free access numbers. When a user assess the communication facilitator and a connection is established, the call is dropped by the communication facilitator and simultaneously the account associated with the user is disabled.

In another aspect of the invention there is a system for reporting an event comprising a communication facilitator associated with at least one network destination address, the at least one network destination address associated with an alphanumeric identifier; a user device having a user identifier, the user identifier associated with a transaction account; and an account database maintaining a state of the transaction account, the account database arranged in data communication with the communication facilitator; wherein when the user device sends a request to establish a connection with the communication facilitator via the alphanumeric identifier, the user identifier is sent to the communication facilitator, and the communication facilitator is then operable to match the user identifier with the associated transaction account and electronically instruct the account database to change the state of the transaction account from a first state to a second state.

In some embodiments, the alphanumeric identifier is a toll-free phone number.

In some embodiments, the user identifier is one of the following: a Mobile Station International Subscriber Directory Number (MSISDN); an email address; a social network account number.

In some embodiments, the account database is a financial institution.

In some embodiments, the first state is an enabled state and the second state is a disabled state.

In some embodiments, after the state of the transaction account is changed from the first state to the second state, the account database is operable to establish a connection with the user device.

In some embodiments, the connection with the user device includes verifying the identity of the user.

In some embodiments, the connection between the user device and communication facilitator is terminated after the communication facilitator receives the unique identifier and before the communication facilitator matches the user identifier with the associated account.

In some embodiments, the connection between the user device and communication facilitator is terminated after the communication facilitator receives the unique identifier and before the state of the account is changed from the first state to the second state.

In some embodiments, the connection between the user device and communication facilitator is terminated after the communication facilitator receives the unique identifier and after the state of the account is changed from the first state to the second state.

In some embodiments, the connection between the user device and communication facilitator is established via an electronic text message.

In some embodiments, there further comprises a registration facilitator for linking the transaction account with a subscriber account of the user device, the subscriber account hosted by a network provider.

In some embodiments, registration of a user with the registration facilitator includes generation of a one time private key. The one time private key may be generated based on a last transaction receipt with the transaction account.

In some embodiments, the last transaction receipt is an Automatic Teller Machine (ATM) receipt.

In some embodiments, the one time private key is generated based on combining a plurality of parameters in the ATM receipt. The plurality of parameters may include the following: time of last ATM transaction, date of the last ATM transaction, a transaction account number, an ATM receipt number, an ATM identifier, a transaction amount, an available balance after transaction. The one time private key may be valid for a pre-determined period of time for registration.

In some embodiments, the registration facilitator is operable to verify the authenticity of the one time private key.

In some embodiments, the one time private key is configured to expire after a pre-determined time elapse after the last transaction.

In another aspect of the invention there is a communication facilitator for use in a system for reporting an event, the communication facilitator associated with at least one network destination address, the at least one network destination address associated with a alphanumeric identifier; the communication facilitator

is further arranged in data communication with an account database; wherein when a user device having a user identifier establishes a connection with the communication facilitator via the alphanumeric identifier, the user identifier is sent to the communication facilitator, and the communication facilitator is then operable to match the user identifier with an associated transaction account and the communication facilitator is configured to issue an electronic instruction to change the state of the transaction account from a first state to a second state.

In some embodiments, the alphanumeric identifier is a toll-free phone number.

In some embodiments, the user identifier is one of the following: a Mobile Station International Subscriber Directory Number (MSISDN); an email address; a social network account number.

In some embodiments, the account database is a financial institution.

In some embodiments, the first state is an enabled state and the second state is a disabled state.

In some embodiments, after the state of the transaction account is changed from the first state to the second state, the account database is operable to establish another connection with the user device.

In some embodiments, the connection with the user device includes verifying the identity of the user.

In some embodiments, the connection between the user device and communication facilitator is terminated after the communication facilitator receives the unique identifier and before the communication facilitator matches the user identifier with the associated account.

In some embodiments, the connection between the user device and communication facilitator is terminated after the communication facilitator receives the unique identifier and before the state of the account is changed from the first state to the second state.

In some embodiments, the connection between the user device and communication facilitator is terminated after the communication facilitator receives the unique identifier and after the state of the account is changed from the first state to the second state.

In some embodiments, the connection between the user device and

communication facilitator is established via an electronic text message or a Unstructured Supplementary Service Data (USSD) electronic trigger.

In some embodiments, the system further comprises a registration facilitator for linking the transaction account with a subscriber account associated with the user device, the subscriber account hosted by a network provider.

In some embodiments, the registration of a user with the registration facilitator includes generation of a one time private key. The one time private key may be generated based on a last transaction receipt with the transaction account.

In some embodiments, the last transaction receipt is an ATM receipt. In these cases, the one time private key is generated based on combining a plurality of parameters in the ATM receipt.

In some embodiments, the plurality of parameters include the following: time of last ATM transaction, date of the last ATM transaction, a transaction account number, an ATM receipt number, an ATM identifier, a transaction amount, an available balance after transaction.

In some embodiments, the last transaction receipt is valid for a pre-determined period of time for registration.

In some embodiments, the registration facilitator is operable to verify the authenticity of the last transaction receipt.

In some embodiments, the one time private key is configured to expire after a pre-determined time elapse after the last transaction.

In accordance with another aspect there is a method for reporting an event comprising the steps of: sending from a user device a request for reporting a fraud to a communication facilitator, the request comprises an user identifier of the user device associated with a transaction account; receiving at the communication facilitator the request for connection; the communication facilitator operable to retrieve the user identifier and simultaneously disconnect from the user device; matching the user identifier against an account database to identify the transaction account associated with the user device; and changing the state of the transaction account from a first state to a second state.

In accordance with another aspect there is a non-transitory computer readable medium containing executable software instructions thereon wherein when executed performs the steps of: sending from a user device a request for

reporting a fraud to a communication facilitator, the request comprises an user identifier of the user device associated with a transaction account; receiving at the communication facilitator the request for connection; the communication facilitator operable to retrieve the user identifier and simultaneously disconnect from the user device; matching the user identifier against an account database to identify the transaction account associated with the user device; and changing the state of the transaction account from a first state to a second state.

In accordance with another aspect there is a registration facilitator for linking a transaction account with a subscriber account hosted by a network provider, comprising a one-time key generator for generating a one-time key; a transaction receipt receiver for receiving at least one transaction receipt; a registration interface for receiving a request for registration from a user; and an authenticator for verifying the request for registration; wherein the one-time key is generated based on a plurality of transaction parameters obtained from the at least one transaction receipt; and the authenticator is operable to compare the obtained plurality of transaction parameters with the one-time key and link the transaction account with the subscriber account if the one-time key corresponds with the plurality of transaction parameters.

In some embodiments, the transaction receipt is an Automated Teller Machine (ATM) receipt.

In some embodiments, the plurality of transaction parameters include the following: time of last ATM transaction, date of the last ATM transaction, a transaction account number, an ATM receipt number, an ATM identifier, a transaction amount, an available balance after transaction.

In some embodiments, the transaction receipt is valid for a pre-determined period of time for registration.

In some embodiments, the one time private key is configured to expire after a pre-determined time elapse after the transaction.

The platform provides financial institutions with an additional robust and real-time layer of security for its customers for achieving at least the following objectives.

- Minimize Fraud
- Improve Security Measures

- Increase Trust

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 is a system diagram in accordance with an embodiment of the invention;

Fig. 2 is a system diagram comprising a registration facilitator for linking a transaction account with a subscriber account associated with the user device according to some embodiments;

Fig. 3 is a flow chart of a method for reporting or responding to a fraudulent event according to some embodiments; and

Fig. 4 is a system diagram comprising a registration facilitator for linking a transaction account with a subscriber account hosted by a network provider.

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

EMBODIMENTS OF THE INVENTION

Particular embodiments of the present invention will now be described with reference to the accompanying drawings. The terminology used herein is for the purpose of describing particular embodiments only and is not intended to limit the scope of the present invention. Additionally, unless defined otherwise, all technical and scientific terms used herein have the same meanings as commonly understood by one of ordinary skill in the art to which this invention belongs.

In according with an aspect of the invention there is a system 10 for reporting a fraudulent event comprising a communication facilitator 12 associated with at least one network destination address, the at least one network destination address associated with an alphanumeric identifier; a user device 14 having an user identifier 104, the user identifier 104 associated with a transaction account; and an account database 18 maintaining a state of the transaction account, the

account database in data communication with the communication facilitator 12; wherein when the user device 14 sends a request to establish a connection with the communication facilitator 12 via the alphanumeric identifier, the user identifier 104 is sent to the communication facilitator 12, and the communication facilitator 12 is then operable to match the user identifier 104 with the associated transaction account and electronically instruct the account database 18 to change the state of the transaction account from a first state to a second state. In some embodiments, the first state is an enabled state and the second state is a disabled state. It is appreciated that the enabled state may be switched to the disabled state via different methods.

In accordance with an embodiment of the present invention as shown in Fig. 1 the system 10 may be implemented for reporting/responding to a transaction fraud attempt. Central to the system is the provisioning of a communication facilitator 12 for interfacing between the user 14 (identified by a user device) and a financial institution 16. The communication facilitator 12 is associated with one or more network destination addresses. In some embodiments, each of the network destination address may be associated with one or more toll-free phone numbers, or the network destination address may be the toll-free phone number. The communication facilitator 12 may or may not be within the same network hosting the user device 14, and could be hosted in another network but the user device 14 may be able to establish data communication via auto-roaming, for example.

The communication facilitator 12 is preferably in data communication with the one or more financial institutions 16. In particular, the communication facilitator 14 is preferably in data communication with the account database 18 held by the financial institution(s) 16 and may therefore access the user database 18 to lock the transaction account associated with a user when a fraudulent activity is suspected or detected.

In some embodiments, the user identifier may comprise one or more of the following: a Mobile Station International Subscriber Directory Number (MSISDN); an email address; a social network account number. In some embodiments, the user identifier may also comprise a combination of any of the aforementioned identifiers.

In some embodiments, when the state of the transaction account is changed from the first state to the second state, the account database is operable to establish a connection with the user device 14. Once connection with the user device 14 is established, verification of the identity of the user takes place. The connection between the user device 14 and communication facilitator 12 is typically cut or terminated before the communication facilitator 12 matches the user identifier with the associated account, but after the communication facilitator 12 has obtained the necessary information including the unique identifier 104 for purpose of checking, matching and/or identifying the transaction account of the user. In such embodiments, the connection between the user device 14 and communication facilitator 12 is cut before the state of the account is changed from the first state to the second state (i.e. drop call) to minimize or completely omit incurrance of costs to the user.

In alternative embodiments, the connection between the user device 14 and communication facilitator 12 is cut or terminated after the state of the account is changed from the first state to the second state.

In some embodiments, connection between the user device 14 and communication facilitator 12 is established via an electronic text message, such as, but not limited to, a SMS message or a USSD message. In other embodiments, connection is established via the user device 14 initiating a Unstructured Supplementary Service Data (USSD) trigger or call dialing the alphanumeric identifier.

In some embodiments, as shown in Fig. 2, there comprises a system 200 comprising a registration facilitator 24 for linking the transaction account with a subscriber account associated with the user device 14, the subscriber account hosted by a network provider, such as, but not limited to, a telecommunications network provider 26. The unique identifier 104 associated with the user device 14 may be also utilized for linkage with the registration facilitator 24. The registration of a user with the registration facilitator 24 may include the generation of a one-time private key. In some embodiments, the one-time private key is generated based on a last transaction receipt with the transaction account. The last transaction receipt may be an Automatic Teller Machine (ATM) receipt in the case of an ATM transaction. In particular, the one-time

private key may be generated based on combining a plurality of parameters in the ATM receipt. The plurality of parameters may include the following: time of last ATM transaction, date of the last ATM transaction, a transaction account number, an ATM receipt number, an ATM identifier, a transaction amount, an available balance after transaction.

In some embodiments, the one-time private key is valid for a pre-determined period of time for the user to perform his/her registration. The pre-determined period may be two to five minutes, for example. Once the one-time private key is provided to the registration facilitator 24, the registration facilitator 24 then operates to verify the authenticity of the one-time private key. This may include retrieving one or more of the plurality of parameters from an authentication database comprising entries of the plurality of parameters associated with the ATM receipt. In some embodiments, the one-time private key is configured to expire after the pre-determined time elapse after the last transaction.

In accordance with another aspect of the invention, wherein like reference numerals designate like parts, there comprises a communication facilitator 12 for use in a system 10 for reporting a fraudulent event, the communication facilitator 12 associated with at least one network destination address, the at least one network destination address associated with an alphanumeric identifier; the communication facilitator 12 is further arranged in data communication with an account database, wherein when a user device 14 having a user identifier 104 establishes a connection with the communication facilitator via the alphanumeric identifier, the user identifier is sent to the communication facilitator, and the communication facilitator is then operable to match the user identifier with an associated transaction account and the communication facilitator is configured to issue an electronic instruction to change the state of the transaction account from a first state to a second state.

In another aspect of the invention and with reference to Fig. 3, wherein like reference numerals designate like parts, there is a method 300 for reporting a fraudulent event comprising the steps of: sending from a user device 14 a request for reporting a fraud to a communication facilitator 12 (step s302), the request comprises a user identifier 104 of the user device 14 associated with a transaction account; receiving at the communication facilitator the request for

connection (step s304); the communication facilitator 12 operable to retrieve the user identifier 104 and simultaneously disconnect from the user device 14; matching the user identifier against an account database to identify the transaction account associated with the user device (step s306); and changing the state of the transaction account from a first state to a second state (step s308).

In another aspect of the invention there comprises a non-transitory computer readable medium containing executable software instructions thereon wherein when executed performs the method 300 comprising steps of sending from a user device a request for reporting a fraud to a communication facilitator, the request comprises an user identifier of the user device associated with a transaction account; receiving at the communication facilitator the request for connection; the communication facilitator operable to retrieve the user identifier and simultaneously disconnect from the user device; matching the user identifier against an account database to identify the transaction account associated with the user device; and changing the state of the transaction account from a first state to a second state.

In another aspect of the invention and with reference to Fig. 4, there comprises a registration facilitator 40 for linking a transaction account 42 with a subscriber account 44 hosted by a network provider 46, comprising a one-time key generator 48 for generating a one-time key; a transaction receipt receiver 50 for receiving at least one transaction receipt; a registration interface 52 for receiving a request for registration from a user; and an authenticator 54 for verifying the request for registration; wherein the one-time key is generated based on a plurality of transaction parameters obtained from the at least one transaction receipt; and the authenticator 54 is operable to compare the obtained plurality of transaction parameters with the one-time key and link the transaction account with the subscriber account if the one-time key corresponds with the plurality of transaction parameters.

In some embodiments, the transaction receipt is an Automated Teller Machine (ATM) receipt.

In some embodiments, the plurality of transaction parameters include the following: time of last ATM transaction, date of the last ATM transaction, a

transaction account number, an ATM receipt number, an ATM identifier, a transaction amount, an available balance after transaction.

In some embodiments, the transaction receipt is valid for a pre-determined period of time for registration.

In some embodiments, the one time private key is configured to expire after a pre-determined time elapse after the transaction.

The system 10 may be operated in the context of an ATM transaction associated with financial institution 16 maintaining the user account/ account database.

When a transaction at an ATM associated with the financial institution 16 has taken place, an electronic receipt, in the form of a SMS or USSD message may be sent to the user device 14. The electronic message is sent almost instanteously by a SMS centre arranged in data communication with the financial institution 16. The electronic receipt contains details of how to report a fraudulent activity should he/she suspect of the same. The alphanumeric identificer, in the form of the toll-free access phone number associated with the communication facilitator 12, is provided in the electronic receipt.

If the user did not make the ATM transaction, he calls the toll-free number to establish a connection. Upon being connected, the unique identifier of the user device 14 is sent to the communication facilitator 12 which then compares with entries in the account database maintained by the financial institution 16. Simultaneously the matching user transaction account, which may be a bank account associated with the user device 14 unique identifier (such as Mobile Identification Number) is locked or disabled. An electronic notification message is sent to the financial customer service department of the financial institution 16. This is achieved without the need of the user 14 to provide any details to authenticate his/her identity, and/or wait for a period (e.g. 5 minutes) because of busy communication traffic, due to, for example, a situation where “all our customer service personnels are busy at the moment”. The connection is then ended (drop call) without the need for the user to speak to any customer service personnel.

At the same time, the communication facilitator 12 which is in data communication with the financial institution 16 then sends a notification or alert

to the bank customer service department, who may thereafter call the user 14 to confirm the details of the fraudulent event, while keeping the (already locked) user's account safe from further fraudulent attempts, which could have taken place if the account was locked later, rather than earlier. It is therefore to be appreciated that time is of essence when dealing with suspected fraudulent activities and the invention is focused to address the report of fraudulent activity in a fast, efficient and cheap manner or at no cost to the user (toll-free access alphanumeric identifier).

In some embodiments, where the user identifier is issued by a host network, such as a telecommunications carrier, the communication facilitator 12 may interface with both the financial institution and the host network of the user 14. Such interface could preferably be in the form of one or more dedicated communication channels and is secured. Where there are multiple host networks in the form of multiple telecommunications carrier around the world, each host network has preferably have its own dedicated communication channel in data communication with the communication facilitator 12.

In some embodiments, the communication facilitator 12 is in direct connection to the SMS center (SMSC) 204 or a USSD server 206 operable to send the electronic receipt, and may take over the management of the SMSC.

A drop call to change the state of the transaction account between unlocked and locked after the occurance of fraud is advantageous over systems which is based on or depends on interaction with authorized personnel. A missed call/droped call does not incur cost for the user. Most voice/call based triggers are priced per minute/per second(pulse charging). But since the call is dropped and is never answered, the backend communication facilitator 12 receives the unique identifier (i.e. mobile number) of the caller and the number or access code dialed. These details together with the date can be used for fraud record and context (Lock, unlock and date).

Using USSD as the trigger for changing the state of the bank account between locked and unlocked is further advantageous compared to the use of other types of triggers. USSD may be initiated via a call with a user interface. It works as toll free at no cost to the user, meaning a user can trigger it even with zero balance and/or roaming outside the host network of the user device 14.

As an added layer of accountability, in addition to the sending of electronic receipts via SMS only, the electronic receipts and further notifications may be sent via a plurality of modes including SMS and email.

The above embodiments describe a technical solution for responding to fraud that is secured and easy to activate (with simply a dial) with savings in time to lock an account. A user do not need to remember common authentication type questions such as 'mother's maiden name', 'First school' etc, to go through a series of such time-consuming activities in order to lock his account, by which time more fraudulent activities could have been carried out.

Further, the toll-free access to the communication facilitator 12 allows easy access especially for pre-paid users who may be without load at the time he/she needs to report a fraudulent event.

A user may choose to register with the communication facilitator 12. As part of the registration process, the user may need to provide a scanned copy of the ATM receipt for a recent withdrawal transactions.

The above is a description of various embodiments of the present invention. It is envisioned that those skilled in the art can design alternative embodiments of this invention that falls within the scope of the invention. In particular:-

- Although the embodiments have been described with reference to responding or reporting to fraudulent events, and change of states of a user transaction account is described with reference to 'unlock to lock'; 'enabled to disabled'; it is to be appreciated that other change of states as known to a skilled person may be applied. In particular, the invention may be applied to systems where speed of reporting an event to change the state of a transaction account pursuant to an event is crucial and important.
- Further, it is to be appreciated that the system is not limited to report or respond to a fraudulent event but may be applied for responding or reporting to other events.

It is to be appreciated that features in various embodiments, not being alternatives to one another, may be combined to form yet further embodiments falling within the scope of the invention.

CLAIMS

1. A system for reporting an event comprising

a communication facilitator associated with at least one network destination address, the at least one network destination address associated with an alphanumeric identifier;

a user device having a user identifier, the user identifier associated with a transaction account; and

an account database maintaining a state of the transaction account, the account database arranged in data communication with the communication facilitator;

wherein when the user device sends a request to establish a connection with the communication facilitator via the alphanumeric identifier, the user identifier is sent to the communication facilitator, and the communication facilitator is then operable to match the user identifier with the associated transaction account and electronically instruct the account database to change the state of the transaction account from a first state to a second state.

2. The system according to claim 1, wherein the alphanumeric identifier is a toll-free phone number.

3. The system according to claim 1 or 2, wherein the user identifier is one of the following: a Mobile Station International Subscriber Directory Number (MSISDN); an email address; a social network account number.

4. The system according to any one of claims 1 to 3, wherein the account database is a financial institution.

5. The system according to any one of claims 1 to 4, wherein the first state is an enabled state and the second state is a disabled state.

6. The system according to any one of claims 1 to 5, wherein after the state of the transaction account is changed from the first state to the second state,

the account database is operable to establish a connection with the user device.

7. The system according to claim 6, wherein the connection with the user device includes verifying the identity of the user.

8. The system according to any one of claims 1 to 7, wherein the connection between the user device and communication facilitator is terminated after the communication facilitator receives the unique identifier and before the communication facilitator matches the user identifier with the associated account.

9. The system according to any one of claims 1 to 7, wherein the connection between the user device and communication facilitator is terminated after the communication facilitator receives the unique identifier and before the state of the account is changed from the first state to the second state.

10. The system according to any one of claims 1 to 7, wherein the connection between the user device and communication facilitator is terminated after the communication facilitator receives the unique identifier and after the state of the account is changed from the first state to the second state.

11. The system according to any one of claims 1 to 10, wherein the request to establish a connection with the communication facilitator is an electronic text message or a Unstructured Supplementary Service Data (USSD) trigger.

12. The system according to claim 1, further comprising a registration facilitator for linking the transaction account with a subscriber account of the user device, the subscriber account hosted by a network provider.

13. The system according to claim 12, wherein registration of a user with the registration facilitator includes generation of a one time private key.

14. The system according to claim 13, wherein the one time private key is

generated based on a last transaction receipt with the transaction account.

15. The system according to claim 15, wherein the last transaction receipt is an Automatic Teller Machine (ATM) receipt.

16. The system according to claim 15, wherein the one time private key is generated based on combining a plurality of parameters in the ATM receipt.

17. The system according to claim 16, wherein the plurality of parameters include the following: time of last ATM transaction, date of the last ATM transaction, a transaction account number, an ATM receipt number, an ATM identifier, a transaction amount, an available balance after transaction.

18. The system according to any one of claims 14 to 17, wherein the one time private key is valid for a pre-determined period of time for registration.

19. The system according to any one of claims 14 to 18, wherein the registration facilitator is operable to verify the authenticity of the one time private key.

20. The system according to any one of claims 14 to 19, wherein the one time private key is configured to expire after a pre-determined time elapse after the last transaction.

21. A communication facilitator for use in a system for reporting an event, the communication facilitator associated with at least one network destination address, the at least one network destination address associated with a alphanumeric identifier; the communication facilitator is further arranged in data communication with an account database
wherein when a user device having a user identifier establishes a connection with the communication facilitator via the alphanumeric identifier, the user identifier is sent to the communication facilitator, and the communication facilitator is then operable to match the user identifier with an associated

transaction account and the communication facilitator is configured to issue an electronic instruction to change the state of the transaction account from a first state to a second state.

22. The communication facilitator according to claim 21, wherein the alphanumeric identifier is a toll-free phone number.

23. The communication facilitator according to claim 21 or 22, wherein the user identifier is one of the following: a Mobile Station International Subscriber Directory Number (MSISDN); an email address; a social network account number.

24. The communication facilitator according to any one of claims 21 to 23, wherein the account database is a financial institution.

25. The communication facilitator according to any one of claims 21 to 24, wherein the first state is an enabled state and the second state is a disabled state.

26. The communication facilitator according to any one of claims 21 to 25, wherein after the state of the transaction account is changed from the first state to the second state, the account database is operable to establish a connection with the user device.

27. The communication facilitator according to claim 26, wherein the connection with the user device includes verifying the identity of the user.

28. The communication facilitator according to any one of claims 21 to 27, wherein the connection between the user device and communication facilitator is terminated after the communication facilitator receives the unique identifier and before the communication facilitator matches the user identifier with the associated account.

29. The communication facilitator according to any one of claims 21 to 27, wherein the connection between the user device and communication facilitator is terminated after the communication facilitator receives the unique identifier and before the state of the account is changed from a first state to a second state.

30. The communication facilitator according to any one of claims 21 to 27, wherein the connection between the user device and communication facilitator is terminated after the communication facilitator receives the unique identifier and after the state of the account is changed from a first state to a second state.

31. The communication facilitator according to any one of claims 21 to 30, wherein the request to establish a connection with the communication facilitator is an electronic text message or a Unstructured Supplementary Service Data (USSD) trigger.

32. The communication facilitator according to claim 21, further comprising a registration facilitator for linking the transaction account with a subscriber account of the user device, the subscriber account hosted by a network provider.

33. The communication facilitator according to claim 32, wherein registration of a user with the registration facilitator includes generation of a one time private key.

34. The communication facilitator according to claim 33, wherein the one time private key is generated based on a last transaction receipt with the transaction account.

35. The communication facilitator according to claim 35, wherein the last transaction receipt is an ATM receipt.

36. The communication facilitator according to claim 35, wherein the one

time private key is generated based on combining a plurality of parameters in the ATM receipt.

37. The communication facilitator according to claim 36, wherein the plurality of parameters include the following: time of last ATM transaction, date of the last ATM transaction, a transaction account number, an ATM receipt number, an ATM identifier, a transaction amount, an available balance after transaction.

38. The communication facilitator according to any one of claims 34 to 37, wherein the last transaction receipt is valid for a pre-determined period of time for registration.

39. The communication facilitator according to any one of claims 34 to 38, wherein the registration facilitator is operable to verify the authenticity of the last transaction receipt.

40. The communication facilitator according to any one of claims 34 to 39, wherein the one time private key is configured to expire after a pre-determined time elapse after the last transaction.

41. A method for reporting a event comprising

sending from a user device a request for reporting a fraud to a communication facilitator, the request comprises an user identifier of the user device associated with a transaction account;

receiving at the communication facilitator the request for connection; the communication facilitator operable to retrieve the user identifier and simultaneously disconnect from the user device;

matching the user identifier against an account database to identify the transaction account associated with the user device; and

changing the state of the transaction account from a first state to a second state.

42. A non-transitory computer readable medium containing executable

software instructions thereon wherein when executed performs the steps of:

sending from a user device a request for reporting a fraud to a communication facilitator, the request comprises an user identifier of the user device associated with a transaction account;

receiving at the communication facilitator the request for connection; the communication facilitator operable to retrieve the user identifier and simultaneously disconnect from the user device;

matching the user identifier against an account database to identify the transaction account associated with the user device; and

changing the state of the transaction account from a first state to a second state.

43. A registration facilitator for linking a transaction account with a subscriber account hosted by a network provider, comprising

a one-time key generator for generating a one-time key;

a transaction receipt receiver for receiving at least one transaction receipt;

a registration interface for receiving a request for registration from a user; and

an authenticator for verifying the request for registration;

wherein the one-time key is generated based on a plurality of transaction parameters obtained from the at least one transaction receipt; and the authenticator is operable to compare the obtained plurality of transaction parameters with the one-time key and link the transaction account with the subscriber account if the one-time key corresponds with the plurality of transaction parameters.

44. The registration facilitator according to claim 43, wherein the transaction receipt is an Automated Teller Machine (ATM) receipt.

45. The registration facilitator according to claim 44, wherein the plurality of transaction parameters include the following: time of last ATM transaction, date of the last ATM transaction, a transaction account number, an ATM receipt

number, an ATM identifier, a transaction amount, an available balance after transaction.

46. The registration facilitator according to any one of claims 43 to 45, wherein the transaction receipt is valid for a pre-determined period of time for registration.

47. The registration facilitator according to any one of claims 43 to 46, wherein the one time private key is configured to expire after a pre-determined time elapse after the transaction.

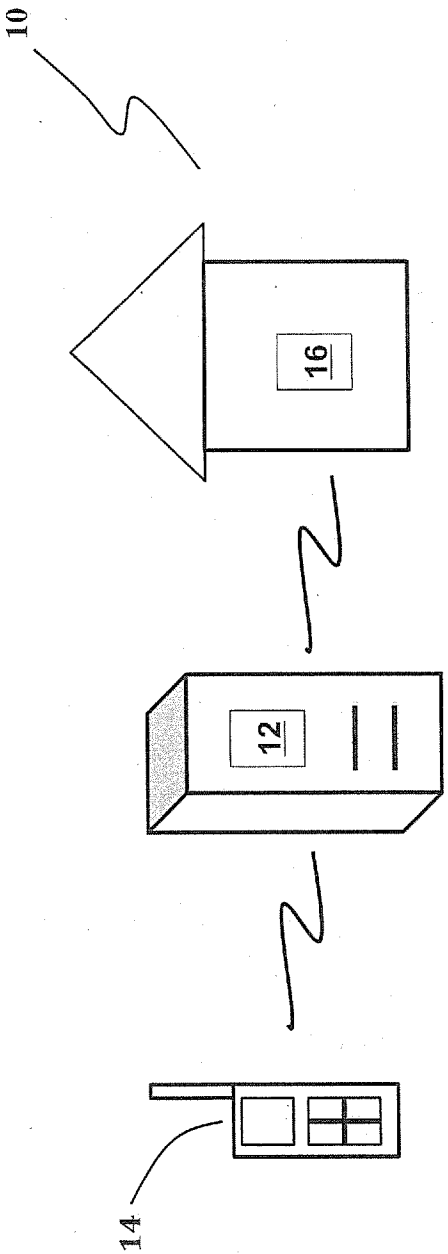

Fig. 1

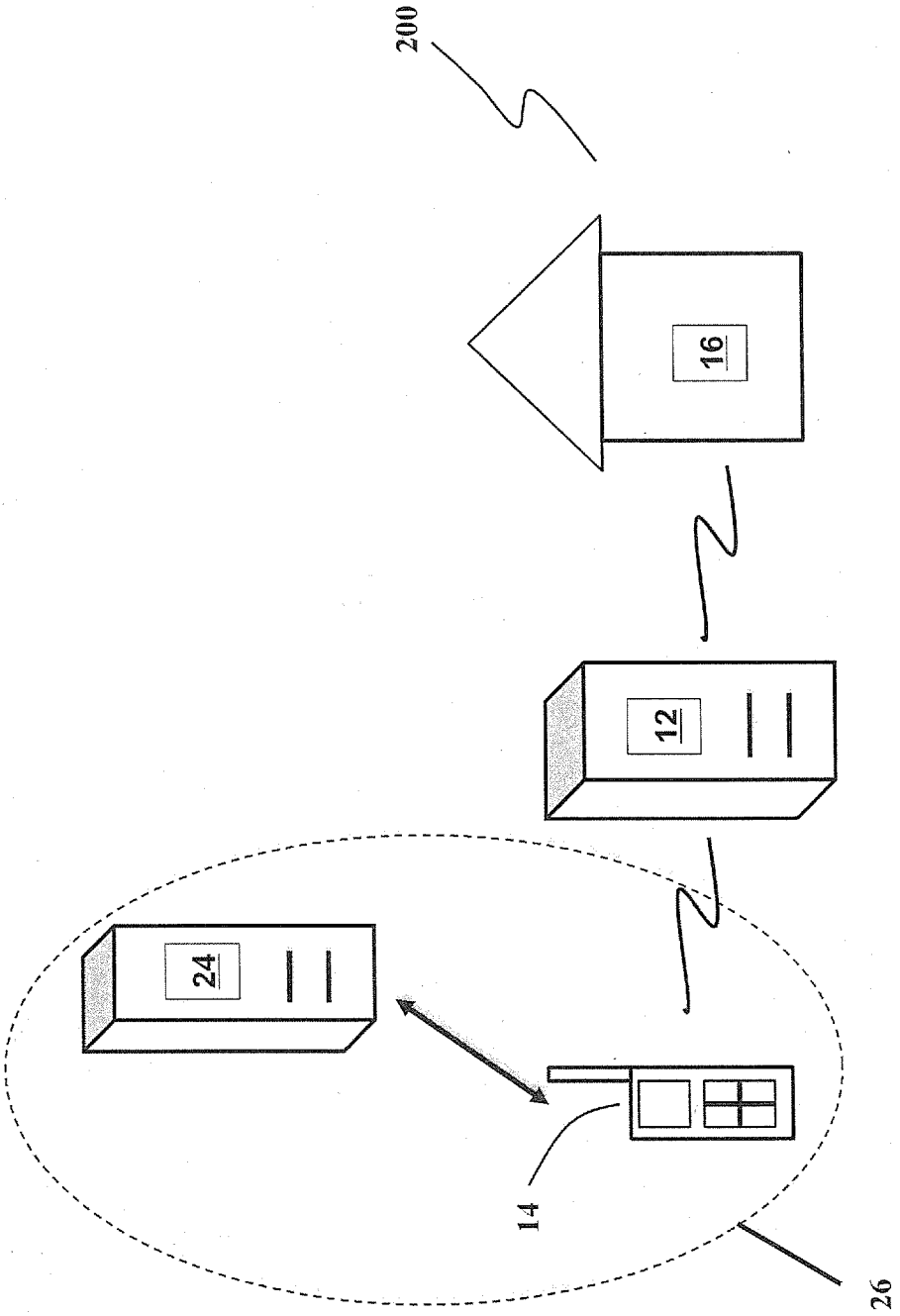

Fig. 2

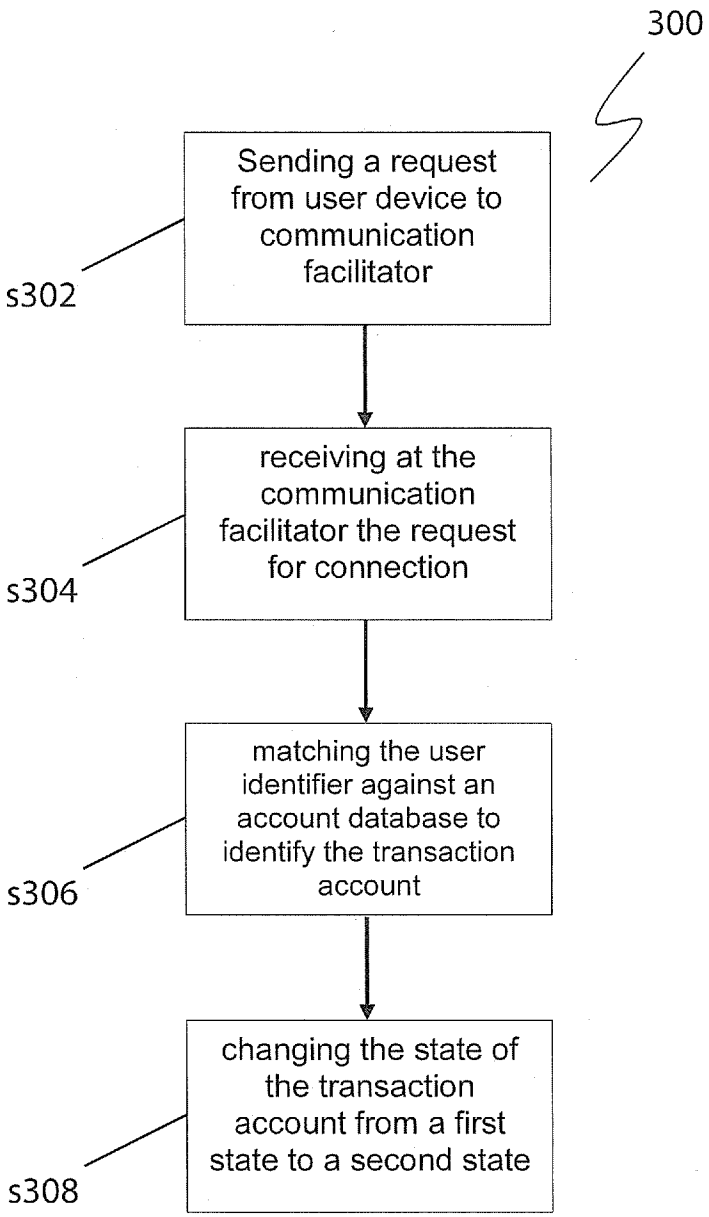
300
Sending a request from user device to communication facilitator
s302
receiving at the communication facilitator the request for connection
s304
matching the user identifier against an account database to identify the transaction account
s306
changing the state of the transaction account from a first state to a second state
s308

Fig. 3

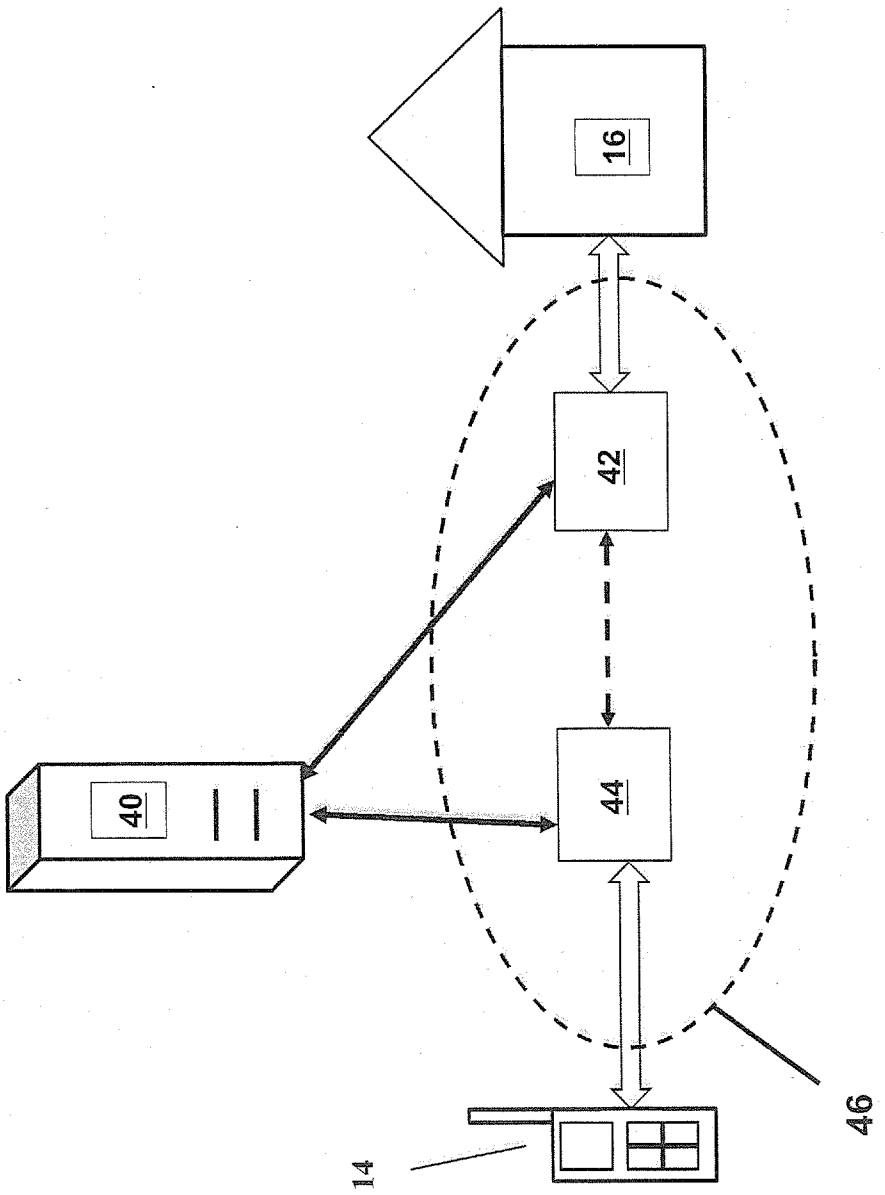

Fig. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SG2017/050017

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/40 (2012.01)

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPODOC, WPIAP: Classmarks EPODOC only (CPC G06Q20/4016, G06Q30/0225); Keywords (detect, identify, fraud, unauthorised, event, activity, transaction, call, connect, advise, notify, third, trusted, party, entity, match, account, lock, unlock, freeze, unfreeze, enable, disable, block, suspend, deactivate, one time, single, use, key, passcode, transaction, atm, receipt, sms, text message and like terms)

Google/Google Patents/ Google Scholar websites: Similar keyword as above also (ATM fraud lock account phone, lock account phone, ATM fraud lock unlock one time key, third party account lock atm fraud, call to lock unlock financial account, account lock alphanumeric and like terms)

Applicant and Inventor name searches on Google patents, AUSPAT and AU Internal Databases

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	Documents are listed in the continuation of Box C	

[X] Further documents are listed in the continuation of Box C [X] See patent family annex

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
3 May 2017	03 May 2017
Name and mailing address of the ISA/AU	**Authorised officer**
AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA Email address: pct@ipaustralia.gov.au	Neil Miller AUSTRALIAN PATENT OFFICE (ISO 9001 Quality Certified Service) Telephone No. 0262104089

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SG2017/050017

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:
the subject matter listed in Rule 39 on which, under Article 17(2)(a)(i), an international search is not required to be carried out, including

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a)

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

See Supplemental Box for Details

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☒ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		International application No. **PCT/SG2017/050017**
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2014/175949 A1 (QUISK, INC.) 30 October 2014 abstract, paras [005]-[007], [0016]-[025], [032]-[034], [037]-[041], [046]-[050], Figs 1, 3, 4 and 5	1-42
X	US 2015/0095984 A1 (YAHOO! INC.) 02 April 2015 paras [0018]-[0058] and Figs 1-3	1-42
X	US 7983979 B2 (HOLLAND, IV) 19 July 2011 Col 4 line 52-Col 8 line 18 and Figs 1-4	1-42
X	US 2013/0024923 A1 (WALLAJA) 24 January 2013 [0006], [0030], [0033]-[0037]	43-47

Supplemental Box

Continuation of: **Box III**

This International Application does not comply with the requirements of unity of invention because it does not relate to one invention or to a group of inventions so linked as to form a single general inventive concept.

This Authority has found that there are different inventions based on the following features that separate the claims into distinct groups:

- Claims 1-42 are directed to systems and methods for changing the status of a users transaction account. The feature of establishing a connection with the communication facilitator via alphanumeric identifier, sending a user identifier to the communication facilitator, matching by the communication facilitator the user identifier to an associated transaction account and issuing instructions to change the state of the transaction account from a first state to a second state is specific to this group of claims.

- Claims 43-47 are directed to a system for linking a transaction account with a subscriber account hosted by a network provider. The feature of generating a one-time key based on a plurality of transaction parameters obtained from the at least one transaction receipt; and linking the transaction account with the subscriber account based on a comparison of the one-time key with plurality of transaction parameters is specific to this group of claims.

PCT Rule 13.2, first sentence, states that unity of invention is only fulfilled when there is a technical relationship among the claimed inventions involving one or more of the same or corresponding special technical features. PCT Rule 13.2, second sentence, defines a special technical feature as a feature which makes a contribution over the prior art.

When there is no special technical feature common to all the claimed inventions there is no unity of invention.

In the above groups of claims, the identified features may have the potential to make a contribution over the prior art but are not common to all the claimed inventions and therefore cannot provide the required technical relationship. Therefore there is no special technical feature common to all the claimed inventions and the requirements for unity of invention are consequently not satisfied *a priori*.

INTERNATIONAL SEARCH REPORT Information on patent family members	International application No. **PCT/SG2017/050017**

This Annex lists known patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document/s Cited in Search Report		**Patent Family Member/s**	
Publication Number	**Publication Date**	**Publication Number**	**Publication Date**
WO 2014/175949 A1	30 October 2014	WO 2014175949 A1	30 Oct 2014
		CN 105283898 A	27 Jan 2016
		EP 2989605 A1	02 Mar 2016
		JP 2016517119 A	09 Jun 2016
		MX 2015014727 A	07 Mar 2016
		US 8788389 B1	22 Jul 2014
		US 2014324694 A1	30 Oct 2014
US 2015/0095984 A1	02 April 2015	US 2015095984 A1	02 Apr 2015
US 7983979 B2	19 July 2011	US 2006204051 A1	14 Sep 2006
		US 7983979 B2	19 Jul 2011
		WO 2006099081 A2	21 Sep 2006
US 2013/0024923 A1	24 January 2013	US 2013024923 A1	24 Jan 2013
		US 9275379 B2	01 Mar 2016
		CN 102906776 A	30 Jan 2013
		US 2016156627 A1	02 Jun 2016
		WO 2011121566 A1	06 Oct 2011

End of Annex

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.