Branchless Banking Regulations

For Financial Institutions desirous to undertake Branchless Banking

(Revised on July 12, 2016)

Banking Policy & Regulations Department
State Bank of Pakistan

The Branchless Banking Team	
Syed Irfan Ali	**syed.irfan@sbp.org.pk**
Shaukat Zaman	**shaukat.zaman@sbp.org.pk**
Azmatullah	**azmatullah@sbp.org.pk**
Rajesh Raheja	**rajesh.raheja@sbp.org.pk**
Nasreen Sohaib	**nasreen.akhtar@sbp.org.pk**
Rehan Masood	**rehan.masood@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 whereby the financial institutions lead the entire branchless banking program, all the responsibilities of program shall rest with the financial institution. 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 overall information 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 banks, 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 Systems & Electronic Fund Transfers Act 2007).

2 Definitions

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

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

Biometric Verification System or BVS, for the purpose of these Regulations, means technology enabled system (verifiable from NADRA or the relevant Government authority) that allows Financial Institutions to obtain biometric fingerprints of the customers at the time of opening of branchless banking account or conducting the branchless banking transactions;

"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. For the purpose of these Regulations, the terms branchless banking and mobile banking shall be used interchangeably and shall have the same meaning. 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 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 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;

"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;

"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, only Bank-led Model of BB is allowed.

3.1 Permissible Models

As stated above, only bank-led model of branchless banking is allowed which may be implemented in different ways. Firstly, it can be implemented either by using agency arrangements or by creating a joint venture (JV) between FI 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 branchless banking services in collaboration with a specific Telco or non-bank partner. This model can be JV-based or

implemented through specific agency agreements between the bank and its partner. 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/non bank entity 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/non banks or alternately, one telco/non-bank can have several one-to-one arrangements with many banks, provided that such arrangements are under proper agency /service level agreements.

One-to-many (1-∞) Model: In this model a bank offers branchless banking services to customers using mobile connection of any Telco. This model offers the possibility to reach to any bankable customer who has a mobile phone connection provided the bank has a priority SMS pipe to enable it to provide quick services. Further, the FI needs to rely upon its own branch network and bear all advertising/marketing expenses.

Many-to-many (∞-∞) Model: In this model many banks and many telcos/non banks join hands to offer services to all bankable customers. To provide enabling environment to the BB industry for interoperability of branchless banking services, the State Bank of Pakistan and Pakistan Telecommunication Authority (PTA) have issued Regulations for Mobile Banking Interoperability and Technical Implementation of Mobile Banking for banking and telecom industries respectively. These Regulations shall not only provide a level playing field for FIs and non-banks, but also introduce a neutral third party model where FIs and their partners can join hands together to create a sustainable mobile banking ecosystem.

This model offers the maximum connectivity and hence maximum outreach and is closer to the desired situation where all banks and all telcos shall be able to entertain each other's customers. All settlements related to interoperable mobile banking services shall take place in accordance with laws, rules and regulations issued and amended by SBP from time to time. FIs and the relevant partners intending to offer many-to-many services under BB umbrella shall refer to the aforesaid Regulations of SBP and PTA.

Alternate Channels: Branchless banking can also be done using agents other than Telcos like Exchange Companies, fuel distribution companies, Pakistan Post, chain stores etc. and using technologies not limited to mobile phone, 3G/4G spectrum, GPRS, POS terminals and internet banking etc. Further, the FIs can issue personalized ATM/debit cards to their branchless banking customers subject to the condition that such cards shall be used for domestic transactions only. However, FIs may offer international transaction facility on ATM/debit cards to Level 2 account holders.

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. Further, FIs may apply for an arrangement, which does not fall exactly under one of the above models. Such arrangements may be allowed by SBP 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 technology service provider's server (the balances shown on mobile phone etc. are merely a reflection of actual account balances). For this purpose, FIs shall have direct ownership of the branchless banking application platform.

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 the 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 can transfer funds to/from their BB account from/to their other BB/ regular bank accounts.
- **Account-to-Person Fund Transfer**: Customers can transfer funds from their BB account to other non-BB accountholders. The transaction limits and KYC requirements are explained in relevant section of these Regulations.
- **Person-to-person Fund Transfer:** Any person without a BB account can also transfer funds to any other non BB accountholder. The transaction limits and KYC requirements are explained in relevant section of these Regulations.
- **Cash-in and Cash-out:** Customers can deposit and withdraw funds to/from their BB account using a variety of options including bank-branch counters, ATM machines and authorized agent locations.
- **Bill Payments:** A BB account can also be used to pay bills for utilities (e.g. Gas, Electricity, Phone etc.) However, the amount of payment of utility bills shall not be counted as part of existing transaction limits allowed to **BB** accountholders. Bills can also be paid on agent locations by account holders and non-account holders.
- **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 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. These accounts can also be used to receive home remittances subject to existing laws and regulations.

In addition to above, the banks may offer any product/service to their customers through BB channels after formulation of BB Products Manual with the approval of the board and subject to compliance with all rules and regulations. However, FIs shall submit for SBP's information a copy of the products/services to be offered by them through BB channels thirty (30) days prior to its launch.

4 Risk-Based Customer Due Diligence

To optimize the gains of Branchless Banking and to extend financial services outreach to the unbanked 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. It may be noted that level 0 and level 1 BB accounts are for individuals only while level 2 accounts can be opened by individuals as well as by joint accounts**,** firms, entities, trusts, Not-for-profit organizations, legal person, merchants, businesses, banking agents, technology service providers and corporations etc.

FIs are allowed to maintain branchless banking customer accounts as remunerative accounts in order to encourage opening of more accounts. For this purpose, FIs shall develop a remuneration mechanism for all Levels of BB accounts.

The KYC requirements, transactional limits, process and minimum technological security requirements applicable to all three levels of accounts are tabulated below.

*4.1 Basic/Entry Level Branchless Banking Accounts**

Account Level	**Level 0**	**Level 1/Biometric Account**
Description	Basic BB Account with low KYC requirements and low transaction limits.	Entry Level account with adequate KYC requirements commensurate with transaction limits.
KYC/Account Opening requirements /conditions	1. Capturing of image of customer's original CNIC. 2. Capturing of Digital photo of the customer. 3. Opening of account and acceptance of terms and conditions by the customers through physical or digital means. 4. Transfer of customer's data to FI. 5. Verification of customer's particulars from NADRA. 6. Allowing one deposit and one withdrawal transaction during account opening.	1. Capturing of image of customer's original CNIC. 2. Confirmation of customer's cell phone number. 3. Capturing of image of customer's original CNIC. 4. Physical/Digital Account Opening Form. 5. Acceptance of terms and conditions by the customers through physical or digital means. 6. Transfer of customer's record to FI. 7. Verification of customer's particulars from NADRA. 8. Allowing three deposits and one withdrawal transaction during account opening. **Note:** In case of accounts opened through Biometric Verification System (BVS), conditions mentioned at Serial Nos. 1, 3, 6, 7 and 8 shall not apply.
Transaction Limits	Rs. 25,000 per day Rs. 40,000 per month Rs.200,000 per year	Rs. 50,000 per day Rs. 80,000 per month Rs.800,000 per year
Maximum Balance Limits	Rs. 200,000	Rs. 400,000

* The transaction limits shall be treated separately for both payments and receipts on BB Accounts.

Further, FIs can also open accounts of the customers through biometric verification system deployed at agent locations subject to the above transaction and balance limits:

4.2 Top Level Branchless Banking Account

Account Level	**Level 2**
Description	All accounts opened by bank subject to full KYC requirement according to the risk profile of the customers.
KYC/Account Opening requirements /conditions	1. The account shall be opened in a bank branch. 2. Filling and signing an Account Opening Form. 3. Fulfillment of all KYC requirements specified under AML/CFT Regulations and Guidelines issued by SBP as amended from time to time and bank's own policy. 4. Customer profiling for identification and monitoring of associated risks. 5. The bank shall carry out due diligence or enhanced due diligence keeping in view the risk profile of the customers as per bank's policy. However, the bank shall invariably carry out enhanced due diligence for BB Agents.
Transaction Limits	As defined by the FI keeping in view FI's own capacity to monitor activities in such accounts.

In line with National Financial Inclusion Strategy to promote financial inclusion in the country, it has been decided to allow opening of remote accounts for Level 0 customers. For this purpose, the bank shall, initially, launch a pilot project for a period of three months. After the pilot project, the FI shall share the results with SBP 07 days prior to final launch. It may be noted that transaction and balance limits for remote account's customers shall remain the same as allowed under Level 0. Further, the FI shall ensure that:-

1. Account of the customer shall be opened against verified SIM Card.
2. Customers have accepted terms and conditions for opening of account.
3. Mobile number shall remain in the name of same person, who is requesting to open the account.
4. Customer shall visit bank branch / agent for initial cash deposit.
5. Verification of particulars of customers.

4.3 Funds Transfers

In addition to account-to-account funds transfers, the KYC requirements, transactional limits, process and minimum technological security requirements applicable to funds transfer service for Account to Person and Person to Person are tabulated as given below:-

	Account-to-Person Person -to-IBFT	**Person-to-Person**
Description	Fund Transfers by BB accountholder to other persons (non- accountholders)/Non-Accountholders to Inter Bank Fund Transfers (IBFT).	Person-to-Person (Non-accountholders) fund transfers. Persons availing this service shall be registered by the FI after due verification process for subsequent transactions.
KYC requirements/ conditions	1. Image or copy of person's original CNIC. 2. Mobile number of the person. 3. Purpose of remittance of transaction shall be recorded. Note: Requirements mentioned at serial No. 1 shall not be applicable after biometric verification of the person.	1. Image or copy of remitter and beneficiary's original CNIC. 2. Mobile numbers of remitter and beneficiary. 3. Attachment of CNIC and mobile number of customer for authenticity of transaction. 4. Verification of CNIC of at least 20% customers from NADRA. 5. Purpose of remittance of transaction shall be recorded. Note: Requirements mentioned at serial No 1, 3 and 4 shall not be applicable after biometric verification of the sender and receiver.

The registered customer shall not be able to avail other branchless banking services except utility bills payment.

Transaction Limits	Rs. 50,000 per month* (With BVS of person).	Rs. 50,000 per month**(With BVS at both sender and beneficiary end)

**Without BVS, the limit of transaction shall remain at Rs. 25,000/- per month.*

*** Without BVS, the limit of transaction shall remain at Rs. 15,000/- per month.*

FIs shall document process flow for all types of transactions as a part of their policy.

The FIs are advised to pace up deployment of biometric machines at agent locations, as the transactions for Over the Counter (OTC) without biometric verification shall remain applicable up to June 30, 2017. For this purpose, FIs are advised to update SBP on monthly basis as per following pattern with effect from September, 2016 till 10th day of following month.

No of Exclusive Agents	No of Non-Exclusive Agents	No of Exclusive Agents with Biometric Device	No of Non-Exclusive Agents with Biometric Device.

Keeping in view the Levels of BB account, the transaction limits allowed and the risk profile of each customer, the FIs' system shall carry out effective due diligence of customers on a continuous basis. For this purpose, FIs must ensure that they have transaction monitoring

system, which is capable of imposing transaction limits associated with each level of customer for both biometric and without biometric accounts as mentioned above.

FIs shall adhere to all requirements related to KYC and AML/CFT stipulated in relevant laws, regulations and instructions issued and amended from time to time including but not limited to availability of BB transaction monitoring system capable of producing meaningful alerts for identifying abnormal/ unusual/out of pattern transactions.

Minors may open a Level - 0, Level 1 or Level - 2 accounts provided their parent/guardian submit a written undertaking to accept any liability arising out of the action(s) of the minors.

Further, the requirement of sending biannual statement of account to the accountholders does not apply to BB accounts. However, accountholders should have an option to view at least the last five (05) 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 the past 12 months).

5 Key Roles & Responsibilities

The ultimate responsibility for branchless banking lies with the FI. FI may, however, take steps it deems necessary to safeguard it 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 laws, 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 of the FIs 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 laws, rules, regulations, policies 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 Use of Technology Service Providers

As opposed to the BB agents, technology service providers provide services related to technological infrastructure etc. Technology service provider shall not perform activities that are attributed to BB agents unless they sign separate agreements with the FI(s) to become BB agents.

While dealing with service providers, FIs should follow 'Guidelines on Outsourcing Arrangements' issued by SBP vide BPRD Circular No. 9 dated July 13, 2007. For this purpose, a proper service level agreement must be put in place for all third-party service arrangements.

7 Risk Management Program

Branchless banking under bank-led model entails two major categories of risks including agent-related and technology-related risks. The FIs need to pay special attention to these risks and consider the branchless banking risk management as a part of FI's overall risk management program. The agent related risks have been covered separately in "Framework for BB Agent Acquisition and management" issued by SBP vide BPRD Circular No. 06 dated June 21, 2016.

The FIs should tailor, adapt and expand overall risk management principles to address the specific risk management challenges created by the characteristics of BB activities.

7.1 Technology related Risks & their Management

During last few years, technology adoption has shown a great momentum and spread at an unbelievable pace across Pakistan. This section of the Regulations is on technology risks with particular emphasis on information, data, software and hardware security based on applicable models of branchless banking. Technology related risks should be recognized, addressed and managed by FIs in a prudent manner. FIs intending to offer branchless banking services shall develop Information Security or IT Security Policy (aligned with FI's overall IT Security Policy) and the same shall be approved by Board of Directors of the FI or its designated authority.

7.2 General Considerations:

i. FIs should, at all times, monitor safety, security and efficiency of their systems' components.
ii. Any security procedure adopted by FIs shall be covered under the existing legal framework of the country.
iii. When assessing compliance with the security recommendations, the FI shall take into account compliance with the relevant international standards.
iv. FIs shall put in place risk based information/data security requirements as well as channels like mobile phones, SMS, USSD, mobile applications, 3G or 4G, WAP, SAT etc. based on the risk associated with each Level of branchless banking account of the customers.

7.3 Risk Management and IT Security Measures

FIs should develop, document, implement and regularly review a formal comprehensive IT security Framework and Policy for their BB systems. The security policy and related control document(s) shall define Security Objectives, Risk Appetite, Risk Assessment both prior and post establishment of services on regular basis, risk identification at every stage of the processes, risk control, risk monitoring and mitigation at every layer and component of the system.

Further to monitor and assess the risks involved in their operations, FIs shall implement security policies and adequate security measures, contingency, incident management and business continuity measures commensurate with the risks inherent in the operations and services being provided.

FIs shall implement security measures in line with their respective security policies in order to mitigate identified risks and comply with the following:-

i. FIs shall employ multiple and layered security tools e.g. Firewall and Intrusion Detection and Prevention Systems, Up-to-date Antivirus Software, Anti-spam and Anti-spyware programs to protect each area against abuse or attacks.
ii. All security measures shall be tested and audited under the supervision of an independent function.

iii. In designing, developing and maintaining products and services, FIs shall pay special attention to the adequate segregation of duties and access rights of resources in information technology (IT) environments to avoid explicit control on their IT systems.
iv. FIs shall keep the systems up to date on all recommended patch serving and security updates after thoroughly testing its effectiveness and impact and also recommend their customers to follow the same practice, wherever required, to protect their end.
v. In order to ensure non-repudiation, accountability, transactional web offering services shall employ authentic and valid third party certificates.
vi. FIs shall implement mechanism and tools to consistently monitor and restrict access to resources such as data, networks, systems, databases, applications, operating systems, security modules, etc. and create, store and analyze appropriate logs and audit trails. User profile, user transaction pattern shall be provided high level of confidentiality and integrity.
vii. FIs shall provide security tools (e.g. tokens, encryption tool, devices and/or properly secured customized browsers) to protect the customer interface against unlawful use/ attacks.
viii. FIs shall ensure that all the activities and transactions are recorded in logging system(s), which remain under the administration of a unit different from the operations or IT.
ix. FIs shall provide adequate and regular information to the customers about necessary requirements for performing secured transactions.
x. The access and initiation of transactions shall be protected by strong and tamper resistant authentication, encryption and authorization to ensure confidentiality of the data and process.
xi. Transactions such as deposit, withdrawal, payment or transfer of cash from or to an account shall be real time.
xii. In case of error, system failure, or any service outage or other defects, the suspended or incomplete transaction(s) shall be reversed and proper information shall be communicated to the customers conducting transactions.
xiii. Obtaining access to or amending sensitive customer or transactional data shall require authentication and authorization.
xiv. FIs shall define and implement rules for management of PIN/Password standards, expiry, failed authentication limits, account locking and unlocking policy and process, time outs for idle, valid or active sessions.
xv. FIs shall ensure high availability of services in normal and unusual circumstances.
xvi. Physical and logical access to information systems (hardware and software) shall be under proper controls to avoid illegitimate access of unauthorized persons.
xvii. FIs shall make efforts to create awareness among customers on possible consequences of storing PIN on mobile devices.

8 Customer Protection, Awareness and Complaint Handling

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

FIs shall devise and enforce effective complaint handling and consumer awareness policy keeping in view the instructions of BB Regulations and BC&CPD Circular No.4 of 2014 on Financial Consumer Protection. Further, FIs shall ensure strict adherence to Guidelines on Consumer Grievance Handling Mechanism issued in terms of BC&CPD Circular No. 1 of 2016 and all other related instructions of SBP issued and amended from time to time.

8.1 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, proper internal controls should be put in place against mis-selling of this loss insurance.

8.2 Customer Awareness

Customer awareness is a key defense against fraud, theft and security breach. Customer awareness program, at a minimum, should cover use of Branchless-Banking account, protection against frauds, blocking procedure for SIM/account in case mobile is lost / snatched.

To be effective, banks should implement and continuously evaluate their customer awareness program. FIs should provide guidance to customers, where needed, on an ongoing or, where applicable, instant basis, and via appropriate means and clear instructions in a language of the customer's choice, such as:

a. information on any requirements and use of customer equipment, software or other necessary tools for the use of their services.
b. guidelines for proper and secure use of personalized security credentials.
c. description of the procedure for the customer to submit and authorize transaction and/or obtain information and consequences of each action.
d. Customer assistance through written, voice, tutorials or in-person communication should be made available by FIs for all questions, complaints, requests etc.
e. Initiating customer education and awareness programs about security issues, rights and obligations enabling customers to use their services safely and efficiently.
f. Educating customers as well as employees about security measures for fraud prevention and use of unsecure wireless networks.

8.3 Complaint Redressal

Each FI willing to offer BB must put in place a proper complaint redressal mechanism for efficiently and quickly disposing of complaints received from BB customers. The mechanism, at a minimum, shall include:-

- 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 the complaint number and estimated time for its disposal.
- Redirecting the complaint to appropriate function for disposal.
- Keep track/logs 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 and at agents' locations in the form of banners or brochures.

9 Branchless Banking Procedures

9.1 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.

9.2 Authorization

1. FIs wishing to provide branchless banking services or to bring in substantial changes in underlying technological infrastructure shall submit to the SBP, 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.

    The application shall accompany a copy of (i) business Plan for BB operations (ii) organogram of the division/department responsible for BB operations (iii) Manpower Planning (iv) a brief description of the system to be used for BB operations (v)

policies and manuals on BB operations (vi) contingency and disaster recovery plans for BB operations (vii) Agent liquidity management procedures.

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:

        a. Minimum capital requirement.
        b. Satisfactory solvency, liquidity and profitability positions.
        c. "Fair" CAMELS composite rating as per last inspection report of FI.
        d. "Fair" rating of systems and controls component as per last inspection report of FI.
        e. There are no outstanding major findings/exceptions noted in the latest SBP inspection report.

3. Based on the review, an in-principle approval of the application will be granted.

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

5. After completion of the pre-launch/ pilot run period/project, banks shall submit to the SBP, the following documentary requirements for evaluation:

    a. Compliance status on the terms and conditions conveyed at the time of grant of principle approval duly signed by Head of Compliance.
    b. Details of products offered through BB channel during test run.
    c. Business targets versus actual achievements during pre-launch period.
    d. Copy of contract(s)/SLAs/ maintenance agreements etc. with the Service providers and/or BB agents.
    e. Internal audit report on the pre-launch review of the BB operations.

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 documentary evidence relating to the issue.

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

8. FIs 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 period within which, they will 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 –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.