Branchless Banking Regulations

for Financial Institutions Desirous to undertake Branchless Banking

Banking Policy & Regulations Department
State Bank of Pakistan
March 31, 2008

The Branchless Banking Team	
Syed Irfan Ali	Syed.Irfan@sbp.org.pk
Sabah uz Zaman	Sabah.Zaman@sbp.org.pk
Qasim Nawaz	Qasim.Nawaz@sbp.org.pk
Muhammad Javaid Ismail	Javaid.Ismail@sbp.org.pk
Muhammad Akhtar Javed	akhtar.javed@sbp.org.pk
Sajid Mahmud	Sajid.Mahmud@sbp.org.pk
Rajesh Raheja	Rajesh.Raheja@sbp.org.pk
Usman Shafiq	usman.shafiq@sbp.org.pk

Table of Contents

1 Introduction

1.1 Background

Branchless Banking (*BB*) represents a significantly cheaper alternative to conventional branch-based banking that allows financial institutions and other commercial players to offer financial services outside traditional bank premises by using delivery channels like retail agents, mobile phone etc. ***BB*** can be used to substantially increase the financial services outreach to the un-banked communities. Provision of enabling regulatory environment by careful risk-reward balancing is necessary to use such models. In line with its responsibility to promote financial inclusion without risking the safety and soundness of banking system, SBP issued a policy paper on regulatory framework for branchless banking in Pakistan which clearly stipulated SBP's strategy for promoting branchless banking in Pakistan. These regulations are being issued as part of the broader strategy to create enabling regulatory environment to promote Bank-led Model of branchless banking. These regulations are applicable to financial institutions (Commercial Banks, Islamic Banks and Microfinance Banks) desirous to undertake branchless banking. However, as financial institutions cannot take on ***BB*** without the help of other market players like telecom companies, technology service providers, agents etc., knowledge of these regulations is also helpful for other parties to understand their roles and responsibilities.

1.2 Objectives

The objectives of these 'Branchless Banking Regulations' are

- To define Branchless Banking activities as a new delivery channel to offer banking services in a cost effective manner.
- To broadly outline activities which constitute ***BB*** and to provide a framework for offering BB services.
- To serve as a set of minimum standards of data & network security, customer protection and risk management to be followed by the Banks desirous to offer mobile banking services.

1.3 Scope

- These regulations are applicable to commercial banks, Islamic banks and microfinance banks (MFBs) (herein after collectively referred to as financial institutions or FIs).
- Activities outlined in these regulations as branchless banking cannot be offered by any person or institution other than FIs.
- All FIs desirous to offer branchless banking services may do so in line with these regulations.
- These regulations do not, in general, supersede or revoke any of the existing rules & regulations unless specifically stated. Further the scope of any such relaxation of rules and regulations will be limited to Branchless banking only and shall not extend to cover any other banking activity.

- The regulations do not cover issuance or handling of e-money for which there exist a separate law (Payment System & Electronic Fund Transfer Act 2007).

2 Definitions

"Authorized Financial Institutions" means financial institutions authorized by State Bank to undertake branchless banking activities.

"Bank" means a banking company as defined in the Banking Companies Ordinance, 1962.

"Branchless Banking" or "*BB*" means conduct of banking activities as outlined in these regulations by Authorized Financial Institutions for customers having a branchless banking account. It does not include the information services already being provided by various FI's to their existing customers using channels like, phone, internet, SMS etc;

"Branchless Banking account" or "*BB* Account" means an account maintained by a consumer in a Financial Institution in which credits and debits may be effected by virtue of Electronic Fund Transfers and which is used to conduct branchless banking activities as outlined in these regulations;

"Branchless Banking Agent" means agent providing basic banking services (as described in these regulations) to the customers of an FI on behalf of the FI under a valid agency agreement.

"Card" means any card including an ATM card, Electronic Fund Transfer point of sale card, debit card, credit card or stored value card, used by a Consumer to effect an Electronic Fund Transfer;

"**Deposit**" means a sum of money paid on terms under which it is to be repaid, either wholly or in part, with or without any consideration, either on demand or at a time or in circumstances agreed by or on behalf of the person making the payment and the person receiving it, and in any other circumstances as may be specified by the State Bank in regulations made by it, but does not include money paid bona fide:

(a) by way of advance or part payment under a contract for the sale, hire or other provision of property or services, and is repayable only in the event that the property or services is not or are not in fact sold, hired or otherwise provided;
(b) by way of security for the performance of a contract or by way of security in respect of loss that may result from the nonperformance of the contract;
(c) without prejudice to paragraph (b), by way of security for the delivery of or return of any property whether in a particular state of repair or otherwise; and
(d) in such other circumstances as may be specified by the State Bank in regulations made by it;

"Electronic Fund" means money transferred through an Electronic Terminal, ATM, telephone instrument, computer, magnetic medium or any other electronic device so as to

order, instruct or authorize a Financial Institution or any other company or person to debit or credit an account.

"Electronic Money" includes monetary value as represented by a claim on the issuer which is stored in an electronic device or Payment Instrument, issued on receipt of funds of an amount not less in value than the monetary value issued, accepted as means of payment by undertakings other than the issuer and includes electronic store of monetary value on a electronic device that may be used for making payments or as may be prescribed by the State Bank;

"Electronic Fund Transfer" means any transfer of funds, other than a transaction originated by cheque, draft or similar paper instrument, which is initiated through an Electronic Terminal, telephonic instrument, point-of -sale Terminal, stored value card Terminal, debit card, ATM, computer magnetic tape or any other electronic device so as to order, instruct, or authorize a Financial Institution or any other company or person to debit or credit an Account;

"Financial Institution" or "FI" mean Commercial Banks, Islamic Banks and Microfinance Banks.

"Microfinance Bank" or "MFB" shall mean companies incorporated in Pakistan and licensed by the State Bank as Microfinance Banks to mobilize deposits from the public for the purpose of providing Microfinance services;

"Mobile payment" or m-payment is not by itself a new payment instrument but an access method to activate an existing means of payment for financial transactions processed by banks between bank customers. An m-payment involves a wireless device that is used and trusted by the customer. M-payments may be card based or non-card based, in both the real and virtual world.'

"Person" includes a legal person or a body of persons whether incorporated or not.

"Prescribed" means prescribed under applicable rules, circulars, directions, orders or bye-laws.

"State Bank" or "SBP" means the State Bank of Pakistan established under section 3 of the State Bank of Pakistan Act, 1956 (XXXIII of 1956);

3 Permissible Branchless Banking Models and Activities

In line with the policy outlined in the Policy Paper on Regulatory Framework for Mobile Banking, presently, only Bank-led Model of ***BB*** is allowed. Nonbank-Led Model will be opened up after the players and stakeholders attain necessary level of maturity and after putting in place necessary controls. Separate regulations will be issued for Nonbank-Led

model as and when the same is launched. In any one financial institution, one customer can have only one branchless banking account.

3.1 Permissible Models

As stated above, only bank-led model of branchless banking is allowed at present which may be implemented in different ways. Firstly, it can be implemented either by using agency arrangements or by creating a JV between Bank and Telco/non-bank. Further, the mobile phone banking which make up for large part of branchless banking can be implemented by using one-to-one, one-to-many and many-to-many models. It is the responsibility of the FI to carry out detailed analysis of pros and cons of each model before offering any of them. These models are briefly explained hereunder.

One-to-one (1-1) Model: In this model one bank offers mobile phone banking services in collaboration with a specific Telco. As a consequence, the services may only be offered to customers using mobile connection of that specific telco. This model can be JV-based or implemented through specific agency agreements between the telco and the bank. It offers greater customization, good service standards, possibility of co-branding and co-marketing. On the other hand, it lacks in outreach as it is limited to the customers of one telco only.

It may be noted that one-to-one model does not necessarily require exclusivity. Therefore, one bank can have several one-to-one arrangements with many telcos or alternately, one telco can have several one-to-one arrangements with many banks. Provided that such arrangements are under proper agency /service level agreements as stipulated in section 6.4 below.

One-to-many (1-∞) Model: In this model a bank offers mobile phone banking services to customers using mobile connection of any Telcos. This model offers the possibility to reach to any bankable customer who has a mobile phone connection. But this model has several limitations in that all telcos may not be ready to offer the bank a priority SMS pipe to enable it to provide quick services which are of essence in mobile phone banking. Further, the FI needs to bear all advertising/marketing expenses. Another serious drawback of this model is that it may require the bank to rely upon its own branch network for product distribution and cash-in cash-out services etc.

Many-to-many (∞-∞) Model: In this model many banks and many telcos join hands to offer services to virtually all bankable customers. Under this system, a central transaction processing system (TPS) is necessitated, which must be controlled by an FI; or by a subsidiary owned and controlled by an FI or a group of FIs; or by a third party service provider under proper agency agreement with a bank. The TPS should be capable of; i) settling all transactions on real time basis, ii) storing all proofs of transactions and iii) providing a day end statement of account to all member banks. All settlements must take place in specific Branchless Banking clearing accounts of all participating banks /telcos/TPS provider kept with a designated bank. This model offers the maximum connectivity and hence maximum outreach and is closer to the desired situation where all banks and all telcos should be able to entertain each other's customers (Just like the

existing ATM network in the country where customer of any bank can use ATM of any other bank).

Alternate Channels: Branchless banking can also be done using agents other then Telcos (like Fuel distribution companies, Pakistan Post, chain stores etc.) and using technologies not limited to mobile phone (like GPRS, POS terminals etc.). The above explained three sub-models (one-to-one, one-to-many and many-to-many) can also be applied to this type of branchless banking (i.e. one FI may join hands with one super-agent [1-1], one FI with many agents [1-∞] or many FIs and many super-agents may join hands to provide ***BB*** services [∞-∞]), provided the complexities of each model are understood, the operating procedures are documented and the risks are identified and taken care of. FIs may come up with an arrangement which does not fall exactly under one of the above models. Such arrangements may be allowed on case to case basis.

In each case customer account relationship must reside with some FI and each transaction must hit the actual customer account and no actual monetary value is stored on the mobile-phone or TPS server (the balances shown on mobile phone etc. are merely a reflection of actual account balances). Consequently the use of the term e-money to represent the services offered under these regulations is prohibited as being technically incorrect.

3.2 Permissible Activities

Under these regulations following products/services may be offered.

- **Opening and maintaining a *BB* Account.** A ***BB*** account can be opened and operated by a customer with a bank through use of BB channels. Banks may associate such account to a particular branch or to a centralized branchless banking unit. Account capabilities/limits are commensurate with the level of customer due diligence (CDD) and KYC procedures the customer has undergone. Risk based KYC and CDD structure is explained in the relevant section of these regulations.
- **Account-to-account Fund transfer:** Customers may transfer funds to/from their ***BB*** account from/to their other pre-registered accounts (current/saving bank accounts, loan limit accounts, credit card accounts etc.)
- **Person-to-person Fund Transfers:** Customer can transfer funds from/to their ***BB*** or regular account to/from ***BB*** or regular accounts of same or some other bank (depending on the model capabilities) or to mobile numbers of other non- ***BB*** account holders[1].
- **Cash-in and Cash-out:** Customers may deposit and withdraw funds to/from their ***BB*** account using a variety of options including bank-branch counters, ATM machines and authorized agent locations.

[1] Such recipients need to become a ***BB*** account holder after completion of formalities to utilize these funds. The message (SMS) of funds transfer to such recipients should always be generated by the FI and must contain necessary procedural details to be followed by the recipient in order to utilize those funds. The recipients should also be able to utilize these funds for making utility (electricity, gas, phone/mobile phone) payments without becoming formal ***BB*** account holder.

- **Bill Payments:** A ***BB*** account can also be used to pay utility bills (e.g. Gas, Electricity, Phone etc.)
- **Merchant Payments:** Customers can use a ***BB*** account to make payments for purchases of goods and/or services.
- **Loan Disbursement/Repayment:** FIs, particularly MFBs may use ***BB*** accounts as a means to disburse small loan amounts to their borrowers having ***BB*** accounts. The same accounts may be used by customers to repay their loan installments.
- **Remittances:** ***BB*** accounts may be used to send / receive remittances subject to existing regulations.

4 Risk-Based Customer Due Diligence

To optimize the gains of Branchless Banking and to extend financial services outreach to the unbaked strata of the society without compromising the requirements of AML/CFT, a risk-based approach to customer due diligence is outlined here. This approach is specific to the ***BB*** accounts and does not apply to the regular full service banking accounts.

Under the risk-based CDD approach, ***BB*** accounts have been categorized in three levels. The KYC requirements, transactional limits and minimum technological security requirements applicable to each type of account are tabulated below. It may be noted that level 1 ***BB*** account are for individuals only, level 2 account can be opened by individuals as well as by firms, entities, trusts, Not-for-profit organizations legal persons etc, and level 3 ***BB*** account is for businesses only.

Account Level =>	**Level 1**	**Level 2**	**Level 3**
Description	Entry Level account sufficient for most low income individuals	Top level account offering all ***BB*** facilities and subject to full KYC requirements as applicable to a full-service banking account.	Account specific for merchants, businesses, banking agents or third-party service providers.
KYC requirements	1. Filling and signing an account opening application form. 2. Photocopy of Computerized National Identity Card. 3. Verification of CNIC by NADRA. 4. At least one personal face-to-face contact with a designated employee of the FI or a biometric fingerprint scan and a	1. Filling and signing an account application form. 2. Fulfillment of all KYC requirements specified under Prudential Regulations issued by SBP as amended from time to time. (Presently given under regulation M-1 of the PRs). 3. Verification of CNIC	1. Fulfillment of all requirements of level 3 account. 2. fulfillment of additional requirements as specified by the FI.

Account Level =>	Level 1	Level 2	Level 3
	digital photo taken by a ***BB*** agent must reach the FI.	by NADRA.	
Maximum Balance Limits (debit/credit)	Rs. 60,000	FI must set limits commensurate with each customer's profile.	FI must set limits commensurate with each customer's profile.
Maximum Throughput Limits (debit/credit)	Rs. 10,000 per day Rs. 20,000 per month Rs. 120,000 per year		
Minimum Technological requirements	As per details given in Section 8.3.1 below)		

Despite the above relaxations in KYC requirements for level 1 account holder, the FIs must adhere to the requirements of other relevant prudential regulations (like PR M2-M5).

FIs must ensure that their transaction processing system is capable of:

- Imposing above limits to avoid any breach.
- Sending alerts to the users if they are close to a limit (These regulations do not suggest that the banks must send such alerts. However, the capability needs to be there.)
- Analyze transaction history to identify those level 1 and level 2 users who need to move to the next higher account level after fulfilling additional KYC requirements.
- Identifying abnormal/ suspicious transactions and to report the same to the FI's compliance setup for further necessary action.

Minor's may open a level 1 or level 2 account provided they submit a written undertaking by their parent/guardian to accept any liability arising out of the action(s) of the minors.

Further, the requirement of sending biannually, statement of account to the account-holders does not apply to ***BB*** accounts. However account-holders should have an option to view at least last 10 transactions using ***BB*** channels (e.g. mobile phone) free of cost and they may also demand a printed statement of account (for a period not more than past 12 months) by paying fee as specified by the FI.

5 Key Roles & Responsibility

The ultimate responsibility for branchless banking lies with the FI. FI may, however, take steps it deems necessary to safeguard itself against liabilities arising out of the actions of its agents, service providers or partners. Within the FI, BOD is responsible for strategic decisions, senior management for effective oversight and compliance and audit functions for ensuring soundness of internal controls and adherence to rules, regulations and operational guidelines.

5.1 Board of Directors

FI's Board of Directors (or senior management, in case of Pakistani branches of foreign FI's) is responsible for developing the bank's branchless banking business strategy and relevant policies.

The Boards of Directors is expected to take an explicit, informed and documented strategic decision as to whether and how the FI is to provide branchless banking services to their customers. BOD should also ensure that the FI has proper security control policies to safeguard e-banking systems and data from both internal and external threats.

5.2 Senior Management

FI's senior management is responsible for implementing branchless banking strategy and for establishing an effective management oversight over branchless banking services.

Effective management oversight encompasses the review and approval of the key aspects of the FI's security control program and process, and to implement security control policies and infrastructure. It also includes a comprehensive process for managing risks associated with increased complexity of and increasing reliance on outsourcing relationships and third-party dependencies to perform critical branchless banking functions.

BOD and Senior Management must ensure that the scope and coverage of their internal audit function has been expanded to commensurate with the increased complexity and risks inherent in branchless banking activities and the Audit department has been staffed with Personnel having sufficient technical expertise to perform the expanded role.

It is also incumbent upon the BOD and FIs' senior management to take steps to ensure that their FIs have updated and modified where necessary, their existing risk management policies and processes to cover their current or planned branchless banking services. The integration of branchless banking applications with legacy systems implies an integrated risk management approach for all banking activities.

5.3 Compliance Officer

FI's Compliance Officer should ensure that proper controls are incorporated into the system so that all relevant compliance issues are fully addressed.

Management and system designers should consult with the Compliance Officer during the development and implementation stages of branchless banking products and services.

This level of involvement will help decrease bank's compliance risk and may prevent the need to delay deployment or redesign programs that do not meet regulatory requirements.

5.4 Internal Auditors

FI's Internal Auditors are responsible to ensure adherence to the policies, rules, regulations and operational guidelines.

Internal Auditors need to work as the eyes and ears of the BOD. They need to incorporate risk-based review of critical branchless banking processes to ensure that the policies, rules, regulations and the operational guidelines are followed and should escalate significant exceptions to the Audit Committee of the BOD. They are also responsible to form a view on the outsourced activities by taking appropriate direct or third party audits of the same as mandated under relevant outsourcing agreements.

6 Agents-Assisted Banking

The true power of branchless banking cannot be unleashed until some trusted third parties are involved in performing some of the activities that are traditionally performed in bank branches by bank staff. Use of the word agent in this context does not include third party service providers who provide certain technical services to banks, such as provision of transaction processing system. However, there is no restriction on a third party technology service provider to become a branchless banking agent provided it meets the criteria for becoming an agent.

6.1 Role of Agents

Agents may perform any or all of the following functions depending on the agency agreement and agent type as detailed in the following sections;

- Opening of ***BB*** Accounts (Level 1 accounts only).
- Cash in / Cash out for ***BB*** accounts.
- Bills Payments (Both from registered ***BB*** customers as well as from walk-in customers (through cash) of any utility company).
- Loan disbursement / Repayment Collection (Without involving into loan marketing/ approval functions).

One Agent can provide services to multiple banks provided he (the agent) has a separate service level agreement with each bank. Alternately, banks may organize their agent network using open architecture so that the agents may entertain other banks' customers using infrastructure provided by one bank.

Agents may not alter/change charges/fees structure provided by the bank in any way. All charges have to be pre-agreed between the bank and the agent and should be clearly communicated to the customers.

Banks/agents may choose to brand their agent network under any brand name. However use of words like Bank, financial intermediary, microfinance bank or any other word suggesting that the agent is itself an FI, is not allowed.

6.2 Agent Structure

Agents may be of three basic types.

Super Agents: These may be organizations having well-established owned or franchised retail outlets, or a distribution setup. These will be responsible for managing and controlling subagents. These may include fuel distribution companies, Pakistan Post, courier companies, chain stores etc.

Direct Agents: These may include large to medium sized stores etc., which have a separate agency/service level agreement with the FI.

Sub Agents: These are the branches/outlets or franchised locations managed by a super agent and not directly controlled by the FI on a day-to-day basis. However, in case of franchised locations, these must have a similar service level agreement with the super agent as the super agent will have with the FI.

6.3 Agent Due Diligence

Use of agents in ***BB*** exposes FI to significant operational and reputational risks. Efficient and foolproof Agent Due Diligence (ADD) procedures must exist to mitigate these risks.

FIs are responsible for having clear, well documented ADD policy and procedures. These procedures, at minimum, should contain new agent take on procedures (NATP), initial due diligence and regular due diligence checks to be performed at specified intervals and a list of early warning signals and corrective actions to ensure proactive agent management. ADD should clearly specify roles and responsibilities of various functions in the bank w.r.t. agent management.

NATP should clearly define various agent types and minimum agent selection criteria for each type. FIs should ensure that agents are well established, enjoying good reputation and having the confidence of the local people. FIs may give wide publicity in the locality about the intermediary engaged by them as Agent and take measures to avoid being misrepresented.

Banks should ensure that proper AML/CFT monitoring process exists for branchless banking, necessary actions to be taken by agents in this regard are well communicated to the agents and the agents' compliance of the same is monitored.

6.4 Agency Agreement

The FI shall submit a **Service Level Agreement (SLA)/Agency Agreement (AA)** (duly signed by concerned parties), and any amendments thereto, detailing the functions/activities to be performed, the respective responsibilities of the bank and its agent and a confidentiality clause. The requirement of SLA/AA as outlined in this section and in the 'Guidelines on Outsourcing Arrangements' issued vide BPRD Circular No. 9 dated July 13, 2007 also apply to third party service providers defined in section 7 below.

The senior management of the FI shall remain responsible for maintaining an effective system of internal control and for providing active oversight of the agent's activities/functions.

There shall be a contingency plan to mitigate any significant disruption, discontinuity or gap in agent's function, particularly for high-risk areas.

The written engagement contract or service level agreement with the agent shall, at a minimum:

i. Define the rights, expectations and responsibilities of both parties;
ii. Set the scope of, and the fees/revenue sharing structure, the work to be performed by the agent;
iii. State that the outsourced services are subject to regulatory review and that SBP inspecting officers shall be granted full and timely access to internal systems, documents, reports, records and staff of the agent;
iv. State that the agent will not perform management functions, make management decisions, or act or appear to act in a capacity equivalent to that of a member of management or an employee of the FI;
v. Specify that the agents must ensure safe-keeping of all relevant record, data and documents /files for at least five years; or alternately, such record is shifted to the FI at regular pre-specified intervals which will then ensure safe-keeping of this record for at least 5 years.
vi. State that all information/data that the agent collects in relation to branchless banking services, whether from the customers or the FI or from other sources, is the property of the FI, and the institution will be provided with copies of related working papers/files it deems necessary, and any information pertaining to the institution must be kept confidential; and
vii. Establish a protocol for changing the terms of the service contract and stipulations for default and termination of the contract.
viii. Mention suitable limits on cash holding by agents/sub-agents as also limits on individual customer payments and receipts.
ix. State the requirement that the transactions are accounted for and reflected in the bank's books by end of day or next working day.

6.5 Agent Development

The essential spirit of Branchless Banking is financial inclusion. ***BB*** aims at putting the national resources to the productive activities and directing financial resources to areas where the same are most needed. In line with this spirit the FIs are required to plan and act for long term development and prosperity of their agents. This requires close coordination/collaboration with agents; providing them opportunities to learn more, to become more efficient and; a fair pricing mechanism for the services provided by the agents.

The FI shall also be responsible for putting in place appropriate product and operations manuals, accounting procedures and systems and for designing necessary forms/ stationary to be used by the agents.

7 Use of Third-Party Service Providers

As opposed to the ***BB*** agents, third-party service providers provide services related to technological infrastructure etc. Third-party services providers may not perform activities that are attributed to ***BB*** agents unless they sign separate agreements with the FI(s) to become ***BB*** agents as provided in section 5 above.

While dealing with service providers, FIs should follow 'Guidelines on Outsourcing Arrangements' issued by SBP vide BPRD Circular No. 9 dated July 13, 2007. A proper service level agreement (as defined in section 6.4 above) must be put in place for all third-party service arrangements.

8 Risk Management Program

While existing risk management principles remain applicable to branchless banking activities, such principles must be tailored, adapted and, in some cases, expanded to address the specific risk management challenges created by the characteristics of ***BB*** activities.

Branchless banking under bank-led model entails two major categories of risks; agent-related and wireless/e-banking -related. The FIs need to pay special attention to these risks. However this risk management should not be done in isolation and should form part of FI's overall risk management program.

8.1 Agents Related Risks

Entrusting retail customer's contact to the agents is riskier than these same functions in the hands of bank tellers in a conventional bank branch. These retail agents may operate in hard-to reach or dangerous areas & they lack physical security systems and specially trained personnel.

8.1.1 Risk Implications of Use of Agents

In the context of agent assisted banking, the FIs should pay special attention to credit risk, operational risk, legal risk, liquidity risk, and reputation risk. The use of retail agents also potentially raises special concerns regarding consumer protection and compliance with rules for combating money laundering and financing of terrorism which deserve FIs' attention.

The time lag between collection from customers and depositing the same to FI by retail agents generates credit risk. There are chances of customers or retail agents committing fraud, loss to bank's equipment or other property from a retail agent's premises, data leaks or data loss from hacker attacks, inadequate physical or electronic security, or poor backup systems etc. All these factors lead to operational risk. Retail agents - especially those that are relatively small, unsophisticated and remote - may not have enough cash to meet customers' requests for withdrawals and may lack experience in the more complex

liquidity management required for offering financial services. When retail agents under perform or are robbed, FI's public image may suffer. Many operational risks mentioned (such as the loss of customer records or the leakage of confidential customer data) also can cause reputation risk, as can liquidity shortfalls in the retail agent's cash drawer. Moreover, reputation risk can spread from one FI to another and take on systemic dimensions. Obviously, any of the foregoing categories of risk triggers consumer protection concerns if the resulting loss falls on customers. Use of retail agents may also increase the risk that customers will be unable to understand their rights and press claims when aggrieved, especially for the poor, remote, or marginalized people.

On the other side of the coin, the FIs bear the risk that customers are improperly identified and that they use the retail agent to launder money or channel funding to terrorists (with or without the retail agent's knowledge or complicity). Outsourcing account opening and retail transaction processing to unsophisticated retail agents may make it difficult for the bank to observe and report suspicious transactions. Further, as with each new initiative, ***BB*** also carries some level of legal and regulatory uncertainty and ambiguity for FIs (and to a lesser extent also for retail agents).

8.1.2 Risk Management for Agent Related Risks

The FI needs to consider the above risks and extend its risk management program to cover the same. NATPs should include proper assessment of agent's credit worthiness and proper limit structure for agents' various activities - commensurate with this assessment - should be in place. All product programs, procedure manuals, customer limit structures should be devised keeping in mind the implications for operational risk and liquidity risk for agents. The FI needs to have a proper complaints redressal mechanism and should ensure proper communication of its complaints redressal setup to the customers (See section 9.3 below for details of complaint redressal machanism). ***BB*** activities will also require risk capital allocation similar to that of normal banking activities.

8.2 Wireless/ e-Banking Technology Risks

During last few years, wireless technology adoption (especially, cellular/mobile communication systems) has shown a great momentum and it is still spreading at an unbelievable pace across Pakistan. Considering the importance of cellular mobile communication system's role and its wide availability, there is great potential to push banking services to far flung areas of Pakistan and un-banked community using this media. However, wireless communication systems have associated data and network security risks which make them susceptible for conducting financial transactions. This discussion is on technology risks regarding information and data security in wireless networks based on applicable models of branchless banking i.e. one-one, one-many and many-many as discussed previously.

Wireless/ e-banking related risks should be recognized, addressed and managed by FIs in a prudent manner according to the fundamental characteristics and challenges of e-banking services. These characteristics include the unprecedented speed of change related to technological and customer service innovation, the ubiquitous and global nature of

open electronic networks, the integration of e-banking applications with legacy computer systems and the increasing dependence of banks on third parties that provide the necessary information technology.

8.2.1 Wireless/E-Banking Technology Risk Implications

While not creating inherently new risks, use of wireless/e-banking increases and modifies some of the traditional risks associated with banking activities, in particular strategic, operational, legal and reputational risks, thereby influencing the overall risk profile of banking.

Wireless banking (which is expected to form a great part of ***BB***) creates a heightened level of potential operations risk due to limitations in wireless technology. Security solutions that work in wired networks must be modified for application in a wireless environment. The transfer of information from a wired to a wireless environment can create additional risks to the integrity and confidentiality of the information exchanged.
Standards for wireless communication are still evolving, creating considerable uncertainty regarding the scalability of existing wireless products. Financial institutions should exercise extra diligence in preparing and evaluating the cost-effectiveness of investments in wireless technology or in decisions committing the institution to a particular wireless solution, vendor or third-party service provider. A more specific discussion of technology risks facing branchless banking is as under.

8.2.1.1 Wireless Networks Risks

- **Communication Protocol risk**

Unilateral authentication is performed in GSM protocol i.e. Base station verifies mobile station but not the other way around, hence mobile station may not guarantee its communication with right recipient and vulnerable to attacks like active identity caching and passive identity caching.

Wireless Application Protocol (WAP) gateway in Telco premises is vulnerable to "WAP gap" unless proper measures have not been taken to ensure protocol translation in server volatile storage.

- **Data Storage risks**

Physical or logical access to Telco facilities by unauthorized person may give access to branchless banking users transaction data especially in case where Short Message Service (SMS) is used which are typically stored in SMS-C storage for SMS messages in Telco premises

- **Availability and QoS (Quality of Service) issue**

Interruption in services of Telco due to technical or non-technical issue and non availability of any parallel system may cause disruption in service availability. Similarly, congestion in network may become a bottle neck in providing Quality of Service to BB user.

8.2.1.2 FI infrastructure and Software Application for BB Risks

- **PIN and user authentication data**

Unencrypted branchless banking user data especially, Personal Identification Number (PIN) stored on branchless banking application servers in FI premises could be misused.

- **Financial data storage**

All financial data like cash amount, loan amount, and loan repayments in BB accounts stored in plain format are vulnerable to leakage which can result into confidentiality compromise of user financial information. An unauthorized change to such financial data may cause a financial scam as well as can cause reputational risk for FI.

- **Non-Financial data storage**

Non-financial data like user transaction logs without high level of integrity controls are vulnerable to unauthorized changes that may result into hiding information to trace fraudulent transactions, financial scams and non-repudiation. User profile, user transaction pattern should be provided high level of confidentiality and integrity.

- **Information Security Procedures and Policies**

FI without laying down proper information security policies and procedures will be in a hap hazard condition of performing information security operations of branchless banking. This may result into serious IT operational risks like data backup issues, segregation of jobs, succession planning, capacity planning, disaster recovery and business continuity planning.

- **Application error and message handling**

Improper error messaging and exception handling in branchless banking application server may facilitate malicious intenders to inject illegitimate queries which help in revealing information about back-end infrastructure.

- **Availability of services and Backup**

FI without business continuity and disaster recovery planning may be on risk of non-availability of services in case of catastrophic events (power breakdowns, fire etc) and natural disasters (flooding, earthquake etc)

8.2.1.3 Agent and TPS infrastructure Risks

- **Authenticity of communication**

Without proper authentication prior to establishing communication between FI and Agent or vice versa may provide risk of masquerading by one of the party that can result into passing of information to illegitimate party.

- **Physical and logical Access to systems**

Physical or logical access to agents and TPS information system without proper controls may result into illegitimate access by disgruntled employees and malicious persons.

- **Data Storage and Data Backup**

Client's profiles and financial data stored unencrypted on information systems of agents and TPS premises is vulnerable to leakage. Similarly, if agent and TPS have not taken proper data backup measures it may result into data loss in case of technical and non-technical major events like storage failures, fire, flooding etc

- **Data Encryption and Message Integrity**

Unencrypted data communication between FI and Agent or vice versa may be vulnerable to change and sniffing during transit. Similar is the case with other parties in communication channel, like TPS and Telco.

8.2.1.4 User Awareness Risks

- **Customer awareness on information security**

Customer without proper awareness might store PIN on his/her mobile device which may be revealed easily on stealing. Customer should be made aware of possible consequences and what s/he should do to avoid such risks. Similarly, fetching mobile phone viruses from other rogue mobile devices may cause improper functioning of branchless banking application on user mobile station.

8.2.2 Wireless/E-Banking Technology Risk Management

For overall e-banking risk management, FIs are advised to refer to the "Risk Management Principles for Electronic Banking" issued by the Basel Committee on Banking Supervision in July 2003. FIs may use these principles as a starting point for their e-banking risk management and may tailor these to suit the level and complexity of their ***BB*** operations. The text of the principles is given in appendix A and a detailed explanation of these principles and several other sound practices can be found in the above referred document.

Risk management of wireless-based technology solutions, although similar to other electronic delivery channels, may involve unique challenges created by the current state of wireless services and wireless devices. A general discussion of these considerations is given in Appendix B. Specific requirements to mitigate technology risk and to ensure data and network security are discussed in section 8.3 below.

8.3 Data & Network Security Considerations

Data and Network security issues are of paramount concern to ensure authenticity, confidentiality, integrity, accountability and non-repudiation for financial transactions performed by BB users, and also to ensure availability of BB services to user. The purpose is to make FI aware of risks regarding data and network security. In section 8.3.1 below, minimum information /data security requirements have been laid down and FI must ensure compliance based on applicable account level transaction. Additional measures for risk mitigation have been explained in section 8.3.2 below, which highlights issues that FI may address depending on appropriate feasible way. Overall information security concerns for each relevant actor are depicted using a grid in section 8.4 below.

There is a special focus on Global System for Mobile communication (GSM) channel to conduct branchless banking operations. It should be noted that discussing GSM does not mean at all to consider it as the only mode or channel available for conducting permissible operations of branchless banking. Other communication technologies either wired or wireless can be adopted for the purpose as also explained in section 3 above. Cellular mobile communications systems are very well matured and provide the widest coverage across Pakistan. Moreover, it is very cheap in connection and maintenance as compared to other communication technologies; and this is the reason it is widely adopted across Pakistan.

Other wire or wireless based communication channels used by Automated Teller Machines (ATM), Internet, and Point of Sale (POS) are already mature market technologies from operations perspective at different FI's in Pakistan. All of these systems have built-in mechanism at network and application layer to provide end to end communication security using different protocol and thus not need to be discussed here.

8.3.1 Risk-Based Information/ Data Security Requirements

Uniform and stringent information/data security requirements may not be a feasible approach. In order to make branchless banking concept more successful by FI and consumers, a flexible approach has been adopted that is based on financial exposure of consumer. This is based on risk-based customer due diligence concept. Similarly, data security requirements are also linked with the account levels of a consumer. Below is the table which tabulates minimum standards for data security using different channels of cellular mobile communication system like Short Message Service (SMS), Unstructured Supplementary Service Data (USSD), Wireless Application Protocol (WAP) and SIM Application Toolkit (SAT).

Account Level	**Level 1**	**Level 2**	**Level 3**
Applicable Channels using cellular mobile communication system.	SMS, USSD	WAP, SAT	WAP, SAT
Minimum Standard Requirements			
Authentication of Client and Service end.	Two-Factor Authentication. PIN (user knowledge) and MSISDN in case of mobile phone (user possession).		
Message Encryption requirements at application level.	Not required / Not applicable	Application level 128 bit using known symmetric algorithms or asymmetric like PKI (Public Key infrastructure).	
Message Integrity Checks at	As appropriate	Keyed Hash functions or Message Authentication Code like MD-5 and SHA-1	

Account Level	Level 1	Level 2	Level 3
application level			
Accountability/ Non-repudiation	All Financial and Non-Financial transaction logs must be securely stored by FI.		
Availability of Services	FI must have infrastructure to support high availability of services in normal circumstances and disaster. FI must also ensure this for while making Service Level Agreements (SLA) with agents and Telco's		

8.3.2 Additional Measures for Risk Mitigation

This section covers security measures that are in addition to minimum standards described above. A few points covered under minimum standards are also discussed in detail to further elaborate them for ensuring overall branchless banking application security and auditing requirements. FIs must be aware of these issues to address them as feasible.

8.3.2.1 Client Accountability and Non-Repudiation

Client financial transactions should be logged for evidence purpose for auditing and for facilitation during forensic investigations in case of criminal incidents. The other main purpose is to make sure that client may not deny the transaction s/he has performed using the branchless banking application service. In this regard, client transaction detail, PIN authentication log and additionally, if possible, FI may also acquire messages log details from Telco.

8.3.2.2 Error Messaging and Exception Handling

Branchless banking application server should be able to properly handle exceptions and reporting errors. It may be noted that if error reporting and exception handling are not properly managed, it can reveal information that can be misused to perform illegitimate queries. A thorough testing of application by financial institutes or service provider or third parties should be done in this regard to make sure that application is handling exceptions and reporting errors properly.

8.3.2.3 Physical Security of Telco, FI, Agent and TPS Facilities

Physical premises of Telco like Mobile Switching Centre (MSC), FI and TPS data centers access should be properly managed. Proper access control and monitoring mechanisms should be in place. Access of employees on leave or those having resigned from service should be immediately stopped. Similarly, logs should be reviewed to assess any unauthorized access.

8.3.2.4 Client Profiling

Branchless banking application server should profile client behavior like spent pattern so that illegitimate abnormal usage can be detected at an early stage. Moreover, client

should be provided additional security options like funds transfer to defined accounts, fund transfer limits etc. As an additional measure, application server should use an alias of user account to transmit across network as a purpose to hide actual user account details on the network.

8.3.2.5 Encrypted PIN and Client data storage

Client PIN is the most confidential data part stored on servers. FI should ensure client PIN and profile data is encrypted and also appropriate controls are in place to ensure data integrity. For this purpose, it is recommended that industry based Hardware Security Modules (HSM) must be used for PIN storage and translations.

8.3.2.6 Availability of Services

Telco, FI and TPS should have proper technology infrastructure backup, disaster recovery plan and technical security infrastructure in place to ensure timely services availability to all clients.

8.3.2.7 End User Information Security Awareness

End user should be aware of the fact that s/he is not supposed to store PIN and other critical information on mobile phones. Similarly, by default enabled blue tooth ports and exchange of data from other rogue mobile devices may cause application errors and issues, especially in case of SAT. FI should make this information the part of their customer awareness program.

8.4 Actors and Relevant Concerns

Actors / **Data & Network Security Concerns**	TELCO	FI	TPS	Agent
Physical security of infrastructure	X	X	X	X
Availability of services	X	X	X	X
Client transit data confidentiality and integrity	X	X	X	X
Client stored data confidentiality and integrity	X	X	X	X
Client profiling		X		
Accountability and Non-Repudiation	X	X	X	X
Error messaging and exception handling		X		

Authentication of client and FI		X		
End User information security awareness		X		

Table: Actors and their relevant information security concerns

9 Customer Protection and Awareness

Appropriate customer protection against risks of fraud, loss of privacy and even loss of service is needed for establishing trust among consumers as trust and customer confidence is the single most necessary ingredient for growth of ***BB***. As we will be dealing with a large number of first time customers with low financial literacy level, banks need to ensure that adequate measures for customer protection, awareness and dispute resolution are in place.

9.1 Customer Protection

Use of retail agents may also increase the risk that customers will be unable to understand their rights and press claims when aggrieved. It is not always clear to customers how they will be protected against fraud when they use retail agents to conduct financial transactions. FIs should devise clear guidelines for customers regarding complaints and dispute resolutions and should make efforts to make these public. FIs must publish their schedule of charges for ***BB*** activities and services on quarterly basis for each calendar quarter and make it available at all its branches / agent locations /website. The charges cannot be increased during a quarter. All agreements/ contracts with the customer shall clearly specify that the bank is responsible to the customer for acts of omission and commission of the Agent.

Customers may also be given the option of obtaining loss insurance. However, the voluntary nature of this insurance must be clearly communicated to the customer.

9.2 Customer Awareness

Customer awareness is a key defense against fraud and identity theft and security breach. Customer awareness program should cover, at minimum, usage of Branchless-Banking account, account activities and protection against fraud, SIM/account blocking procedures in case of mobile is lost / snatched. Appendix C provides some precautions that banks should convey to their customers.

To be effective, banks should implement and continuously evaluate their customer awareness program. Methods to evaluate a program's effectiveness include tracking the number of customers who report fraudulent attempts to obtain their authentication credentials (e.g., ID/password), the number of clicks on information security links on websites, the number of inquiries, etc.

9.3 Complaint Redressal

Each FI willing to offer ***BB***, must put in place a proper complaint redressal setup capable of efficiently and quickly redressing complaints received from ***BB*** customers. CR, at minimum should be capable of:

- Receiving and processing customers' complaints 24 hours through, SMS, IVR and email,
- Generate acknowledgement of complaint giving it a unique complaint number.
- Communicate acknowledgement to customer giving either the redressal or the complaint number and estimated time to redressal.
- Redirecting the complaint to appropriate function for redressal.
- Keep track/log of all complaints and give status of every complaint.

The complaint redressal mechanism and the relevant phone numbers/emails etc. of the FI should be widely publicized using appropriate communication channels and should also be placed at FI's website.

10 Branchless Banking Procedures

10.1 Preparation

Only authorized Financial Institution can provide Branchless Banking services as stipulated in these regulations. Before applying for such an authorization, FIs should thoroughly prepare themselves in the light of these regulations. The process should start from top level strategic decision of entering into branchless banking activities. Once the decision is made, preparation of necessary policies & procedure manuals, strengthening of existing risk management & audit functions as required and identification of partners, service providers and agents should be done. The FI may then approach SBP for a formal authorization to conduct ***BB***.

10.2 Authorization

1. Banks wishing to provide branchless banking services or to bring in substantial changes in underlying technological infrastructure shall submit to the State Bank, an application describing the services to be offered / infrastructure modifications and how these services fit in the bank's overall strategy. This shall be accompanied by a certification signed by FIs President/CEO to the effect that the FI has complied with the following minimum pre-conditions:

    a. An adequate risk management process is in place to assess, control, monitor and respond to potential risks arising from the proposed branchless banking activities;

b. A manual on corporate security policy and procedures exists that shall address all security issues affecting its branchless/e-banking system, in line with these regulations
c. A business continuity planning process and manual have been adopted which should include a section on electronic banking channels and systems.

Following documents should also accompany the application.

a. A copy of the relevant portion(s) of the security policies and procedures manual containing (i) a description of the bank's security organization; (ii) definition of responsibilities for designing, implementing, and monitoring information security measures; and (iii) established procedures for evaluating policy compliance, enforcing disciplinary measures and reporting security violations;

2. SBP, shall pre-screen the overall financial condition of the FI as well as the compliance with the SBP rules and regulations based on the latest available onsite and offsite reports / other sources to ensure that:

   a. the applicant FIs' overall financial condition can adequately support its branchless banking activities and that it shall have complied with certain comprehensive prudential requirements such as, but not limited to, the following:

      i. *Minimum* capital requirement ;
      ii. Satisfactory solvency, liquidity and profitability positions;
      iii. CAMELS composite rating of at least 3 with rating of systems and controls component not below 3 based on the latest regular examination;
      iv. There are no uncorrected major findings/exceptions noted in the latest SBP inspection.

3. Based on the review, a principle approval of the application will be granted.

4. After getting this principle approval the FI shall, in turn notify the SBP on the actual date of launching/ enhancement of its ***BB*** services.

5. Within thirty (30) days from such launching/enhancement, banks shall submit to the SBP, the following documentary requirements for evaluation:

   a. A discussion on the banking services to be offered/enhanced, the business objectives for such services and the corresponding procedures, both automated and manual, offered through the electronic banking channels;
   b. A description (including diagrams) of the configuration of the bank's electronic banking system and its capabilities showing (i) how the electronic banking system is linked to other host systems or the network infrastructure in the bank; (ii) how transaction and data flow through the network; (iii) what types of telecommunications channels and remote access capabilities (e.g. direct modem

dial-in, internet access, or both) exist; and (iv) what security controls/measures are installed;

c. A list of software and hardware components indicating the purpose of the software and hardware in the electronic banking infrastructure;
d. A brief description of the contingency and disaster recovery plans for electronic banking facilities and event scenario/problem management plan/program to resolve or address problems, such as complaints, errors and intrusions and the availability of back-up facilities;
e. Copy of contract(s)/SLAs/ maintenance agreements etc. with the Service providers and/or ***BB*** agents; arrangements for any liability arising from breaches in the security of the system or from unauthorized/fraudulent transactions;
f. Latest internal/external report on the periodic review of the system, if applicable.
g. FI's confirmation that the system had been tested prior to its implementation and that the test results are satisfactory. As a minimum standard, appropriate systems testing and user acceptance testing should have been conducted.

6. If after the evaluation of the submitted documents, SBP still finds some unresolved issues and grey areas, the bank may be required to make a presentation and/or to submit any documents relating to of its branchless banking to SBP.

7. Upon completion of evaluation, the Authorization will be granted.

9. Banks with existing branchless banking services who do not qualify for authorization as a result of the pre-screening process mentioned in item 2 hereof, shall be given three (3) months within which to show proof of improved overall financial condition and/or substantial compliance with SBP prudential requirements. Those failing to comply with these requirements will be asked to smoothly phase out their BB services and settle all customer liabilities within one month period.

Appendices

Appendix A – Risk Management Principles for Electronic Banking

Following is the text of the 14 principles suggested by the Basel Committee on Banking Supervision in their document titled "Risk Management Principles for Electronic Banking" issued in July 2003. FIs may use these principles as a starting point for their e-banking risk management and may tailor these to suit the level and complexity of their *BB* operations. For a more elaborate discussion of these principles, FIs are advised to refer the actual document which is available at BIS website (http://www.bis.org/publ/bcbs98.htm). The document also contains several sound practices in the areas of Security Controls, Management of outsourced e-banking functions, Application authorization and audit trail.

Board and Management Oversight (Principles 1 to 3)

Principle 1: The Board of Directors and senior management should establish effective management oversight over the risks associated with e-banking activities, including the establishment of specific accountability, policies and controls to manage these

Principle 2: The Board of Directors and senior management should review and approve the key aspects of the bank's security control process.

Principle 3: The Board of Directors and senior management should establish a Comprehensive and ongoing due diligence and oversight process for managing the bank's outsourcing relationships and other third-party dependencies supporting e-banking.

Security Controls (Principles 4 to 10)

Principle 4: Banks should take appropriate measures to authenticate18 the identity and authorization of customers with whom it conducts business over the Internet.

Principle 5: Banks should use transaction authentication methods that promote no repudiation and establish accountability for e-banking transactions.

Principle 6: Banks should ensure that appropriate measures are in place to promote adequate segregation of duties within e-banking systems, databases and applications.

Principle 7: Banks should ensure that proper authorization controls and access privileges are in place for e-banking systems, databases and applications.

Principle 8: Banks should ensure that appropriate measures are in place to protect the data integrity of e-banking transactions, records and information.

Principle 9: Banks should ensure that clear audit trails exist for all e-banking transactions.

Principle 10: Banks should take appropriate measures to preserve the confidentiality of key e-banking information. Measures taken to preserve confidentiality should be commensurate with the sensitivity of the information being transmitted and/or stored in databases.

Legal and Reputational Risk Management (Principles 11 to 14)

Principle 11: Banks should ensure that adequate information is provided on their websites to allow potential customers to make an informed conclusion about the bank's identity and regulatory status of the bank prior to entering into e-banking transactions.

Principle 12: Banks should take appropriate measures to ensure adherence to customer privacy requirements applicable to the jurisdictions to which the bank is providing e-banking products and services.

Principle 13: Banks should have effective capacity, business continuity and contingency planning processes to help ensure the availability of e-banking systems and services.

Principle 14: Banks should develop appropriate incident response plans to manage, contain and minimize problems arising from unexpected events, including internal

Appendix B – Some Risk Management Considerations for Wireless Banking

B. 1. Message Encryption

Encryption of wireless banking activities is essential because wireless communications can be recorded and replayed to obtain information. Encryption of wireless communications can occur in the banking application, as part of the data transmission process, or both.

Transactions encrypted in the banking application (e.g., bank-developed for a PDA) remain encrypted until decrypted at the institution. This level of encryption is unaffected by the data transmission encryption process. However, banking application-level encryption typically requires customers to load the banking application and its encryption/decryption protocols on their wireless device. Since not all wireless devices provide application-loading capabilities, requiring application level encryption may limit the number of customers who can use wireless services.

Wireless encryption that occurs as part of the data transmission process is based upon the device's operating system. A key risk-management control point in wireless banking occurs at the wireless gateway-server where a transaction is converted from a wireless standard to a secure socket layer (SSL) encryption standard and vice versa. Wireless network security reviews should focus on how institutions establish, maintain, and test the security of systems throughout the transmission process, from the wireless device to the institutions' systems and back again. For example, a known wireless security vulnerability exists when the Wireless Application Protocol (WAP) transmission encryption process is used. WAP transmissions deliver content to the wireless gateway server where the data is decrypted from WAP encryption and re-encrypted for Internet delivery. This is often called the "gap-in-WAP" (e.g., wireless transport layer security (TLS) to Internet-based TLS). This brief instant of decryption increases risk and becomes an important control point, as the transaction may be viewable in plain text (unless encryption also occurred in the application layer). The WAP Forum, a group that oversees WAP protocols and standards, is discussing ways to reduce or eliminate the gap in- WAP security risk.

Institutions must ensure effective controls are in place to reduce security vulnerabilities and protect data being transmitted and stored.

B. 2. Password Security

Wireless banking increases the potential for unauthorized use due to the limited availability of authentication controls on wireless devices and higher likelihood that the device may be lost or stolen. Authentication solutions for wireless devices are currently limited to username and password combinations that may be entered and stored in clear text view (i.e., not viewed as asterisks "****"). This creates the risk that authentication credentials can be easily observed or recalled from a device's stored memory for unauthorized use.

Cellular phones also have more challenging methods to enter alphanumeric passwords.

Customers need to depress telephone keys multiple times to have the right character displayed. This process is complicated if a phone does asterisk password entries, as the user may not be certain that the correct password is entered. This challenge may result in users selecting passwords and personal identification numbers that are simple to enter and easy to guess.

B. 3. Standards and Interoperability

The wireless device manufacturers and content and application providers are working on common standards so that device and operating systems function seamlessly. Standards can play an integral role in providing a uniform entry point to legacy transaction systems. A standard interface would allow institutions to add and configure interfaces, such as wireless delivery, without having to modify or re-write core systems. Interoperability is a critical component of mobile wireless because there are multiple device formats and communication standards that can vary the users' experience.

B. 4. Wireless Vendors

Institutions typically rely on third-party providers to develop and deliver wireless banking applications. Reliance on third parties is often necessary to gain wireless expertise and to keep up with technology advancements and evolving standards. Third-party providers of wireless banking applications include existing Internet banking application providers and as well as new service providers specializing in wireless communications. These companies facilitate the transmission of data from the wireless device to the Internet banking application. Outsourced services may also include managing product and service delivery to multiple types of devices using multiple communication standards. Institutions that rely on service providers to provide wireless delivery systems should ensure that they employ effective risk management practices.

B. 5. Product and Service Availability

Wireless communication "dead zones" – geographic locations where users cannot access wireless systems – expose institutions and service providers to reliability and availability problems in some parts of the world. For some areas, the communications dead zones may make wireless banking an unreliable delivery system. Consequently, some customers may view the institution as responsible for unreliable wireless banking services provided by third parties. A financial institution's role in delivering wireless banking includes developing ways to receive and process wireless device requests.

Institutions may find it beneficial to inform wireless banking customers that they may encounter telecommunication difficulties that will not allow them to use the wireless banking products and services.

B. 6. Disclosure and Message Limitations

The screen size of wireless devices and slow communication speeds may limit a financial institution's ability to deliver meaningful disclosures to customers. However, use of a wireless delivery system does not absolve a financial institution from disclosure requirements. Moreover, limitations on the ability of wireless devices to store documents may affect the institution's consumer compliance disclosure obligations.

Wireless banking may expose institutions to liability for unauthorized activities if devices are lost or stolen. The risk exposure is a function of the products, services, and capabilities the institution provides through wireless devices to its customers. For example, the loss of a wireless device with a stored access code for conducting electronic fund transfers would be similar to losing an ATM or debit card with a personal identification number written on it. However, the risk to the institution may be greater depending on the types of wireless banking services offered (e.g., bill payments, person-to-person payments) and on the authentication process used to access wireless banking services.

Appendix C –Electronic Banking Customer Awareness Program

To ensure security in their e-banking transactions and personal information, customers should be oriented of their roles and responsibilities which, at a minimum, include the following:

1. Wireless Products and Services

a) Secure Password or PIN

- Do not disclose Password or PIN to anyone.
- Do not store Password or PIN on the mobile devise.
- Regularly change password or PIN and avoid using easy-to-guess passwords such as birthdays.

b) Keep personal information private.

- Do not disclose personal information such as address, mother's maiden name, telephone number, bank account number or e-mail address — unless the one collecting the information is reliable and trustworthy.

c) Keep records of wireless transactions.

- Regularly check transaction history details and statements to make sure that there are no unauthorized transactions.
- Review and reconcile periodical bank statements for any errors or unauthorized transactions promptly and thoroughly.
- Check e-mail for contacts by merchants with whom one is doing business. Merchants may send important information about transaction histories.
- Immediately notify the bank if there are unauthorized entries or transactions in the account.

d) Be vigilant while initiating or authorizing/ responding to transactions.

- Before doing any transactions or sending personal information, make sure that correct wireless banking number and message format is being used. Beware of bogus or "look alike" SMS messages which are designed to deceive consumers.
- Be particularly cautious while responding to a voice call that claims to be from a bank. Never give any personal information to such a caller.

f) Take special care of your mobile device.

- Do not leave your mobile device unattended. It may be used wrongfully by someone having access to your personal information and/or PIN.

f) Learn by heart and keep handy your account blocking procedures.

In case your mobile phone is snatched / stolen please immediately proceed with account blocking/theft reporting procedures. For this, you need to familiarize yourself with the procedures to be followed, learn by heart the number provided by your bank for the

purpose and either remember or keep handy the information (such as your mobile account number, CNIC number, secret question etc.) you may be required to complete account blocking procedures.

2. Other Electronic Products

a) Automated Teller Machine (ATM) and debit cards

- Use ATMs that are familiar or that are in well-lit locations where one **feels** comfortable. If the machine is poorly lit or is in a hidden area, use another ATM.
- Have card ready before approaching the ATM. Avoid having to go through the wallet or purse to find the card.
- Do not use ATMs that appear to have been tampered with or otherwise altered. Report such condition to the bank.
- Memorize ATM personal identification number (PIN) and never disclose it with anyone. Do not keep those numbers or passwords in the wallet or purse. Never write them on the cards themselves. And avoid using easily available personal information like a birthday, nickname, mother's maiden name or consecutive numbers.
- Be mindful of "shoulder surfers" when using ATMs. Stand close to the ATM and shield the keypad with hand when keying in the PIN and transaction amount.
- If the ATM is not working correctly, cancel the transaction and use a different ATM. If possible, report the problem to the bank.
- Carefully secure card and cash in the wallet, handbag, or pocket before leaving the ATM.
- Do not leave the receipt behind. Compare ATM receipts to monthly statement. It is the best way to guard against fraud and it makes record-keeping easier.
- Do not let other people use your card. If card is lost or stolen, report the incident immediately to the bank.

b) Credit cards

- Never disclose credit card information to anyone. The fraudulent use of credit cards is not limited to the loss or theft of actual credit cards. A capable criminal only needs to know the credit card number to fraudulently make numerous charges against the account.
- Endorse or sign all credit cards as soon as they are received from the bank.
- Like ATM card PINs, secure credit card PINs. Do not keep those numbers or passwords in the wallet or purse and never write them on the cards themselves.
- Photocopy both the front and back of all credit cards and keep the copies in a safe and secure location. This will facilitate in the immediate cancellation of the card if lost or stolen.
- Carry only the minimum number of credit cards actually needed and never leave them unattended.

- Never allow credit card to use as reference (credit card number) or as an identification card.
- Never give your credit card account number over the telephone unless dealing with a reputable company or institution.
- When using credit cards, keep a constant eye on the card and the one handling it. Be aware of the "swipe and theft" scam using card skimmers. A skimmer is a machine that records the information from the magnetic stripe on a credit card to be downloaded onto a personal computer later. The card can be swiped on a skimmer by a dishonest person and that data can then be used to make duplicate copies of the credit card.
- Do not leave documents like bills, bank and credit card statements in an unsecured place since these documents have direct access to credit card and/or deposit account information. Consider shredding sensitive documents rather than simply throwing them away. (Some people will go through the garbage to find this information).
- Notify the bank in advance of a change in address.
- Open billing statements promptly and reconcile card amounts each month.
- Do not let other people use your card. If card is lost or stolen, report the incident immediately to the bank.
- Do not disclose your Mobile Banking Pin (MPIN) to anyone.
- Regularly change the MPIN.
- Do not let other people use your mobile phone enrolled in a mobile banking service. If the phone is lost or stolen, report the incident immediately to the bank.
- Be vigilant. Refrain from doing mobile banking transactions in a place where you observe the presence of "shoulder surfers".
- Keep a copy of the transaction reference number provided by the Bank whenever you perform a mobile banking transaction as evidence that the specific transaction was actually executed.

Since customers may find it difficult to take in lengthy and complex advice, banks should devise effective methods and channels for communicating with them on security precautions. Banks may make use of multiple channels (e.g. banks websites, alert messages on customers mobile phone, messages printed on customer statements, promotional leaflets, circumstances when bank's frontline staff communicate with their customers) to enforce these precautionary measures.