(12) UK Patent Application (19) GB (11) 2459850 (13) A

(43) Date of A Publication 11.11.2009

(21) Application No: 0808204.2

(22) Date of Filing: 07.05.2008

(71) Applicant(s):
Keith Hall
Islay View, 236 Wharf Road, EALAND,
North Lincolnshire, DN17 4JN, United Kingdom

(72) Inventor(s):
Keith Hall

(74) Agent and/or Address for Service:
Keith Hall
Islay View, 236 Wharf Road, EALAND,
North Lincolnshire, DN17 4JN, United Kingdom

(51) INT CL:
G06Q 2/00 (2006.01) ***G07F 7/10*** (2006.01)

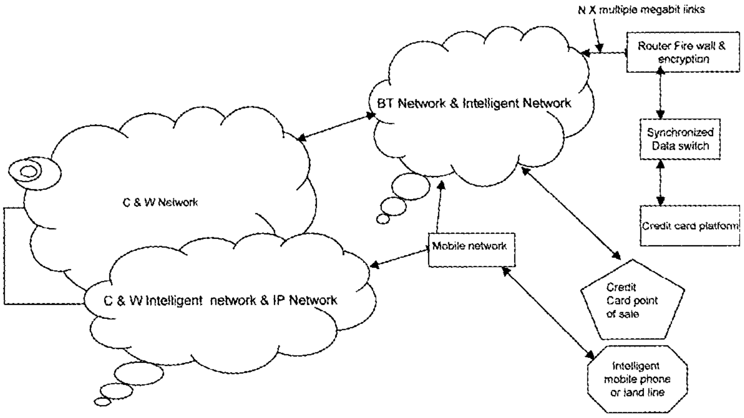
(56) Documents Cited:
GB 2378294 A **WO 2006/024080 A**
WO 2005/015452 A **US 20070244813 A**

(58) Field of Search:
UK CL (Edition X) **G4V**
INT CL **G06Q**
Other: **Online: WPI, EPODOC**

(54) Abstract Title: **Using a mobile phone for fraud prevention in credit card transactions**

(57) A fraud prevention system utilizes a intelligent mobile phone and the mobile network to communicate with the credit card provider. It has the ability of down loading, via text, credit card transaction information and for the credit card user has the ability to switch on or off credit card transactions. The credit card user will also have the ability to set credit card transaction limits from a mobile or land line phone. The intelligent phone has software or possible chip and pin hardware and software that is synchronized and compatible with the credit card that is registered to the mobile or land line phone. After registration and network set up, the credit card user determines the maximum credit card transaction for that period in time. This is achieved by communicating to the credit card provider via the intelligent mobile phone and encrypted text messaging. The credit card user can bar or allow transactions via the mobile or land line phone.

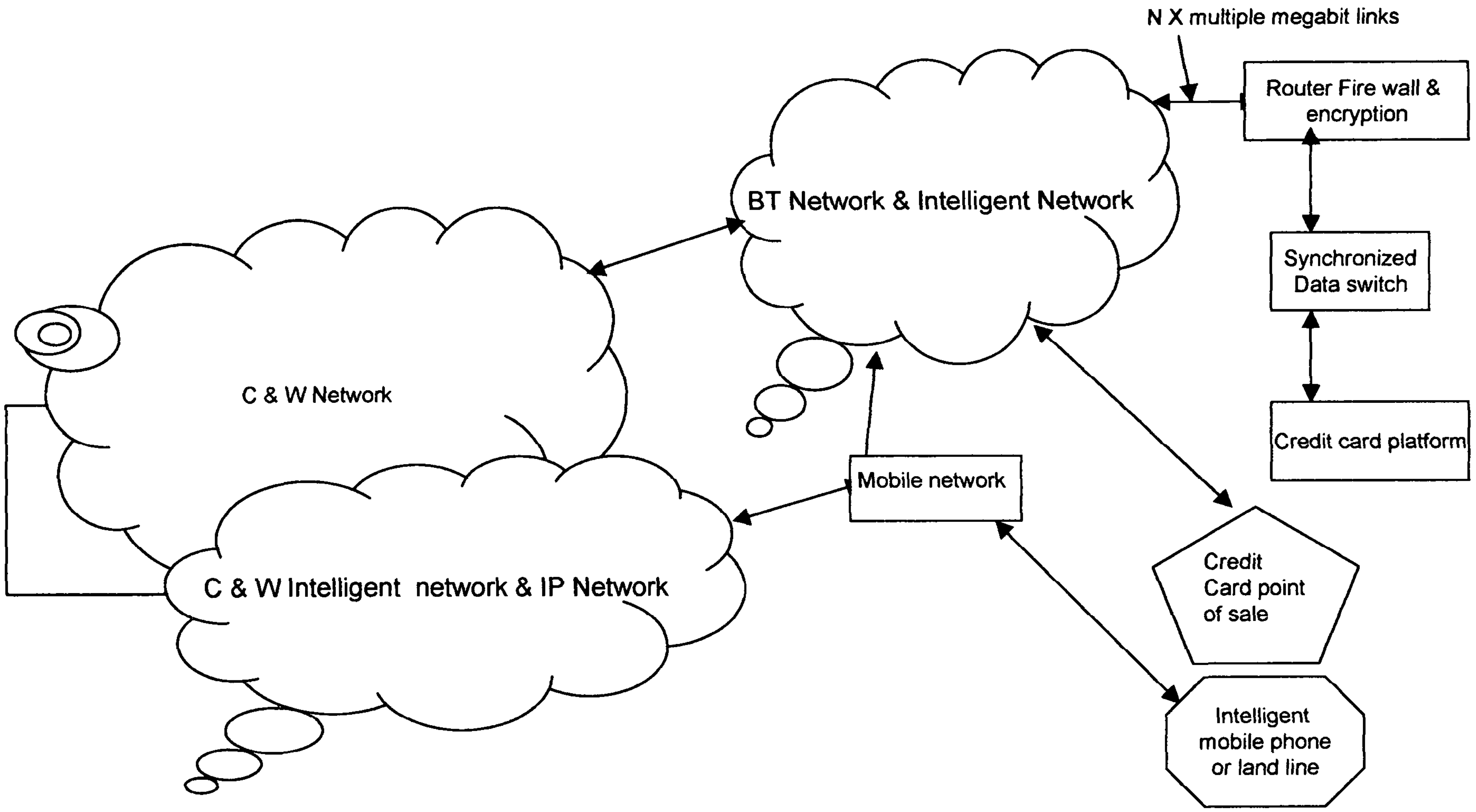
Network design


N X multiple megabit links
Router Fire wall & encryption
BT Network & Intelligent Network
Synchronized Data switch
C & W Network
Credit card platform
Mobile network
C & W Intelligent network & IP Network
Credit Card point of sale
Intelligent mobile phone or land line

Credit Card Fraud Protection Network

Digital networking

Network design


N X multiple megabit links
Router Fire wall & encryption
BT Network & Intelligent Network
Synchronized Data switch
Credit card platform
C & W Network
Mobile network
C & W Intelligent network & IP Network
Credit Card point of sale
Intelligent mobile phone or land line

Objective

To provide a fraud prevention system utilizing an intelligent mobile phone and the mobile network to communicate with the credit card provider. Thus being able to down load via text, credit card transaction information and the ability to switch on or off the authorized credit card holders account. Also the ability to set credit card transaction limits by the authorized credit card user.

Goals

To be able to offer this facility to all credit card networks giving them the ability to reduce credit card fraud. The intelligent phone will be able to interact with the credit card provider via the telecommunication and data infrastructure that already exists.

Solution

The intelligent phone will have software or possible chip and pin software that is compatible with the credit card that is registered to the mobile phone. After registration and network set up, the credit card user determines the maximum credit card transaction for that period in time, this is achieved by communicating to the credit card provider via the intelligent mobile phone and encrypted text messaging. The credit card user can bar or allow transactions via the mobile phone.

Once this has been engaged the credit card user will be able to make or deny transactions. The transaction is delivered to the credit card provider in the normal way via the telecoms and data network. The user can choose to be text on all transactions or limit the information of the transactions keeping the authorized credit card holder aware of the credit card usage. In the event that the credit card holder's details have been fraudulently used, a number of events will happen. Different transaction settings could be invoked by the authorized credit card holder. The list is not exhaustive but for instance, turn the account on or off, set maximum transaction limits, set notification of all transactions, or set notification of any transaction over the maximum allowed.

1. If the authorized credit card holder has barred transactions they will receive a notification via the intelligent phone that their credit card has been used to make a transaction but has been refused. If the transaction was undertaken by the valid credit card holder they will have a time out period to validate the transaction. If this is not conducted within the time out period the card will be barred by the credit card provider. The authorized credit card holder will then have to inform the credit card company and a new card issued.

2. If the authorized credit card holder has set a transaction limit for their credit card and the credit card is used in excess of that limit, the transaction will be refused. The authorized credit card holder will be notified of the transaction via the intelligent mobile phone. A time out period could be engaged to prevent further fraudulent use.

3. In the event that the credit card has been used by a fraudulent user whilst the authorized credit card holder has authorized the credit card to make transactions, with all transaction notification set on the account. The transaction

notification will be text to the authorized credit card holder giving them the ability to stop that transaction and further transaction from occurring. This would prevent fraud at the earliest opportunity.

4. The authorized credit card holder will have the ability to bar or allow transactions at any time on their account, thus stopping the credit card being used when a bar on the account is in place. Notifying the authorized credit card holder if transaction levels are exceeded or the credit card has been used. The combination of an intelligent mobile phone or land line utilizing dynamic networking linked to a credit card network providers platform would reduce credit card fraud dramatically.

5. The mobile phone could take a number of forms but the basic concept is the ability to text from a phone to alter features on a credit card account. This could be in the form of a chip within the phone or software similar to the iphone or blackberry. Networking synchronization with the mobile phone or land line will be established when communicating with the credit card provider. This could be achieved in a number of ways, one being via the chip and pin within the phone, which could change every 30 seconds via synchronized numbering schemes, thus limiting network tapping within that 30 second time period. Once network synchronization with the mobile phone or land line user has been established pre set registration details will come into force authorizing transaction information to pass between the mobile phone user and the credit card company, utilizing chip & pin type technology. The mobile phone data is encrypted before transmission and then synchronized with the credit card providers platform before transaction information is allowed to be communicated between the authorized credit card holder and the credit card provider. This allows better security between the credit card operator and authorized credit card holder.

6. The credit card point of sale could also be utilized for validation purposes of the chip and pin within the mobile phone and for transaction barring and unbarring.

7. If chip and pin technology is not utilized within the mobile phone or land line then simple text messaging communicating with the credit card platform could be used.

8. The use of synchronized data between the two platforms or end users would reduce fraud hacking to a minimum, a number of synchronizing product platforms could be intergraded between mobile network providers and the credit card providers data servers.

Ideal solution

The ideal solution is a complete network package offering a mobile phone with a credit card facility that utilizes a single network provider. The network provider that combines these two products could be the fore runner of reducing credit card fraud globally.

The Ideal solution can be achieved.

S L Hall Consultants has researched over the last four years networking solutions and mobile products that could provide the ultimate credit card fraud prevention system, which would offer a complete credit card fraud management system.

Telecom network providers provide a number of networks one being the PSTN (Public Switched Telephone Network). This network is normally the first connection point of all services. The data path for the credit card transactions start on this network. Data calls travel along designated routes these being; PSTN dial up routes, leased line data routes, IP data network routes which utilize the telecom providers intelligent networks.

This unique offering combines all of the existing network systems but synchronizes these networks to allow limited credit card data to transit the mobile network from a credit card providers data switch.

The transaction from the credit card is carried out in the normal way using chip and pin. The data is then sent to the credit card company across a number of networks and network providers interconnect points in the normal way. Once the data is received by the credit card companies data switch, a flag is set on the credit card holder account notifying the data switch that parameters have been set. These parameters could be varied and proprietary. This data is then sent to another secure data switch which has the ability to send text or real time data information to the telecommunication providers network this could be PSTN or a mobile network.

An intelligent mobile phone or PSTN phone utilizing chip and pin technology could then be synchronized with the the data from the credit card company. Transaction information or transaction barring could then be relayed between the two points. Real time data synchronization could be used. The mobile phone at the point of sale could be synchronized with the credit card being registered or the credit card companies security platform, a random number sequence changing every 30 seconds which would be unique to the data platform being used. Once authentication has occurred a number of actions could then be allowed which may be dependent on a number of factors, type of account and credit limits set, credit card holder defined limits invoked, the list could be endless.

If chip and pin were not used in the mobile phone, data sequencing could still be achieved utilizing calling line ID, mobile phone number verification, or simple pin number identification which had been sent in the post. All of these methods have differing degrees of network security and cost.

A mobile phone company offering an intelligent phone with credit card secure encryption linked up with a proprietary credit card data switch and network security, would be able to offer a unique global product.

CLAIM

1. The Credit Card Fraud system is the first attempt at utilizing a number of data and telecommunication networking features to deliver a one stop solution to tackle credit card fraud.

2. The network design and the use of intelligent technology in a mobile or fixed land line phone communicating with the users credit card platform is unique.

3. The use of intelligent information being utilized in a mobile or land line phone to interact with a credit card platform is unique.

4. The ability to be able to turn on and off a credit card utilizing mobile or land line telephony via a secure and synchronization network is unique.

5. The use of credit card chip and pin hardware or intelligent software in a mobile or land line phone is unique.

6. Secure Data synchronization across a mobile telecommunication platform communicating with a credit card companies credit card platform for the purpose of allowing the credit card users to control credit card transactions is unique.

7. Providing a design concept to link a credit card platform to a mobile telecommunication platform for credit card fraud prevention has not yet been achieved. Thus, being able to have the ability of down loading via text, credit card

Application No:	GB0808204.2	**Examiner:**	Tom Sutherland
Claims searched:	1	**Date of search:**	16 October 2008

Patents Act 1977: Search Report under Section 17

Documents considered to be relevant:

Category	Relevant to claims	Identity of document and passage or figure of particular relevance
X	1 - 7	WO 2006/024080 A (MARKETS-ALERT PTY LTD) Whole document relevant. Note page 7 line 22 to page 8 line 7 and page 8 line 30 onwards.
X	1 - 7	WO 2005/015452 A (PAYCOOL INTERNATIONAL LTD) See page 3 first paragraph.
A	-	GB 2378294 A (HALTFERN LTD)
A	-	US 2007/0244813 A (ZHOU) Note the Figures.

Categories:

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

Field of Search:

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC^{X} :

G4V

Worldwide search of patent documents classified in the following areas of the IPC

G06Q

The following online and other databases have been used in the preparation of this search report

WPI, EPODOC

International Classification:

Subclass	Subgroup	Valid From
G06Q	0020/00	01/01/2006
G07F	0007/10	01/01/2006