Branchless Banking Regulations

For Financial Institutions desirous to undertake Branchless Banking

(Revised on December 30, 2019)

Banking Policy & Regulations Department
State Bank of Pakistan

Table of Contents

1 Introduction

1.1 Background

a) **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.

b) 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

a) The objectives of these 'Branchless Banking Regulations' are:

i) To define Branchless Banking activities as a new delivery channel to offer banking services in a cost effective manner.
ii) To broadly outline activities which constitute BB and to provide a framework for offering BB services.
iii) 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

a) These Regulations are applicable to Commercial Banks, Islamic Banks and Microfinance Banks (MFBs) (herein after collectively referred to as banks, financial institutions or FIs).
b) Activities outlined in these Regulations as branchless banking cannot be offered by any person or institution other than Authorized Financial Institutions (AFIs).
c) All FIs desirous to offer branchless banking services may do so in line with these Regulations.
d) 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.

e) 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

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

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

c) 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 biometrics of the customers at the time of opening of branchless banking account or conducting the branchless banking transactions;

d) "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;

e) "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;

f) "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;

g) "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;

h) "**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:

i) 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;

ii) 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;

iii) without prejudice to paragraph (ii), by way of security for the delivery of or return of any property whether in a particular state of repair or otherwise; and

iv) in such other circumstances as may be specified by the State Bank in regulations made by it;

i) "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 an electronic device that may be used for making payments or as may be prescribed by the State Bank;

j) "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;

k) "Financial Institution" or "FI" means Commercial Banks, Islamic Banks and Microfinance Banks;

l) "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;

m) "Person" includes a legal person or a body of persons whether incorporated or not;

n) "Prescribed" means prescribed under applicable rules, circulars, directions, orders or bye-laws;

o) "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

a) 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

a) 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.

b) **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.

c) **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.

d) **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.

e) **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

a) Under these Regulations, following products/services may be offered:-

i) **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.

ii) **Account-to-Account Fund Transfer:** Customers can transfer funds to/from their BB account from/to their other BB/ regular bank accounts.

iii) **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.

iv) **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.

v) **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.

vi) **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.

vii) **Merchant Payments:** Customers can use a BB account to make payments for purchases of goods and/or services.

viii) **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.

ix) **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.

b) In addition to above, FIs 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

4.1 Risk Assessment and Mitigation

a) Authorized Financial Institutions (AFIs) shall take appropriate steps to identify, assess, and understand their Money laundering/ Terrorist Financing (ML/TF) risks for customers, geographic areas they operate in, products & services they offer, and the delivery channels being utilized. This shall include:-
   i) Document their risk assessments;
   ii) Consider all the relevant risk factors before determining what is the level of overall risk and the appropriate level and type of mitigation to be applied;
   iii) Keep these assessments up-to-date; and
   iv) Have appropriate mechanisms to provide risk assessment information to competent authorities.

b) AFIs shall formulate a risk matrix to assess ML/TF risks including threats, vulnerabilities, effectiveness of related controls and residual risks. This exercise shall be conducted on yearly basis keeping in view country's National ML/TF Risk Assessment and overall risk profile of Branchless Banking (BB) operations.

c) AFIs shall:
   i) Have policies, controls and procedures, which are approved by senior management, to enable them to manage and mitigate the risks that have been identified.
   ii) Monitor the implementation of those controls and to enhance them if necessary; and
   iii) Take enhanced measures to manage and mitigate the risks where higher risks are identified.
   iv) Develop risk-based scenarios on the results of risk matrix for monitoring and reporting all suspicious transactions to Financial Monitoring Unit.

4.2 Simplified Due Diligence for Branchless Banking (BB) Operations

a) AFIs shall adopt simplified due diligence procedures for opening of BB accounts to extend benefits of financial services to common people especially unbanked/under banked segments of population through agents and alternate delivery channels. However, AFIs shall not adopt Simplified Due Diligence measures in following situations:
   i) When there is a suspicion of money laundering or financing of terrorism;
   ii) In case of certain high risk factors are identified by SBP, by AFIs in its own internal risk assessment or as per international standards viz-a-viz FATF Recommendations etc.
   iii) In relation to customers that are from or in jurisdictions which have been identified for inadequate AML/CFT measures by FATF or identified by the bank itself having poor AML/CFT standards or otherwise identified by the SBP.

b) For the purpose of Simplified Due Diligence, AFIs shall :
   i) Categorize BB accounts in two levels including level-0 and level-1. It may be noted that BB accounts are for individuals only and shall not be opened in the name of legal persons and legal arrangements; high-risk customers and high-risk geographies as identified by the AFI in the process of internal ML/TF risk assessment.
   ii) Onboard and monitor agents as per criteria laid down in "Framework for Branchless Banking Agent Acquisition & Management' issued vide BPRD Circular No 06

dated 21st June, 2016, amended from time to time. Further, agent accounts including other existing level-2 account holders shall be treated as full-fledged KYC/CDD accounts and are subject to SBP's AML/CFT Regime as amended from time to time.

iii) Not open BB accounts on behalf of other individuals. Further, AFIs shall not allow operation in these accounts to any individual on behalf of the account holder.

iv) Apply simplified Customer Due diligence (CDD) measures for level-0 and level-1 accounts, where they have identified lower risks through adequate risk analysis. The simplified CDD measures shall commensurate with lower risk factors and these procedures shall not be applicable on specific higher risk scenarios.

v) Verify the identity of the customers before opening of their accounts.

vi) Not keep anonymous accounts or accounts in obvious fictitious names.

vii) Undertake CDD measures when they have doubts about the veracity or adequacy of previously obtained customer identification data.

viii) Understand and, if required, obtain information on the purpose and intended nature of the business relationship.

ix) Not allow agents to perform elements of CDD measures including identification of the customer, identification of the beneficial owner and understanding the nature of business to introduce business etc. as set out in SBP's AML/CFT regulations issued from time to time. In this context, the role of BB agent is only limited to facilitate the customers to forward their information to concerned AFI through electronic channel. AFIs shall conduct all measures of CDD at their end.

x) Apply CDD requirements to existing customers on the basis of materiality and risk, and to conduct due diligence on such existing relationships at appropriate times, taking into account whether and when CDD measures have previously been taken and adequacy of data obtained.

xi) Not open account where it is unable to comply with relevant CDD measures at the time of account opening.

xii) Not conduct the transaction; and terminate the business relationship; and file Suspicious Transaction Report (STR) in relation to the customer, where it is unable to comply with relevant CDD measures at the time of performing the transaction of customers.

xiii) Not pursue the CDD process and instead shall file STR, where AFIs form a suspicion of money laundering or terrorist financing, and they reasonably believe that performing the CDD process will tip-off the customer.

xiv) Scrutinize transactions undertaken throughout the course of the relationship through Automated Transaction Monitoring System (ATMS) to ensure that the transactions being conducted are consistent with FIs' knowledge of the customers, their business and risk profile, including, where necessary, the source of funds; and report suspicious transaction including attempted transactions to Financial Monitoring Unit (FMU) as per law.

4.3 Types of BB Accounts

The KYC requirements, transactional limits, record retention and AFIs responsibilities applicable to 'level 0'and level '1' accounts are tabulated below:

Account Level	Level 0	Level 1
1.Description	Basic BB Account with low KYC requirements and low transaction limits.	Entry Level account with simplified KYC requirements commensurate with transaction limits.

<table>
<tr><td>2. KYC/Account Opening Mandatory requirements /conditions</td><td>a) Verification of customer identity from NADRA
b) Pre-screening the name and CNIC against proscribed/designated persons and entities as per the Statutory Notifications issued by Federal Government from time to time.
c) Call Back Confirmation or generation of One-Time Password (OTP) for verification in remote account opening.</td><td>a) Biometric Verification of customer from NADRA
b) Pre-screening the name and CNIC against proscribed/designated persons and entities as per the Statutory Notifications issued by Federal Government from time to time.
c) Call Back Confirmation or generation of One-Time Password (OTP) for verification in remote account opening.</td></tr>
<tr><td>3. Process Flow</td><td colspan="2">a) AFIs shall develop Account opening process flow and any additional requirement as per their internal risk assessment.
b) AFIs shall invariably conduct BV of customers of other AFIs for fund transfers from their agent network.
c) Level-0 account holders cannot perform Account-to-Person transfers, Cash in, and cash out till their Biometric Verification (BV).
d) Level-0 can be upgraded to Level-1 account after biometric verification of customer from NADRA upon customer’s request</td></tr>
<tr><td rowspan="2">4.Transaction Limits</td><td>a. Rs. 25,000 per day
b. Rs. 50,000 per month
c. Rs. 200,000 per year
d. Rs. 200,000/- maximum balance limit</td><td>a. Rs. 50,000 per day [This limit shall not be applicable on: (i)credit from employers for salaried persons against proof of employment and (ii) payment to trusted merchants including schools and hospitals etc.]
b. Rs. 200,000 per month</td></tr>
<tr><td colspan="2">a. The transaction limits shall be treated separately for both payments and receipts on BB Accounts.</td></tr>
<tr><td>5.Record Retention</td><td colspan="2">a) AFIs shall keep all necessary record obtained through CDD measures, account files and business correspondence and results of any analysis undertaken, for at least ten years following the termination of the business relationship.
b) AFIs shall ensure that documents, data or information collected under the CDD process is kept up to date and relevant, by undertaking reviews of existing records.</td></tr>
<tr><td>6.Responsibilities of AFIs</td><td colspan="2">a) Verification of data received from customer and Agents.
b) Verification of customer’s identity from NADRA.
c) Verification of information and documents for account opening.
d) Pre-screen the particulars of customers against the proscribed/designated persons/entities.
e) Send account opening confirmation to the customer.
f) Ensure that no customer’s data and document is retained by the agent.</td></tr>
</table>

4.4 Domestic 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-Account	**Person-to-Person**
1.Description	Fund Transfers by BB accountholder to other persons (non-accountholders)/Non-Accountholders to BB Accountholders.	Person-to-Person (Non-accountholders) fund transfers.
2.KYC/ Account Opening Mandatory requirements/ conditions	a) Take Mobile number of the person. b) Record purpose of remittance of transaction c) Biometric verification of Person at the time of payment/receipt of Cash. At the time of cash collection or disbursement, Pre-screen the name and CNIC of remitter or beneficiary against proscribed/designated persons and entities as per the Statutory Notifications issued by Federal Government from time to time.	a) Take Mobile numbers of remitter and beneficiary. b) Record purpose of remittance of transaction. c) Biometric verification of remitter and beneficiary at the time of transaction At the time of cash collection & disbursement (in case of different AFIs agent), Pre-screen the name and CNIC of remitter and beneficiary against proscribed/designated persons and entities as per the Statutory Notifications issued by Federal Government from time to time.
Record Retention	a) AFIs shall keep all necessary record on transactions for at least ten years following completion of the transaction. b) AFIs shall maintain sufficient transaction record that can facilitate reconstruction of individual transactions so as to provide, if required, evidence of prosecution of criminal activity. c) AFIs shall keep record of all attempted transactions for at least ten years from the date of transaction.	
4.Transaction Limits for persons	Rs. 25,000/- per month separately for sender and receiver with effect from February 01, 2020. Further, AFIs shall gradually phase out Person-to-Person fund transfer latest by June 30, 2020.	

4.5 General Requirements

a) AFIs shall extend BB services to Afghan refugees holding Proof of Registration (PoR) after Biometric verification or NADRA Verisys as per the Branchless Banking Regulations requirement. For this purpose, AFIs may accept the valid PoR Card issued by NADRA as identity document Card.

b) AFIs shall maintain/ open remunerative as well as non-remunerative branchless banking (BB) accounts as per customer's request.

c) AFIs may open a BB accounts of minors provided their parent/guardian submit a written undertaking to accept any liability arising out of the action(s) of the minors.

d) AFIs are encouraged to place live BV devices for the verification of customers at agents' locations.
e) 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).
f) AFIs shall define dormancy of BB accounts in line with relevant AML/CFT Regulations issued and revised by the State Bank of Pakistan from time to time. However, dormant accounts shall be activated upon customer's request and successful BV.
g) ATM only or Debit Card issued against 'Level 0' accounts shall only be activated after BV of the customers, if not conducted previously.
h) AFIs shall satisfy, on timely basis, any enquiry or order from the relevant competent authorities including law enforcement agencies and FMU for supply of all CDD information and transaction records as per law.
i) AFIs shall comply with Electronic Fund Transfers (EFT) Regulations issued vide PSD Circular No. 03 of 2018 dated May 09, 2018, amended from time to time for domestic fund transfer conducted through BB channel.
j) AFIs shall deal with unclaimed deposits or uncollected transactions as per applicable laws.
k) AFIs shall ensure compliance with SBP's AML/CFT regulations/regime, updated from time to time, including those areas, which are not specifically mentioned in these Regulations.

5. Home Remittances

a) AFIs shall maintain separate limit for Home Remittance Account (HRA) as per instructions issued vide BPRD Circular No: 09 of 2017 dated December 22, 2017 and amended from time to time. ***(Annexure-A)***
b) AFIs shall not permit cross border outward remittance transactions from BB accounts.
c) AFIs shall ensure that Home Remittance above or equal to USD 1000 are always accompanied by the following:
    i. Originator information including:
        a. the name of the originator;
        b. the originator account number where such an account is used to process the transaction or, in the absence of an account, a unique transaction reference number which permits traceability of the transaction; and
        c. the originator's address, or national identity number, or customer identification number, or date and place of birth.
    ii. Beneficiary information:
        a. the name of the beneficiary; and
        b. the beneficiary account number where such an account is used to process the transaction or, in the absence of an account, a unique transaction reference number which permits traceability of the transaction.
d) AFIs shall ensure that all Home Remittance transfers below than USD 1000 are always accompanied by the following:
    i. Originator information including:
        a. the name of the originator; and
        b. the originator account number where such an account is used to process the transaction or, in the absence of an account, a unique transaction reference number

which permits traceability of the transaction.

ii. Required beneficiary information:
   a. the name of the beneficiary; and
   b. the beneficiary account number where such an account is used to process the transaction or, in the absence of an account, a unique transaction reference number which permits traceability of the transaction

e) The information mentioned in criteria (d) need not to be verified for accuracy. However, AFIs shall be required to verify the information pertaining to its customer, where there is a suspicion of ML/TF.

f) Where several individual Home Remittance transfers from a single originator are bundled in a batch file for transmission to beneficiaries, the batch file shall contain the required and accurate originator information and full beneficiary information that is traceable.

g) AFIs shall verify the information pertaining to its customer where there is a suspicion of ML/TF in a home remittance transaction.

h) If an intermediary financial institution is within Pakistan, it shall ensure that all originator and beneficiary information that accompanies Home Remittance is retained with it for a period of at least ten years following completion of the transaction.

i) Where technical limitations prevent the originator or beneficiary information accompanying Home Remittance from remaining with a related domestic electronic fund transfer, the intermediary financial institution within Pakistan shall keep a record, for at least ten years, of all the information received from abroad or another intermediary financial institution.

j) AFIs and intermediary financial institutions within Pakistan shall take reasonable measures, which are consistent with straight-through processing, to identify inward Home Remittance lack required originator information or required beneficiary information.

k) AFIs and intermediary financial institutions involved in Home Remittance transactions shall formulate risk-based policies and procedures for determining:
   i. when to execute, reject, or suspend a home remittance lacking required originator or required beneficiary information; and
   ii. the procedure for appropriate follow-up action.

l) AFIs shall take reasonable measures, which may include post-event monitoring or real-time monitoring where feasible, to identify Home Remittance lacking originator information or required beneficiary information.

6. Key Roles & Responsibilities

The ultimate responsibility for branchless banking lies with the AFI. AFI 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 AFI, 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.

6.1 Board of Directors

a) AFI'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.

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

6.2 Senior Management

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

b) 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.

c) BOD and Senior Management must ensure that the scope and coverage of their internal audit and compliance functions have been expanded to commensurate with the increased complexity and risks inherent in branchless banking activities and these departments are staffed with Personnel having sufficient technical expertise to perform the expanded role.

d) It is also incumbent upon the BOD and AFIs' 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.

6.3 Compliance Officer

a) AFI's Compliance Officer shall ensure that proper controls are incorporated into the system so that all relevant compliance issues are fully addressed.

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

6.4 Internal Auditors

a) AFI's Internal Auditors are responsible to ensure adherence to the laws, rules, regulations, policies and operational guidelines.

b) Internal Auditors shall undertake risk-based review of critical branchless banking processes to ensure that the policies, rules, regulations and the operational guidelines are followed.

c) Internal Audit shall also review the outsourced activities by taking appropriate direct or third party audits of the same as mandated under relevant outsourcing agreements.

d) Internal Audit shall escalate significant exceptions to the Audit Committee of the BOD.

6.5 Use of new technologies for Product Development

a) AFIs shall identify and assess the ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products.

b) AFIs shall:

i. undertake the risk assessments prior to the launch or use of such products, practices and technologies; and

ii. take appropriate measures to manage and mitigate the risks

7. Use of Technology Service Providers

a) 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 AFI(s) to become BB Agents.

b) While dealing with service providers, AFIs shall follow 'Framework for Risk Management in Outsourcing Arrangements by Financial Institutions' issued by SBP vide BPRD Circular No. 06 dated June 20, 2017 as amended from time to time. For this purpose, a proper service level agreement must be put in place for all third-party service arrangements.

8. Technology related Risks & their Management

a) 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, channel, software and hardware security based on applicable models of branchless banking. Technology related risks should be recognized, addressed and managed by AFIs in a prudent manner.

b) AFIs intending to offer branchless banking services shall develop Information Security or IT Security Policy (aligned with AFI's overall IT Security Policy) and the same shall be approved by Board of Directors of the AFI or its designated authority.

8.1 General Considerations:

a) AFIs should, at all times, monitor safety, security and efficiency of their systems' components.

b) Any security procedure adopted by AFIs shall be covered under the existing legal framework of the country.

c) When assessing compliance with the security recommendations, the AFI shall take into account compliance with the relevant international standards.

d) AFIs 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.

8.2 Risk Management and IT Security Measures

a) AFIs 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.

b) Further to monitor and assess the risks involved in their operations, AFIs 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.

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

   i. AFIs 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, AFIs 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. AFIs 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. AFIs 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. AFIs 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. AFIs 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. AFIs 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. AFIs 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. AFIs 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. AFIs shall make efforts to create awareness among customers on possible consequences of storing PIN on mobile devices.

9. Customer Protection, Awareness and Complaint Handling

a) 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 AFIs 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.

b) AFIs shall initiate outreach programs to encourage and educate walk-in customers to open 'level

-1' Account. This program should also encompass the basic knowledge about the available BB products of the banks to promote and enhance the level of financial literacy among the general masses. Further, AFIs shall take adequate measures for the capacity building of agents through trainings etc. especially in the area of ML/TF risks and its implications.

c) AFIs shall integrate BB transaction processing system with Fraud Detection System for early detection of fraud through BB channel latest by June30, 2020.

d) AFIs 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.

e) AFIs 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.

9.1 Customer Protection

a) Use of retail agents may also increase the risk that customers will be unable to understand their rights and process 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. AFIs should devise clear guidelines for customers regarding complaints and dispute resolutions and should make efforts to make these public.

b) AFIs 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.

c) 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.

9.2 Customer Awareness

a) 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.

b) To be effective, banks should implement and continuously evaluate their customer awareness program. AFIs 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:

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

9.3 Complaint Redressal

a) Each AFI 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:-
   i) Receiving and processing customers' complaints 24 hours through, SMS, IVR and email.
   ii) Generate acknowledgement of complaint giving it a unique complaint number.
   iii) Communicate acknowledgement to customer giving the complaint number and estimated time for its disposal.
   iv) Redirecting the complaint to appropriate function for disposal.
   v) Keep track/logs of all complaints and give status of every complaint.

b) 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.

10 Branchless Banking Authorization

10.1 Preparation

a) 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

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

b) 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:

i) 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. "Fair" CAMELS composite rating as per last inspection report of FI.
IV. "Fair" rating of systems and controls component as per last inspection report of FI.
V. There are no outstanding major findings/exceptions noted in the latest SBP inspection report.

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

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

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

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

f) 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.

g) Upon completion of evaluation, the Authorization will be granted.

h) 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.

Annexure "A"

Branchless Banking – Home Remittances Account (HRA)

Branchless Banking – Home Remittances Account (HRA)	
1. Objective	i. To facilitate swift and cost effective Home Remittances through Branchless Banking channel. ii. To increase financial inclusion through enhanced usage in Branchless Banking (m-wallet) accounts.
2. Applicability	i. All Branchless Banking (BB) provider banks including Commercial Banks, Islamic Banks and Microfinance Banks (MFBs) termed as Financial Institutions (FIs) or banks. ii. All individuals receiving Home Remittances through m-wallet accounts.
3. Eligibility	i. Only individuals can open these accounts on singular basis. ii. One CNIC holder can open only one HRA in a FI. iii. This account is meant for beneficiaries of home remittances i.e. individuals having Pakistani nationality only.
4. Nature of Account	i. Special Level 1 (L1) accounts tagged as Home Remittances Accounts (L1-HRA) or HRA. ii. The HRA could be new accounts or existing L1 accounts can also be tagged as HRA. iii. FIs shall use HRA as sub account under the main mobile wallet/ m-wallet i.e. Level 1 BB account (without any change in the account number) in order to keep track of remittance transactions and related privileges/limits. However, for the customers; this shall be seamless and single account. Further, AFIs can also use single account for both Home Remittances and inland transactions. In case of single account, AFIs shall keep track of transactions (Home Remittances & Inland) separately and implement controls related to privileges/ transactions limits on both types of transactions as per regulatory requirements iv. FIs shall offer these accounts as saving or any other remunerative category. v. These accounts shall be Mobile accounts to be served through BB Agents.
5. Account Holder Data	i. Simplified account opening form preferably electronic form. ii. In case of paper based forms, these forms should also be stored electronically in scanned form. iii. 3. Data/ information contained in these forms should also be stored at a centralized repository in a structured manner.
6. Account Opening Form	i. Account Opening Form (AOF) should be simple and cover basic customer information e.g. Name, Father/Spouse Name as written on CNIC, Date of Birth, Place of Birth, Mother's Maiden Name, CNIC Number, Mobile Number, Address, Occupation, Source of income, Purpose of Account and

	disclosure of international remittance locations, relationship with the originator, specimen signature, Next of Kin. ii. In case of more than one originator, the FI shall obtain information about all originators. iii. AOF should be available in Urdu and English. iv. Terms & Conditions (T&C) or any declaration should be simple, clear and legible in Urdu and English. v. One copy of AOF and T&C signed by customer should be provided physically or electronically to the customer as proof of account opening. vi. HRA can also be opened through Mobile App provided that the identity of customer shall be verified through Biometric Verification System (BVS).
7. Customer Due Diligence (CDD) Requirements	i. Identification and verification requirements as per BB Level-1 accounts. ii. In addition: a. NADRA's Biometric Verification shall be conducted at the time of opening of account to activate the HRA instantly. However, cost of such verification should not be passed on to the customer to encourage inflow of remittances. b. The FI shall ensure compliance of requirements for inward and outward wire/fund transfers outlined under AML/CFT Regulations and other laws as amended from time to time. c. The FI shall take necessary action(s) in accordance with law including filing Suspicious Transaction Reports (STRs) with FMU in case any unusual transaction/activity or high risk factor is observed.
8. Account Opening Point	i. BB agent having biometric device or Bank Branches. ii. Accounts may also be opened by the FI's permanent employee/staff through BVS by visiting customers' places of business/ residences.
9.Account Activation	Accounts may be opened and activated instantly after due diligence checks including biometric verification.
10. Transaction Limit Inflow of Home Remittance*	**Inward per day limit:** No Limit *(subject to maximum balance limit)* **Maximum balance limit:** PKR.1,500,000/- Credit in HRA can only be made through Home Remittances.
11.Transaction Limit Withdrawal of Cash*	**Total Cash withdrawal per Month:** Rs. 500,000/-
12. Cash withdrawal mechanism	At BB agent location/ home delivery after biometric verification or at bank branch.
13.Geographic Coverage	Nationwide
14.Initial Deposit and Minimum Balance Requirement	There shall be no initial deposit and minimum balance requirement on these accounts.

15.Account Statement	FIs shall provide electronic mini statement/statement of account on customers' demand and / or within the frequency set under relevant SBP requirements.
16.Conversion of existing m-wallet holders	i. Existing m-wallet holders intending to open HRA shall be required to undergo the one time registration process (to be designed by the FIs) including information on intended senders and relationship with beneficiaries and expected originating remittances countries. ii. The existing m-wallet holders who register for HRA through mobile application or other remote means shall be required to personally visit once to the nearby agent for face to face contact and for cash withdrawal from their HR Account. No debit transaction shall be allowed before the completion of the registration process. iii. The representative of FI can also visit the customer at his place for face to face contact.
17.FIs' Responsibility and Agent Management	i. FIs shall: a. Allow opening of HRA and related transactions only at those agent locations where biometric devices are available to serve the customers. b. Seek interest from agents and revise service level agreements with them where needed. c. Conduct enhanced due diligence of interested agents and continue effective on going monitoring including periodic audit of such agents. d. Reassess the liquidity capacity of the agent for serving HRAs and ensure availability of cash at agent locations. e. Ensure to protect customers' financial and non-financial data from leakage and misuse. f. Ensure that the agents are properly trained to serve the customers. g. Ensure that HRA will be fed with the proceeds of home remittances. h. Monitor these accounts in accordance with account purpose and customer profiles. i. Ensure that no service charges are recovered by FI at the time of opening and closing of an account. The matters like dormancy and activation of accounts, treatment regarding unclaimed deposits, prohibition of personal accounts for business purposes, updating of customers profiles, record keeping and reporting of suspicious transactions under the relevant law shall be governed under applicable rules/ regulations.
18.Home Delivery	i. For home delivery of remittances, FIs shall ensure additional controls and monitoring since it carries a risk of misappropriations. ii. FIs shall couple the home delivery service with real time SMS intimations to customer about amount of remittance received, withdrawn and the charges deducted. iii. FIs shall also maintain a separate MIS of such withdrawals, for quicker resolution in case any complaints that may arise.

19. Incentives to promote remittances	The incentive of airtime of Rs. 2 shall be provided against each USD received through M-Wallet. Further, the entire amount of incentive to HRA customers shall be borne by the Government of on account of technical up-gradation of their systems & operations for Financial Inclusion.
20. Consumer Protection & Financial Literacy /Awareness	Following steps will be taken: i. The call center of the FIs shall: a. update the sender as well as the receiver regarding the status of their remittances. b. manage complaint registration and ensure their redressal in shortest time period and as per regulatory requirements. c. spread consumer awareness through short messages. ii. FIs shall provide a dedicated line for HRA holders to contact call center representatives directly to get HRA related information. This line must have a facility to receive a direct call by call-representative upon identification of HRA customers thus to avoid call center hassles or customer waiting time while they being on calls. iii. In addition, PRI's customer facilitation and complaint management system would be available 24/7. iv. A mass media campaign will be launched to aware the masses regarding the benefits of the scheme. v. Special briefings will be arranged for immigrants at different departure points. vi. FIs shall provide instant electronic messaging service for Cash withdrawals by HRA holders at dedicated locations of FI.

* The transaction limits shall be on the aggregate balance of main as well as sub account. However, in case no foreign remittance is received, the amount of withdrawal will not increase the current limit

Annexure "B"–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.