Study Paper

# AML/CFT Regulations for Mobile Money

## Policy Options for Bangladesh

**Bangladesh Financial Intelligence Unit**
Bangladesh Bank
Dhaka, Bangladesh

# AML/CFT Regulations for Mobile Money

## Global Standards & Practices
## Risk & Trend
## Policy Options for Bangladesh

**Prepared by**
Focus Group
Bangladesh Financial Intelligence Unit

First Edition: May, 2017
Second Edition: April, 2018

# FOCUS GROUP

## CHAIRMAN

**Dr. Md. Kabir Ahmed**
General Manager, Bangladesh Bank
Former Deputy General Manager, Bangladesh Financial Intelligence Unit

## MEMBERS

**Mr. Md. Shah Alam**
Additional Deputy Inspector General, CID, Bangladesh Police

**Mr. Md. Ashraful Alam**
Deputy General Manager, Financial Inclusion Department, Bangladesh Bank; and
Former Chairman, SME Finance Working Group, Alliance for Financial Inclusion

**Lt. Colonel Mohammad Zulfikar**
Director, Bangladesh Telecommunication Regulatory Authority; and
Member, Focus Group on Digital Financial Services, International Telecom. Union

**Mr. Mohammad Abdur Rab**
Joint Director, Bangladesh Financial Intelligence Unit

**Mr. Debashish Sarkar**
Joint Director, Payment Systems Department, Bangladesh Bank

**Mr. Jayanta Kumar Bhowmick**
System Analyst (JD), IT Operation and Communication Department, Bangladesh Bank

**Mr. Mohammad Rokonuzzaman**
Joint Director, Financial Integrity and Customer Services Department, Bangladesh Bank

**Mr. Muhammad Omar Sharif**
Deputy Director, Bangladesh Financial Intelligence Unit

**Mr. Md. Al-Amin Reiad**
Deputy Director, Bangladesh Financial Intelligence Unit

**Captain Saber Sharif (Retired)**
Head of Corporate Affairs and DCAMLCO, bKash Limited

**Mr. Mohammed Mesbahul Alam**
Deputy Head of Financial Inclusion Division, Dutch-Bangla Bank Ltd.

**Mr. A.N.M. Tawhidul Islam**
In-charge, Mobile Financial Services Dept., Islami Bank Bangladesh Ltd.

## COORDINATOR

**Mr. Md. Rashed**
Joint Director, Bangladesh Financial Intelligence Unit; and
Member, Focus Group on Digital Financial Services, International Telecom. Union
E-mail: md.rashed@bb.org.bd

**Cover Design**
Mr. Tariq Aziz, Assistant Director, DCP, Bangladesh Bank

Fazle Kabir
**Governor**

# BANGLDESH BANK
(Central Bank of Bangladesh)

## MESSAGE

It is my great pleasure to know that Bangladesh Financial Intelligence Unit (BFIU) is going to publish a Study Paper, titled "AML/CFT Regulations for Mobile Money: Policy Options for Bangladesh". The study has aptly identified the existing and emerging Money Laundering (ML)/ Terrorist Financing (TF) risks in the Mobile Financial Services (MFS) of Bangladesh and suggested policy recommendations to promote an effective and sustainable supervisory regime for MFS.

After decades of impressive economic growth, Bangladesh is seeking to move to the next level of prosperity fostering social and financial inclusion so that the benefits of growth can reach the country's rural and lower-income population. In this effort MFS has enabled us to serve the excluded, the under-served and the unbanked segments of the society. I believe that MFS platform will provide a variety of financial services to unlock and widen further economic opportunities for these segments of population in future. Any threat to this service may deter our broader financial inclusion and also the attaining of the objectives of sustainable development goals. Early detection of risks and vulnerabilities in this service is undoubtedly a praiseworthy effort for timely intervention.

I am glad that as BFIU is moving towards evidence based policy research this study is going to mark a significant step forward. The information, analysis and recommendations contained in the paper will be beneficial to policy makers, service providers, risk managers and researchers at home and abroad. BFIU has already issued a detailed AML/CFT circular for MFS and taken measures to prevent abuses of MFS for illegal delivery of foreign remittances based on the recommendations of the study. The efforts have already begun to yield significant positive outcomes. I hope that some other recommendations of the paper would be implemented phase by phase.

Finally, my heartfelt appreciation goes to the Focus Group for their endeavor to present such an insightful report that will contribute to build a secured, transparent and pro-poor digital finance platform.

(Fazle Kabir)

# BANGLADESH FINANCIAL INTELLIGENCE UNIT

Bangldesh Bank
Motijheel, Dhaka

## PREFACE

Financial Technology (FinTech) has brought incredible dynamism as well as new dimensions in financial services. FinTech opens up new opportunities to reach previously untapped market and serve large segment of customers with limited physical infrastructure. Mobile Financial Services (MFS) is one of the finest FinTech innovations in the last decade- reshaping the financial service delivery models especially in the developing economies. It has enabled the financial service providers to include the bottom of the pyramid population into formal financial services which was otherwise impossible.

MFS was launched in Bangladesh in 2011 and gained popularity within a short span of time. Total number of MFS accounts has crossed the fifty million mark in just six years making Bangladesh one of the fastest growing MFS markets in the world. It has brought revolutionary changes in local money transfer services where low income population is the main customer. Other services such as merchant payment and social benefit disbursement are gaining momentum in recent times.

However, any financial services including MFS are not insulated from potential abuses for illicit purposes. We have observed several typologies of abuse of MFS in our market. These are unique in nature compared to other financial services. Culprits are also innovating new techniques of fraud that make the task of regulators and law enforcement agencies more challenging. Perpetrators have been seen to use this service to receive and transfer proceeds of crime anonymously. In this context, Bangladesh Financial Intelligence Unit (BFIU) felt the necessity to conduct a detailed study on the risks and vulnerabilities of MFS in Bangladesh based on FATF standards by forming a Focus Group comprising regulators, government agencies and service providers.

The study has not only identified recent trend, typologies and emerging risks but also put forward policy recommendations to be implemented by BFIU, Bangladesh Bank and other concerned agencies. It has laid down a clear direction to service providers regarding regulatory expectations on AML/CFT risk management. I am confident that the Paper would be guiding principles for AML/CFT regulations and supervision of MFS in the next couple of years.

I would like to urge all the stakeholders, concerned regulatory agencies and service providers to grasp the maximum benefit of this study. Finally, I extend my heartfelt thanks to the members of the Focus Group who had done the tremendous and valuable job for the MFS arena.

**Abu Hena Mohd. Razee Hassan**
Head of BFIU & Deputy Governor

# ACKNOWLEDGEMENTS

The Focus Group has received valuable inputs from colleagues of Bangladesh Bank and other stakeholders as well. Their constructive suggestions, thoughtful discussion as well as feedback were essential to complete the study successfully. We would like to take this opportunity to thank and express our gratitude to them.

We are grateful to the Executive Director and Deputy Head of BFIU Mr. Muhammad Mijanur Rahman Joddar for his encouragement and guidance to expedite the publication of this study paper. We owe to former Executive Directors Mr. Mohammad Naushad Ali Chowdhury and Mr. Subhankar Saha; Consultant Mr. Debaprosad Debnath, late General Manager Md. Nasiruzzaman and General Manager Ms. Lila Rashid of Bangladesh Bank for their overall support.

We would also like to specially recognize the contributions of Mr. Kamal Hossain, Mohammad Shafikul Imdad, Md. Khairul Anam, Md. Ikramul Hasan, Md. Azmal Hossain and Md. Hedayetullah of BFIU; Ms. Prajna Paramita Saha of Payment Systems Department and Md Iqbal Hossain of Banking Regulation and Policy Department for their feedback on the draft report. Our especial thanks to Mr. Mirza Abdullahel Baqui and Md. Mahbubul Alam of Bangladesh Police; and Hisham Uzzaman Chowdhury of bKash Ltd. for their valuable inputs during Focus Group discussion.

# TABLE OF ACRONYMS

| | |
|---|---|
| AML | Anti-Money Laundering |
| AOF | Account Opening Form |
| ATA | Anti-Terrorism Act |
| ATr | Anonymous Transaction |
| BB | Bangladesh Bank |
| BDT | Bangladesh Taka |
| BFIU | Bangladesh Financial Intelligence Unit |
| CAMLCO | Chief Anti-Money Laundering Compliance Officer |
| CDD | Customer Due Diligence |
| CFT | Combating Financing of Terrorism |
| CICO | Cash In – Cash Out |
| C-KYC | Centralized KYC |
| FinTech | Financial Technology |
| INR | Interpretive Note of Recommendation 'X' |
| IP | Influential Person |
| KYC | Know Your Customer |
| MFS | Mobile Financial Services |
| M-money | Mobile Money |
| MFSP | Mobile Financial Services Provider |
| ML | Money Laundering |
| MLPA | Money Laundering Prevention Act |
| NID | National Identity Document |
| NPPS | New Payment Products and Services |
| NPSA | National Payment System Act |
| OTC | Over The Counter |
| PEP | Politically Exposed Person |
| PIN | Personal Identification Number |
| SAR | Suspicious Activity Report |
| STR | Suspicious Transaction Report |
| TF | Terrorist Financing |
| UNSCR | United Nations Security Council Resolution |

# TABLE OF CONTENTS

# TABLE OF CONTENTS

# TABLE OF CONTENTS

# EXECUTIVE SUMMARY

Access to financial system by the lower segment of the society is assumed as one of the seminal steps to establish a poverty free equitable society. Serving the poor through Mobile Financial Services is a much-praised agenda in the global development forum. Bangladesh is playing flagship role in using this vehicle to expedite investment activities of the poor through quick delivery of financial resources. However, like many other countries, the country is also experiencing abuse of Mobile Financial Services (MFS) for criminal purposes. Consequently, it has become necessary to address this issue from the regulatory and supervisory perspectives so that maximum benefits of this sector can be enjoyed by the stakeholders of the economy. To this end, Bangladesh Financial Intelligence Unit (BFIU) has formed a Focus Group with participation from the key stakeholders and industry practitioners. The Focus Group has developed this study paper in line with global standards and practices related with Anti Money Laundering and Combating Financing in Terrorism (AML/CFT) related regulations and provides policy recommendations for concern authorities of Bangladesh to promote an effective and sustainable supervisory regime for MFS.

**1.0 Global AML/CFT standards and practices for MFS**

FATF (Financial Action Task Force), the global standard setter for AML/CFT regulations, provides specific recommendations to minimize customer related risk as well as agent risk. To address customer level risk, they provide the following recommendations: (i) countries need to follow risk-based approach to address ML/TF risks for MFS. Depending on the degree of risk, limit needs to be imposed on the frequency and amount of transactions in m-money services. (ii) The countries should consider applying a "progressive" or "tiered" KYC approach whereby low transaction/ payment/balance limits could reduce ML/TF vulnerabilities. A point-based progressive KYC approach presumes that the more KYC evidence a customer is able to provide, the more the customer can be trusted. Services will be offered to an extent proportional to the identification provided. However, the lower risk circumstances will have to be confirmed based on a thorough and documented risk assessment. (iii) FATF assumes non-face-to-face business relationships or transactions as potentially higher risk categories. They suggest collection of verifiable identification information to minimize risk.

In branchless banking and mobile money business models, agents are viewed by the FATF as simply an extension of the financial services provider. The duties of the agents commonly include providing cash-in and cash-out services, account opening, customer care, perform specific AML/CFT checks, record-keeping and reporting obligations, etc. As the m-money provider maintains Customer Due Diligence (CDD) and comprehensive record of the transactions of customers, the main monitoring obligation should remain on the provider. In this respect, agent monitoring is viewed as a significant element in an effective AML/CFT program. FATF therefore suggests that institutions must scrutinize their agents closely and manage the potential ML risk by performing appropriate due diligence measures when engaging agents. It is also essential that the regulatory supervisors review MFS providers' oversight functions by examining the relevant policies, procedures and training. They

need to ensure that monitoring system of agents is put in place by the MFS provider along with inspection of a representative sample of retail outlets.

The World Bank has emphasized that some issues need to be addressed by the country policy makers while designing AML/CFT regulatory framework for mobile money. They suggest that countries should conduct risk assessment prior to drafting AML/CFT regulation for m-money activities. The assessment should aim to identify all role players in the jurisdiction, understand the products that are offered and are likely to be offered, and potential future patterns and trends. It should also assess the nature, types, and levels of ML/TF risk, identify the main vulnerabilities that are specific to m-money and address them accordingly.

AML/CFT guidelines for m-money services should be implemented through ongoing collaboration and dialogue between the public and private sectors. Customize guidelines to specific local circumstances and conditions considering the financial infrastructure of the country (both formal and informal sector), number of unbanked population with demographic composition, etc. is also equally important.

World Bank further suggests that AML/CFT regulatory framework should encompass a clear delineation of responsibilities between providers and agents. The regulators should consider drafting agency regulations or guidelines that delineate minimum provisions to be included in agency agreement, basic eligibility criteria, technical and operational requirements, limits of transaction, customer authentication procedures and agent network management, etc.

**2.0 Mobile money in Bangladesh**

Mobile money was introduced in Bangladesh in 2011 and earns rapid growth within a very short period of time. Bangladesh Bank has issued 19 licenses to commercial banks to rollout mobile money. Among them, 17 banks have launched their operation till December, 2016. The total number of registered clients is 41.08 million and daily average number and value of transaction are 4.46 million and BDT 7,737.90 million respectively as of December, 2016. The service is now even available to the poorest segment of the population and mainly serves as low value domestic money transfer system. Other types of services are also expanding slowly.

**Risk assessment for m-money in Bangladesh** has been conduced based on the risk matrix developed by FATF. Considering the m-money operational models, maturity and regulatory approaches of Bangladesh, some high risk elements have been identified. Due to absence of verification of customer's identity on the basis of reliable, independent source documents, data or information, CDD verification has been identified as high risk. CDD monitoring is also determined as high risk due to inadequate KYC; and effective monitoring of large number of micro transactions appear to be difficult. Absence of regulation on maximum amount of e-money stored per account and lack of enforcement on number of account per person creates a high risk scenario. Predominance of anonymous funding source (e.g. cash) and person to person transfer (P2P) also pose high risk. There

is strong evidence of abuse of MFS for illegal money remittance (hundi/hawala) in recent times which is blamed for downward trend of foreign remittance in Bangladesh. However, most of the high risk elements discussed above can be mitigated through effective regulation, enforcement and monitoring.

Recent trend of abuse of MFS in Bangladesh has also been analyzed as part of risk assessment. We have seen several ways of abuse of MFS such as collection of ransom for vehicle theft, abduction/ kidnapping; fraud by promising fake lottery prize, gift, job or hidden treasure from 'genier badsha'; marriage with expatriate bride; extortion by the name of top terrorists. In most cases, account with fake KYC or personal accounts of agents have been used by the criminals. In recent times, we have observed declining trend of foreign remittance in Bangladesh and DFS based hundi (Digital hundi) through MFS has been identified as one of the major causes of it. Ample opportunities of virtually anonymous transaction is contributing significantly for such criminal abuse of MFS.

There are several factors which are contributing for the abuse of m-money in Bangladesh. Agents acquire and register multiple SIM cards to conduct anonymous transaction (ATr) of the customers. Customers, having low academic qualification, find it difficult to navigate the mobile menu (in English language) required to conduct transaction. Customer acquisition based on previous falsely registered SIM along with lack of unique identification documents for all citizens and ID verification tools for the MFS providers; and inadequate monitoring mechanism for the agents are contributing heavily for the abuse of MFS.

## 3.0 Recommendations to strengthen AML/CFT regulations for MFS in Bangladesh

Based on the analysis of international standards, practices and local circumstances, Focus Group recommends the following policy options for the regulatory and supervisory authorities of Bangladesh:

### (a) AML/CFT compliance structure for MFS providers

All MFS Providers (MFSPs) should have their own AML & CFT Policy/Manual. MFS companies should set up a Central Compliance Committee (CCC) headed by a 'Chief Anti Money Laundering Compliance Officer' (CAMLCO). The CCC should consist of at least 5 (five) members who will be high officials of different departments. Banks, which are providing MFS within their existing organizational structure, should nominate an AML/CFT Compliance Officer for their MFS operation and include him in Central Compliance Committee (CCC). The CAMLCO or AML/CFT Compliance Officer should have at least 5 (five) years of experience on AML/CFT compliance. S/he should ensure compliance of AML/CFT policies/strategies of the organization. MFSPs which have more than 20 thousand agents or 01 million customers should form a separate AML/CFT Compliance Section/Wing (or whatever name it may be called) with adequate manpower in addition to CCC. MFSPs should nominate/appoint appropriate numbers of Field Compliance Officer (or whatever name it may be called) depending on the organizational structure of its operations who will monitor transactions of customer, agent and distributor accounts, compliance during account opening and submit STR/SAR, etc.

**(b) Regulations for personal account**

MFSPs should collect sufficient customers' information as per unique Account Opening Form. Physical presence of the customer in front of the agent/concern officer of MFSP is necessary except in permissible exception cases. At least a verifiable photo identification document issued by any government authority should be collected from the customer and verified by MFSP. The intended customer should have mobile SIM registered in his name and necessary verification should be made.

**Progressive KYC:** At least three types of information should be required for opening a MFS account. Required KYC information are: a) collection of information properly as per prescribed account opening form, b) Collection and verification of government issued photo identity document, c) recent photograph or real time electronic photograph of the customer, d) SIM registration information, e) presence of the customer at the customer care point of the MFSP, f) MFS account linked with any bank account of the customer and, g) biometric information as part of e-KYC. One point shall be created for each KYC information collected from a customer. If KYC information of an account receives three (3) points, it will be termed as **Level-1 account** and four/five (4-5) points recipient will be termed as **Level-2 account** and more than five (6-7) point recipients will be termed as **Level-3 account.** Based on the risk involved due to variation of quality of KYC discussed above, daily and monthly transaction limit and highest account balance should be determined by Bangladesh Bank.

MFS account can be linked with any existing bank account of the same customer upon request. Additional KYC should not be required for the Link Account, if both the accounts are operated within the same bank or with subsidiary of the same bank. Both inward and outward transfer can be done between bank and MFS A/C. A customer should not operate more than 01 (one) personal account in a MFS platform. However, an individual may not has a government issued photo identity document (i.e. age below 18 years) but need an MFS account. In such cases, one of his/her 'relative' may introduce while opening an MFS account and KYC of both persons would be necessary. Non-resident Bangladeshis and foreign nationals living in Bangladesh may open MFS account with copies of valid passport and visa.

**(c) Regulations for impersonal/merchant/institutional account**

Any entity or organization may open MFS account for its operational/business purposes. Information of the organization and relevant individuals along with specific documents should be collected as per specific Forms for opening such accounts. Higher transaction in such accounts would require additional KYC information and those should be linked with a bank account of the organization. Physical verification of the business premise of the customer along with transaction profile should be collected. However, MFSP should implement Risk Based Approach (RBA) and take additional measures as appropriate to monitor transaction in such accounts.

**(d) Regulations for agents and distributors**

MFSPs should collect information and documents described in specific Forms as minimum requirements while opening an agent/distributor account. MFSPs should collect NID of relevant

individuals and trade license of the business premise along with other information/documents. MFSP should conduct visit of the business premise of the agent/ distributor before appointment and verify information/documents. Agents should have knowledge and skills to comply with AML/CFT compliance requirements and at least one day long training should be provided to them. MFSPs should report rogue customers/agents to Bangladesh Bank and one central depository should be developed and shared with MFSPs. Any customer/agent blacklisted in the database should not be appointed as agent/distributor.

Risk assessment procedures for agents and distributors should be developed by the MFSPs based on volume of business, geographical location, previous records and any other information available to the MFSP and apply CDD/EDD accordingly. MFSPs should develop automated mechanism for monitoring of transactions of agent and distributor account and should ensure that every agent point and distributor office is visited at least once in every year. One agent should not maintain more than one agent A/C and one personal A/C in his/her name. MFSP should develop operational procedures in line with circular/guidelines of regulatory/supervisory authorities regarding selection and monitoring activities of agents and distributors.

MFSPs should develop own policies and procedures to conduct on-site inspections covering at least 5% of the agents in every year. The provider may use "mystery shoppers"—staff of the provider who may visit agents and pretend to be regular customers to test the agent's integrity and competence in carrying out its roles. The CCC should review the inspection reports and submit a summary report to BFIU annually.

**(e) Transaction monitoring mechanism**

MFSPs should develop automated system based monitoring mechanism for analysis of transactions and identification of suspicious transactions. If any transaction is found to be suspicious, STR/SAR should be submitted to BFIU immediately. MFSPs should adopt Risk Based Approach (RBA) for transaction monitoring based on risk assessment. While conducting risk assessment, geographical locations, nature of customers and agents, quality of KYC information, previous records of MFS abused etc. should be taken into consideration along with any indicators informed by BFIU. Based on the risk assessment, transaction monitoring tools and procedures should be developed.

**(f) Prevention of anonymous transaction and digital hundi**

Ensuring presence of the customer at agent point during Cash In and Cash Out is the most important tool to prevent anonymous transaction (ATr) as well as some other types of abuse of m-money, such as DFS based hundi (digital hundi). When sender's and/or beneficiary's information is absent in any transaction trail, there are high risks of abuse of such transactions by criminals. A criminal will certainly be encouraged if s/he knows that nobody can identify her/him after fraud/crime. To mitigate such risks, biometric authentication (as part of e-KYC) of customer during Cash In and Cash Out transaction are the most effective tools to ensure presence of customer at the agent point. Implementation of biometric identification and authentication for financial inclusion customers in phase should be considered.

Alternatively, MFSP should develop/establish functionality so that customer's name appear in the agent's device from the MFSP's database after account number is entered by the agent during Cash In and Cash Out. The customer shall be present in the agent premise and will show a photo ID document to the agent. The name of the customer in the ID document and customer's name as appeared in the agent's device must be matched along with photo of the ID document with customer's appearance. MFSPs should inspect their agent points as mystery shoppers to identify agents' misconduct/noncompliance and agency agreement should be cancelled in appropriate cases.

**(g) Other recommendations**

Field compliance officers, distributors and agents should follow the procedures set by MFSPs to identify and report suspicious transactions/activities. Service providers may consider a toll free AML/CFT related hotline for agents and distributors and provide incentives to encourage them for submission of STR/SAR. MFSPs should provide training to their staffs, agents and distributors on ML/TF issues. MFSPs should also take awareness programs on a regular basis to aware customers, agents and distributors regarding AML/CFT issues. The Focus Group has also developed unique Account Opening Forms for personal a/c, impersonal a/c, agent & distributor a/c and format for transaction profile.

# CHAPTER 1

## AML/CFT Regulations for Mobile Money : Global Standards & Practices

### 1.1 Introduction

Access to financial system by the lower segment of the society is assumed as one of the seminal steps to establish a poverty free equitable society. Serving the poor through Mobile Financial Services (MFS) is a much-praised agenda in the global development forum. Bangladesh is playing flagship role in using this vehicle to expedite investment activities of the poor through quick delivery of financial resources.

Mobile money was introduced in Bangladesh in 2011 and earns rapid growth within a very short period of time. The total number of registered clients was 41.08 million and daily average number and value of transaction was 4.46 million and BDT 7,737.90 million respectively as on December, 2016. The service is now even available to the poorest segment of the population and mainly serves as low value domestic money transfer system. Other types of services are also expanding slowly.

However, due to rapid growth of the service in a very short period of time, accompanied by reliance on new technology and agent network, risk management has not been well developed in MFS compared to other financial services. As a result, Bangladesh has been experiencing abuse of MFS for criminal purposes like some other developing markets. Many types of offences have been reported to the concerned agencies and many incidents have also been surfaced in the media reports in recent times. For these reasons, it became urgent to act from the regulatory and supervisory authorities to guide the sector appropriately, so that it cannot be abused further.

To this end, Bangladesh Financial Intelligence Unit (BFIU) has formed a Focus Group with participation from the key stakeholders and industry practitioners. The Focus Group has developed this study paper on global standards and practices related to Anti Money Laundering and Combating Financing of Terrorism (AML/CFT) regulations for Mobile Financial Services (MFS) to find lessons for Bangladesh including recommendations. The recommendations are aimed for the consideration of Bangladesh Financial Intelligence Unit (BFIU), Bangladesh Bank and other relevant authorities to promote an effective supervisory regime for mobile financial services in the country.

### 1.2 Structure of the study paper

This study paper has been divided into three chapters. Chapter 1 discusses the global standards related with ML/FT regulations of MFS. It mainly focused on FATF Recommendations which have special relevance with MFS and how those are implemented by some other countries. Several case studies are also included to depict the examples of other jurisdictions.

Chapter 2 describes the recent trend about abuse of m-money for criminal purposes in Bangladesh. Many types of abuse of m-money have been observed in recent years and most common types are discussed in this chapter. Moreover, some case studies are also included to understand the innovative techniques used by the criminals.

Chapter 3 focuses on the key learning and recommendations for Bangladesh. After reviewing the discussions of previous two chapters, key learning has been identified. Based on the learning and intense discussion in the Focus Group, some recommendations have been adopted which are expected to be implemented by the concern agencies and MFS providers.

### 1.3 Integrity risk in mobile money operations

The abuse of m-money could stem from four major risk categories: anonymity, elusiveness, rapidity, and poor oversight. Whereas the first three risk categories may be inherent in the operation of the m-money business model, poor oversight could create conditions that increase the likelihood of abuse emerging from the other three risk factors.[1]

#### i) Anonymity

Anonymity in the context of m-money refers specifically to the risk that a criminal may gain access to m-money using a false name or may be allowed to access the services by not disclosing his identity to the service provider. If identification processes are absent, criminals are able to access to m-money with ease. If identification is undertaken, but verification processes deliver weak authentication, it is easier to commit identity fraud successfully. Regarding many of the current m-money programs, there are two main reasons for which verification processes may not be robust:

1. Responding to the needs of the country, national regulations governing the m-money model allow non–face-to-face verification.
2. The country's verification infrastructure (for example, availability of reliable national identification documentation and electronic databases with identification and profiling data on all residents) is weak.[2]

#### ii) Elusiveness

Elusiveness may exist in the use of m-money to facilitate money movements. Mobile phone "pooling" in poorer communities where few mobile phones are used to serve hundreds of villagers or the delegation of personal assistant to use mobile of his/her superior in an office environment or mobile SIM registered in the name of parent, but used by other family members are the examples of elusiveness. If mobile money transactions are conducted through those mobile phones, identification of beneficial owner would be difficult as registered customer and actual beneficiary are totally different persons. In such cases, the actual beneficiary may abuse mobile money account in disguise of the registered user.

---

[1] 'Protecting Mobile Money against Financial Crimes', The World Bank (2011), P.33

[2] ibid, p.33

**iii) Rapidity**

The convenience of m-money programs—the ability to use them quickly and practically anywhere at any time- makes layering much easier than in traditional transfer methods that can require face-to-face interaction with bank personnel at each step. A criminal sitting in one spot with several phones in hand could easily move funds across multiple m-money accounts.

**iv) Poor oversight**

The risk of poor oversight has emerged because current and emerging m-money programs may fall outside AML/CFT regulations in some countries together with confusion about determining right government authority to oversee m-money. World Bank research found that national regulators and supervisors are struggling to understand and assess the actual risks (including those from ML/TF) stemming from such technologies.[3]

The Groupe Spécial Mobile Association (GSMA) has also identified potential vulnerabilities for risk categories at each stage of a mobile money transaction:

| General risk factors | Sample exploitation of vulnerabilities at each stage | | |
|---|---|---|---|
| | Loading | Transferring | Withdrawing |
| **Anonymity** | Multiple accounts can be opened by criminals to hide the true value of deposits | Suspicious names cannot be flagged by system, making it a safe-zone for known criminals and terrorists. | Allows for cashing out of illicit or terrorist-linked funds. |
| **Elusiveness** | Criminals can smurf proceeds of criminal activity into multiple accounts | Criminals can perform multiple transactions to confuse the money trail and true origin of funds. | Smurfed funds from multiple accounts can be withdrawn at the same time. |
| **Rapidity** | Illegal monies can be quickly deposited and transferred out to another account. | Transactions occur in real time, making little time to stop it if suspicion of terrorist financing or laundering. | Criminal money can be moved through the system rapidly and withdrawn from another account. |
| **Lack of oversight** | Without proper oversight, services can pose a systemic risk. | | |

*Source:* GSMA Risk Assessment Methodology (2010)

[3] 'Protecting Mobile Money against Financial Crimes', p. 38, The World Bank (2011).

### 1.4 Challenges related with AML/CFT regulation for m-money

New financial products and services have been created in the past few years which may contribute to expanding access to new markets and clients. To date, challenges have appeared in how to effectively apply AML/CFT mechanisms to these new products and services. This is particularly evident with branchless and mobile financial services.[4] AML/CFT obligations can increase the cost of doing business, which may be borne by financial institutions, reducing potential profits and making it less attractive for the private sector to reach out to the unbanked and provide them with essential financial products and services. The costs may also be transferred to customers, potentially discouraging some from using the formal financial system, particularly if informal options are cheaper and equally reliable.[5]

It is important to keep in mind that underserved clients represent a very heterogeneous category with very different risk profiles in different jurisdictions. As a consequence, they cannot be classified as lower risk clients solely on the basis that they are low income individuals, who have recently been integrated into the formal financial system.[6]

### 1.5 CDD requirements of FATF

Customer due diligence (CDD) requirements under FATF Recommendation 10 are intended to ensure that financial institutions can effectively identify, verify and monitor their customers and the financial transactions in which they engage, in relation to the money laundering and terrorist financing risks that they pose.

The institutions, professions and businesses subject to AML/CFT obligations must:

a) Identify the customer and verify that customer's identity, using reliable, independent source documents, data or information.

b) Identify the beneficial owner, and take reasonable measures to verify the identity of the beneficial owner, such that the financial institution is satisfied that it knows who the beneficial owner is.

c) Understand and, as appropriate, obtain information on the purpose and intended nature of the business relationship.

d) Conduct ongoing due diligence on the business relationship and scrutinize transactions throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer and its business and risk profile, including, where necessary, the source of funds.

4 'Anti-money laundering and terrorist financing measures and financial inclusion', para. 30, FATF (2013).

5 ibid, para. 31

6 ibid, para. 44

### 1.5.1 CDD measures - lower risk scenarios

The revised FATF Recommendations (2012) allow for simplified CDD measures where there is a lower risk of money laundering and terrorist financing (INR. 1 par.5. and INR 10. par.16 to 18 and par.21). Jurisdictions may consider establishing a simplified CDD regime, for specifically defined lower risk customers and products. In any case, simplified CDD measures is not permitted if there is any suspicion of money laundering, or terrorist financing, or where specific higher-risk scenarios apply.

In all situations of simplified CDD, the lower risk circumstances will have to be confirmed based on a thorough and documented risk assessment, conducted at the national, sectoral or at the financial institution level (INR. 10 par. 16). In general, targeted products may include several specific conditions such as the customer being a natural person, limited transactions in amount and limited account balance at any time etc. The FATF explicitly includes as one lower risk example "financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes".

But, FATF also suggest that countries should not exempt some of the FATF Recommendations to money or value transfer services (MVTS) even if it is carried out by a natural or legal person on an occasional or very limited basis, such that there is low risk of money laundering and terrorist financing [INR. 1, par. 6].

In a financial inclusion context, the beneficial owner will in most instances be the customer him/herself, or a closely related family member. Situations where suspicions arise that the account holder is used as a straw man or front man and is not the real owner, it should not be treated as a lower risk and enhanced measures should be applied (INR. 10 par. 15a).

FATF suggested countries to consider applying a so called "progressive" or "tiered" KYC/CDD approach whereby low transaction/payment/balance limits could reduce money laundering and terrorism financing vulnerabilities. The stricter the limits that are set for particular types of products, the more likely it would be that the overall ML/TF risk would be reduced and that those products/services could be considered as lower risks. Simplified CDD measures might therefore be appropriate. This approach may provide undocumented (financially excluded) individuals access to accounts or other financial services with very limited functionalities. Access to additional services (e.g., higher transaction limits or account balances, access through diversified delivery channels) should be allowed only if/when the customer provides proof of identity and address.[7]

[7] 'Anti-money laundering and terrorist financing measures and financial inclusion', para. 74, FATF (2013).

### 1.5.2 CDD measures – customer identification

The FATF Recommendations allow countries' laws or regulations to apply Risk Based Approach (RBA) to the types of customer information that must be collected to start a business relationship. A carefully balanced approach has to be taken, because if identification processes are too lean, monitoring may make a limited contribution to risk mitigation, and manual or electronic scanning of transactions may not be able to identify individual suspicious activity effectively. In some countries, differentiated CDD requirements have been introduced, in relation to certain types of financial products. For instance in Colombia, simplified AML/CFT procedures for low-value electronic accounts and mobile accounts that are opened via agents (who receive and forward the application materials) has been introduced in 2009.[8]

### 1.5.3 CDD measures – verification of customer identification

The FATF Recommendations require financial institutions to verify the customer's identity using reliable, independent source documents, data or information. When determining the degree of reliability and independence of such documentation, countries should take into account the potential risks of fraud and counterfeiting in a particular country.[9]

On the other hand, rigorous verification requirements can act as a disincentive for financial inclusion. Using an RBA, local authorities have often allowed a broader range of documentation in pre-defined types of business relationships and for specific (financial inclusion) products and accounts, with low balance limits. Countries should take advantage of the RBA to facilitate proportionate requirements with regard to acceptable IDs that will support the provision of relevant services to un-served groups.[10]

Amongst the examples of simplified CDD measures in INR. 10 para. 21, the verification of the customer's (and beneficial owner) identity after establishment of the business relationship is envisaged, i.e. if account transactions rise above a defined monetary threshold. As part of a tiered CDD approach, customers can be provided with limited and basic services, and access to a full or expanded range of services or higher transactions ceilings would only be granted once full identity verification has been conducted.[11] This flexible approach for limited purpose accounts, where verification is postponed but not eliminated, allows clients to get access to basic products with limited functionalities and for low value transactions.

---

8 'Anti-money laundering and terrorist financing measures and financial inclusion', FATF (2013), para.76

9 ibid, para. 77

10 ibid', para. 80

11 ibid, para. 84

### 1.5.4 CDD measures - identification in non face-to-face scenarios

INR.10, par.15 of the new FATF Recommendations identifies non-face-to-face business relationships or transactions as examples of potentially higher risk scenarios. The absence of face-to-face contact may indicate a higher ML/TF risk situation. If customer identification and verification measures do not adequately address the risks associated with non-face-to-face contact, the ML/TF risk increases, as does the difficulty in being able to trace the funds. While monitoring and reporting mechanisms can be put in place to identify suspicious activity, an absence of CDD increases the difficulty for the service provider to do so. For example, this impacts on the ability of the service provider to identify instances of customers holding multiple accounts simultaneously.[12]

In the new technology/business practices/financial inclusion context, it is worth noting that the FATF Recommendations (INR.10, par.11) allow financial institutions in non-face-to-face scenarios to verify the identity of the customer following the establishment of the business relationship (and not before or during the course of establishing a business relationship) when essential to not interrupt the normal conduct of business and provided that the money laundering risks are effectively managed.[13]

### 1.5.5 CDD for legal persons

The FATF requirements regarding CDD for legal parson (INR.10, para.5) are particularly relevant to merchants/institutional customers of the digital financial services providers. Financial institutions are required to identify and verify the customer, and understand the nature of its business, and its ownership and control structure to prevent the unlawful use of legal persons and arrangements. By gaining a sufficient understanding of the customer financial institutions will be able to properly assess the potential money laundering and terrorist financing risks associated with the business relationship and to take appropriate steps to mitigate the risks. These also include identification of the beneficial owners of the customer and take reasonable measures to verify the identity of such persons.

### 1.5.6 Reliance on identification and verification already performed

The CDD measures set out in Recommendation 10 do not imply that financial institutions have to repeatedly identify and verify the identity of each customer every time that a customer conducts a transaction. An institution is entitled to rely on the identification and verification steps that it has already undertaken, unless it has doubts about the veracity of that information.[14] Examples of situations that might lead an institution to have such doubts could be where there is

12 'Guidelines for a risk based approach: Prepaid cards, mobile payments and internet-based payment services', para. 40-41, FATF (2013).

13 ibid, para. 92

14 FATF Recommendations (2012), INR.10, para. 10.

a suspicion of money laundering in relation to that customer, or where there is a material change in the way that the customer's account is operated, which is not consistent with the customer's business profile.

The requirement stated above has particular relevance with money remittance services. When such service is provided to existing customers of the financial institution, CDD measures should not be required while conducting each transaction. Because, CDD measures has already been done while establishing business relationship. But, when remittance service is provided in one off basis and is not required to open an account, CDD measures are required while conducting each transaction. In such cases, extend of CDD measures shall depends on risk involved.

### 1.5.7 CDD of existing customers

Financial institutions should be required to apply CDD measures 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 undertaken and the adequacy of data obtained.[15] This requirement is particularly relevant when rapid customer uptake is observed by digital financial services and branchless banking in the developing world using agents with minimum CDD requirements. If customers request for more functionalities or new kind of risk emerges, financial institutions should review the CDD of such customers.

### 1.5.8 CDD measures based on business relationship

The RBA would allow financial institutions in appropriate circumstances (i.e., with respect to particular types of customers or services/products) to *infer* the purpose and nature of the business relationship from the type of account established and transactions conducted, instead of collecting *specific* information and carrying out specific measures intended to satisfy this obligation (INR 10, par. 21).

### 1.5.9 Enhanced Due Diligence (EDD) if ML/TF is suspected

Under INR 10.21, simplified CDD measures will not be applicable if there is any suspicion of money laundering, or terrorist financing. Neither are they applicable where specific higher-risk scenarios apply. So, CDD measures designed for lower risk products should therefore be required enhanced due diligence measures where such suspicions may be harbored or where higher-risk scenarios are encountered. For example, Mobile Financial Services (MFS) has been launched in many developing countries in recent years with simplified CDD as a financial inclusion product. If it is observed that the service is being abused, service providers should be required to perform enhanced due diligence measures in appropriate cases.

15 FATF Recommendations (2012), INR.10, para. 13.

### 1.5.10 CDD measures - conducting ongoing due diligence and monitoring

Monitoring refers to manual or electronic scanning of transactions based on certain parameters, such as source or destination of transaction, its value and nature, names of clients and beneficiaries, geographical location, etc. The scanning process may flag a number of transactions for internal investigation and the investigator will typically require more information about the client and the transaction before a reasonable conclusion.

The degree and nature of monitoring by a financial institution will depend on the ML/TF risks that the institution faces. In applying an RBA in monitoring, financial institutions and their regulatory supervisors must recognize that not all transactions, accounts or customers will be monitored in the same way. The degree of monitoring will be based on the identified risks associated with the customer, the products or services being used by the customer and the location of the customer and the transactions.[16] Technology-based service models often offer greater ease of monitoring, and this should be particularly considered by countries in a financial inclusion context.

Monitoring under an RBA allows a financial institution to create monetary or other thresholds below which an activity will receive reduced or limited monitoring. Defined situations or thresholds and monitoring system should be reviewed periodically. Some form of monitoring, whether automated or manual, a review of exception reports or a combination of screening criteria, is required in order to detect unusual and hence possibly suspicious transactions. However, if little CDD is undertaken, so that the financial institution lacks a sufficient range of available information, manual or electronic scanning of transactions may not be able to deliver significant benefit.[17]

### 1.5.11 CDD measures – the specific case of wire transfers

In addition to CDD requirements, wire transfers are subject to specific rules relating to the customer/originator and beneficiary to ensure full transparency throughout the payment chain (Recommendation 16). Countries may adopt a de minimis threshold (no more than USD/EUR 1000), below which reduced information requirements can be applied (INR 16).

## 1.6 Record-keeping requirements

Under Recommendation 11, financial institutions should maintain records of all domestic and cross-border transactions (including occasional transactions) and identification data obtained through the CDD process for at least five years after the transaction or the business relationship is ended. The record keeping requirement is not dependent on risk levels and it is fully applicable to the CDD, transaction and other information collected, whatever the range of this information (INR. 16).

16 'Anti-money laundering and terrorist financing measures and financial inclusion', para. 97, FATF (2013).

17 ibid, para. 102

Under the FATF Recommendations, the record keeping requirement does not require retention of a photocopy of the identification document(s) presented for verification purposes; it merely requires that the information on that document be stored and kept for five years. A number of countries, such as the United States, Australia and Canada, have considered, but rejected, imposing photocopying obligations on their regulated institutions for a number of reasons: for example, the photocopies could be used to commit identity fraud; their retention may breach privacy laws and they may reveal information about the client that could form the basis of discriminatory practices, such as the refusal of credit facilities.[18]

Depending on the size and sophistication of a mobile provider's record storage, the following record retention techniques are also acceptable and can constitute a valid alternative to hard copies[19]:

- Scanning the verification material and holding it electronically
- Keeping electronic copies of the results of any electronic verification checks
- Recording reference details (particularly useful in the context of mobile banking where m-money agents are often simple corner shops), including
  - any reference numbers on documents or letters,
  - any relevant dates, such as dates of issue, expiration, or writing,
  - details of the issuer or writer,
  - all identity details recorded on the document.

**Case Study**

In **Malawi**, when a potential customer does not have the requisite documentation, a close relative (brother or sister) can submit his or her reference (passport details) in support of an application by the person who does not have the necessary documentation. Also, the use of biometrics in the CDD process helped tackle identification challenges.

### 1.7 Suspicious transactions reporting

FATF Recommendation 20 stipulates that if a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity or are related to terrorist financing, it should be required to report the incident promptly to the country's Financial Intelligence Unit (FIU). This obligation applies to all financial institutions that are subject to AML/CFT obligations, including those that serve disadvantaged and low income people. The implementation of such a requirement requires financial institutions to put in place appropriate internal monitoring systems to identify any unusual behaviour.

The RBA is, however, appropriate for the purpose of identifying potentially suspicious activity, for example, by directing additional resources at those areas (customers, services, products, locations etc.) that a financial institution has identified as higher risk. A financial institution should also

18 ibid, para. 110

19 'Protecting Mobile Money against Financial Crimes', The World Bank (2011), P.86

periodically assess the adequacy of its system for identifying and reporting suspicious transactions.[20] Detecting patterns of suspicious activity among thousands of low-value transactions in m-money (due to transaction limit imposed) will not be easy, given the current approaches to detecting suspicious transactions. In practice, suspicions are often triggered by "large and complex" transactions, not by micro or nano operations.[21] In the context of m-money, customer profiling, automated monitoring of transaction and internal control are the key to identify suspicious transaction.

### 1.7.1 Customer profiling

Customer profiles are usually built by the provider, using information gathered at the time of customer acquisition, and they are subjected to ongoing modification. Data collected by providers may include the customer's income level, transaction history, and type of services and channels frequently used. This information may be used by m-money providers to identify any unusual transaction patterns.[22]

### 1.7.2 Automated monitoring and internal controls

The information systems of m-money operators may also support sophisticated monitoring and internal control systems. They normally have automated controls embedded in information technology systems and supported by some manual controls. This is particularly relevant to AML/CFT risk mitigation because automated controls can quickly scan the name, date of birth, and other relevant identification information and compare the data with various UNSCR lists and others of its kind. The more information received by the m-money provider during the initial customer profiling stage, the better a provider's monitoring and internal control systems can work to monitor customer activities and transactions and to compare those transactions with the initial customer profile.[23]

## 1.8 The use of agents to carry out AML/CFT functions

The use of non-bank agents to distribute financial services is part of an increasingly popular model for financial inclusion in many countries. The financial institution grants authority for another party, the agent, to act on behalf of and under its control to deal with a client/ potential client. In these branchless banking and mobile money business models, agents are viewed by the FATF as simply an extension of the financial services provider, and consequently, the conduct of CDD by these agents is treated as if conducted by the principal financial institution. The customers themselves generally view the retailer as a point of access and as a representative of the principal financial institution.[24]

---

20 'Anti-money laundering and terrorist financing measures and financial inclusion', FATF (2013), para. 113-114.

21 ibid, p.90

22 'Protecting Mobile Money against Financial Crimes', p. 51, World Bank (2011)

23 ibid, p.52

24 'Anti-money laundering and terrorist financing measures and financial inclusion', FATF (2013), para. 119

### 1.8.1 Who can be an agent?

Many countries permit a wide range of individuals and legal persons or other entities to be agents for financial institutions. Other countries restrict the list of legally eligible agents. For example, India permits a wide variety of eligible agents, such as certain non-profits, post offices, retired teachers, and most recently, for-profit companies, including mobile network operators. Kenya requires agents to be for-profit actors and disallows non-profit entities. Brazil permits any legal entity to act as an agent, but prevents individuals from doing so. This range of approaches reflects that countries have different regulatory concerns that balance agent eligibility requirements from an AML/CFT perspective with financial inclusion objectives.[25] The above examples are mainly relevant for the branchless banking context, but not for m-money where agents are mostly neighborhood small shops, such as mobile top up, grocery or medicine shops, etc. where m-money service is an additional product. However, in any of the above context, financial institution is ultimately liable for compliance with the AML/CFT requirements as required by FATF Recommendations.

### 1.8.2 AML/CFT functions of the agent and related challenges

The duties of the agents commonly include to perform specific AML/CFT checks, record-keeping and reporting obligations in most countries. It is essential that the duties of the agents are clearly specified in the agency agreement signed with financial institution. Although the precise role of a retailer agent may differ from business model to model, it generally involves providing cash-in and cash-out services. It may also extend to other customer interface functions such as account opening and customer care. Most regulations permit agents to process cash-in and cash-out transactions. Many countries permit agents to conduct CDD, and agents routinely verify customer identity. In other countries, agents' ability to conduct CDD measures is limited to certain lower risk financial products. The challenges related to the identification of the customer and verification of the identity will therefore greatly vary from country to country.[26]

The agent should have a duty to report a customer's suspicious conduct to the m-money provider, but the agent cannot carry the full burden of conducting on-going due diligence on the business relationship and scrutinizing all transactions undertaken throughout the course of that relationship. Many agents are modest shops that are not equipped to perform extensive monitoring functions, and they may not have access to the customer profile that the m-money provider holds. This would make it impossible to consider whether a customer's transactions are consistent with the institution's knowledge of that customer. Furthermore, an agent will view only those transactions that are conducted via its shop. The m-money provider, on the other hand, will have a

25 'Anti-money laundering and terrorist financing measures and financial inclusion', FATF (2013), para. 120

26 ibid, para. 125-126

comprehensive record of the transactions conducted by the particular customer. From a policy perspective, however, it is strongly suggested that the main monitoring obligation remains that of the m-money provider because it is in the best position to oversee customers' activities. The m-money provider should ensure that the retail outlets provide appropriate support to guarantee that it can meet its obligations in this regard.[27]

### 1.8.3 Know your agents (KYA)

Agent monitoring is a very important element in an effective AML/CFT program. The degree and nature of agent monitoring will depend on factors such as the transaction volume and values handled by the agent, the monitoring method being utilised (manual, automated or some combination), and the type of activity under scrutiny. In applying a risk-based approach to agent monitoring, the degree of monitoring will be based on the identified risks, both external and internal, associated with the agent, such as the products or services provided by the agent, and the agent's location.

Due diligence measures for agents should be consistent with the risks posed by the agency relationship. When the agent is entrusted with account-opening functions, higher due diligence standards are appropriate. Agents know the m-money provider's system better than the customers know it, so the outlets may be able to abuse their positions within the framework to launder funds and perpetrate other offenses. Generally, they are able to ignore suspicious activities that should be reported to the m-money provider. Depending on the design of the particular m-money model, they may be in positions to falsify records. Even honest agents may render the system vulnerable to abuse by failing to perform their functions diligently. So, institutions must scrutinize their agents closely and manage the attendant ML risk by performing appropriate due diligence measures when engaging agents. When an agency relationship is established, appropriate training and support must be provided. In addition, agents must be monitored for compliance with their AML/CFT duties.[28]

### 1.8.4 Regulatory oversight of agents

Since agents are viewed by FATF as an extension of the principal financial institution, it is appropriate for regulatory supervision and oversight to focus primarily on the principal financial institution. Monitoring and supervising thousands of agents would be extremely challenging for most, if not all, countries. The oversight of agents is mainly performed by the principal financial institution, in a similar manner as it monitors employees (R.18). It is nevertheless also essential that the regulatory supervisor reviews financial institutions' oversight functions, including by examining the policies, procedures, training and monitoring of agents put in place by the principal financial institutions.[29] Where appropriate, the supervisor should visit a representative sample of retail outlets to determine if the financial institution is performing its required functions effectively.

27 'Protecting Mobile Money against Financial Crimes', World Bank (2011), p. 95

28 ibid, p.97

29 'Anti-money laundering and terrorist financing measures and financial inclusion', FATF (2013), para. 131

**Case study: Oversight of agents**

In **Kenya**, Safaricom requires retail outlets to pass an AML test to ensure their familiarity with integrity issues and procedures. Zain, another MFS provider, verifies the business permits of retail outlets through lawyers and notaries, and it performs random on-site visits by "mystery shoppers".

In **Peru**, financial institutions are obligated to train their retail outlets on KYC and other CDD obligations.

In the **Philippines**, Globe Telecom requires all retail outlets to undergo an accreditation process led by a committee comprising representatives from its finance, legal, business operations, and information technology departments.

In the **Russian Federation**, payment agents are required to register with the Federal Financial Monitoring Service (FFMS) for AML purposes and to have their internal control rules approved by FFMS before accepting payments. In addition, all transactions processed by retail outlets go through the operator's information technology system and will be subject to AML/CFT rules.

In **Zambia**, the central bank reviews applications to ensure that retail outlet personnel are adequately trained in front-end procedures (including KYC) and allows the provider to monitor its retail outlets.[30]

### 1.8.5 Specific requirements for MVTS agents

FATF defined an agent as any natural or legal person providing Money or Value Transfer Service (MVTS) on behalf of an MVTS provider, by contract with or under the direction of the MVTS provider (R.14). FATF requires that any natural or legal person working as an agent of an MVTS provider is either licensed or registered by a competent authority, or alternatively, the MVTS provider (the principal) is required to maintain an updated list of agents which must be made accessible to the designated competent authorities in the countries in which the MVTS provider and its agents operate, when requested.

## 1.9 Requirements for new products and technologies

FATF Recommendation 15 requires that countries and financial institutions identify and assess the specific 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 existing and new products. This requirement is particularly important for digital financial services, as basic foundation of this service is technological innovation which changes very rapidly.

In the case of financial institutions, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies, and they should

30 'Protecting Mobile Money against Financial Crimes', World Bank (2011), p.98

take appropriate measures to manage and mitigate those risks. The initial, pre-launch risk assessment will be refined and adjusted in light of the experience, as part of the requirement that financial institutions regularly review and adapt their RBA measures (INR. 1.8.).

## 1.10 Techniques used to effectively mitigate m-money risks

Various jurisdictions have implemented regulatory and supervisory requirements to mitigate any potential risks emerging from mobile money. These requirements include specially set KYC procedures, advanced identification mechanisms, limits on transaction amounts, customer profiling, monitoring and internal controls, centralized registries of account holders, guidelines on AML/CFT, and licensing for m-money providers.[31]

### 1.10.1 KYC tailored for m-money

An increasing number of countries now require registration of the SIM card. Prepaid SIM registration is currently mandated in around 90 countries.[32] Many countries including Bangladesh have already implemented biometric SIM registration and verification against national ID database. Mandatory telecommunications registration reduces the risk of anonymity and aids in monitoring accounts against criminal activity.

In order to allow m-money providers to acquire customers in non face-to-face scenario, some countries have adopted alternative verification measures. The main procedures implemented are (1) legal exceptions to verifying customer's residential address during initiation of the banking relationship (if transactions do not exceed prescribed limits), (2) alternative verification procedures, and (3) restricted functionality. Customer's identity is established by cross-checking customer information against third party database, such as a national tax or social security database.

Countries may consider applying the so-called **progressive KYC/CDD approach** whereby payment limits vary, based on the identification check: the better the identification process, the higher the limits. For people without adequate documents, this may imply access to very limited functionalities; and access to broader services (such as higher limits, and transfers, including cross-border) would be allowed only if the customer provides proof of identity and address.[33]

However, appropriate regulation and internal control measures can be determined only in the context of the risk based approach when a comprehensive risk assessment has been performed. A risk assessment determines whether there are higher or lower risks, and provides grounds for an evidence-based shaping of the regulatory and risk-management regimes to identify those circumstances that will justify reduced KYC measures, as recommended by the FATF.

---

31 'Protecting Mobile Money against Financial Crimes', World Bank (2011), p.49

32 http://www.gsma.com/newsroom/blog/mandatory-real-name-registration-prepaid-sim-card-users-considerations-policymakers/

33 'Protecting Mobile Money against Financial Crimes', World Bank (2011), p.77

Among those countries that have applied a risk-based approach, the most common approach has been to relax the verification controls on low-value transactions or products. These approaches have significantly limited the impact of AML on access to financial services.

**Case Study : progressive KYC/CDD approach**

In Mexico, the AML/CFT legal framework recognizes three categories of accounts that allow different levels of KYC and CDD requirements. Mobile accounts may fall into either of these categories:

- "low-transaction accounts" (Mex$8,720 or 2,000 UDI [inflation-indexed units] in monthly deposits): under this category, clients' files should contain the full name, birth date, and address and must be integrated and saved.
- "low-risk accounts" (Mex$174,400 or 40,000 UDI in monthly deposits and withdrawals): under this category, clients' files contain complete data related to the client and must be integrated and saved.
- "unlimited accounts": under this category, clients' files contain complete data related to the client and copies of the documentation to be integrated and saved.[34]

In South Africa, Guidance Note 6/2008 on mobile banking allows customers to register for mobile banking service by opening their bank accounts remotely, using their mobile phones. This means that there is no need to go to a bank branch initially, provided that a customer is a natural person who is a citizen of or resident in South Africa and who has a valid South African identity number; and provided that transaction and account limits are observed. The client is identified, and reasonable steps are taken to verify the person's identification details (especially comparing the client's personal data to a third-party database with official data). The client, therefore, may start using the mobile banking service by transacting small amounts without going to a bank branch to provide an address. Clients who wish to exceed the strict transaction limits that are imposed under Guidance Note 6/2008, can submit themselves to the more comprehensive identification and verification requirements. In this case, the client must normally provide documentary proof of identity in the form of an identification card or number; residential address/ particulars do not need to be obtained or verified. Clients may migrate from the above limited functionality products to standard products that are not subject to account and transaction limits by undergoing face-to-face identification and verification processes and providing documentary proof such as their identification cards or numbers and proof of address.[35] This approach, therefore, is proportionate to risk because the identification requirements become more onerous as the transaction sizes—and the related risk—increase.

34 'Protecting Mobile Money against Financial Crimes', World Bank (2011), p. 79

35 de Koker, Louis. 2009. "The Money Laundering Risk Posed by Low-Risk Financial Products in South Africa: Findings and Guidelines." Journal of Money Laundering Control 12 (4): 323–39.

### 1.10.2 Innovative mechanisms for identification

Customer identification and verification are the key elements of ML/TF risk mitigation. If identification and verification processes are not performed correctly, the integrity of the financial system is at risk because significant amounts of dirty money will continue making the rounds. However, strict identification and especially verification requirements form barriers that prevent people without the required documentation or data—mainly the low income and socially marginalized populations—from accessing m-money services. On the other hand, less-stringent provisions may encourage significant integrity abuse. Indeed, implementing identification and verification requirements has proved quite problematic in low-capacity settings.

Some countries are using innovative digital solutions for identification of financial inclusion customers. Malawi has introduced verification of biometric identification for the financial inclusion customers. In Rwanda and Kenya, storing electronic finger prints is permitted and in both countries credit unions have piloted fingerprint identification technology for rural poor customers. MTN Banking, a division of the Standard Bank of South Africa has tested a biometric voice identification system for m-money.

**Case Study: Digital identification in India**

India is embarking on a project to provide every Indian resident a 12-digit biometric identification number, formerly called the Unique Identity Number (UID) and now called the Aadhaar number, tied to three pieces of biometric data (fingerprints, iris scans, and a facial picture) and limited demographic information. The Aadhaar number is intended to allow individual identification anytime, anywhere in the country through online identity verification from a central database. If successfully implemented, it would be the first biometrically verified unique ID implemented on a national scale and would provide the "identity infrastructure" for financial inclusion, as well as for strengthening AML/CFT implementation, delivery of social services, subsidies and other programs and national security, and anti-corruption efforts.

### 1.10.3 Transaction limits

Limited transaction amounts and imposed reporting thresholds are the most popular control measures adopted by regulators and the private sector. Using the risk based approach suggested by FATF, limit imposed on frequency and amount of transactions in m-money to mitigate risk. For example, transaction amounts are grouped into three categories in South Korea that fall under increasingly stringent security measures, relative to the transaction amount. Financial institutions may also apply greater security controls, according to the profile of the customer.[36] Another approach is a point-based KYC approach. This system presumes that the more KYC evidence a

36 'Protecting Mobile Money against Financial Crimes', World Bank (2011), p.52

customer is able to provide (national identification card, driving license, passport, physical presence, and so forth), the more the customer can be trusted. Services are offered to an extent proportional to the identification provided.[37]

### 1.11 Additional reporting requirements

Some countries require all transactions exceeding a certain amount to be reported, whether suspicious or not. In Kenya, a reporting institution must file reports of all cash transactions exceeding $10,000 or its equivalent in any other currency.[38] Additional reporting requirement of m-money providers may be determined based on risk assessment. Based on the assessment, which types of customers and agents, geographical location, transaction threshold, etc. would be identified as higher risk, should be brought under reporting. Such reporting, however, must be in electronic form so that the supervisory authority able to further analyse the data and identify unusual/suspicious transaction.

### 1.12 AML/CFT policy guidance for m-money regulators

World Bank emphasized some issues need to be addressed by the country policy makers while designing AML/CFT regulatory framework for mobile money.[39] The recommendations which are particularly relevant for Bangladesh are discussed below:

#### 1.12.1 Designing the broad regulatory framework and approach

i) **Adopt a more comprehensive approach to AML/CFT.** In some cases, multiple stakeholders in the m-money community have a narrow AML/CFT approach to m-money that focuses exclusively on customer due diligence (CDD) and FATF Recommendation 10. Although CDD is an essential component of AML/CFT, policy makers should pay equal attention to the other elements of effective AML/CFT regulation. AML/CFT obligations cover a wide spectrum of issues, ranging from CDD to reporting obligations, internal controls and mechanisms, training, dissemination, national and international cooperation, and outreach, among others.

ii) **Conduct an assessment of the m-money ecosystem.** In an ideal situation, countries should survey the m-money ecosystem and its overall level of integrity risks prior to drafting AML/CFT regulation for m-money activities. The survey should aim to identify all role players in the jurisdiction, understand the products that are offered and are likely to be offered, and potential future patterns and trends. A risk assessment should also be performed to determine the nature, types, and levels of ML/TF risk. Countries will need to identify the main vulnerabilities that are specific to m-money and address them accordingly.

37 'Protecting Mobile Money against Financial Crimes', World Bank (2011), p.60

38 ibid, p.91

39 ibid, p.107

Under ideal conditions, the appropriate regulatory and supervisory approach for m-money should also support the financial system's longer-term systemic stability, rather than merely its current flows. Any reluctance by policy makers to contemplate preventive measures because of their potential costs should be balanced by a consideration of the cost of restoring public confidence if there were any wide-scale incidents involving the m-money channel.

iii) **Adopt technology-neutral regulations.** Policy makers should avoid adopting AML/CFT regulations that specifically target m-money. A uniform approach for all new payment technologies and m-money providers (banks, MNOs, and third-party providers) is important because m-money is simply an alternative means of performing financial transactions. Generally, therefore, there is no justifiable reason m-money should be subjected to a regulatory scheme that differs from the one that applies to other new payment technologies.

iv) **Focus on risks that the product and clients represent.** When the regulator considers appropriate CDD controls for m-money, it should focus on the risks that the product and the clients represent. Practical constraints and opportunities presented by the national context should also be considered to ensure a pragmatic and responsive m-money risk-control framework.

v) **Adopt regulation that balances financial inclusion with financial integrity.** International standards for AML/CFT are challenging—and their flexibility has not always been clearly communicated or understood. In addition, countries very often prefer to err on the safe side to avoid the risk of noncompliance. As a result, too many countries over-regulate and, thus, create barriers to business and inclusion. Many countries have not allowed simplified CDD where it was justified by the low risk, as permitted by the FATF's risk-based approach.

vi) **Sequence the implementation of AML/CFT obligations.** The analysis of national AML/CFT frameworks in developing economies shows that a gradual or sequenced implementation of the FATF recommendations can reduce adverse effects on financial inclusion. Sequenced implementation allows the system to be grown and expanded over a period of time to eventually ensure full compliance with the international standards. A sequenced process would start by implementing key FATF recommendations for the sectors and transactions presenting the higher risks of ML/TF; and progressively expand to lower categories of risk as the country develops its capacity to properly identify and mitigate the risks involved.

vii) **Promote a collaborative, step-by-step approach between financial regulators and industry.** A successful regulatory outcome requires a participatory approach among all stakeholders—especially the regulators, the banking supervisors, the banking and telecommunications industries, and the national authorities responsible for AML/CFT issues.

### 1.12.2 Issuing guidelines for m-money providers

i) **Issue clear and well-articulated AML/CFT guidelines for m-money services.** Clear regulatory guidelines for m-money providers have proved helpful. Guidelines are useful to bring clarity to AML/CFT legislation and national and international standards, particularly in cases in which laws were adopted recently. Guidelines for m-money providers can provide information on appropriate ways to interpret obligations and implement AML/CFT policies. It often extends to AML/CFT risk assessments, the design of CDD measures, recordkeeping requirements, suspicious transaction reports (STRs), and maintenance of an adequate level and mix of expertise through staff training.

ii) **Implement guidelines through ongoing collaboration and dialogue between the public and private sectors.** This will enable the regulator to ensure guidelines that are practical, effective, and clear to all relevant stakeholders. Such engagement will also foster discussion on how best to effectively implement and enforce the guidelines internally within the m-money provider.

iii) **Customize guidelines to specific local circumstances and conditions** considering the financial infrastructure of the country (both formal and informal sector), number of unbanked population with demographic composition, etc.

### 1.12.3 Regulating agents

During World Bank fieldwork (2011), it was particularly noticeable that authorities and providers alike were struggling to determine the correct and most appropriate status of agents under the AML/CFT supervisory regime. World Bank Report[40] suggested national authorities to consider taking the following steps to design an appropriate AML/CFT regulatory framework in relation to m-money agent networks which covers the following requirements:

i) **Clear delineation of responsibilities between providers and agents:** Agents should be seen only as representatives or functionaries of the providers who ultimately bears the responsibility for AML/CFT. Therefore, agency or outsourcing relationships should be contractually established and defined in formal contracts between the agents and the provider.

40 'Protecting Mobile Money against Financial Crime', World Bank (2011), p.114-118

ii) **Know your agents:** Provision should be made to require that CDD be carried out on agents prior to engaging them. The level of trust that m-money providers invest in their agents is often determined by how well they know them. The provider, however, should be allowed to perform such know-your-agents measures on a risk basis.

iii) **Ensure that agents undertake AML/CFT obligations:** It is advised to clearly specify the AML/CFT duties delegated to the retailers in the business agreements. Agents may be entrusted to perform some AML/CFT checks, including know-your-customer (KYC) checks and record keeping. In addition, it is possible to entrust retail outlets with the duties of conducting ongoing monitoring of transactions and reporting of suspicious activities to the provider. But, the main monitoring obligations shall be rest on the provider.

iv) **Establish mechanisms to scrutinize agents:** Agents should be subject to appropriate monitoring to ensure that they comply with AML/CFT obligations delegated to them by the provider. As a result, the contract between the provider and an agent should give the provider the right to audit the agent's performance of its obligations. For example, the provider may wish to use "mystery shoppers"—staff of the provider who visit agents and pretend to be regular customers to test the agent's integrity and competence in carrying out its roles. The provider's policies, procedures, training, and monitoring of agents should be scrutinized, in turn, by the supervisor. To that end, supervisors are advised to perform on-site visits in a sample of agents to determine whether the provider is performing the required functions correctly with regard to its network of agents.

v) **Create an AML/CFT telephone hotline:** Because agents are playing a central role in the customer interface and are tasked with several AML/CFT duties, providers may wish to create a hotline for AML/CFT purposes that would be accessible only to their agents. In case of difficulties, the agents would seek assistance and guidance on issues related to customer identification or unusual operations, among other matters.

vi) **Draft clear agent regulations or guidelines:** The issue of agent is one of the most contentious and difficult aspects of the regulation of m-money. The regulators should consider drafting agency regulations or guidelines that delineate minimum provisions to be included in agency agreement, basic eligibility criteria, technical and operational requirements, limits of transaction, customer authentication procedures and agent network management, etc.

### 1.12.4 Cooperating and coordinating

The field of m-money is not only new and fast evolving; it also sits at the overlap of several regulatory domains—those of banking, telecommunications, and payment system supervisors and of AML/CFT agencies. The overlap substantially raises the risk of coordination failure, where legislation or regulatory approaches are inconsistent or contradictory. As a result, implementing a mechanism of inter-agency coordination is of paramount importance to ensure business growth in a safe and sound environment. So, appropriate cooperating and coordinating mechanism among the AML/CFT stakeholders, regulatory and supervisory authorities, FIU and industry are most essential.

### 1.12.5 Supervising and enforcing[41]

i) **Determine an organizational model that ensures an effective m-money oversight:** It is the responsibility of each jurisdiction to devise and establish its own organizational framework for AML/CFT supervision. During the fieldwork of World Bank (2011), it was observed that several countries where m-money is booming have chosen the central bank as the primary authority to regulate and supervise m-money providers. Countries should also make sure that vesting central banks with supervisory power over m-money providers, including AML/CFT matters, does not contradict or undermine the supervisory responsibilities that may have been delegated to the FIU. Supervision of AML/CFT compliance in some countries is entrusted to the FIU only, whereas oversight of other types of issues falls under the umbrella of the financial supervisor.[42] However, there is a deep debate regarding appropriate ways to regulate and coordinate these different but overlapping responsibilities within the same authority.

ii) **Promote a clear and effective supervisory regime for m-money providers:** With very few exceptions, m-money is not yet prudentially supervised. Supervisors have uneven levels of familiarity with m-money and, until recently, many were not well versed on the implications of innovative branchless banking and other e-money concepts. Lack of resources, limited experience with AML/CFT issues, and an unstable regulatory regime for m-money may seriously hamper effective supervision.[43]

However, AML/CFT examiners will have to be entrusted with the same responsibilities and should be able to carry out the same tasks as they would for any type of financial institution as per FATF Recommendations. Jurisdictions should also provide AML/CFT

41 'Protecting Mobile Money against Financial Crime', World Bank(2011), p.120-125

42 ibid, p.121

43 ibid, p.122

supervisors with the financial, human, and technical resources they need. These resources should correspond with the size, level of risk, and quality of AML/CFT controls in the m-money sector.

iii) **Provide AML/CFT training to m-money supervisors:** AML/CFT compliance supervision in m-money services is a new issue for financial institution examiners. Employees at all levels need continual training on the application of new laws and preventive measures, as well as on new interpretations of existing matters. In addition, training programs need to keep abreast of ever-changing ML/TF techniques and tactics. In this regard, there is clearly a need for broad support and capacity building, especially because weak capacity of supervisors is one of the enduring country risks. Multilateral bodies and donors have a meaningful role to play in this regard.[44]

World Bank also provided a detail AML/CFT guidance for m-money providers in its policy notes "Protecting Mobile Money against Financial Crimes" (2011) which included recommendations on internal policies, risk management practices and transaction monitoring, reporting obligations, staff and agent training and awareness, etc.

44 Protecting Mobile Money against Financial Crimes", World Bank (2011), p.125

# CHAPTER 2

## Mobile Money in Bangladesh : Risk and Trend

### 2.1 Mobile money in Bangladesh

Bangladesh Bank understands that bank-led MFS model is more secured and engages households with formal banking services, thus helps to build a broad-based financial system which is more resilient to any shock. Under this belief, central bank has adopted this model when a customer's account, termed a "Mobile Account", opened with a commercial bank and is accessible through the customer's mobile device. This mobile account is a non-chequing account classified separately from a standard banking account. Hence, a MFS customer is primarily a customer of the bank and the bank can use the services of the MNO as a channel and distributor network partner.

Bangladesh Bank has issued 19 licenses to commercial banks to rollout mobile money. Among them, 18 banks have launched their operation till December, 2017. MFS presents an opportunity to build an alternative delivery channel and to make transaction points even more widely and remotely available to rural poor households. Given the need to continue to advance financial inclusion, Bangladesh Bank presumes that fully developed m-money services can facilitate a higher proportion of the population in getting access to basic formal financial services, particularly deposit and payment services. These services may eventually lead to product innovations in insurance, credit and government payments that would reach millions of unbanked population. These interactive financial and payment services have considerable role in fuelling equitable growth of the economy.

Some of the prominent m-money brands in Bangladesh are bKash (BRAC Bank subsidiary), Rocket (DBBL mobile banking), mCash (Islami Bank), uCash (United Commercial Bank), SureCash (consortium of few banks) and MYCash (Mercantile Bank), etc.

**Table 1 : Status of MFS in Bangladesh[45]**

| Serial | Description | Dec/2015 | Dec/2016 | Dec/2017 |
|---|---|---|---|---|
| 1 | No. of approved banks | 28 | 19 | – |
| 2 | No. of banks providing MFS | 18 | 17 | 18 |
| 3 | No. of agents | 561,189 | 710,026 | 786,459 |
| 4 | No. of registered customers (in million) | 31.85 | 41.08 | 58.81 |
| 5 | No. of active accounts (in million) | 13.22 | 15.87 | 21.01 |
| 6 | Total no. transaction (in million) | 114.85 | 133.73 | 166.32 |
| 7 | Total value of transaction (in million taka[46]) | 161,248.10 | 232,136.70 | 285,714.00 |
| 8 | No. of daily average transactions (in million) | 3.83 | 4.46 | 5.37 |

45 Source: Bangladesh Bank website

46 Bangladesh currency is known as taka (BDT). USD 1 = BDT 82.70 (as on January, 2018)

| Serial | Description | Dec/2015 | Dec/2016 | Dec/2017 |
|---|---|---|---|---|
| 9 | Average daily transaction volume (in million taka) | 5,374.90 | 7,737.90 | 9,217.00 |
| 10 | Additional information | Amount (in million taka) | | |
| a) | Inward Remittance | 42.5 | 81.2 | 46.0 |
| b) | Cash In transaction | 68,299.2 | 100,164.4 | 120,279.0 |
| c) | Cash Out Transaction | 59,311.0 | 90,463.3 | 108,947.0 |
| d) | P2P transaction | 27,508.4 | 33,682.1 | 44,252.0 |
| e) | Salary Disbursement (B2P) | 1,541.5 | 2,348.5 | 4,054.0 |
| f) | Utility Bill Payment (P2B) | 1,091.2 | 1,813.4 | 1,847.0 |
| g) | Merchant Payment | -- | -- | 1,300.3 |
| h) | Government Payment | -- | -- | 1,282.1 |
| i) | Others | 3,454.3 | 3,583.9 | 3,705.9 |

## 2.2 Risk assessment of m-money in Bangladesh context

FATF has developed a risk matrix for new payment products and services (NPPS), which helps to identify the risks associated with any types of individual NPPS. FATF suggested not considering the risk factors listed in the matrix one-by-one, but the risks, risk mitigations and functionality of a particular NPPS to considered together to determine whether the product poses a high or low ML/TF risk. Based on the risk matrix of FATF, such a matrix[47] has also been developed for MFS of Bangladesh considering the existing business model and regulation:

| Criteria | | High risk factors | Low risk factors | Bangladesh context | Risk grading |
|---|---|---|---|---|---|
| CDD | Identification | Anonymous | Customers are identified | A/c opened with customer's identification document | Low |
| | Verification | Customer's identity is not verified on the basis of reliable, independent source documents, data or information | Customer's identity is verified on the basis of reliable, independent source documents, data or information | Verification is mostly absent yet | High |
| | Monitoring | None | Ongoing monitoring of business relationships | Due to inadequate KYC & large number of micro transaction, effective monitoring absent yet | High |

47 The risk matrix has been taken from "Guidelines for a RBA: Prepaid Cards, Mobile payments and Internet based payment services", FATF(2013) and modified to assess ML/TF risks of MFS market of Bangladesh.

| Criteria | | High risk factors | Low risk factors | Bangladesh context | Risk grading |
|---|---|---|---|---|---|
| Record keeping | | Electronic transaction records are generated, but not retained or not made accessible to LEA upon request | Electronic transaction records retained and accessible to LEA upon request | Transaction records are retained and accessible to LEA | Low |
| Value limits | Max. amount stored on A/C or A/C per person | No limit | Amount limit | Regulation and enforcement are present | Low |
| | Max amount per trans. (inc. loading/ withdrawal transactions) | No limit | Amount limit | Do | Low |
| | Max. transaction frequency | No limit | Transaction limit | Do | Low |
| Method of funding | | Anonymous funding source (e.g. cash); also multiple sources of funds, e.g. third parties | Funding through accounts held at a regulated financial or credit institution, or other identified sources which are subject to adequate AML/CFT obligations and oversight | Cash In transaction is dominant. Bank a/c to MFS a/c transfer yet very low. Anyone can Cash In to a/c of others. | High |
| Geographical limits | | Transfer of funds or withdrawal across national borders | Transfer of funds or withdrawal only domestically | Evidence of serious abuse of MFS for *digital hundi*. | High[48] |
| Usage limits | Negotiability (merchant acceptance) | High number of accepting merchants/point of sale (POS) | Few accepting merchants/POS | Merchant payment is yet low | Low |
| | Utility | p2b, b2b, p2p, online usage possible | p2b, b2b, online usage possible, but no p2p | p2p is dominant; p2b, b2b, online transaction is yet low | High |
| | Withdrawal | Anonymous and unlimited withdrawal (e.g. cash through ATMs) | Limited withdrawal options (e.g. onto referenced accounts only); limited withdrawal amounts and frequency | Limited amount & frequency of withdrawal | Low |

48 There is evidence of abuse of MFS for illegal money remittance (hundi) as described in paragraph 2.5.8. Thus, MFS of Bangladesh is crossing domestic boundaries and treated as high risk.

| Criteria | | High risk factors | Low risk factors | Bangladesh context | Risk grading |
|---|---|---|---|---|---|
| Segmentation of services | Interaction of service providers | Several independent service providers carrying out individual steps of the transaction without effective oversight and coordination | Whole transaction carried out by one service provider | MNOs provide USSD channel only, rest steps of transaction conducted by MFS providers | Low |
| | Outsourcing | Several singular steps are outsourced; outsourcing into other countries without appropriate safeguards; lack of oversight and clear lines of responsibility | All processes completed in-house to a high standard | All processes are mostly completed in-house. | Low |

Based on the risk analysis above, we can observe that few high risk factors are inherent for mobile money (e.g. Cash In, p2p transfer) which cannot be eliminated, but other high risk factors can be mitigated through enhance regulation and monitoring (e.g. CDD verification and monitoring, maximum number of account per customer, etc.). So, the Chapter 3 of this Study Paper focuses on risk mitigation through changes in existing regulation, enhance monitoring and encouraging low risk business practices, etc.

### 2.3 Underlying causes of abuse of MFS in Bangladesh

Based on the analysis of MFS related complaints/cases received by different agencies and research findings, the following key factors have been identified which are contributing for the abuse of m-money in Bangladesh:

a) Agents acquire and register multiple SIM cards and thus mobile money accounts to use them for transactions. As a result, customers do not need a registered mobile account and transactions can be made anonymously. Moreover, customers see registration as an unnecessary step to take when service can be easily obtained without registering.

b) People prefer agents as they find it difficult to navigate the mobile menu required to conduct transaction. The mobile menu is in English which makes it difficult for customers, having low academic qualification, who are not well conversant in English.

c) KYC of mobile phone SIM was not accurate largely before 2016 and most of MFS accounts are based on those inaccurately registered SIMs. However, bio-metric registration of mobile SIMs has been completed in 2016 and customer information of MFS account need to be updated accordingly.

d) No face to face contact of customers with MFS providers.

e) Highly dependence on Agents, who are mainly small shop keepers, with minimum control over them by the MFS providers.

f) Lack of unique identification documents for all citizens and absence of ID verifica tion tools for all MFS providers. Some low income population lack acceptable KYC documents which are required for account opening.

g) Lack of appropriate monitoring tools to identify irregularities of the agents.

h) Adequate monitoring and supervision mechanism is yet to be developed and deployed by the MFS providers and the regulators.

i) Aggressive marketing strategy of a few MFS provider(s) for rapid customer acquisition compromising the legal/regulatory requirements.

### 2.4 Abuse of mobile money in Bangladesh

Analysis of typologies related with abuse of products/services is a very crucial part of any risk assessment. In the last few years, we have observed abuses of MFS in many ways and the trend is rapidly evolving in nature. During analysis/investigation of MFS related criminal cases, it has been observed that criminals mostly abuse mobile accounts registered with fake identity. "While we ask for KYC information during investigation of any relevant crime, 99 out of 100 KYCs are turned out to be with false registration. Of course, if criminals have easy opportunity to open mobile account in fake names, why will they open account exposing their real names?" quipped an investigator from CID, Bangladesh Police in 2014. A section of agents simply ignore minimum CDD as per regulatory and service provider's requirements during opening accounts. In many cases, agents themselves are found actively involved in various kinds of criminal activities including collection of ransom money by human trafficking, extortion, fraud by maintaining several accounts with mostly false and sometimes with real identity.[49]

Agents are mostly small corner shops who are not adequately trained on ML/TF risk and mitigations. They, being quasi-independent operators, find little problem in violating regulation in order to make money. Their interest is in processing as many transactions as possible as their earning depends on commissions rendered on transactions. Inadequate monitoring mechanism for agent network by the service providers aggravated the problem.

### 2.5 Typologies on abuse of MFS

The increasing number of mobile phone based crimes has become a major concern to the general public and law enforcement agencies in the last few years. After emergence of MFS, criminals exploited it due to inadequate CDD and monitoring along with limitations of regulatory, law enforcement and intelligence agencies' effort in using new technology. Common types of fraud that are committed through abuse of MFS are presented in next sections. Such cases are analyzed and investigated by BFIU and LEAs of Bangladesh in recent times.

[49] "New-fangled Crime trend about Mobile Financial Services in Bangladesh", CID, Bangladesh Police (2015), p.16

### 2.5.1 Fraud through auto-theft

Organized criminals use to hijack/steal motorcycle, auto-rickshaw, microbus, etc. and they call the owners instead of looking for customers to sell the stolen vehicles and asked them to send money through MFS promising to return their vehicles. Sometimes they return the stolen vehicles, but mostly they do not return it after receiving the money from the owners. They earn between BDT 30,000 and BDT 5,00,000 per vehicle depending on the value of the stolen vehicle . The MFS accounts used are either registered with fake documents or accounts operated by agents for OTC. In both cases, the criminals cannot be identified.

### 2.5.2 'Hello party' fraud

Organized criminal groups use mobile numbers which resemble mobile network operators' service center number (e.g. 0xxx9000000 or 0xxx1123456) and pretend to be representatives of MNOs. Victims are informed about 'winning' a set of ornaments, lottery, a piece of land or a flat in the capital, etc. Sometimes, the criminals use special welcome tune or caller tune that represents a big company or a LEA. Victims are then asked to send a small amount of money through MFS accounts for 'registration' of the program or to bear the initial expenses. Once a victim pays the small amount, then the criminals try to exploit their prey further. Even educated people, like retired senior government and military officer, in-service Vice Chancellor of university or member of civil society were the victim of such criminal groups. Most of the criminals, who hardly completed secondary education, exploited greediness of their victims. Several villages of two districts under Dhaka division in Bangladesh become infamous for the activities of such all-on-a-sudden-rich people. But, most victims feel shy to put formal complaint to LEA to hide their sheer stupidity.[50]

### 2.5.3 Fraud by so-called company/firm, expatriate family, etc.

In many cases, mass media are used to lure people with lucrative offers. In such a case, a prospective groom responded to an advertisement published in a national daily with an aim to marry an Australia based expatriate bride! As soon as the prospective groom contacted in the number provided in the advertisement, he was asked if he had passport. As the victim did not have a passport, the fraudster asked the victim to send Tk. 5000 to the fraudster's MFS account to expedite the processing of passport. After Police arrested the 'bride', the investigators found that her impersonated 'father' was actually her husband and none of them had Australian citizenship.

### 2.5.4 Fraud and extortion by *'Genier Badsha'* (King of Genie)

Perhaps one out of 25 regular mobile users of Bangladesh has received phone call from 'genie of the 4th sky', who promise to give one big jar with full of ancient gold coins. The

50 "New-fangled Crime trend about Mobile Financial Services in Bangladesh", CID, Bangladesh Police (2015)

call recipient just need to top up Tk. 25 to the caller's mobile number as the 'genie' made the super-natural communication through mobile phone of a human and made financial loss to him. Ninety nine out of 100 recipients, of course, simply ignore the caller. Then the genie starts delivering sermons to that rare believer time to time. By and large, people from rural areas, mostly women, become victims of such genie. The crime starts with a fraudulent call but mostly continues with threat and extortion. The genie claims that victim herself or her son or husband or other important family member will instantly die, if she fails to comply genie's order or if she informs it to anybody else before receiving the jar- full of gold coins. The 'genie' trapped the victims and in many previous cases, they paid the 'genie' even by stealing or selling their own properties. A northern district of Bangladesh is infamous to run such 'genie' business, where rickshaw pullers to upazila chairman, shopkeepers to MFS agents are involved with such crime. There are numerous victims from all around the country who became their prey. But when a victim reports to police, he or she has no evidences but a falsely registered mobile number vis-à-vis MFS accounts of the fraudster. Nonetheless, the criminals change SIM and/or mobile hand set after each successful operation and look for new prey.

**Case study : Master-of-all trades TV-saint**

In the dead of night, few satellite TV channels in Bangladesh broadcast program on saints of various religions, who are simply master-of-all-trades. The TV programs portray that the blessings of these saints or their 'tabiz' will certainly solve any kind of problem. If you want to win a lottery or the heart of your most desired girl/boy or want to defeat enemy or control your boss, or want to get rid of sufferings from old diseases, the TV saints will help to overcome those crisis. The solution is only a call away! Expatriates are mostly target of such TV saints, which are broadcasted between 0200 hrs to 0400 hrs of Bangladesh time. CID of Bangladesh Police had investigated a case of a middle-east based expatriate in 2015 who lost BDT 62 lakh ($80,000) to such a TV saint. CID team had identified a number of criminal gangs based on a northern district of Bangladesh who are linked with some capital city based electronic and print media. In another case, CID investigators have found that a Dhaka-based housewife had a severe brain stroke after she understood that she had been cheated by the TV-saint. She fell victim to a TV saint and lost Tk.7,50,000.00 ($9500) – which is of course, a lot of money for a middle-class housewife.[51] In all cases, payments were made through MFS accounts.

### 2.5.5 Extortion by the name of top terrorists

There are many cases where businessmen, industrialists or service holders receive unknown call and the caller introduce themselves as infamous terrorists or as their close associates and demand for money. Sometimes, the so called 'terrorist' is the neighbor's iniquitous lad or sometimes

51 "New-fangled Crime trend about Mobile Financial Services in Bangladesh", CID, Bangladesh Police (2015)

a wanted criminal calling from the land-border with neighboring country. Criminals use the terrorists' names that receive more media coverage. Criminals use lines such as 'haven't you see in the last week on TV; that is us - who have committed that murder' and order their victims to send money. Such types of extortion are in rise after the introduction of MFS, especially because of easy access to anonymous transaction. The 'terrorist' sometimes provide detail information of the victim and threaten to abduct/kill his family members. As the victims do not have any face to face conversation with the 'terrorist', he/she have no clue to know the real culprit. Sometimes, they are afraid of reporting the incident to the LEA fearing safety of family members.

### 2.5.6 Abduction/kidnapping for ransom

Traditionally, organized group abduct a man or kidnap a child and ask for ransom. But, there is new version of kidnapping where criminals offer a short-lift to a home bound job holder or a city dweller (e.g. a distance of 10 km from Kawran Bazar to Uttara of Dhaka city). Criminals usually take their victims into their vehicle. Once the victim gets inside the vehicle, the criminals compel the victim to call his/her spouse or other family member to pay a 'tolerable' amount of money (e.g. BDT 15,000 to 30,000). The criminals actually keep on roaming around the city or in the highway with the victim inside the vehicle. They release the victim just after ransom money is paid through MFS accounts. No hideout, no watchman, no feeding arrangement is required for such kidnapping. This is a crime with one vehicle and few MFS account numbers and those are the personal accounts of a nearby MFS agent![52]

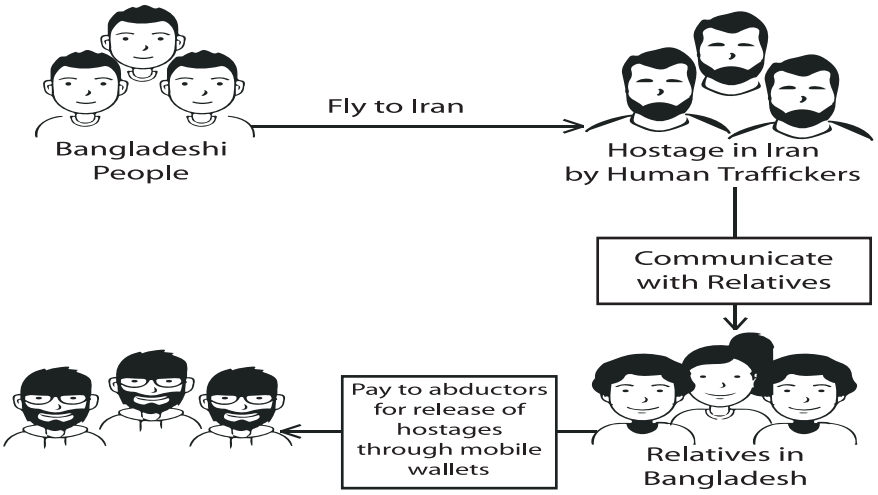
**Case study : When MFS agent is a part of international human trafficking gang**

A gang of unscrupulous Bangladeshi human traffickers lured some young men to fly to Iran on the promise of providing them better jobs and handsome salary. Traffickers lured Bangladeshi expatiates mostly from Dubai and Sharjah in the United Arab Emirates (UAE) at different times with the promise of lucrative jobs in Saudi Arabia, Iraq and Greece. These men were picked up separately and taken to Iran where they were confined inside a house secretly. Their passports, documents and other valuables were confiscated.

The traffickers then forced the hostage to contact with their families in Bangladesh to pay ransom for their release. Each hostage were forced to pay between BDT 1,50,000 (USD 1948) to BDT 3,00,000 (USD 3896) through a popular mobile financial service provider of Bangladesh for their release. The case was forwarded to CID of Bangladesh Police by Bangladesh Financial Intelligence Unit for investigation and 13 kidnapped persons were rescued from Iran with the help of Iranian Authority.[53]

52 "New-fangled Crime trend about Mobile Financial Services in Bangladesh", CID, Bangladesh Police

53 Annual Report 2014, Bangladesh Financial Intelligence Unit, P. 58




CID arrested an MFS agent, Farid with 87 SIMs - all with falsely registered personal MFS account. Farid was an agent and also user of all these 87 accounts. He collected the ransom (BDT 2.15 million) from victims' family and channeled those to trafficker's family members - surprisingly one of whom is a college teacher, while agent Farid himself is a school teacher. Some associates of the traffickers received money from another Chittagong based MFS agent who was also arrested by CID after conducting a number of operations.[54]

### 2.5.7 Anonymous transaction (ATr)

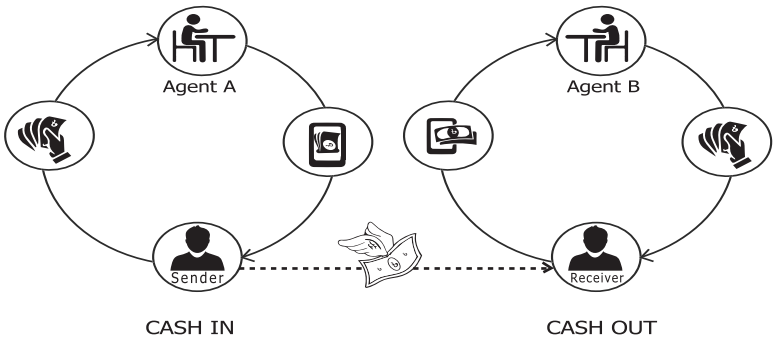
ML/TF prevention laws require accurate and complete information of customers in any financial transaction. Bangladesh Bank regulation requires each customer to have their own wallet to avail mobile financial services. Over The Counter (OTC) transaction is not permitted in the existing regulation. But, we have been observing a trend of anonymous transaction in MFS of Bangladesh from the very beginning; where sender's or receiver's or information of both is absent in the transaction trail. It has been evident from the MFS related crime investigation that in almost all cases, criminals resort to Anonymous Transaction (ATr) to disguise their identity. A criminal will certainly be encouraged if s/he knows that nobody can identify her/him after the crime.

To prevent abuse of MFS, Bangladesh Bank regulation (2014) permits a customer to maintain only one personal account with an MFS provider. But, BFIU findings revealed that millions of personal accounts have been still operated violating the existing regulation and those are mostly used for anonymous transaction.

54 "New-fangled Crime trend about Mobile Financial Services in Bangladesh", CID, Bangladesh Police (2015)

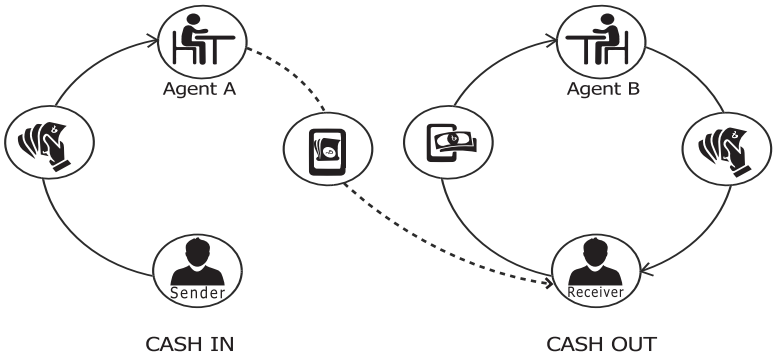
There are several process of anonymous transaction observed in Bangladesh. Those are described graphically below:

**P2P Transaction: Ideal Scenario**



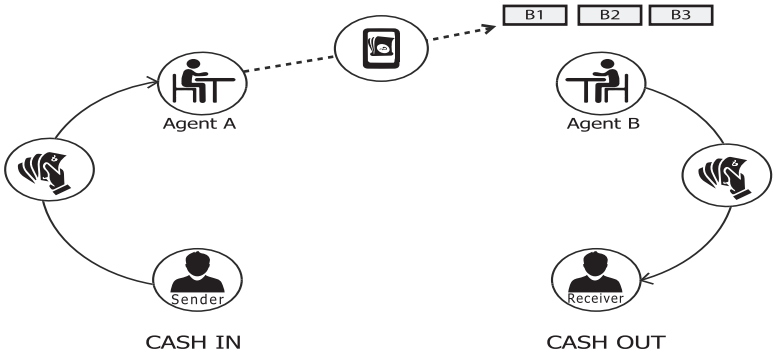

**P2P transaction :** In an ideal scenario, sender and receiver suppose to have their own MFS wallet and use them for P2P transaction.

**Anonymous Transaction (ATr)**

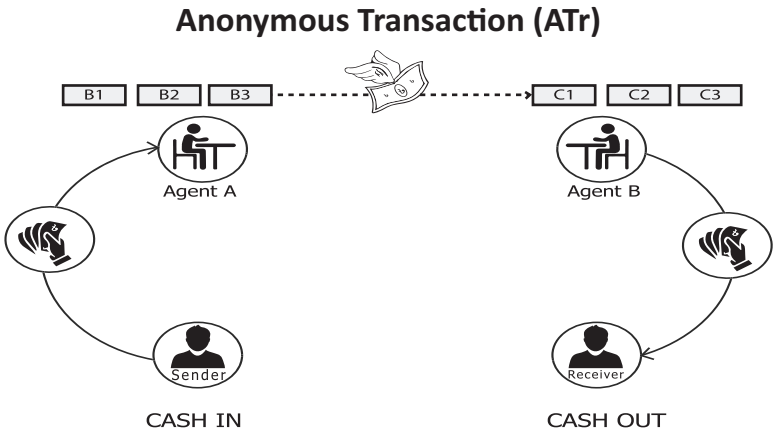



**ATr (type- A) :** Sender does not have/use own wallet, rather Agent A made direct deposit to receiver's wallet. In such cases, sender is absent in transaction trail.

**Anonymous Transaction (ATr)**

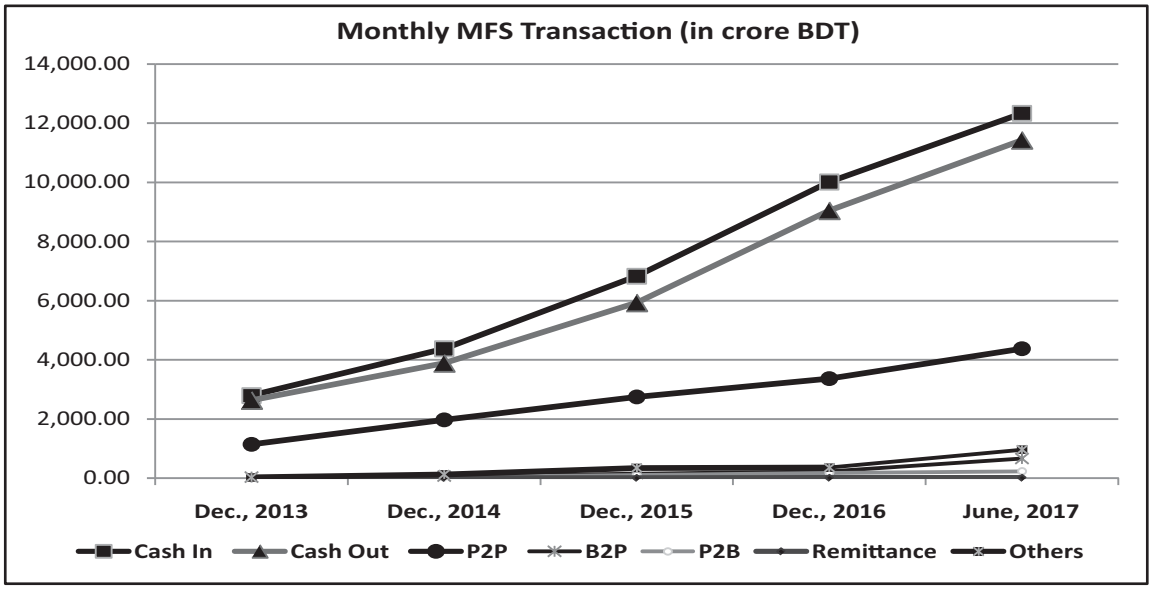



**ATr (type-B) :** When sender and receiver do not have/use their own wallet and Agent-A made Cash In to personal wallet of Agent B. In such cases, both sender and receiver are absent in the transaction trail. Agent B uses personal wallets - may be registered in the name of different individuals- to receive e-money from Agent-A and paid cash to receiver.




**ATr (type- C) :** When sender and receiver do not have/use their own wallet, agents made P2P transaction with their personal wallets on behalf of the customers. In such cases sender, receiver and respective Agent accounts are absent in the transaction trail.

If we analyze the pattern of transaction of MFS in Bangladesh Cash In, Cash Out and P2P are the dominant, and volume of other types of transaction is still low. Cash In and Cash Out transaction are growing in the same pace, but a wide gap observed with P2P. High prevalence of anonymous transaction can be explained as the main cause for such gap. The P2P transactions shown in the graph are also includes anonymous transaction in the form of P2P (ATr type-C described above). Though the actual estimation of anonymous transaction is difficult, but available facts and figures indicates that the percentage would be very high.

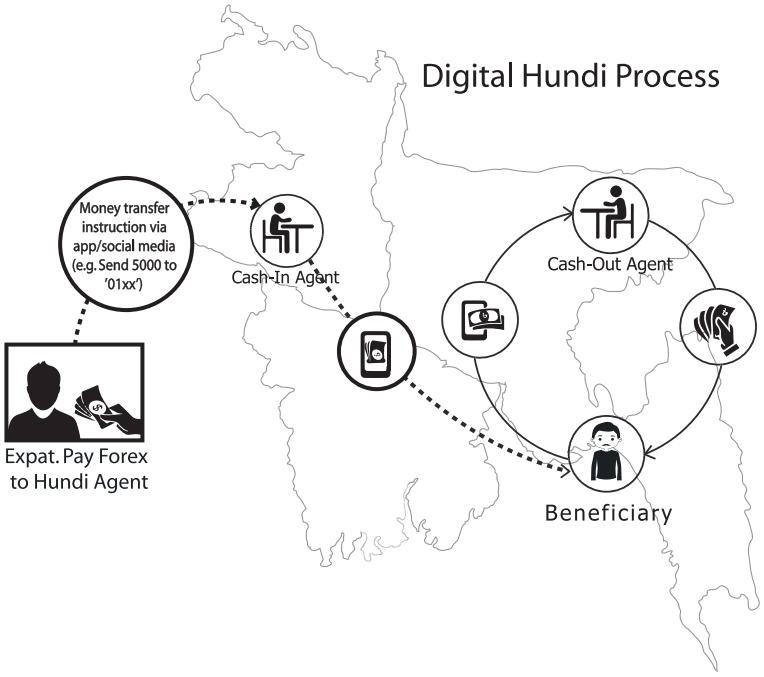



### 2.5.8 Abuse of MFS for illegal foreign remittance (Digital hundi)

Bangladesh Bureau of Statistics conducted "The Survey of Investment from Remittance (SIR) 2016" to find out utilizations of inward foreign remittance in Bangladesh. As per their survey, 14.31% inward foreign remittances in Bangladesh are coming through

mobile banking.[55] Bangladeshi expatriates in Saudi Arabia, UAE and Malaysia are the major remittance senders and 16.98%, 11.65% and 14.11% of those remittances respectively are coming through MFS in Bangladesh. Highest 35.29% remittance from Maldives is coming through MFS. Foreign remittance can be channeled through MFS account via banks and it was less than USD 1.00 million in June, 2016 which is a very insignificant amount. But, major portion of inward remittance is coming through illegal channel, including hundi through DFS (Digital hundi). Meanwhile, total receipts of workers' remittance decreased by 17.83 percent during July-September, 2016 and stood at USD 3.23 billion as compared to the same period of the previous fiscal year.[56] There is probably direct correlation between increasing trend of Digital hundi and decreasing trend of workers remittance.

Bangladeshi exchange houses working abroad and commercial banks have complained to the respective central banks that small size foreign remittance has fallen drastically in recent times and those are coming in Bangladesh through MFS illegally. MFS is mostly used for Digital hundi, i.e. remittance agents receive foreign currency and MFS account information from the sender in abroad. Then the remittance agent sends the information to his Bangladeshi counterpart, who might be an MFS agent. He sends e-money to the beneficiary's MFS account. Thus, no foreign currency enter in Bangladesh and most of the times, transactions are conducted anonymously which creates great risk of ML/TF. Bangladesh Bank and Bangladesh FIU have also taken initiatives to identify those illegal foreign remittance channels in 2017 and combat those through enforcement and cooperation with foreign and local counterparts. The mitigation measures have already yield significant positive inflow of foreign remittance in Bangladesh.




55 'Report of the Survey on Investment from Remittance 2016', Bangladesh Bureau of Statistics, P. 15

56 'Major Economic Indicators: Monthly Update', October 2016, Bangladesh Bank, P.17

# CHAPTER 3

## AML/CFT Regulations for MFS : Policy Options for Bangladesh

### 3.1 Legal framework for regulation of MFS in Bangladesh

i) **Bangladesh Bank Order, 1972:** Bangladesh Bank had issued "Guideline on Mobile Financial Services for the Banks" through DCMPS Circular 8 in September, 2011 which laid the foundations for the mobile financial services in Bangladesh. The guidelines issued as per the Article 7A(e) of Bangladesh Bank Order, 1972 and Section 4 of Bangladesh Payment and Settlement Systems Regulations, 2009.

Article 7A(e) describes one of the main function of Bangladesh Bank "to promote, regulate and ensure a secure and efficient payment system, including the issue of bank notes". Bangladesh Bank approves banks to provide MFS under para 7.1 of the "Guideline on Mobile Financial Services for the Banks" . Bangladesh Bank may withhold, suspend or cancel such approval if 'it considers any action by any of the parties involved in the system detrimental to the public interest."

ii) **Proposed National Payment System Act:** Bangladesh Bank has proposed enactment of NPS Act for the establishment and operation of a national payment system and for its regulation; and oversight of electronic payment. A draft of the Act has already been in the final stage after public consultation. There are provisions for licensing and oversight of payment services, offences and penalties, etc. The proposed Act empowers Bangladesh Bank to regulate and oversee the national payment system. After promulgation of the Act, MFS providers shall also be licensed and supervised under the provision of it and oversight would hopefully be robust enough.

iii) **MLPA, 2012 & ATA, 2009:** 'Any company or institution which remits or transfers money or money value' has been included as Reporting Organization under the provisions of Section 2(w)(v) of Money Laundering Prevention Act, 2012 and Section 2(20)(e) of Anti Terrorism Act, 2009. As Mobile Financial Services (MFS) providers offer such types of services, so those are also treated as Reporting Organization under the said provisions.

The responsibilities of the reporting organizations under MLPA, 2012 are [Section 25(1)]: collect accurate and complete information of its customers, preserve information of customers for five years after closure of business relationship, provide the said information to BFIU as requested and send suspicious transaction reports to BFIU spontaneously. As per provision contained in Section 25(2) of MLPA 2012, BFIU and Bangladesh Bank may impose sanctions on reporting organizations for non-compliance of provisions contained in Section 25(1) of

the said Act. The sanctions include penalty from BDT 50,000.00 (USD 610) to 2.5 million (USD 30,500) and additionally, cancellation of license/approval of branch, service center, booth or agents or may request licensing/registration authority to take necessary action.

As per FATF Recommendation 27, supervisors should have adequate powers to supervise or monitor, and ensure compliance by financial institutions with requirements to combat money laundering and terrorist financing including the authority to conduct inspections. Supervisors should have powers to impose a range of disciplinary and financial sanctions, including the power to withdraw, restrict or suspend the financial institution's license, where applicable.

There are few enforceable tools under the provisions of Bangladesh Bank Order, 1972. On the other hand, provision for financial and disciplinary sanctions under MLPA, 2012 meet the FATF criteria and are enforceable by both BFIU and Bangladesh Bank.

## 3.2 Recommendations to mitigate ML/TF risks related with MFS in Bangladesh

After analyzing global AML/CFT related standards, practices, relevant acts/regulations and trend of abuses of MFS in Bangladesh, the Focus Group would like to recommend the following policy options for the regulatory and supervisory authorities. Any instruction/guidance issued following the recommendations should be applicable for all companies/institutions which are authorized by Bangladesh Bank to provide Mobile Financial Services under the relevant act/order/regulation/ guidelines.

### 3.2.1 AML/CFT compliance structure of MFS providers

#### i) AML & CFT policy/manual

All MFS Providers (MFSPs) should have their own AML & CFT Policy/Manual that conforms to the relevant international standards, laws and regulations in force in Bangladesh and instructions of concern authorities for prevention of ML & TF. The policy/manual should address recommendations contained in this chapter and it should be approved by the Board of Directors of the institution. The AML & CFT policy/manual should be reviewed periodically and amended/changed, if necessary.

#### ii) Declaration of commitment on AML & CFT program

Company that solely provide MFS (referred as 'MFS company' thereafter) should communicate a Statement of Commitment issued by its CEO to all of their employees which clearly states organizational stance against ML & TF. Schedule banks that provide MFS should include a separate paragraph stating their stance against abuse of MFS in the Statement of Commitment issued by CEOs annually. All MFSPs should ensure the implementation of the commitment.

### iii) Central Compliance Committee (CCC) & CAMLCO/Compliance Officer

(1) To protect m-money from the risks of ML & TF and for the proper compliance of all existing acts, rules and instructions issued by competent authority, MFSPs should follow the following instructions:

a) MFS companies should set up a Central Compliance Committee (CCC) to mitigate the risk of abuse of MFS from ML & TF. CCC should be headed by a senior level officer (not below the 2nd level of the CEO in organizational hierarchy) and will be known as 'Chief Anti Money Laundering Compliance Officer' (CAMLCO). The activities of CCC should be directly reportable to the CEO of the MFSP. If the CAMLCO is changed, it should be communicated to BFIU without delay. Before assigning the CAMLCO any other duties, the management has to ensure that AML & CFT activities of the MFSP will not be hampered. MFSPs may also nominate a high level official as Deputy Chief Anti Money Laundering Compliance Officer (DCAMLCO) in the CCC depending on the size and operation of the MFSP.

b) The CCC should consist of at least 5 (five) members who will be high officials of different departments of the MFS company including the CAMLCO. Among them, 3 (three) members should be nominated from Commercial/Operation Division, Distribution Division and Technology/IT Division (one member from each Division). But, no official from Internal Audit Division should be included as a member of CCC.

c) Banks, which are providing MFS within their existing organizational structure, should nominate an AML/CFT Compliance Officer (not less than one level below of the Head of concern department) for their MFS operation and include him in Central Compliance Committee (CCC) of the bank. The said officer should be reportable to CAMLCO of the bank through Head of concern department.

d) The CAMLCO of MFS Company or AML/CFT Compliance Officer of banks should have at least 5 (five) years of experience on AML/CFT compliance.

e) All members of CCC and Compliance officials of MFSPs should have in-depth knowledge on the existing acts, rules/regulations, instructions issued by BFIU and international standards related to prevention of ML & TF.

(2) To mitigate ML/TF risk, all MFSPs should set their institutional strategies and procedures and review those from time to time. CCC should ensure the implementation of AML/CFT policy and strategies under the leadership of CAMLCO of the organization.

(3) CAMLCO of MFS Companies and AML/CFT Compliance Officer (MFS) of banks should have the following responsibilities:

a) Ensure compliance of AML/CFT policies and strategies of the organization;

b) Monitor, review and coordinate application and enforcement of the AML/CFT compliance policies which include AML/CFT risk assessment, practices, procedures and quality controls of account opening, KYC procedures and ongoing transaction monitoring for detecting suspicious transaction/activity;

c) Monitor changes in relevant laws/regulations and directives of BFIU and any other regulatory agencies, and revise the internal AML/CFT policies and procedures of the organization accordingly;

d) Respond to AML/CFT compliance questions and concerns of the staffs and provide necessary advice or assistance for solutions to potential issues involving AML/CFT compliance and risk management;

e) Ensure that the AML/CFT policy/manual is complete and up-to-date in maintaining ongoing awareness of new and changing business activities and products and to identify potential compliance issues that should be considered;

f) Develop and maintain ongoing relationships with regulatory authorities, external and internal auditors, business channel partners and other stakeholders to ensure AML/CFT compliance;

g) Monitor the business through self-assessment for AML/CFT compliance and take corrective measures, if required;

h) Explore, analyze and assess companywide ML/TF risk and recommend mitigation measures;

i) Identification of suspicious transaction/activity indicators through appropriate transaction monitoring and sanction screening and train relevant officials;

j) Send suspicious transaction/activity report to BFIU after analysis by concerned officials;

k) Undertake capacity building programs for employees, distributors, agents, and other channel partners on AML & CFT; and

l) Any other responsibilities to ensure AML & CFT compliance.

(4) CCC of all MFSPs should submit a report on AML/CFT initiatives taken by the MFSP including the progress of implementation with recommendations on a yearly basis (January–December) to the CEO of the MFSP for information and further instructions. Any initiative, if adopted by BFIU on preventing ML and TF for MFS should be included in that report. With the instructions and comments of the MD/CEO, the report should

be presented in the meeting of Board of Directors or highest Management Committee and a copy of the report should be sent to BFIU within 2 (two) months on completion of the respective year of reporting.

(5) MFSPs which have more than 20 thousand agents or 01 million customers should form a separate AML/CFT Compliance Section/Wing (or whatever name it may be called) with adequate manpower in addition to CCC. Such Section/Wing will assist CCC and CAMLCO to perform its responsibilities including identification of STR/SAR by transaction monitoring, review of KYC and provide AML/CFT training, etc.

(6) MFSPs should nominate/appoint appropriate numbers of Field Compliance Officer (or whatever name it may be called) depending on the organizational structure of its operations. The responsibilities of the Field Compliance Officer should be:

- Monitor transactions of specific number of customer, agent and distributor accounts to identify suspicious transaction;
- Inspect agent and distributor offices to check compliances;
- Send Suspicious Transaction/Activity Report (STR/SAR) to CAMLCO or AML/CFT Compliance Unit/Department;
- Monitor compliance of AML/CFT regulations while opening accounts; and
- Send quarterly report to CAMLCO or AML/CFT Compliance Unit/ Department on AML/CFT compliance monitoring, etc.

### 3.2.2 Definition of customer

In the context of identifying customer of MFSP and verifying the customers' identity for ML/TF risk management, customer refers to the individual or entity that maintains/operates an account with the MFSP (except agents and distributors). The customer accounts may be two types:

(1) Personal Account

(2) Business/merchant/organizational Account

### 3.2.3 Customer identification

(1) It is an obligation for MFSPs to collect complete and accurate information of their customers to mitigate ML/TF risk. To comply with it, MFSPs should conduct Know Your Customer (KYC) procedure to ensure that all the necessary/proper information of the customers has been accumulated and verified.

(2) To mitigate ML/TF risk and ensure sustainable advancement of financial inclusion, MFSPs should adopt electronic KYC (e-KYC) for registration of their customers and introduce biometric authentication in phases. Information of the customers should be collected as per Account Opening Forms attached with this Study Paper and preserved in database as part of e-KYC. In that case, hard copies of the KYC documents may be replaced by electronically collected information.

### 3.2.4 Customer acceptance policy

MFSPs should have a well defined customer acceptance policy. Such policy should cover the following issues:

(1) No account shall be registered using a fictitious name or pseudonym or numbered only. Title of the account shall be same as appeared in the photo ID document(s) and SIM registration database.

(2) At least one verifiable photo ID document issued by a government authority should be collected against each account.

(3) Any person or mobile number which is blacklisted in Bangladesh Bank database based on the complaint by any MFSP on attempted/proven fraud/financial crime should not be accepted as a customer/agent/distributor by other MFSPs

(4) MFSP should have the right to deny providing services to any customer, if there is suspicion that MFS may be abused for criminal purposes by the person or reputation risk may arise from such business relationship.

(5) Accounts can neither be registered nor be operated by the persons or entities listed in United Nations Security Council Resolutions (UNSCR) and Domestic Sanction List. Domestic Sanction List refers to the persons or entities enlisted in public gazettes by the Government of Bangladesh under the power conferred in Section 18 of ATA, 2009. Both the UNSCR and Domestic Sanction Lists can be downloaded from the following web links:

http://www.un.org/sc/committees/index.shtml and
http://www.bb.org.bd/aboutus/dept/bfiu/sanction_list.php

### 3.2.5 Account opening procedures for personal account

(1) MFSPs should collect customers' information as per relevant Forms discussed later parts of this Study Paper as minimum requirements. MFSP/agent should collect sufficient information, so that the customers can be identified and located later on.

(2) Physical presence of the customer in front of the agent/Customer care center of the MFSP should be mandatory.

(3) Photo identity document of the customer issued by the government (e.g. NID) should be collected and verified by MFSP.

(4) Photograph, ID photo and appearance of the customer should match with each other.

(5) The intended customer/account title holder of MFS should have mobile SIM registered in his/her name and necessary verification should be made.[57]

(6) MFS A/C may be opened remotely, but physical presence of the customer at Customer care center/agent point of MFSP is mandatory for registration/activation of such account. Physical presence of customer as well as separate KYC is not mandatory for 'Link A/C' associated with existing bank account of the customer.

(7) After opening an account in agent point or remotely, only Cash In may be allowed before verification of KYC and registration of the account by the MFSP. After registration of the account with proper verification, other types of transaction may be conducted.

(8) One individual can maintain/operate only one personal account with a MFS provider, except in the circumstances described in the next paragraph.

(9) To ensure access to financial services for all segments of population and mitigating risk as well, the following exceptions may be allowed for certain circumstances:

a) If an intended customer does not have verifiable photo identification document and/or registered SIM, another identity document (e.g. birth registration, passport, etc.) of the customer should be collected and he/she should be introduced by his/her parents/siblings/spouse/offspring (any one) having verifiable photo identification document. However, the title of the account may be in the name of the introducer (as respective SIM is registered in his/her name), but account may be operated by the operator after written authorization by the introducer. The introducer along with the operator should be present while opening the account and KYC of both persons should be collected. However:

- A person should not introduce more than 02 (two) of his/her relatives to operate MFS accounts opened in the name/title of the person.
- An adult person (Age 18+) should submit a verifiable photo identification document of his/her within two (2) years after opening of such an account.

[57] Bangladesh Telecommunication Regulatory Authority (BTRC) made bio-metric SIM registration mandatory submitting NID of the customer. However, customers lacking NID may register SIM temporarily for 06 (six) months submitting passport/driving license/birth registration certificate. Non-resident Bangladeshis and foreign nationals can register SIM with their passport copy. All SIM registration without NID must be done in Customer care center of MNOs (Ref.: BRTC order in 13/12/2015)

b) Foreign nationals living in Bangladesh and non-resident Bangladeshis can open MFS account by submitting copy of valid passport. Foreigners are also required to submit valid visa and work permit. Such accounts of foreign nationals should be closed after expiry of visa/work permit or the customer leaves Bangladesh.

c) All types of 'exception' accounts can only be opened at the Customer care center/branch of the service provider and would be for limited purpose (maximum Level-1 account) only.

### 3.2.6 Progressive KYC for personal accounts

MFSP should open customer account as per procedures described in the previous paragraph. There are several ways of collection and verification of customers' information/documents described as follows:

| SL | Know Your Customer (KYC) Tools | Yes = 1<br>No = 0 |
|---|---|---|
| A)* | Has the information stated in account opening form been properly collected? | |
| B)* | Has a government issued photo identity document been collected & verified? | |
| C)* | Has recent photograph or real time electronic photograph of the customer been collected and matched with ID document photo? | |
| D) | Has the concern SIM registration information been verified[58]? | |
| E) | Has the account been opened at the customer care point of the MFSP in the presence of the customer? | |
| F) | Has the MFS account been linked with a bank account of the customer? | |
| G) | Has the biometric information of the customer been collected and included in e-KYC? | |
| | **Total Points =** | |

One point shall be assigned against each affirmative response of the above KYC tools. Based on the reliability of KYC, personal accounts may be categories in the following 3 (three) Levels:

a) If KYC information of a customer receives three (3) points, the account will be termed as **Level-1 account**.

[58] As per decision of the 5th Ministerial Meeting on Law and Oder situation of GoB, informed by the Ministry of Home Affairs on 30.12.2014, all SIMs shall be re-verified by the MNOs against NID database. Then, MFS accounts would be opened based on the registered SIM. Ministry of Home Affairs also have taken a decision on 10.06.2014 that all MFS customers must have SIM registered in his/her name.

b) Accounts with four and five (4-5) points will be termed as **Level-2 accounts**.

c) Accounts more than five (6-7) points will be termed as **Level-3 accounts**.

However, first 03 (three) KYC requirements are mandatory for opening any MFS account.

### 3.2.7 Transaction profile for personal accounts

a) Based on the risk involved due to variation of quality of KYC/CDD discussed above, daily and monthly transaction limit, merchant payment, remittance acceptance and highest account balance should be determined by Bangladesh Bank.

An example has been given here for illustration only:

| **Types of account** | **Daily maximum transaction limit** (debit & credit separately) | **Monthly maximum transaction limit** (debit & credit sum separately) | **Maximum account balance** |
|---|---|---|---|
| Level- 1 | Tk. 10,000.00 | Tk. 25,000.00 | Tk. 25,000.00 |
| Level- 2 | Tk. 25,000.00 | Tk. 50,000.00 | Tk. 50,000.00 |
| Level- 3 | Tk. 50,000.00 | Tk. 2,00,000.00 | Tk. 1,00,000.00 |

b) Foreign remittance received in MFS accounts should be beyond the transaction limit stated above provided that the customer provides relevant documents (copies of passport, visa & work permit) of sender(s) to MFSP at once. The MFSPs shall follow the regulation/approval of Foreign Exchange Policy Department and Payment System Department of Bangladesh Bank regarding foreign exchange transaction.

c) Considering the technological, financial and management challenges, instructions contained in paragraphs no 3.2.5, 3.2.6 & 3.2.7 should be effective after 06 (six) months of the issuance of the relevant guidelines/circular.

### 3.2.8 MFS account linked with bank account

a) MFS account can be linked with any existing bank account of the same customer upon informed consent. Additional KYC should not be required for the Link Account, if both the accounts are operated within the same bank; or with subsidiary of the same bank - if relevant law/regulation permits sharing of KYC of banking customer with its subsidiaries. In other cases, separate KYC should be required and necessary verification should have to be done. However, the ultimate responsibility regarding KYC of MFS A/C will lie on the MFSP.

b) Both inward and outward transfer may be allowed between bank and MFS A/C. There will be no limit for transfer of fund from MFS A/C to bank A/C. But, in case of transfer from bank A/C to MFS A/C, the transaction limit applicable for concern MFS A/C may be applied or as determined by the concern bank.

### 3.2.9 Opening of business/merchant/organizational account

a) Any entity or organization may open MFS account for its operational/business purposes.

b) MFSPs should collect information/documents as per KYC form attached in Annex-2 as minimum requirements while opening impersonal accounts. The information of relevant individuals of the organization/entity should be collected as per Annex- 3. The documents listed under each category of organization in Annex-4 should be collected. However, additional identity/business documents may be collected as per satisfaction of the MFSP.

c) If monthly transaction (debit or credit separately) of any business/merchant/ organizational account exceeds Tk. 50,000.00 in any month, KYC procedures applicable for Level- 2 or 3 personal accounts should be followed for the key individuals/owner of the entity/organization.

d) Physical verification of the business premise(s) should be conducted along with business volume assessed by the MFSP before opening such account.

e) Business/merchant/organizational account can receive and make payment and may Cash out from bank branch or distributor's office of the MFSP.

f) Business/merchant/organizational account with high volume of transaction should be linked with a bank account of the entity/organization and fund may be transferred between the said accounts.

g) Transaction Profile of the customer should also be assessed as per Annex- 5 against each impersonal account based on nature of business, location of business, monthly sales/turn over, etc. However, MFSP should implement Risk Based Approach (RBA) and take additional measures as appropriate to monitor transaction in such accounts.

h) Merchant/organization/institutions may be allowed to operate multiple MFS accounts for business purposes.

### 3.2.10 Customer due diligence

a) Considering the ML/TF risk of the customer, CDD should be conducted at the following stages:

   i. While establishing a business relationship with the customer;

   ii. For existing customers while carrying out transaction;

   iii. Information and documents previously obtained for the purpose of identification or verification seems insufficient.

   iv. Monitoring of transactions to identify suspicious transactions.

b) MFSP should take necessary measures to identify Influential Person (IP) while opening an account (including agent and distributor account) as well as through ongoing CDD and implement enhance due diligence (EDD) for such cases.

c) MFSP should take necessary measures to review and update the KYC of the customers after every 5 (five) years. However, MFSP should update the KYC if any relevant information of the customer received earlier than schedule of next review.

d) If conducting the CDD becomes extremely difficult because of the non-cooperative behavior of the customer or if the collected information seemed to be unreliable, i.e. MFSP could not be satisfied with the information on customer identification and could not verify that, following measures should be taken:

   i. MFSP should not establish business relationship with the customer or may terminate any existing business relationships with the customer. Prior to closing such existing account, the customer should be notified through SMS in this regard.

   ii. If the circumstances seem suspicious, STR/SAR should be submitted to BFIU immediately.

MFSP should have detail procedures to deal with such cases.

### 3.2.11 Opening of agent account

a) MFSPs engage agents to serve the retail customers on their behalf and agent accounts are opened for the purposes of providing MFS.

b) MFSPs should collect information and documents contained in Annex-3, 4 & 6 as minimum requirements while opening an agent account. MFSPs should collect photocopy of verifiable identification documents (e.g. NID etc.) of relevant individuals and trade license of the business premise along with other information/documents while opening agent accounts.

c) Transaction profile for each agent should also be assessed/collected as per Annex-7.

d) An agent should render his/her/its services at the premise stated in the trade license and permitted by MFSP. MFSP should conduct visit of the business premise of the agent before appointment and shall verify information provided by the intended agent.

e) To mitigate the ML/TF risk associated with MFS, the agent should have knowledge and skills to comply with AML/CFT compliance requirements. MFSP should provide at least one day long training to the agents on regulatory requirements including AML/CFT.

f) MFSPs should report rogue customers/agents to Bangladesh Bank and one central depository should be developed and shared with MFSPs. Customer/agent blacklisted in the database should not be appointed as agent/distributor by any MFSP.

### 3.2.12 Opening of distributor account

a) MFSP may appoint distributors (or super agent, whatever name it may be called) to bridge agents with them and distributor accounts may be opened for this purpose. The distributors should not serve any retail customers, but only the agents of the MFSP.

b) The information and documents contained in Annex- 3, 4 & 6 should be collected as minimum requirements while opening distributor accounts. Transaction profile for each distributor should also be assessed/collected as per Annex-7.

c) The systems and procedures discussed for opening of agent accounts in previous paragraph should also be applicable for distributor account.

d) In case of contractual arrangement between MFSP and other institutions such as NGOs, post office or MNOs for providing distribution network service to the MFSP, the institution should be regarded as distributor of the MFSP and customer service points of the institution should be regarded as agent of MFSP and operation should be conducted accordingly. Each distributor and agent account should be maintained with the MFSP, so that it can monitor transaction of every account.

e) A high official of the MFSP should approve the final appointment of the distributor.

### 3.2.13 Agent and distributor network monitoring

a) Risk assessment procedures for agents and distributors should have to be developed by the MFSPs based on volume of business, geographical location, previous records and any other information available to the MFSP and it should apply CDD/EDD accordingly.

b) MFSPs should develop automated mechanism for monitoring of transactions of agent and distributor account.

c) MFSPs should ensure that every agent point is visited at least once in every year and distributor office quarterly by Field Compliance Officer (FCO) or any other MFSP official and agent/distributors are operating business in the specific premise as stated in the contract and trade license. If any agent is found to render services from any other location, agreement with it should be cancelled immediately.

d) One agent should maintain only one agent A/C in each agent point and one personal A/C in his/her name. Moreover, any agent should not operate more than 2 (two) afore-said MFS A/Cs from its business premise/agent point.

e) MFSPs should develop own policies and procedures to conduct on-site inspections regarding AML/CFT compliance covering at least 5% of the agents selected following risk based approach in every year. The provider may use "mystery shoppers"—staff of the provider who visit agents and pretend to be regular customers to test the agent's integrity and competence in carrying out its roles.

f) The CCC should review the inspection reports and prepare a summary of all irregularities found including its observations and recommendations and submit the same to the CEO/MD of the MFSP in a yearly basis. With the comments of CEO/MD, such report should have to be presented at the meeting of the Board of Directors or Management Committee of the MFSP. Aforesaid summary report with the comments of the CEO/MD and Board of Directors or Management Committee including measures taken should be submitted to BFIU within 2 (two) months on the completion of the respective year of reporting, along with yearly report mentioned in paragraph 3.2.1(iii)(4).

g) If any agent is identified for non-compliance on AML/CFT issues, he/she/it should be warned. Moreover, agency relationship should be temporarily suspended or permanently closed depending on the severity of non-compliance. If any agent account is permanently closed, agent information should be reported to Bangladesh Bank for inclusion in the blacklisting database.

h) If any agent is suspected for involvement or facilitation of ML/TF, MFSP should submit Suspicious Transaction Report (STR) or Suspicious Activity Report (SAR) to BFIU immediately.

i) All the agents and employees working under the distributor should perform their functions complying with the instructions issued by BFIU and the respective MFSP. Distributor should ensure AML/CFT compliance by their respective agents and employees. But, the ultimate responsibility of compliance of agents and distributors should lie with the MFSP.

j) MFSP should be responsible for the AML/CFT related capacity building of its agents and distributors. The distributors should co-operate MFSPs in this regard.

k) MFSP should develop operational procedures regarding selection and monitoring activities of agents and distributors.

### 3.2.14 Transaction monitoring

a) MFSPs should develop automated system based monitoring mechanism for all types of accounts for analysis of transactions and identification of suspicious transactions.

b) Any transaction that deviates from the regular pattern should be identified and monitored closely. If any transaction is found to be suspicious, STR/SAR should be submitted to BFIU immediately.

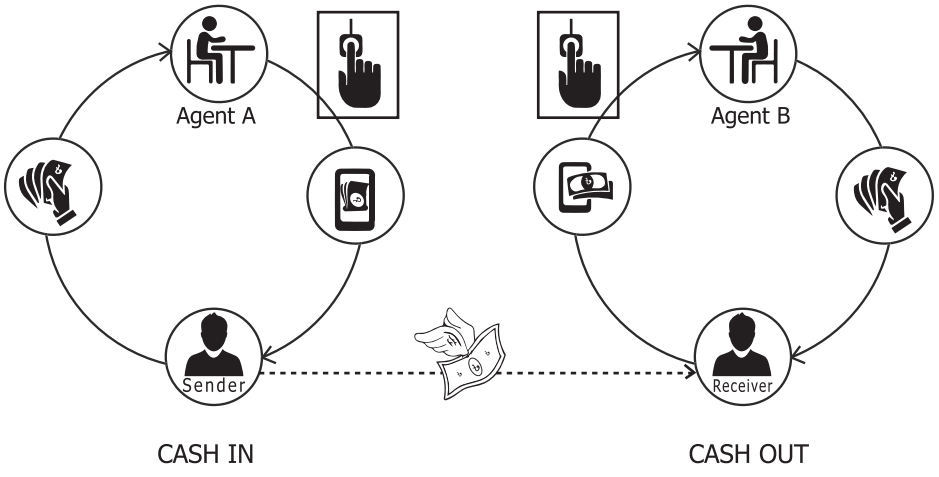
c) MFSPs should adopt Risk Based Approach (RBA) for transaction monitoring based on risk assessment. While conducting risk assessment, geographical locations of the agents and customers during transaction, nature of customers and agents, quality of KYC information, previous records of MFS abused etc. should be taken into consideration along with any indicators informed by BFIU. Based on the risk assessment, transaction monitoring tools and procedures should be developed.

### 3.2.15 Prevention of anonymous transaction and *Digital Hundi*

Ensuring physical presence of customer during Cash In and Cash Out at the agent point is the most important tool for the prevention of anonymous transaction (ATr) and some other types of abuse of m-money including *Digital Hundi*. MFSP may take the following measures to combat anonymous transaction:

a) Biometric authentication (i.e. finger print, iris, facial/voice recognition) of the customer during Cash In and Cash Out transaction rather than PIN is more secured tools to prevent abuse of MFS, including anonymous transaction (ATr) and Digital hundi, etc. Some countries have already implemented biometric authentication including India and Pakistan for financial inclusion customers; and prevalence of abuse of MFS has also been observed low in those countries. Bangladesh should consider implementing biometric identification and authentication for financial inclusion customers in phase. Accounts with high volume of transaction (e.g. Level-3 a/c) as well as high value individual transactions should be brought under biometric authentication in the 1st phase.

**Biometric Authentication**



b) As the recommendation stated above would need time to implement, alternative measures should be taken. MFSP may develop/establish functionality so that customer's name appeared in the agent's device from the MFSP's database after account number entered by the agent during Cash In. The respective customer shall be present in the agent premise and will show a photo ID document to the agent. The name of the customer in the ID document and customer's name as appeared in the agent's device must matched along with photo of ID document with customer's appearance.

c) Identification of geographical location of the agent and customer during each transaction and reflection of it in the respective account statement may be an important tool to identify anonymous transaction. So, MFSP may deploy such technology to prevent anonymous transaction and other types of abuse of MFS.

d) MFSPs should inspect their agent points as mystery shoppers to identify agents' misconduct/noncompliance and agency agreement should be cancelled in appropriate cases.

e) Present market analysis of Bangladesh indicates that there is a significant demand for OTC mainly to the low income formally illiterate population. They either feel shaky to use their own wallet or do not have it. Bangladesh Bank may consider allowing OTC transaction subject to proper (preferably digital) customer identification. However, higher transaction fee should be imposed on OTC transfer compare to P2P with lower transaction limit to discourage it.

### 3.2.16 Risk management for new services or technologies

Before introducing any new service, technology or delivery channel, the ML/TF risks that may arise from it should be assessed and risk management procedures should be developed. Such assessment and risk management procedures should be approved by BFIU and regulatory authority prior to launching of such service, technology or delivery channel.

### 3.2.17 Suspicious Transaction/Activity Report (STR/SAR)

a) As per instructions contained in Section 25(1)(d) of MLPA, 2012 and Section 16(1) of ATA 2009, MFSPs should develop procedures to identify and report suspicious transactions/activities. The definitions of 'Suspicious Transaction' mentioned in Section 2(z) of MLPA, 2012 and Section 2(16) of ATA, 2009 shall also be applicable for MFS.

b) Field Compliance Officers, distributors and agents should follow the procedures set by MFSPs to identify and report suspicious transactions/activities. After identifying any suspicious transaction/activity, agent/distributor/official of a MFSP should send it to AML/CFT Compliance Officer (for banks) or CAMLCO (for MFS Companies) with

primary comments and relevant documents immediately as per **Annex- 8** form (untill the electronic reporting system is being established) for further analysis. A compliance official of MFSP should analyze the reported transaction or activity and maintain a detailed record of the same. If the transaction or activity is still deemed suspicious, then STR/SAR should be submitted to BFIU through 'goAML' software STR/SAR reporting template.

c) The agent/distributor/official of MFSP associated with reporting of suspicious transaction/activity should ensure the overall confidentiality of the issue.

d) Agents, distributors and relevant employees of MFSP should be trained in regard to the procedure of submitting STR/SAR.

e) Providers may create a toll free hotline for AML/CFT purposes that would be accessible to their agents and distributors. MFSPs may also consider providing incentives to agents and distributors to encourage them for submission of STR/SAR.

f) MFSPs should preserve the information/documents related to any suspicious transaction/activity reporting until further instruction of BFIU.

### 3.2.18 Security of cash

Payment Systems Department of Bangladesh Bank may consider the following recommendations to be issued for MFSPs:

a) MFSPs, its agents and distributors should be careful to ensure physical security of cash, especially for cash in transit.

b) MFSPs should aware and issue instructions to its agents, distributors and relevant officials on security of cash.

c) MFSPs should be encouraged to use "Link Account" for transferring money between agents and distributors.

### 3.2.19 Self assessment procedures

MFSPs should prepare a Self Assessment Report in the month of February for the preceding year based on gaps identified related with AML/CFT compliance and quarterly report received from Field Compliance Officer. A copy of the Self Assessment Report shall be submitted to BFIU following the same procedures as stated in paragraph 3.2.1(iii)(4) and all reports should be submitted to BFIU together.

### 3.2.20 Prevention of financing of terrorism

a) MFSPs should establish policy and procedure for detection and prevention of financing of terrorism, should issue instructions about the responsibilities of MFSP officials, agents and distributors and review those instructions from time to time.

b) If any news of terrorism or financing of terrorism is published in any mass media, MFSPs should check their databases if individuals/entities involved with the said act are also related with the MFSP as customer, agent, distributor or employee etc. MFSPs should also analyze the transactions of customer and agent accounts conducted near to the location of the terrorist activity or location of the terrorists themselves. If any such involvement is identified, the details of the individual and transaction, if any, should also be reported to BFIU immediately.

c) MFSPs should electronically preserve the updated list of persons or entities listed under United Nations Security Council Resolutions (UNSCRs) and any person or banned entity listed by the Government of Bangladesh. MFSPs should regularly monitor whether there is any account or any transaction in the name of the listed person or entity listed under different UNSCRs and any person or banned entity listed by Government of Bangladesh. If any such account or transaction is identified, the MFSP should immediately stop payment and/or transaction and communicate the same with detailed information to BFIU on the following working day.

### 3.2.21 Recruitment/appointment, training & awareness

a) MFSPs should follow proper Know Your Employee (KYE) procedure in the recruitment process to mitigate the risk of ML & TF.

b) MFSPs should also conduct background check before appointing any agent or distributor.

c) MFSPs should provide training to their staffs, agents and distributors on ML & TF issues on regular basis to ensure proper compliance of AML/CFT regulations.

d) MFSPs should also take awareness programs on a regular basis to aware customers, agents and distributors regarding AML/CFT issues, such as:

i) Install poster/banner on visible places of each branch/customer care center, distributor's office and agent point using Bangla content on AML/CFT.

ii) Publish/telecast/broadcast advertisements, documentaries, etc. in mass media with special focus on the following issues:

- Motivate customer to use his/her personal wallet for own transaction.
- The risks and consequences of using personal wallet to conduct transaction of other individuals.
- Motivate agents to open customer account(s) as per regulatory guidelines.
- Aware the customers and agents about common and emerging fraud techniques used by criminals.

e) Any message of advertisement/media campaign of any MFSP shall not directly or indirectly contradict with any regulatory directive/guideline.

### 3.2.22 Preservation of records and necessary information/documents

a) MFSPs should preserve account and transaction information/documents for at least 5 (five) years after closure of the account.

b) MFSPs should provide account and transaction information/documents to BFIU, time to time, on demand.

c) Record all transaction in such a manner that is easily comprehendible by the regulatory/supervisory agencies. The MFS A/C statement should contain the following information at the top: account number, account type, name of the account, present/mailing address, and location of account opening agent. There should be separate column for transaction date and time, transaction type, account number, name & type of the counter party (personal/impersonal/agent account), location of the agent and/or customer, debit amount, credit amount and balance.

### 3.2.23 Other recommendations

a) The balance amount of closed accounts and non-operative dormant accounts should be transferred to 'Unclaimed Deposit A/C' after 3 years of last transaction and should be shown in the liability side of the balance sheet of the MFSP. Such deposit should be maintained by the MFSP as per provision of the relevant act/regulation or instruction issued from Bangladesh Bank.

b) MFSP should use/develop customer friendly user interface with content in local language so that any customer having no formal education can easily understand the step by step instruction to conduct transaction. MFSP may develop mobile application with graphical presentation to facilitate customer adoption.

c) If a customer or agent transfer/send e-money to another customer wallet mistakenly and report it to the MFSP, it should take measure to reverse such transaction after proper verification.

d) MFSPs should ensure the confidentiality of the customers' information including KYC and transaction history and should not provide such information to any other party beyond the provision of the relevant acts/regulations.

e) With a view to establish an effective AML/CFT regime, all MFSPs should ensure that AML/CFT set up of the organization is equipped with analytical software, hardware and adequate human resources having sufficient knowledge on the existing acts, rules, regulations and instructions on prevention of ML & TF.

f) MFSPs should request clarification/permission from the relevant authority if any instruction of the authority needs to be more specific or need review/relaxation in any particular case, as the case may be.

g) When a customer takes different services from different financial institutions, s/he needs to provide KYC information in every instance, which is quite cumbersome and act as a barrier to access to financial services. Creation of a Central Unique Identification Database (c-KYC) based on biometric identification and other information of the customer would enable quick and easy access to financial services including MFS. Central bank should take such an initiative with participation by banks and other financial institutions which would check customers' information while on-boarding of a new customer in the database and automatically create a unique ID. While opening a new account or carry out a transaction with another financial institution, it can easily verify customers' information by using unique ID number.

h) DFS providers of Bangladesh should consider establishing association/forum to enable mutual sharing of fraud risk related information and benchmarking against industry best practices. It should also address stakeholder challenges and convey stakeholder concerns to regulators and other agencies.

= = = = = = =

# GLOSSARY

a) **Agent**

An authorized representative of MFS provider who serves retail customers. An agent shall provide 'cash in' and 'cash out' facility to the customers, and/or open customer account.

b) **Anonymous Transaction (ATr)**

Any transaction where names of the sender, receiver and other parties involve are absent in the transaction trail.

c) **Distributor/ Super Agent**

Any business entity which exists between the Agents and MFSP in the distribution channel, whatever name it may be called, will be termed as Distributor/ Super Agent for the purpose of this study paper.

d) **e-KYC**

Collection of required KYC information electronically and preserve the collected information in database.

e) **e-Money**

Electronic money (e-Money) is a record of funds or value available to a consumer stored on a payment device such as chip, prepaid cards, mobile phones [it termed as mobile money (m-money) in such case], or on computer systems as a non-traditional account with a banking or non-banking entity.

f) **Digital hundi**

Illegal money remittance services where mobile money is used for collection or disbursement of illegal remittances. In Digital hundi, foreign remittances are collected from the migrant remittance sender by a hundi/hawala agent and he send the information (recipient's MFS number and corresponding amount) to another hundi/hawala agent residing in migrant's home country. Then the agent mentioned later send e-money to the MFS account of the recipient.

g) **MFS Company**

Companies established solely for the purpose of providing MFS which are registered under Companies Act, 1994.

h) **Mystery shopping**

It's a tool to measure quality of service, or compliance with regulation, or to gather specific information about products and services where identity and purpose of the interviewer is generally not known by the establishment being evaluated.

# ANNEX - 01 : Account opening form (personal a/c)

কোম্পানী/সেবাদানকারী প্রতিষ্ঠানের নাম ও লোগো

গ্রাহকের সদ্য তোলা পাসপোর্ট আকারের ছবি

**মোবাইল একাউন্ট খোলার ফরম (ব্যক্তি হিসাব)**

| তারিখ | দি | ন | মা | স | ব | ৎ | স | র |
|---|---|---|---|---|---|---|---|---|

| নতুন হিসাব | | তথ্য হালনাগাদ/সংশোধনঃ | | শুধুমাত্র সেবাদানকারী প্রতিষ্ঠান/এজেন্ট কর্তৃক ব্যবহারের জন্য |
|---|---|---|---|---|

মোবাইল একাউন্ট নংঃ

১। নাম ঃ (বাংলায়)

(In English)

২। জন্ম তারিখ ঃ দি ন মা স ব ৎ স র  লিঙ্গ ঃ ☐ পুরুষ ☐ মহিলা

৩। পেশার বিস্তারিত বিবরণ/আয়ের উৎস ঃ_____ আনুমানিক মাসিক আয় ঃ.....

৪। গ্রাহকের পরিচয়পত্রঃ

| পরিচয়পত্রের ধরন ঃ | পরিচয়পত্র নং ঃ |
|---|---|
| জাতীয় পরিচয়পত্র | |
| পাসপোর্ট | |
| ড্রাইভিং লাইসেন্স | |
| অন্যান্য (উল্লেখ করুন) | |

| | বাংলায় | In English |
|---|---|---|
| ৫। পিতার নামঃ | | |
| ৬। মাতার নাম ঃ | | |
| ৭। স্বামী/স্ত্রীর নামঃ | | |
| ৮। বর্তমান/ যোগাযোগ/ অফিসের ঠিকানা ঃ | | |
| উপজেলা ঃ | | Upazila : |
| জেলা ঃ | | District : |
| ৯। স্থায়ী ঠিকানা ঃ | | |
| উপজেলা ঃ | | Upazila : |
| জেলা ঃ | | District : |

১০। মোবাইল নং ঃ
(যা মোবাইল একাউন্ট হিসেবে ব্যবহৃত হবে)

১১। নমিনীঃ

আমি এতদ্বারা আমার মোবাইল একাউন্টে জমাকৃত অর্থ আমার অবর্তমানে নিম্নলিখিত ব্যক্তিকে বিধি মোতাবেক প্রদানের জন্য মনোনীত করলাম-

| নাম | ঠিকানা | সম্পর্ক | প্রাপ্য শতকরা ভাগ (%) |
|---|---|---|---|
| | | | |
| | | | |

**জ্ঞাতব্যঃ মানিলন্ডারিং প্রতিরোধ আইন, ২০১২ এর ধারা ৮(২) অনুযায়ী কোন ব্যক্তি জ্ঞাতসারে অর্থের উৎস বা নিজ পরিচিতি বা হিসাব ধারকের পরিচিতি সম্পর্কে বা কোন হিসাবের সুবিধাভোগী বা নমিনী সম্পর্কে মিথ্যা তথ্য প্রদান করলে তিনি অনধিক ০৩ (তিন) বছর পর্যন্ত কারাদন্ড বা অনুর্ধ্ব ৫০ (পঞ্চাশ) হাজার টাকা পর্যন্ত অর্থদন্ড বা উভয় দন্ডে দন্ডিত হবেন।**

**আমি ঘোষণা করছি যে, উপরে প্রদত্ত সকল তথ্য সঠিক ও পূর্ণাঙ্গ এবং আমি সংশ্লিষ্ট আইনের বিধান সম্পর্কে অবগত।**

_____

আবেদনকারীর স্বাক্ষর/ বাম হাতের বৃদ্ধাঙ্গুলির ছাপ

**এজেন্টের ব্যবহারের জন্য**

আমি নিশ্চিত করছি যে, আবেদনকারী আমার সামনে স্বাক্ষর করেছেন এবং ছবিটি আবেদকারীর নিজের। এছাড়া, হিসাব খোলায় ব্যবহৃত মোবাইল নম্বরটি গ্রাহকের সঙ্গে ছিল।

.....

নামসহ স্বাক্ষর, সীল ও তারিখ

**অতিরিক্ত তথ্য (প্রযোজ্য ক্ষেত্রে)**

**১২। মা/বাবা/ভাই/বোন/সন্তান/স্বামী/স্ত্রী এর তথ্যাবলী (হিসাবধারকের সরকার কর্তৃক ইস্যুকৃত ফটোযুক্ত পরিচয়পত্র না থাকলে) ঃ**

| | | | |
|---|---|---|---|
| ক) আত্মীয়ের নামঃ | | | |
| খ সরকার কর্তৃক ইস্যুকৃত ফটোযুক্ত পরিচয়পত্রের ধরণ ও নং ঃ | | গ) মোবাইল ফোন নংঃ | |

**এ মর্মে প্রত্যয়ন করা যাচ্ছে যে, হিসাব খুলতে আগ্রহী গ্রাহক আমার---------- এবং তার প্রদত্ত তথ্যাবলি আমার জানামতে সঠিক। আমার রেজিস্ট্রিকৃত সিমের বিপরীতে মোবাইল ব্যাংকিং হিসাব খোলা ও পরিচালনার জন্য তাকে অনুমতি প্রদান করা হলো।**

**----------**

**(আত্মীয়ের স্বাক্ষর ও তারিখ)**

**১৩। ব্যাংক একাউন্ট এর তথ্যাবলী (যদি থাকে)ঃ**

| | | | |
|---|---|---|---|
| ক) ব্যাংকের নামঃ | | খ) শাখা ঃ | |
| গ) একাউন্ট নং ঃ | | | |

উল্লিখিত ব্যাংক হিসাবটি মোবাইল ব্যাংকিং হিসাবের সাথে লিংক করতে চাইলে টিক (√) দিন। ☐

**মোবাইল ফাইন্যান্সিয়াল সার্ভিস প্রদানকারী প্রতিষ্ঠানের ব্যবহারের জন্যঃ**

| ক্রমিক | গ্রাহকের তথ্য যাচাইকরণ | হ্যাঁ = ১<br>না = ০ |
|---|---|---|
| ক)* | হিসাব খোলার ফরমে উল্লিখিত তথ্যাদি যথাযথভাবে গ্রহণ করা হয়েছে কি-না? | |
| খ)* | সরকার কর্তৃক ইস্যুকৃত ফটোযুক্ত পরিচয়পত্র যাচাই ও সঠিক পাওয়া গিয়েছে কি-না? | |
| গ)* | গ্রাহকের সাম্প্রতিক কালের প্রিন্টেড ছবি বা তাৎক্ষণিকভাবে গৃহিত ছবির (real time picture) ইলেকট্রনিক কপি সংগ্রহ এবং পরিচয়পত্রের ফটোর সাথে মিল রয়েছে কি-না? | |
| ঘ) | গ্রাহকের সিমের রেজিস্ট্রেশন সংক্রান্ত তথ্য যাচাই ও সঠিক পাওয়া গিয়েছে কি-না? | |
| ঙ) | সেবাদানকারী প্রতিষ্ঠানের গ্রাহক সেবা কেন্দ্রে গ্রাহকের উপস্থিতিতে হিসাবটি খোলা হয়েছে কি-না? | |
| চ) | গ্রাহকের মোবাইল হিসাবটি কোন ব্যাংক হিসাবের সাথে লিংক করা হয়েছে কি-না? | |
| ছ) | গ্রাহকের বায়োমেট্রিক তথ্য সংগ্রহ করা এবং e-KYC তে যুক্ত করা কি-না? | |
| | **মোট পয়েন্ট** | |

বিঃ দ্রঃ সকল হিসাবের ক্ষেত্রে তারকা (*) চিহ্নিত তথ্যাবলী আবশ্যিকভাবে নিশ্চিত করতে হবে।

| **KYC - তে সংগৃহিত তথ্য অনুযায়ী হিসাবের লেবেল/পর্যায়ঃ** | | | | | |
|---|---|---|---|---|---|
| **লেভেল-১ = ৩ পয়েন্ট** | | **লেভেল-২ = ৪-৫ পয়েন্ট** | | **লেভেল-৩ = ৬-৭ পয়েন্ট** | |

হিসাব খোলার ফরমে উল্লিখিত গ্রাহকের তথ্যাবলী যাচাই করা হয়েছে এবং সঠিক পাওয়া গেছে।

.....

কর্মকর্তার নামসহ স্বাক্ষর, সীল ও তারিখ

# ANNEX - 02 : Account opening form (impersonal a/c)

কোম্পানী/সেবাদানকারী প্রতিষ্ঠানের নাম ও লোগো

**মোবাইল একাউন্ট খোলার ফরম (বাণিজ্যিক/মার্চেন্ট/প্রতিষ্ঠানিক হিসাব)**

| তারিখ | দি | ন | মা | স | ব | ৎ | স | র |
|---|---|---|---|---|---|---|---|---|

| নতুন হিসাব | | তথ্য হালনাগাদ/সংশোধনঃ | | শুধুমাত্র সেবাদানকারী প্রতিষ্ঠান/এজেন্ট কর্তৃক ব্যবহারের জন্য |
|---|---|---|---|---|

| মোবাইল একাউন্ট নংঃ | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|

১। হিসাবের নাম ঃ .....

২। প্রতিষ্ঠানের ধরণ (টিক দিন)ঃ ☐ প্রাইভেট লিমিটেড কোম্পানী ☐ পাবলিক লিমিটেড কোম্পানী ☐ অংশীদারী ☐ যৌথ উদ্যোগ ☐ একক মালিকানা ☐ সরকারী/আধা সরকারী/স্বায়ত্বশাসিত ☐ এনজিও ☐ ক্লাব/সোসাইটি ☐ অন্যান্য (নির্দিষ্টভাবে).....

৩। প্রতিষ্ঠানের ঠিকানা ঃ

(ক) রেজিষ্টার্ড ঠিকানা ঃ.....

(খ) ব্যবসাস্থল/অফিসের ঠিকানা ঃ.....

৪। ট্রেড লাইসেন্স নম্বর ঃ ..... তারিখ ঃ .....

ইস্যুকারী কর্তৃপক্ষ ঃ.....

৫। নিবন্ধন কর্তৃপক্ষ ঃ.....

৬। নিবন্ধন নম্বর ঃ..... তারিখ ঃ .....

৭। ট্যাক্স আইডি নম্বর (TIN) (যদি থাকে) ঃ.....

৮। ভ্যাট রেজিঃ নম্বর (যদি থাকে) ঃ.....

৯। ব্যবসায়ের প্রকৃতি (বিস্তারিত) ঃ .....

১০। অর্থের উৎস/উৎসসমূহ ঃ (নির্দিষ্ট ও বিস্তারিত উল্লেখ করতে হবে).....

১১। মোবাইল নং ঃ
(যা মোবাইল একাউন্ট হিসেবে ব্যবহৃত হবে)

১২। প্রতিষ্ঠানের অন্যান্য মোবাইল ব্যাংকিং হিসাবঃ
(যদি থাকে)

১৩। (ক) গ্রাহকের ব্যাংক হিসাবের তথ্য (যদি থাকে)ঃ

| ক্রমিক | ব্যাংক | শাখা | হিসাব নং | হিসাবের প্রকৃতি |
|---|---|---|---|---|
| | | | | |
| | | | | |

(খ)উপরিউক্ত ব্যাংক হিসাবের মধ্যে কোনটিকে মোবাইল হিসাবের সাথে লিংক করতে চাইলে উল্লেখ করুনঃ ----------

**জ্ঞাতব্যঃ মানিলন্ডারিং প্রতিরোধ আইন, ২০১২ এর ধারা ৮(২) অনুযায়ী কোন ব্যক্তি জ্ঞাতসারে অর্থের উৎস বা নিজ পরিচিতি বা হিসাব ধারকের পরিচিতি সম্পর্কে বা কোন হিসাবের সুবিধাভোগী বা নমিনী সম্পর্কে মিথ্যা তথ্য প্রদান করলে তিনি অনধিক ০৩ (তিন) বছর পর্যন্ত কারাদন্ড বা অনুর্ধ্ব ৫০ (পঞ্চাশ) হাজার টাকা পর্যন্ত অর্থদন্ড বা উভয় দন্ডে দন্ডিত হবেন।**

১৪। আমি/আমরা ঘোষণা করছি যে, উপরে প্রদত্ত সকল তথ্য সঠিক ও পূর্ণাঙ্গ এবং আমি/আমরা সংশ্লিষ্ট আইনের বিধান সম্পর্কে অবগতঃ

| ক্রমিক | আবেদনকারী(গণের) নাম | পদবী | মোবাইল নং | স্বাক্ষর | তারিখ |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |

১৫। মোবাইল ব্যাংক হিসাবটি পরিচালনাকারীর নাম উল্লেখ করুনঃ ----------

| **এজেন্টের ব্যবহারের জন্য** | **মোবাইল ফিন্যান্সিয়াল সার্ভিস প্রদানকারী কর্মকর্তার ব্যবহারের জন্য** |
|---|---|
| আমি নিশ্চিত করছি যে, আবেদনকারী(গণ) আমার সামনে স্বাক্ষর করেছেন এবং ছবিটি আবেদকারী(গণের) নিজের/নিজেদের। এছাড়া, হিসাব খোলায় ব্যবহৃত মোবাইল নম্বরটি হিসাব খোলার সময় গ্রাহকের সঙ্গে ছিল।<br><br>----------<br>স্বাক্ষর, সীল ও তারিখ | হিসাব খোলার ফরমে উল্লিখিত গ্রাহকের তথ্যাবলী যাচাই করা হয়েছে এবং সঠিক পাওয়া গেছে।<br><br>----------<br>স্বাক্ষর, সীল ও তারিখ |

# ANNEX - 03 : Account opening form (information of individuals)

কোম্পানী/সেবাদানকারী প্রতিষ্ঠানের নাম ও লোগো

**মোবাইল একাউন্ট খোলার ফরমঃ ব্যক্তি সংক্রান্ত তথ্যাবলি**

(বাণিজ্যিক/মার্চেন্ট/প্রতিষ্ঠানিক/এজেন্ট/ডিস্ট্রিবিউটর হিসাব সংশ্লিষ্ট ব্যক্তির তথ্য সংগ্রহের জন্য ব্যবহার্য্য)

| তারিখ | দি | ন | মা | স | ব | ৎ | স | র |
|---|---|---|---|---|---|---|---|---|

| নতুন হিসাব | | তথ্য হালনাগাদ/সংশোধনঃ | | শুধুমাত্র সেবাদানকারী প্রতিষ্ঠান/এজেন্ট কর্তৃক ব্যবহারের জন্য |
|---|---|---|---|---|

মোবাইল একাউন্ট নংঃ

১। হিসাবের নামঃ

হিসাব পরিচালনাকারীর নামঃ

২। হিসাবের সাথে ব্যক্তির সম্পর্ক (নীচে প্রযোজ্য ক্ষেত্রে টিক দিন) ঃ

☐ ১ম আবেদনকারী ☐ ২য় আবেদনকারী ☐ ৩য় আবেদনকারী ☐ পরিচালক ☐ অংশীদার ☐ একক সত্ত্বাধিকারী

☐ হিসাব পরিচালনাকারী ☐ প্রকৃত সুবিধাভোগী

৩। জন্ম তারিখ ঃ দি ন মা স ব ৎ স র

৪। লিঙ্গ ঃ ☐ পুরুষ ☐ মহিলা

৫। পেশার বিস্তারিত বিবরণ ও আয়ের উৎস ঃ_____

৬। আনুমানিক মাসিক আয়ঃ.....

৭। ব্যক্তির পরিচয়পত্রঃ

| পরিচয়পত্রের ধরন ঃ | পরিচয়পত্র নং ঃ |
|---|---|
| জাতীয় পরিচয়পত্র | |
| পাসপোর্ট | |
| ড্রাইভিং লাইসেন্স | |
| অন্যান্য (উল্লেখ করুন) | |

| | বাংলায় | In English |
|---|---|---|
| ৮। পিতার নামঃ | | |
| ৯। মাতার নাম ঃ | | |
| ১০। স্বামী/স্ত্রীর নামঃ | | |
| ১১। বর্তমান/ যোগাযোগ/ অফিসের ঠিকানা ঃ | | |
| উপজেলা ঃ | | Upazila : |
| জেলা ঃ | | District : |
| ১২। স্থায়ী ঠিকানা ঃ | | |
| উপজেলা ঃ | | Upazila : |
| জেলা ঃ | | District : |

১৩। মোবাইল নম্বর ঃ

১৪। গ্রাহক/এজেন্ট/ডিস্ট্রিবিউটর প্রভাবশালী ব্যাক্তি কি-না (সেবাদানকারী প্রতিষ্ঠান কর্তৃক পূরণীয়)? হ্যাঁ ☐ না ☐

**জ্ঞাতব্যঃ মানিলন্ডারিং প্রতিরোধ আইন, ২০১২ এর ধারা ৮(২) অনুযায়ী কোন ব্যক্তি জ্ঞাতসারে অর্থের উৎস বা নিজ পরিচিতি বা হিসাব ধারকের পরিচিতি সম্পর্কে বা কোন হিসাবের সুবিধাভোগী বা নমিনী সম্পর্কে মিথ্যা তথ্য প্রদান করলে তিনি অনধিক ০৩ (তিন) বছর পর্যন্ত কারাদন্ড বা অনুর্ধ্ব ৫০ (পঞ্চাশ) হাজার টাকা পর্যন্ত অর্থদন্ড বা উভয় দন্ডে দন্ডিত হবেন।**

আমি ঘোষণা করছি যে, উপরে প্রদত্ত সকল তথ্য সঠিক ও পূর্ণাঙ্গ এবং আমি সংশ্লিষ্ট আইনের বিধান সম্পর্কে অবগত।

---

আবেদনকারীর স্বাক্ষর/ বাম হাতের বৃদ্ধাঙ্গুলির ছাপ

| **এজেন্ট/ডিস্ট্রিবিউটর কর্তৃক ব্যবহারের জন্য (প্রযোজ্য ক্ষেত্রে)** | **মোবাইল ফিন্যান্সিয়াল সার্ভিস প্রদানকারী কর্মকর্তার ব্যবহারের জন্য** |
|---|---|
| আমি নিশ্চিত করছি যে, আবেদনকারী আমার সামনে স্বাক্ষর করেছেন এবং ছবিটি আবেদকারীর নিজের। | হিসাব খোলার ফরমে উল্লিখিত গ্রাহকের তথ্যাবলী যাচাই করা হয়েছে এবং সঠিক পাওয়া গেছে। |
| ---------- | ---------- |
| নামসহ স্বাক্ষর, সীল ও তারিখ | নামসহ স্বাক্ষর, সীল ও তারিখ ও তারিখ |

# ANNEX - 04 : Indicative list of information/documentary requirements

## অব্যক্তিক/এজেন্ট/ডিস্ট্রিবিউটর হিসাবের জন্য প্রয়োজনীয় তথ্য/দলিলাদির নির্দেশক তালিকা।

**(১) ব্যক্তি মালিকাধীন প্রতিষ্ঠান ঃ**

ক) স্থানীয় সরকার প্রতিষ্ঠান কর্তৃক ইস্যুকৃত ট্রেড লাইসেন্স।
খ) প্রতিষ্ঠানের স্বত্ত্বাধিকারীর সরকার কর্তৃক ইস্যুকৃত ফটোযুক্ত পরিচয়পত্র।
গ) হিসাব পরিচালনাকারী/প্রতিষ্ঠানের স্বত্তাধিকারীর "ব্যক্তি সংক্রান্ত তথ্যাবলী"।
ঘ) ট্যাক্স আইডি নম্বর (TIN) সার্টিফিকেট (যদি থাকে)।
ঙ) প্রতিষ্ঠানের ভ্যাট রেজিঃ নম্বর (যদি থাকে)।

**(২) পার্টনারশীপ ঃ**

ক) স্থানীয় সরকার প্রতিষ্ঠান কর্তৃক ইস্যুকৃত ট্রেড লাইসেন্স।
খ) পার্টনারশীপ ডিড।
গ) প্রতিষ্ঠানের অংশীদারগণের সরকার কর্তৃক ইস্যুকৃত ফটোযুক্ত পরিচয়পত্র। কারো সরকার কর্তৃক ইস্যুকৃত ফটোযুক্ত পরিচয়পত্র না থাকলে তার অন্য কোন পরিচয়পত্র। তবে, হিসাব পরিচালনাকারীর অবশ্যই সরকার কর্তৃক ইস্যুকৃত ফটোযুক্ত পরিচয়পত্র গ্রহণ করতে হবে।
ঘ) অংশীদারগণের পরিচিতির বিষয়ে "ব্যক্তি সংক্রান্ত তথ্যাবলী" ফরম যথাযথভাবে পূরণ।
ঙ) ট্যাক্স আইডি নম্বর (TIN) সার্টিফিকেট (যদি থাকে)।
চ) প্রতিষ্ঠানের ভ্যাট রেজিঃ নম্বর (যদি থাকে)।

**(৩) লিমিটেড কোম্পানী ঃ**

ক) স্থানীয় সরকার প্রতিষ্ঠান কর্তৃক ইস্যুকৃত ট্রেড লাইসেন্স।
খ) সার্টিফিকেট অব ইনকর্পোরেশন,
গ) আর্টিকেলস অব এসোসিয়েশন,
ঘ) মেমোরেন্ডাম অব এসোসিয়েশন,
ঙ) হিসাব খোলার বিষয়ে বোর্ডের সভায় গৃহীত আনুষ্ঠানিক সিদ্ধান্ত (resolution),
চ) পরিচালক সম্পর্কিত ঘোষণা (Form XII)
ছ) হিসাব পরিচালনাকারীসহ সকল পরিচালকের "ব্যক্তি সংক্রান্ত তথ্যাবলী" ও জাতীয় পরিচয়পত্রের কপি।
জ) ট্যাক্স আইডি নম্বর (TIN) সার্টিফিকেট।
ঝ) প্রতিষ্ঠানের ভ্যাট রেজিঃ নম্বর (প্রযোজ্য ক্ষেত্রে)।

**(৪) সরকারী প্রতিষ্ঠানের হিসাব (বিভিন্ন মন্ত্রণালয়, বিভাগসহ), সরকারী মালিকানাধীন প্রতিষ্ঠান, আধা সরকারী বা স্বায়ত্তশাসিত প্রতিষ্ঠানের হিসাব, বিভিন্ন মন্ত্রণালয়ের অধীনে পরিচালিত প্রকল্পের হিসাব ঃ**

ক) হিসাব খোলা ও পরিচালনার জন্য সংশ্লিষ্ট উপযুক্ত কর্তৃপক্ষ কর্তৃক প্রদত্ত অনুমতিপত্র
খ) হিসাব পরিচালনাকারীর "ব্যক্তি সংক্রান্ত তথ্যাবলী" ও জাতীয় পরিচয়পত্রের কপি।

**(৫) অন্যান্য সংগঠনের হিসাব ঃ**

**(ক) ক্লাব/সোসাইটি ঃ** অফিস কর্মকর্তাগণের বিবরণ (office bearers), বাই-লজ বা সংবিধান, লাইসেন্স/রেজিস্ট্রেশন সার্টিফিকেট/ সরকারী অনুমোদনপত্র ইত্যাদিসহ প্রতিষ্ঠানের সভাপতি, সাধারণ সম্পাদক ও কোষাধ্যক্ষের "ব্যক্তি সংক্রান্ত তথ্যাবলী" ও জাতীয় পরিচয়পত্রের কপি।

**(খ) সমবায় সমিতি/লিমিটেড সোসাইটি ঃ** সমবায় অধিদপ্তরের সংশ্লিষ্ট কর্মকর্তা কর্তৃক সত্যায়িত বাই-লজ, অফিস কর্মকর্তাদের (office bearers) বিবরণ, হিসাব খোলার বিষয়ে সিদ্ধান্ত (resolution), সার্টিফিকেট অব রেজিস্ট্রেশন ইত্যাদি এবং হিসাব পরিচালনাকারীসহ সংশ্লিষ্টদের "ব্যক্তি সংক্রান্ত তথ্যাবলী" ও জাতীয় পরিচয়পত্রের কপি।

**(গ) স্কুল, কলেজ, মাদ্রাসা ঃ** গভর্নিং বডি বা ম্যানেজিং কমিটির সদস্যগণের পূর্ণ পরিচিতি (বেসরকারী প্রতিষ্ঠানের ক্ষেত্রে), হিসাব খোলার বিষয়ে সিদ্ধান্ত (resolution) ইত্যাদিসহ প্রতিষ্ঠানের অধ্যক্ষ/প্রধান শিক্ষক ও হিসাব পরিচালনাকারীর "ব্যক্তি সংক্রান্ত তথ্যাবলী" ও জাতীয় পরিচয়পত্রের কপি।

**(ঘ) ট্রাস্ট ঃ** ডিড অব ট্রাস্ট এর সার্টিফাইড কপি, ট্রাষ্টি বোর্ড এর সদস্যগণের পূর্ণ পরিচিতি, হিসাব খোলার বিষয়ে সিদ্ধান্ত (resolution) ইত্যাদিসহ ট্রাস্টের নিয়ন্ত্রণকারী কর্মকর্তাগণ ও হিসাব পরিচালনাকারীর "ব্যক্তি সংক্রান্ত তথ্যাবলী" ও জাতীয় পরিচয়পত্রের কপি।

## ANNEX - 05 : Transaction profile (for business/merchant/organizational a/c)

### লেনদেনের অনুমিত মাত্রা (Transaction Profile)

**(বাণিজ্যিক/মার্চেন্ট/প্রতিষ্ঠানিক হিসাবের জন্য প্রযোজ্য)**

১) হিসাবের নাম ঃ

২) হিসাব নম্বর ঃ

৩) প্রতিষ্ঠানের ব্যবসা/কার্যক্রমের ধরণঃ

৪) প্রতিষ্ঠানের স্থানঃ

| ক) গ্রাম | | খ) বড় বাজার/গঞ্জ | | গ) পৌরসভা | | ঘ) সিটি কর্পোরেশন | |
|---|---|---|---|---|---|---|---|

৫) মাসিক আনুমানিক বিক্রয়/টার্ণওভারের পরিমানঃ.. .. ..... লক্ষ টাকা।

৬) তন্মধ্যে মোবাইল ব্যাংকিংয়ের মাধ্যমে বিক্রয়/টার্ণওভারের পরিমানঃ ..... লক্ষ টাকা; শতকরা .. .. .....%

৭) মাসিক সম্ভাব্য লেনদেনের পরিমানঃ

| **লেনদেনের ধরণ** | **মাসিক সম্ভাব্য মোট লেনদেনকৃত অর্থের পরিমান** | **একক লেনদেনে সম্ভাব্য সর্বোচ্চ অর্থের পরিমাণ** |
|---|---|---|
| ট্রান্সফারের মাধ্যমে গ্রহণ | | |
| ট্রান্সফারের মাধ্যমে প্রদান | | |
| নগদ উত্তোলন | | |

আমি নিম্নস্বাক্ষরকারী এ মর্মে নিশ্চয়তা প্রদান করছি যে, লেনেদেনের অনুমিত মাত্রা আমার প্রতিষ্ঠানের স্বাভাবিক সম্ভাব্য লেনদেন। আমি আরো নিশ্চয়তা প্রদান করছি যে, প্রয়োজনবোধে আমি লেনদেনের অনুমিত মাত্রা সংশোধন/হালনাগাদ করবো।

**গ্রাহক/হিসাব পরিচালনাকারীঃ**

স্বাক্ষর ঃ
নাম ঃ
পদবী ঃ
তারিখ ঃ

### মোবাইল ফাইন্যান্সিয়াল সার্ভিস প্রদানকারী প্রতিষ্ঠানের ব্যবহারের জন্যঃ

গ্রাহকের লেনদেনের সম্ভাব্য অনুমিত মাত্রা তার ব্যবসার প্রকৃতি ও ব্যবসায়িক লেনদেনের সাথে সামঞ্জস্যপূর্ণ। এ প্রেক্ষিতে উক্ত গ্রাহক হিসাবে মাসিক মোট জমা/উত্তোলনের পরিমান ---------- হাজার টাকা নির্ধারণ করা হলো।

কর্মকর্তার নামঃ
পদবী ঃ
স্বাক্ষর ঃ
তারিখ ঃ

(বিঃ দ্রঃ গ্রাহকের ব্যবসার ধরণ, অবস্থান, মাসিক বিক্রয়/টার্নওভার এর উপর ভিত্তি করে প্রদত্ত লেনদেনের অনুমিত মাত্রার সাথে গ্রাহকের প্রকৃত লেনদেন এমএফএস প্রতিষ্ঠান কর্তৃক যাচাই এবং প্রয়োজনে গ্রহণযোগ্য ব্যাখ্যা সাপেক্ষে তা হালনাগাদ করতে হবে। এমএফএস প্রতিষ্ঠান একে লেনদেন মনিটরিংয়ের উপাদান হিসেবে ব্যবহার করবে।)

# ANNEX - 06 : Account opening form (agent/distributor a/c)

কোম্পানী/সেবাদানকারী প্রতিষ্ঠানের নাম ও লোগো

**মোবাইল একাউন্ট খোলার ফরম (এজেন্ট/ডিস্ট্রিবিউটর হিসাব)**

| তারিখ | | | | | | | | |
|---|---|---|---|---|---|---|---|---|

| নতুন হিসাব | | তথ্য হালনাগাদ/সংশোধনঃ | |
|---|---|---|---|

শুধুমাত্র সেবাদানকারী প্রতিষ্ঠান কর্তৃক ব্যবহারের জন্য

| মোবাইল একাউন্ট নং ঃ | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|

১। হিসাবের নাম ঃ .....

২। প্রতিষ্ঠানের ধরণ (টিক দিন)ঃ ☐ প্রাইভেট লিমিটেড কোম্পানী ☐ পাবলিক লিমিটেড কোম্পানী ☐ অংশীদারী

☐ যৌথ উদ্যোগ ☐ একক মালিকানা ☐ সরকারী/আধা সরকারী/স্বায়ত্বশাসিত ☐ এনজিও ☐ ক্লাব/সোসাইটি

☐ অন্যান্য (নির্দিষ্টভাবে).....

৩। প্রতিষ্ঠানের ঠিকানা ঃ

(ক) রেজিষ্টার্ড ঠিকানা ঃ.....

(খ) ব্যবসাস্থল/অফিসের ঠিকানা ঃ.....

৪। ট্রেড লাইসেন্স নম্বর ঃ ..... তারিখ ঃ .....

ইস্যুকারী কর্তৃপক্ষ ঃ.....

৫। নিবন্ধন কর্তৃপক্ষ ঃ.....

৬। নিবন্ধন নম্বর ঃ..... তারিখ ঃ .....

৭। ট্যাক্স আইডি নম্বর (TIN) (যদি থাকে) ঃ.....

৮। ভ্যাট রেজিঃ নম্বর (যদি থাকে) ঃ.....

৯। এজেন্ট/ডিস্ট্রিবিউটরের অন্যান্য ব্যবসায়ের বিবরণঃ

ক) ব্যবসা প্রতিষ্ঠানের নাম ঃ .....

খ) ব্যবসায়ের প্রকৃতি (বিস্তারিত)ঃ .....

১০। মোবাইল নং ঃ
(যা মোবাইল একাউন্ট হিসেবে ব্যবহৃত হবে)

১১। এজেন্ট/ডিস্ট্রিবিউটরের ব্যক্তিগত/স্বার্থ সংশ্লিষ্ট অন্যান্য মোবাইল ব্যাংকিং হিসাব (যদি থাকে)ঃ

১২। (ক) এজেন্ট/ডিস্ট্রিবিউটরের ব্যাংক হিসাবের তথ্য (যদি থাকে)ঃ

| ক্রমিক | ব্যাংক | শাখা | হিসাব নং | হিসাবের প্রকৃতি |
|---|---|---|---|---|
| | | | | |
| | | | | |

(খ) উপরিউক্ত ব্যাংক হিসাবের মধ্যে কোন একটিকে মোবাইল হিসাবের সাথে লিংক করতে চাইলে উল্লেখ করুন ঃ----------

**জ্ঞাতব্যঃ মানিলন্ডারিং প্রতিরোধ আইন, ২০১২ এর ধারা ৮(২) অনুযায়ী কোন ব্যক্তি জ্ঞাতসারে অর্থের উৎস বা নিজ পরিচিতি বা হিসাব ধারকের পরিচিতি সম্পর্কে বা কোন হিসাবের সুবিধাভোগী বা নমিনী সম্পর্কে মিথ্যা তথ্য প্রদান করলে তিনি অনধিক ০৩ (তিন) বছর পর্যন্ত কারাদন্ড বা অনুর্ধ্ব ৫০ (পঞ্চাশ) হাজার টাকা পর্যন্ত অর্থদন্ড বা উভয় দন্ডে দন্ডিত হবেন।**

১৩। আমি/আমরা ঘোষণা করছি যে, উপরে প্রদত্ত সকল তথ্য সঠিক ও পূর্ণাঙ্গ এবং আমি/আমরা সংশ্লিষ্ট আইনের বিধান সম্পর্কে অবগত।

| ক্রমিক | আবেদনকারী(গণের) নাম | পদবী | মোবাইল নং | স্বাক্ষর | তারিখ |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |

১৪। এজেন্ট/ডিস্ট্রিবিউটর হিসাবটি পরিচালনাকারীর নাম উল্লেখ করুনঃ ----------

**মোবাইল ফিন্যান্সিয়াল সার্ভিস প্রদানকারী কর্মকর্তার ব্যবহারের জন্য**

উপরিউক্ত তথ্যাবলী যাচাই করা হয়েছে এবং সঠিক পাওয়া গেছে।

---

স্বাক্ষর, সীল ও তারিখ

# ANNEX - 07 : Transaction profile (for agent/distributor a/c)

## লেনদেনের অনুমিত মাত্রা (Transaction Profile)

**(এজেন্ট/ডিস্ট্রিবিউটর হিসাবের জন্য প্রযোজ্য)**

১) হিসাবের নাম ঃ

২) হিসাব নম্বর ঃ

৩) প্রতিষ্ঠানের স্থানঃ

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| ক) গ্রাম | | খ) বড় বাজার/গঞ্জ | | গ) পৌরসভা | | ঘ) সিটি কর্পোরেশন | |

৪) মাসিক সম্ভাব্য লেনদেনের পরিমানঃ

| **লেনদেনের ধরণ** | **মাসিক সম্ভাব্য মোট লেনদেনকৃত অর্থের পরিমান** |
|---|---|
| ট্রান্সফারের মাধ্যমে গ্রহণ | |
| ট্রান্সফারের মাধ্যমে প্রদান | |

আমি নিম্নস্বাক্ষরকারী এ মর্মে নিশ্চয়তা প্রদান করছি যে, লেনেদেনের অনুমিত মাত্রা আমার প্রতিষ্ঠানের স্বাভাবিক সম্ভাব্য লেনদেন। আমি আরো নিশ্চয়তা প্রদান করছি যে, প্রয়োজনবোধে আমি লেনদেনের অনুমিত মাত্রা সংশোধন/হালনাগাদ করবো।

**এজেন্ট/ডিস্ট্রিবিউটর হিসাব পরিচালনাকারীঃ**

স্বাক্ষর ঃ

নাম ঃ

পদবী ঃ

তারিখ ঃ

**মোবাইল ফাইন্যান্সিয়াল সার্ভিস প্রদানকারী প্রতিষ্ঠানের ব্যবহারের জন্যঃ**

উপরিউক্ত তথ্য পর্যালোচনান্তে এই এজেন্ট/ডিস্ট্রিবিউটর হিসাবে মাসিক মোট লেনদেন সীমা ---------- হাজার টাকা নির্ধারণ করা হলো।

কর্মকর্তার নামঃ

পদবী ঃ

স্বাক্ষর ঃ

তারিখ ঃ

## ANNEX - 08 : Suspicious transaction/activity report (STR/SAR) format

### সন্দেহজনক লেনদেন/কার্যকলাপ বিবরণী

(এজেন্ট/ডিস্ট্রিবিউটর/সেবাদানকারী প্রতিষ্ঠানের কর্মকর্তা কর্তৃক অভ্যন্তরীণ রিপোর্টিংয়ের ক্ষেত্রে ব্যবহার্য)

| নতুন রিপোর্ট | | পূর্বতন রিপোর্টের সংযোজনী | |
|---|---|---|---|

ক) সন্দেহভাজন ব্যক্তি/প্রতিষ্ঠান সম্পর্কিত তথ্যাবলীঃ

১. মোবাইল হিসাব নম্বরঃ

২. ব্যক্তি/প্রতিষ্ঠানের নামঃ.. . . . . .. . . . . .

৩. পরিচালনাকারী এর নাম (হিসাবধারী প্রতিষ্ঠান হলে)ঃ

৪. ১. সন্দেহজনক লেনদেন সংক্রান্ত তথ্যঃ

| ক্র.নং. | তারিখ | লেনদেনের ধরণ | প্রেরক | প্রাপক | লেনদেনকৃত অর্থের পরিমাণ |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |

৪.২. লেনদেন সন্দেহজনক মনে করার কারণঃ

| |
|---|
| |

৫. সন্দেহজনক কার্যকলাপের বিবরণঃ

| |
|---|
| |

৬) সন্দেহজনক লেনদেন/কার্যকলাপ চিহ্নিতকারীর তথ্যঃ

১. এজেন্ট/ডিস্ট্রিবিউটর/কর্মকর্তার নাম ও স্বাক্ষর ঃ

২. প্রতিষ্ঠানের নাম ও ঠিকানা (প্রযোজ্য ক্ষেত্রে) ঃ

৩. সন্দেহজনক লেনদেন/কার্যকলাপ চিহ্নিতকরণের তারিখঃ

Published by G.M. Abul Kalam Azad, General Manager, Department of Communications and Publications, Bangladesh Bank, Head Office, Motijheel, Dhaka-1000, Bangladesh.
website : www.bb.org.bd, Printed by Srout Advertising, 205/5, Fakirapool, Dhaka-1217.

DCP : 05-2018-200