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

(51) International Patent Classification:
G06Q 40/00 (2012.01)

(21) International Application Number:
PCT/IB2014/059484

(22) International Filing Date:
6 March 2014 (06.03.2014)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2013/01792   8 March 2013 (08.03.2013)   ZA

(71) Applicant: OLTIO (PROPRIETARY) LIMITED
[ZA/ZA]; 1st Floor Summit Place, cnr. Summit and Rivo-
nia Roads, 2 196 Morningside (ZA).

(72) Inventor: ROUX, Petrus, Daniel, Jacobus; 5 Nellmapius
Road, Irene, 0157 Centurion (ZA).

(74) Agents: SPOOR & FISHER et al; P O Box 454, 0001
Pretoria (ZA).

(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, 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, KN, KP, KR,
KZ, LA, LC, LK, LR, LS, LT, 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, 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).

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

(54) Title: A METHOD OF IMPLEMENTING VERIFICATION FOR A TRANSACTION AND A SYSTEM THEREFOR

FIGURE 1
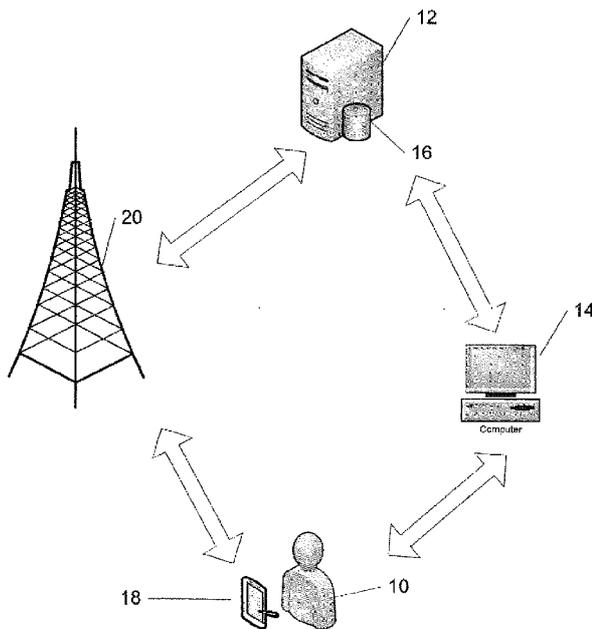
(57) Abstract: A method and system for verification
of a transaction includes receiving a request from a
user via the internet to upload a beneficiary bank ac-
count number. A request is then transmitted to the
user to enter at least part of the beneficiary bank ac-
count number again via a different communications
channel, typically via a USSD session using their
mobile telephone on a mobile network. The returned
part of the beneficiary bank account number is com-
pared with the beneficiary bank account number
entered via the internet and if these two match then
the transaction is verified so that the beneficiary
bank account number can be entered or changed in
the banking system.

WO 2014/136072 A1

A METHOD OF IMPLEMENTING VERIFICATION FOR A TRANSACTION AND A SYSTEM THEREFOR

BACKGROUND OF INVENTION

The present application relates to a method of implementing verification for a transaction and a system therefor.

On-line transactions, especially on-line financial transaction are fraught with fraud. A common fraud approach is a man in the middle scheme where a fraudster sends a user a fake URL and collects data from the user.

Where the fraudster is able to collude with a Mobile Network Operator back-office official, they are able to redirect any one-time password to a phone that they also control.

They now are able to change a beneficiary bank account number subtly without the user knowing so that the user pays the fraudster instead of the intended beneficiary.

The present invention seeks to address this.

SUMMARY OF INVENTION

According to one example embodiment, a method of implementing a verification for a transaction, the method including:

receiving a request from a user via the internet to upload a beneficiary bank account number;

transmitting a request to the user to enter at least part of the beneficiary bank account number again;

receiving from the user via another communications channel the requested at least part of the beneficiary bank account number;

comparing the received at least part of the beneficiary bank account number with at least a part of the bank account number received via the internet; and

if these match then verifying the transaction so that the beneficiary bank account number can be entered.

The method may also include storing an identity of a mobile communication device of the user, which mobile communication device will be used by the user to transmit the requested at least part of the beneficiary bank account number.

In one example embodiment, the transaction is only verified if the mobile communication device from which the requested at least part of the beneficiary bank account number is received matches the stored identity of the mobile communication device.

The requested at least part of the beneficiary bank account number may be received via USSD from the user.

-3-

According to another example embodiment there provided an electronic system for implementing verification for a transaction, the system including:

a communications module for receiving a request from a user via the internet to upload a beneficiary bank account number, transmitting a request to the user to enter at least part of the beneficiary bank account number again and receiving from the user via another communications channel the requested at least part of the beneficiary bank account number; and

a verification module for comparing the received at least part of the beneficiary bank account number with at least a part of the bank account number received via the internet and if these match then verifying the transaction so that the beneficiary bank account number can be entered.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1   is a block diagram illustrating an example system to implement the methodologies described herein; and

Figure 2   is a block diagram illustrating the server of Figure 1 in more detail.

DESCRIPTION OF EMBODIMENTS

Referring to the accompanying figures, a system and method of implementing verification for a transaction is described.

A user 10 accesses a server 12 of a financial institution, typically a bank, using a computer 14 to transmit and receive data via the Internet.

-4-

The server 12 includes a number of modules and an associated memory 16.

The modules described below may be implemented by a machine-readable medium embodying instructions which, when executed by a machine, cause the machine to perform any of the methods described below.

It will be appreciated that embodiments of the present invention are not limited to such architecture, and could equally well find application in a distributed, or peer-to-peer, architecture system. Thus the modules illustrated could be located on one or more servers operated by one or more institutions.

In any event, the user 10 accesses the server 12 in order to conduct financial transactions using ubiquitous Internet banking services.

During Internet banking, one action a user needs to implement is to specify and upload to the bank a beneficiary's bank account number. Occasionally, if the beneficiary is an existing beneficiary, the user may need to change the beneficiary's bank account number and they will also do this via the Internet banking services.

The methodology and system are aimed at verifying any new beneficiary bank account number or any requested change to a beneficiary bank account number to prevent a fraudster from altering a beneficiary bank account number thereby causing the user 10 to inadvertently pay the fraudster rather than the intended beneficiary.

Thus the server 12 receives a request, typically via a communications module 22, from a user via the internet to upload a beneficiary bank account number.

The request typically includes the beneficiary bank account number that the user 10 wishes to upload. This is stored in the memory 16.

-5-

In response, the communications module 22 transmits a request to the user to enter at least part of the beneficiary bank account number again.

This request could be transmitted to the user in any one of a number of ways. For example, the request could be transmitted back to the user's computer 14 via the Internet.

Alternatively or in addition, the request could be transmitted to a mobile communications device 18 via a mobile communications network 20.

Either way, the user 10 is prompted to enter at least part of the beneficiary bank account number via another communications channel.

In the illustrated embodiment, the other communications channel is the mobile communications network 20 and the user uses the mobile communications device 18 to enter the at least part of the beneficiary bank account number.

In one example embodiment, this is done via a USSD session which can be either user initiated or network initiated.

In either case, the server 12 receives from the user 10 via the other communications channel the requested at least part of the beneficiary bank account number.

A verification module 24 compares the received at least part of the beneficiary bank account number with at least a part of the bank account number uploaded and received via the internet and if these match then verifying the transaction so that the beneficiary bank account number can be entered in the banking system.

-6-

In one example embodiment, the at least part of the beneficiary bank account number is the last four digits of the beneficiary bank account number.

A further layer of security can be added to verify that the mobile communications device 18 from which the at least part of the beneficiary bank account number is received is in fact the mobile communications device of the user 10.

This is accomplished by requiring the user 10 to register the mobile communications device 18.

Data identifying the mobile communication device 18 and/or SIM card inserted into the mobile communication device 18 are stored in the memory 16.

In one example embodiment, when the at least part of the beneficiary bank account number is received from the mobile communication device 18, the IMEI identifying the device and/or IMSI identifying the SIM card are received and compared to the IMEI and/or IMSI stored in the memory 16 and associated with an MSISDN of the device.

In a further layer of security, the user could also be requested to enter a personal identification number via the mobile communications device 18 at the same time that they have entered the at least part of the beneficiary bank account number.

Although use of the USSD protocol has been described above, in an alternate embodiment, an executable application may be downloaded onto the mobile communication device 18.

When the user is prompted to enter the at least part of the beneficiary bank account number, they will execute the application on the mobile communication device 18 and enter the at least part of the beneficiary bank

account number into the application together with a personal identification number where required.

The application will now transfer this data back to the server 12 but in this embodiment this will typically not be via the USSD protocol.

in any event, it will be appreciated that in order to upload beneficiary bank account information, verification is required without which the beneficiary bank account information will not be accepted.

This, together with authentication of the mobile communication device, provides a comprehensive security mechanism to defeat fraudsters.

CLAIMS:

1. A method of verification of a transaction, the method including:

   receiving a request from a user via the internet to upload a beneficiary bank account number;

   transmitting a request to the user to enter at least part of the beneficiary bank account number again;

   receiving from the user via another communications channel different to the internet, the requested at least part of the beneficiary bank account number;

   comparing the received at least part of the beneficiary bank account number with at least a part of the bank account number received via the internet; and

   if these match then verifying the transaction so that the beneficiary bank account number can be entered.

2. A method according to claim 1 wherein the method also includes storing an identity of a mobile communication device of the user, which mobile communication device will be used by the user to transmit the requested at least part of the beneficiary bank account number.

3. A method according to claim 2 wherein the transaction is only verified if the mobile communication device from which the requested at least part of the beneficiary bank account number is received matches the stored identity of the mobile communication device.

4. A method according to claim 3 wherein the identity of the mobile communication device stored is an IMEI number identifying the mobile

communication device and/or an IMSI number identifying a SIM card used in the mobile communication device.

5. A method according to claim 2 wherein the other communications channel via which the requested at least part of the beneficiary bank account number is received from the user is a mobile communications network.

6. A method according to claim 5 wherein the requested at least part of the beneficiary bank account number is received via a USSD session from the user.

7. A method according to claim 1 wherein the request to the user to enter at least part of the beneficiary bank account number again is transmitted via one or more of the Internet and a mobile communications network.

8. An electronic system for verification of a transaction, the system including:

   a communications module for receiving a request from a user via the internet to upload a beneficiary bank account number, transmitting a request to the user to enter at least part of the beneficiary bank account number again and receiving from the user via another communications channel different to the internet the requested at least part of the beneficiary bank account number; and

   a verification module for comparing the received at least part of the beneficiary bank account number with at least a part of the bank account number received via the internet and if these match then verifying the transaction so that the beneficiary bank account number can be entered.

9. A system according to claim 8 further including a memory for storing an identity of a mobile communication device of the user, which mobile communication device will be used by the user to transmit the requested at least part of the beneficiary bank account number.

10. A system according to claim 9 wherein the verification module only verifies the transaction if the mobile communication device from which the requested at least part of the beneficiary bank account number is received matches the stored identity of the mobile communication device.

11. A system according to claim 10 wherein the identity of the mobile communication device stored is an IMEI number identifying the mobile communication device and/or an IMSI number identifying a SIM card used in the mobile communication device.

12. A system according to claim 8 wherein the other communications channel via which the requested at least part of the beneficiary bank account number is received from the user Is a mobile communications network.

13. A system according to claim 12 wherein the requested at least part of the beneficiary bank account number is received via a USSD session from the user.

14. A system according to claim 13 wherein the request to the user to enter at least part of the beneficiary bank account number again is transmitted via one or more of the Internet and a mobile communications network.
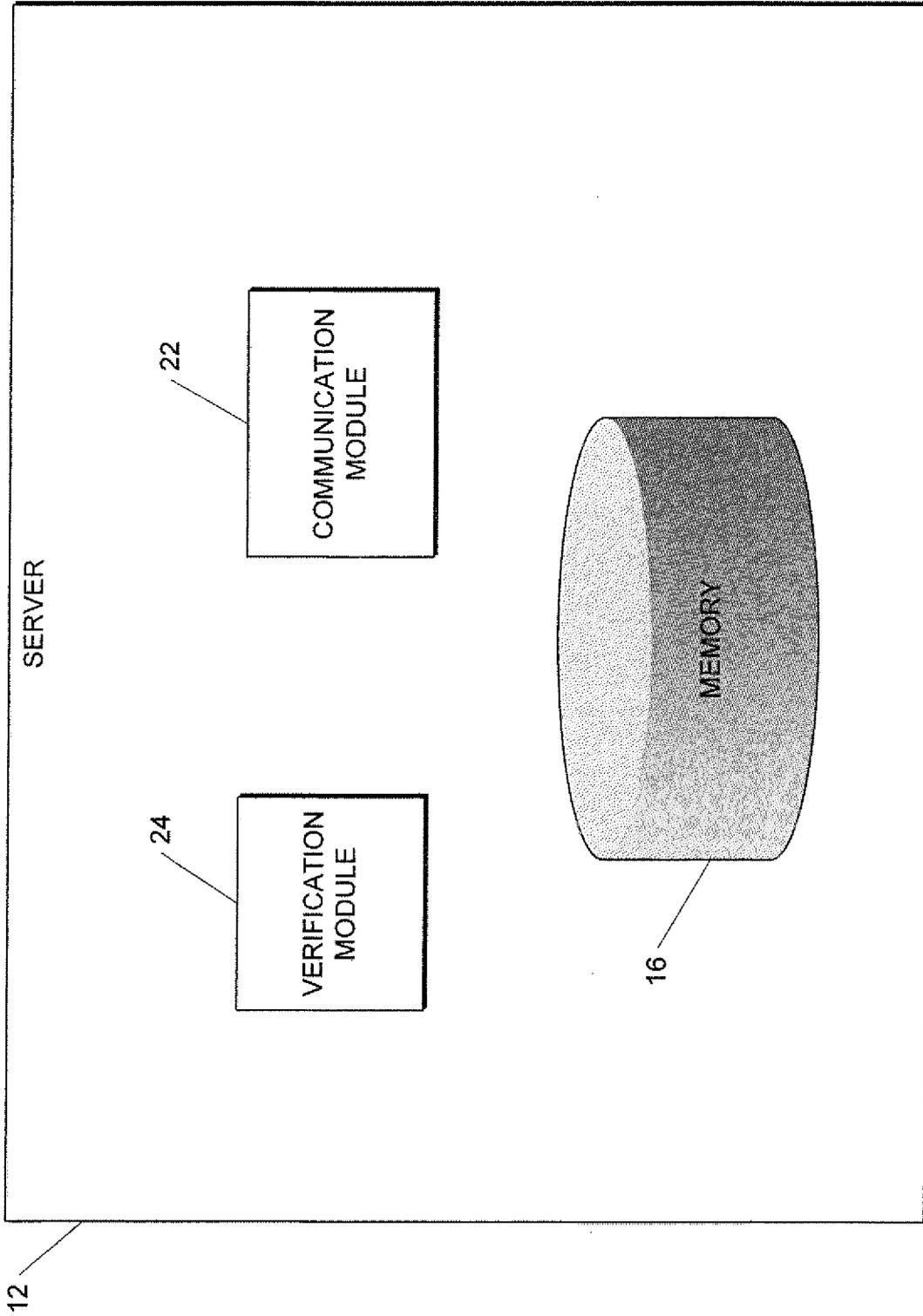
FIGURE 1
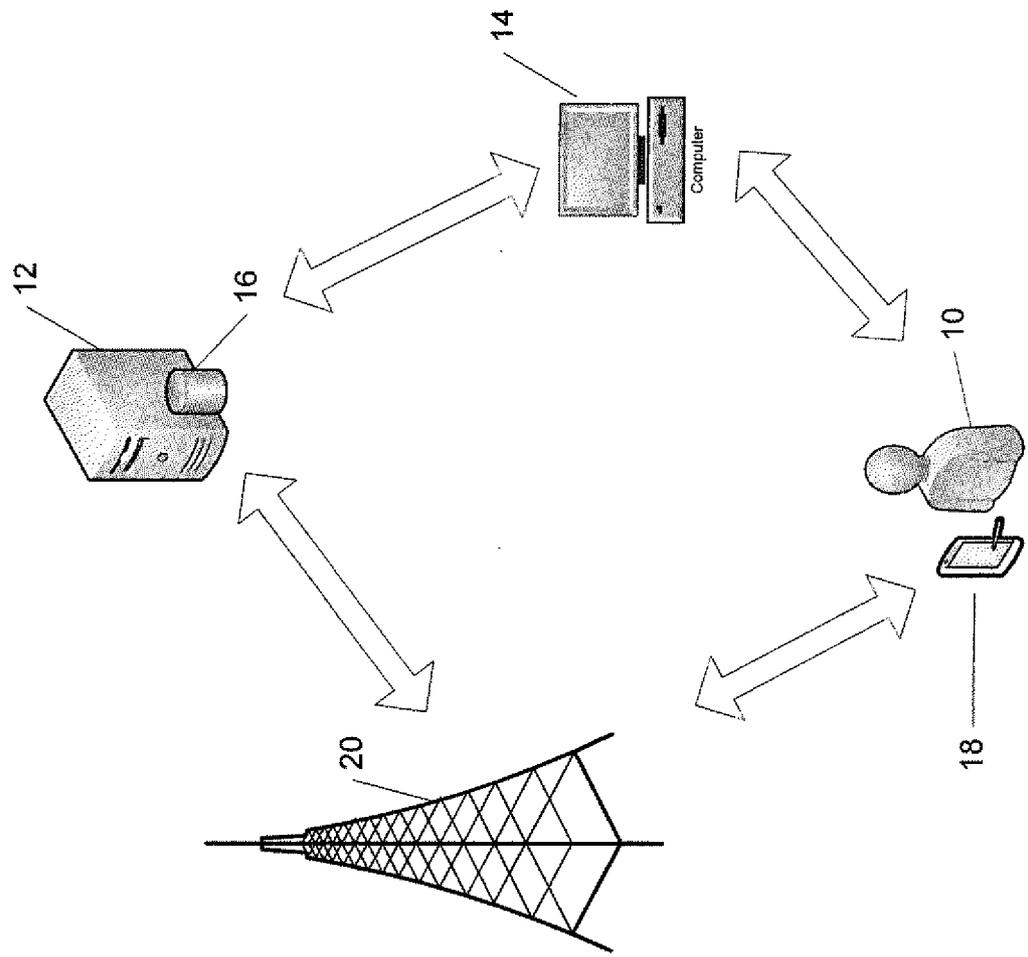
SERVER

12

24

VERIFICATION
MODULE

22

COMMUNICATION
MODULE

MEMORY

16

FIGURE 2

A. CLASSIFICATION OF SUBJECT MATTER

IPC(8) - G06Q 40/00 (2014.01)
USPC - 705/39

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)
IPC(8): G06Q 40/00 (2014.01)
USPC: 705/39

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
IPC(8): G06Q 40/00 (2014.01)
USPC: 705/1 .1, 35, 39, 44, 50, 64, 75; 726/2 (keyword limited; terms below)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
PatBase; Google(Web); Search terms used: verification transaction bank account number change upload new beneficiary recipient payee friend family reenter confirm again enter mobile cellular phone device IMEI IMSI USSD sequence series

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2013/0013501 A1 (Rackley, III et al.) 10 January 2013 (10.01 .2013), entire document especially para [0170]-[0176], [0187], [0199], [0205], [0206], [0254], [0264], [0278], [0279], [0365], [0377]-[0381], [0390], [0407], [0413], [0438], [0475], [0487], [0483], [0489]-[0492]	1-14
Y	US 2006/0190374 A1 (Sher) 24 August 2006 (24.08.2006), abstract; para [0003], [0048], [0174], [0177], [0251]	1-14
Y	US 201 2/0303534 A1 (Keller et al.) 29 November 2012 (29.1 1.2012), para [0017], [0019], [0024], [0025], [0029]	4, 6, 11, 13, 14

☐ Further documents are listed in the continuation of Box C.

* 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

15 May 2014 (15.05.2014)

Date of mailing of the international search report

1 8 JUN 2014

Name and mailing address of the ISA/US
Mail Stop PCT, Attn: ISA/US, Commissioner for Patents
P.O. Box 1450, Alexandria, Virginia 22313-1450
Facsimile No. 571-273-3201

Authorized officer:
Lee W. Young

PCT Helpdesk: 371-272-4300
PCT OSP: 571-272-7774