Comments on TRAI's Consultation Paper on Issues arising out of Provisioning and Delivery of Basic Financial Services using Mobile Phones in the context of Pricing of Services by Mobile Service Providers

Dated 25th January, 2011

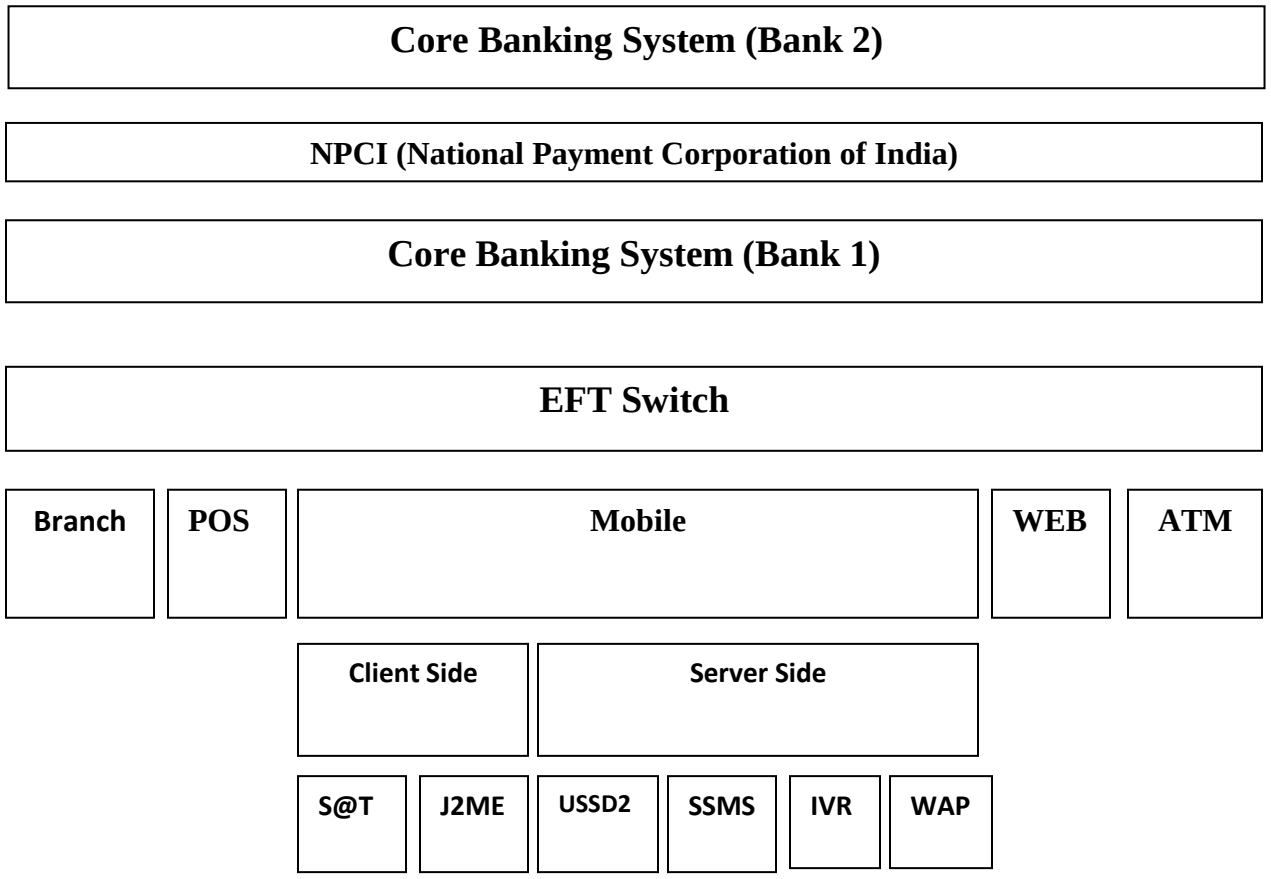
Rekha Jain
Executive Chair, IIMA-Idea Telecom Centre of Excellence
IIM, Ahmedabad

With research support from
Nikita Khubchandani
Business Research Associate
IIMA-Idea Telecom Centre of Excellence
IIM, Ahmedabad

There are many channels through which a bank delivers its services such as Branch, ATM, Internet and POS. Mobile is another channel which extends the existing infrastructure of the bank for delivering the services of the bank and increasing its reach to the potential and existing customers.

It has a prospect of adding convenience for accessing banking and payment services to existing banked customers. The addition of a new channel brings new **operational risks** to providers. Operational risk is defined as the risk of loss arising from the failure of operational procedures.

Let us understand first how the mobile technologies are related to the Banking systems:



A bank's core banking system, the system that houses the consumer's account and related transaction management and history, would require a means to translate banking instructions,

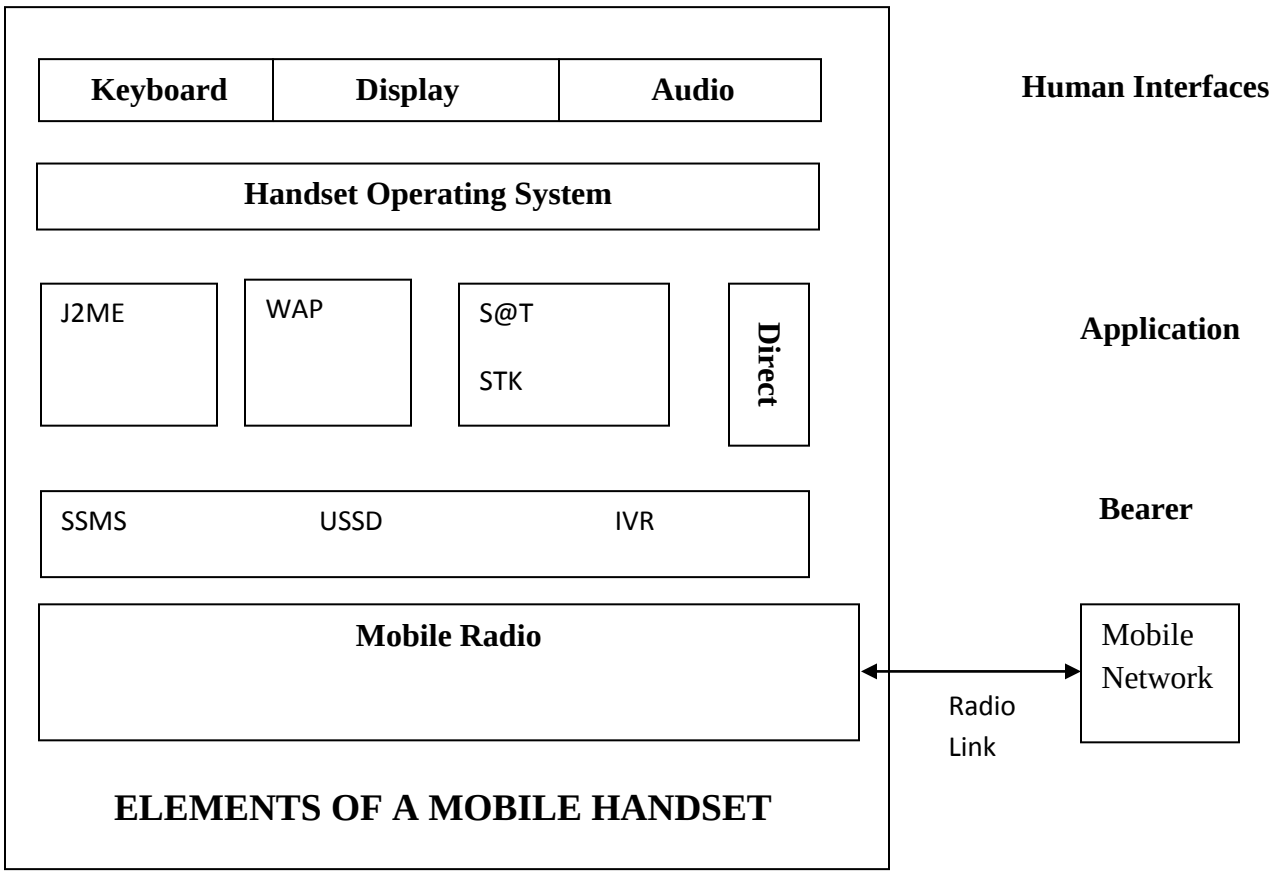
received from consumers, through one of the bank channels such as ATMs or the internet, into a format that the core banking system can process. This translation is normally performed by an EFT channel switch. The EFT channel switch would switch transactions from the channel to the appropriate area within the core banking system. An Electronic Funds Transfer, EFT, or Financial Switch accepts, translates and forwards transactions from multiple channels to the bank's core systems. This can sit within the bank or the bank's third party processor.

Client-side applications are applications that reside on the consumers SIM card or on their actual mobile phone device. Client-side technologies include J2ME and S@T.

Server-side applications are developed on a server away from the consumer mobile phone or SIM card. Server-side technologies include USSD2, IVR, SSMS and WAP.

When we talk about various mobile banking technologies, its firstly important to understand the elements of a mobile channel. There are two elements of a mobile channel:

- The Mobile Device itself
- The communications channels offered by mobile network operators.



There are human interfaces of a mobile phone such as Keyboard, Display and Audio. The operating system ties all the elements of the handset together. Mobile radio communicates to the mobile network and has the capability to send SMS, USSD, voice data over the radio interface.

The mobile network comprises the components which carry a data message to and from the handset to the MSP.

This is a brief framework of the technologies surrounding Mobile Banking.

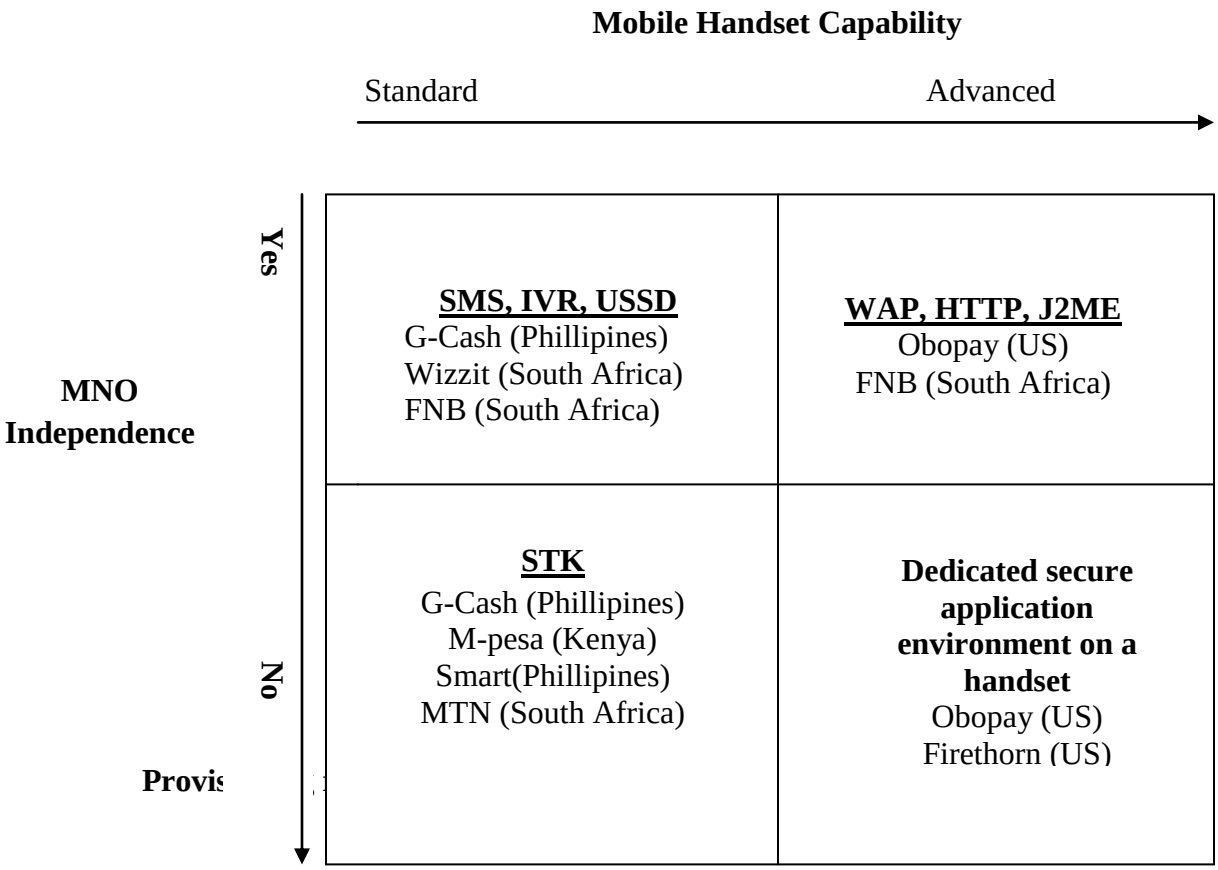
Issue 1:

The customer would approach a Business Correspondent or its agent for opening of a non-frills account. Would there be any provisioning requirements at the service provider's end in any of the methods/options listed under para 2.9?

Response:

Every technology mentioned above both in the client side as well as on the server side has its advantages and disadvantages. As we talk about the rural markets it is very important to consider the characteristics of that market and select a technology that caters to its needs effectively and the basic financial services are delivered upto the last mile.

Various technology options can be placed in a matrix depending upon the capability of the mobile handset and the dependency upon MNO.



Technologies Used	Handset Provisioning	Sim provisioning
IVR	None	Not applicable
SMS	None	Not applicable
USSD2	None	Not applicable
STK/S@T	None	At personalization or by download
WAP	Setup download and/or manual settings of GPRS and WAP server address.	Not applicable
HTTPS	Setup download and/or manual settings of GPRS	Not applicable
J2ME	Setup download and/or manual settings of GPRS and application download	Not applicable

As stated above, the provisioning requirements for SMS, IVR, USSD and STK are none for the service providers as the existing handsets have these technologies inbuilt and people are familiar with them. USSD may not be available on all standard handsets and in case of STK the service provider has to install the application on a sim card and the customer needs to change his/her sim card in order to take benefit of mobile banking in a completely secured manner.

While the other three technologies, namely, WAP, HTTPS and J2ME, require skills sets on the customers side as to how to set up a download and operate a WAP browser or GPRS. These technologies require an advanced mobile handset and hence these technologies cannot be targeted at the entire population. 65% of the population has mobile phones, out of 30% have bank accounts. Of these financially included, only 30% have smart phones which support these technologies. They anyway have access to banking facilities in some or the other way. It can be through a branch or ATM. However, only around 65% of the top 30% is using the modern banking technologies such as internet banking, ATMs, etc. The issue here is how to target the unbanked rural population large numbers of who may not be able to afford high end handsets.

This population mostly carries standard handsets which only support the SMS, IVR, USSD (in most cases) and STK applications. These are easier to use and convenient to use for the customers. The standard handsets do not provide facilities to secure or encrypt data before sending it to server based applications at MSP and do not have the ability to run programs on the handset. This is a compromise on the security part but as is mentioned in the second response we may see that if proper security levels are built at various stages then it would be difficult to for a mobile hacker to get into the channel communication and access the confidential information of the customer.

Issue two:

Please correlate and comment on the recommended compensation for mobile service providers reproduced under para 2.3, with various options for carrying messages for financial services as described in para 2.9.

Response:

The IMG report mentions many assumptions for the Capex and Opex of the REMIT switch, Account Mapper and INFAST.

With these assumptions IITCOE would not like to comment on the costs for the above mentioned entities.

However we would like to mention the initial current charges associated with various technologies that are used for mobile banking.

Channel Technology	Approximate cost
IVR	As per regular tariff.
SSMS	**Rs. 3-Rs.6.** Average transaction would require two SMS from the consumer and two returned from the bank. The bank would pay for it at a negotiated bulk rate. Total Consumer bearer cost per transaction would be Rs. 6 to Rs 12 and for the bank Rs. 2.5.
USSD2	A single session lasts about 40 seconds for the transaction to get completed. Charges to the customer per transaction : **Rs 3**
J2ME	Initial download charges would apply. Approximately Rs 10-Rs 15. Per transaction cost would be approximately Rs. 0.50 to Rs. 2. Also GPRS rates would apply.
WAP	No download required. Per transaction cost would be approximately Rs. 0.50 to Rs. 2. Also GPRS rates would apply.
STK	The customers are required to change their sim card. The cost for the sim card. Rs. 30 – Rs. 50 (as it has the application built into it) Also initial download is required with SMS facility. These SMS are free for the customers but are chargeable for the bank. The bank pays it at a bulk rate. Approximately Rs. 2 per sms. There may be a max cap as well.

Issue three:

There may be requirements of prioritization and encryption of the messages exchanged for financial transactions. In your opinion what effect would these have on the provisioning and pricing of services?

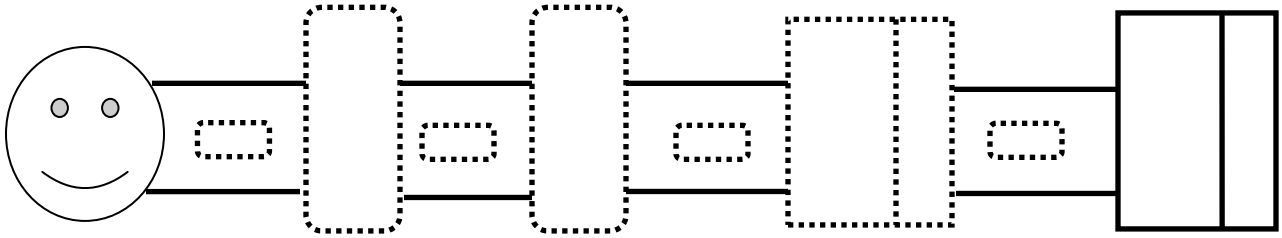
GSM security is as strong, and if not stronger, than that of traditional fixed line communications. It would take money, time and effort to be able to actually penetrate the GSM network, steal data, and then use it fraudulently. Moreover, if this were probable in Mobile Banking, the fraudster would still only be able to access a limited amount of funds from a consumers account for the reasons given below.

The fraudster would have to know where the customer would be at the time of the call, and also know the customer's mobile number, and be able to travel as fast as the call is travelling from one base station to the next. On top of the mobility challenge, the fraudster would then still need to decipher the GSM encryption, and find a way to identify the particular mobile communication, considering that the customer identification as a GSM consumer is kept hidden for privacy purposes.

If one assumes that the fraudster was able to do achieve all of the above, they would then be subjected to the relevant velocity checks and transaction limits levied by the bank or their platform provider. It therefore seems not feasible for a fraudster to expend his money and energies on attempting to break the communication layer. But it may still not be sufficient for banking in that it only provides unencrypted data through an encrypted channel.

Let's have a look at how the information is carried across through various channels.

SMS Banking Data Security:



Customer **Base Station 1** **Base Station 2** **Mobile Operator** **Bank**

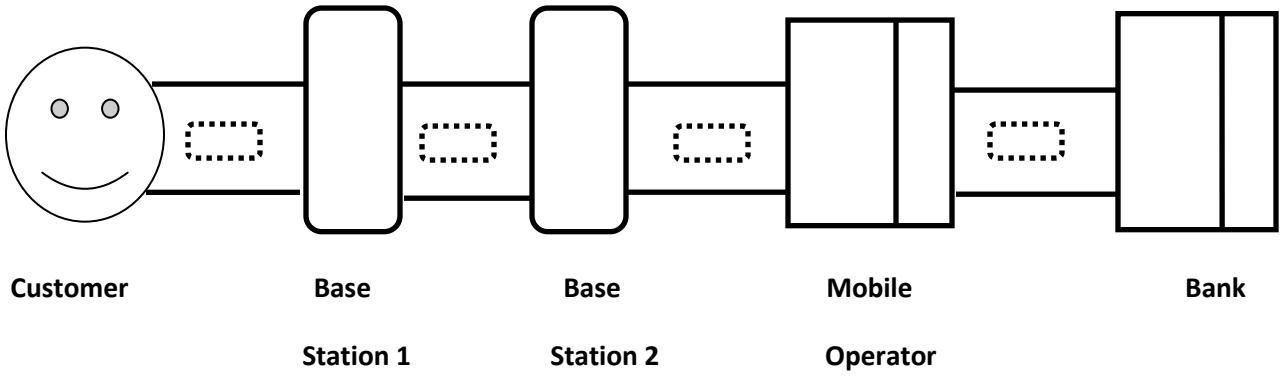
The customer initiates a transaction by sending an sms from his mobile phone. This sms is automatically stored on the handset of the customer and anyone can see it. This is viewed to be the least secure of all technologies.

The flow of information through the SMS channel is not encrypted when the information flows from the customer's handsets to the bank. There are three levels where the information is insecure. At the MNO level too data is stored in an unencrypted manner. But the transactions which occur are over an encrypted line of communication which is protected by standard GSM security protocols. The subscriber identity is also protected. So there is a security present at that level. This would make it difficult for anyone to get into the channel of communication, however, the unencrypted data is at risk. At the bank the data remains secured.

Note: Unencrypted data .....

Encrypted data ———

IVR, USSD2 Banking Data Security:



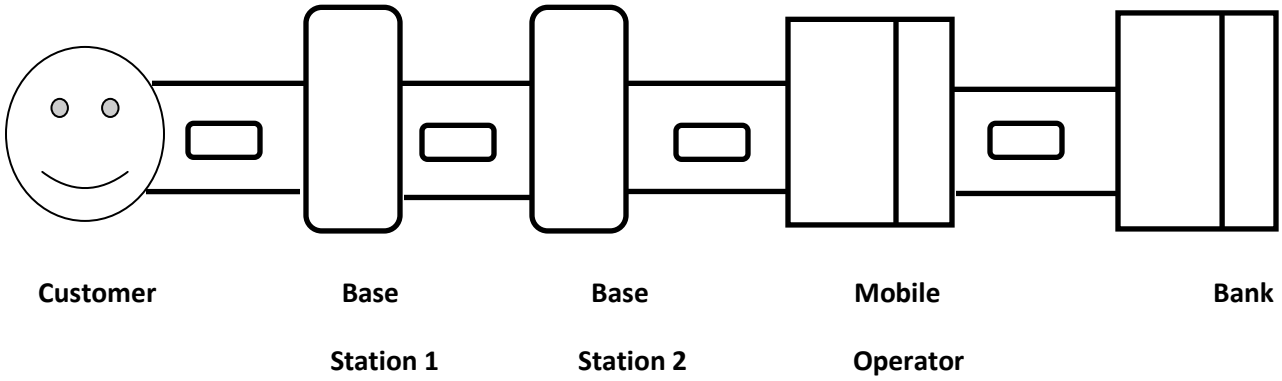
IVR is more secured as compared to SMS because it is a voice call and is protected by the communication layer. It goes directly to the banks IVR and is same.

In USSD too, there is a single session in which data is exchanged between the customer and the MNO. The only way in which is different from sms that in sms the data gets stored and here the data is stored and the communication is not broken into different pieces.

Therefore the only risk in the data that is carried which in unencrypted because the communication layer is secured.

The data carried across these channels is stored on a bank server and not on the handset. This data is encrypted. The threat remains when the handset and and sim along with authentication pins are stolen.

J2ME, WAP and STK banking data security:



With J2ME the data is encrypted the moment it leaves the handset because it has security around the handset nad is sent across the GPRS channel. The data travels encrypted and can be decrypted only at the bank. Customers have to careful whicle downloading the application, that it is downloaded from a genuine source.

WAP is just similar to the internet browser the difference being it is used for mobile internet and hence is faces the same threats as internet banking faces. However it is more secure than internet because the WAP allows for a GPRS session to be opened between the handset web browser and the web application at the bank. The data travels through an encrypted communication layer.

STK is the most secure method of mobile banking. It allows the bank to load its own encryption keys onto the SIM card with the bank's own developed application. Thus the consumer's data can be stored on the SIM Card and the consumer can be authenticated on the handset prior to having to carry any data across the mobile network. The data is also encrypted prior to leaving the handset and only decrypted using the banks encryption keys within the bank.

All these technologies have a different provisioning requirement and pricing structure. The mobile technology providers have to be aware of the above mentioned risks while implementing a particular kind of technology. The pricing also would differ in case of different technologies.

Issue 4: Whether tariff for telecom services for providing basic financial services using mobile phone should be under forbearance or should be brought under regulation? If they should be regulated, whether a ceiling should be prescribed TRAI? Please explain your answer/suggestions.

Response:

The tariff for telecom services for providing basic financial services for Financial Inclusion using mobile phones should be regulated by TRAI as such people may avoid the transactions because of high charges. Rs. 3 to Rs. 5 may be sufficient enough to prevent the poor away from not using mobile banking services. Hence, we recommend that tariffs arrived at in Issue 3 should be borne by banks and some facility such as prepaid instruments should be given to the unbanked by the banks so as to induce amongst them mobile banking. The banks should be compensated for this from funds like USOF of other financial inclusion funds from the government.

This should be regulated until there is competition. To estimate costs, appropriate cost models need to be developed and reviewed frequently in collaboration with the service providers.

Issue 5: Any other comments relating to provisioning and pricing of mobile services for financial transactions.

Response:

Once the accounts are opened for the financially excluded, MMID (Mobile Money identification) can also help in promoting mobile banking. This is currently in use by only 7 banks. RBI should make some effort in promoting it. This is a very simple and easy way to transfer money to some other account. The best thing is money gets transferred on a real time basis. Also there is no need to share the account information. The remitter just needs to know the beneficiaries mobile number and the MMID. Mobile banking is the most cost effective channel amongst all the banking channels namely branch, ATM, Internet, POS etc. As the traditional 'brick and mortar' branches can penetrate into remote areas of our vast country only to a limited extent, this model presents banks with a workable option to provide banking services in hitherto inaccessible areas in a cost-effective manner. The increasing penetration of mobile phones and the increasing incomes of the Indian customers will prove to be complementary in achieving the financial inclusion.