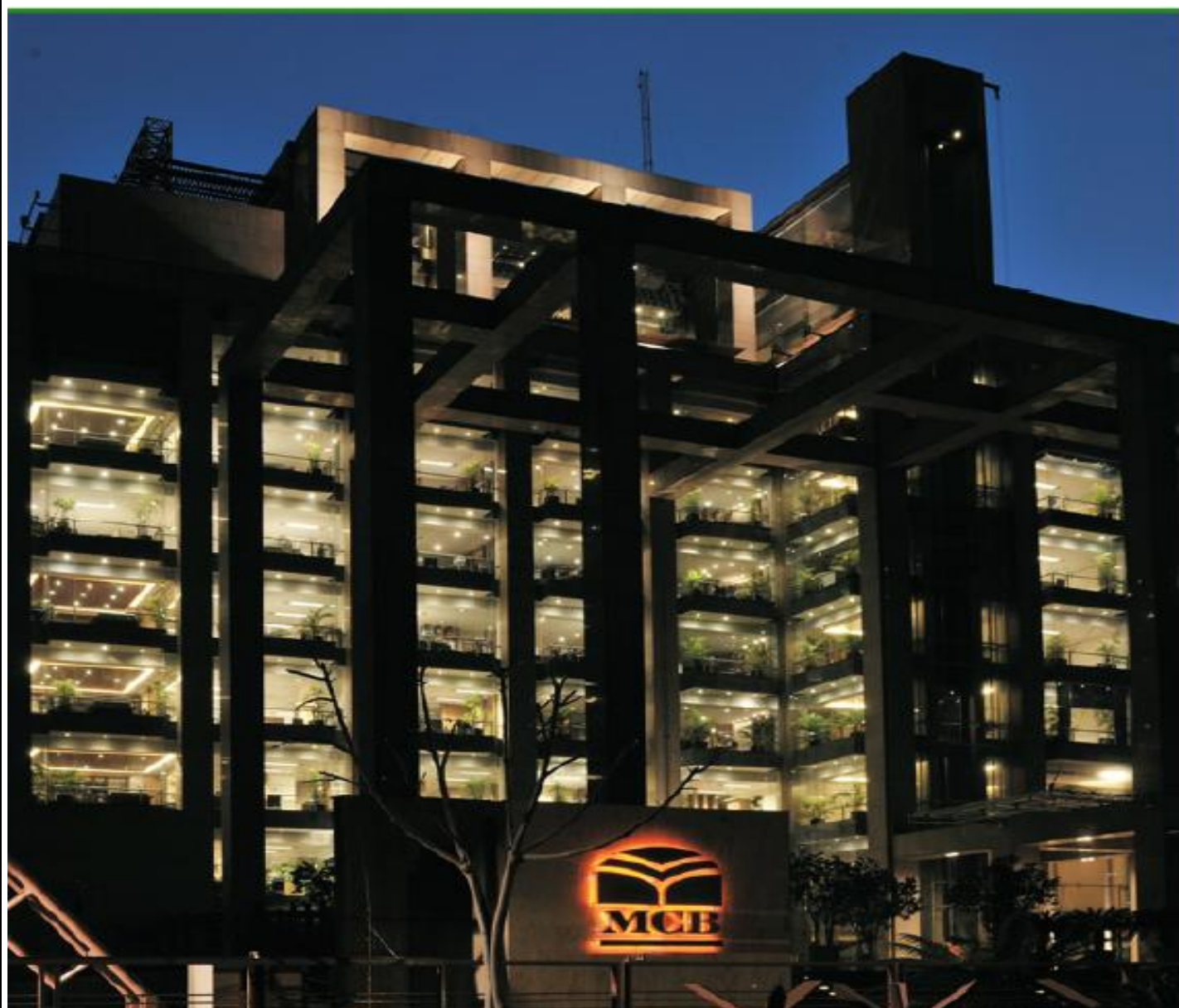




**CUSTOMER DUE DILIGENCE /  
KNOW YOUR CUSTOMER (CDD/KYC)  
&  
ANTI – MONEY LAUNDERING (AML)**

**PROCEDURES HANDBOOK**



**Revised 2010**

## TABLE OF CONTENTS

<b>1</b>	<b>INTRODUCTION.....</b>	<b>5</b>
1.1	BACKGROUND AND PURPOSE OF HANDBOOK.....	5
1.2	WHAT IS MONEY LAUNDERING.....	7
1.3	THE BANK'S ROLE IN PREVENTING MONEY LAUNDERING.....	7
1.4	STAGES OF MONEY LAUNDERING.....	8
1.5	THE BANK'S VULNERABILITIES.....	9
1.6	OVERSEAS NETWORK.....	9
<b>2</b>	<b>THE CURRENT LEGAL POSITION AND PENALTIES.....</b>	<b>10</b>
2.1	POSITION.....	10
2.2	WHAT DOES THIS MEAN IN PRACTICE?.....	11
2.3	PROCEDURE AND MANNER OF PROVIDING INFORMATION TO FMU.....	12
<b>3</b>	<b>THE BANK'S POLICY.....</b>	<b>13</b>
3.1	PROCEDURES WILL BE MAINTAINED TO ENSURE THE FOLLOWING:.....	13
3.2	SENIOR MANAGEMENT IS RESPONSIBLE FOR:.....	14
3.3	THE RESPONSIBILITIES OF COMPLIANCE:.....	15
3.4	ALL EMPLOYEES ARE RESPONSIBLE FOR:.....	15
3.5	COMPLIANCE GROUP IS RESPONSIBLE FOR:.....	16
3.6	PROVISION OF EDUCATION AND TRAINING.....	16
<b>4</b>	<b>CUSTOMER IDENTIFICATION &amp; ACCEPTANCE CRITERIA.....</b>	<b>17</b>
4.1	FOUR KEY ELEMENTS OF CDD / KYC.....	17
4.2	CUSTOMER DUE DILIGENCE & KNOW YOUR CUSTOMER (CDD / KYC).....	18
4.2.1	The Need to Verify Identity and Address.....	19
4.2.2	Completion of Account Opening and Know Your Customer Forms.....	20
4.2.3	Completion of Account Opening Formalities and Authorisation.....	20
4.2.4	Reporting of Suspicious Circumstances.....	21
4.3	CUSTOMER IDENTIFICATION – WHOSE IDENTITY MUST BE VERIFIED.....	21
4.4	CUSTOMER IDENTIFICATION - ACCOUNT OPENING DOCUMENTATION.....	22
4.5	MINIMUM DOCUMENTATION REQUIREMENTS TO OPEN ACCOUNT.....	23
4.6	PROCEDURES WHERE IDENTIFICATION CANNOT BE COMPLETED.....	27
4.6.1	Circumstances for Declining New Accounts.....	28
4.7	CUSTOMER IDENTIFICATION FOR NON ACCOUNT HOLDERS (WALK-IN-CUSTOMERS).....	28
4.7.1	Cash Remittances / Payments.....	28
4.7.1.1	Outward Remittances.....	28
4.7.1.2	Inward Remittances (For Non-Account Holders).....	28
4.8	CUSTOMER IDENTIFICATION - SPECIAL CIRCUMSTANCES.....	29
4.8.1	3 <sup>rd</sup> Party Mandate Holder(s).....	29
4.9	MAINTAINING RECORD FOR THE ACCOUNTS OPENED AND CLOSED.....	30
4.10	KNOWING THE CUSTOMER'S BUSINESS.....	30
4.11	CUSTOMER ACCEPTANCE.....	31
4.12	POLITICALLY EXPOSED PERSON (PEP).....	31
4.13	TRANSACTIONS THROUGH CORRESPONDENT RELATIONSHIPS.....	33
4.14	NEW REQUIREMENT FOR SWIFT MT 103.....	34
4.15	COMBATING THE TERRORIST FINANCING.....	34

<b>5</b>	<b>REVIEWING AND MONITORING CUSTOMER ACCOUNTS .....</b>	<b>37</b>
5.1	THE NEED FOR VIGILANCE, MONITORING OF RECENTLY OPENED ACCOUNTS .....	37
5.2	UPDATING KNOWLEDGE OF THE CUSTOMER .....	37
5.3	HALF – YEARLY CERTIFICATION FOR CDD / EDD - REVIEW OF ACCOUNTS .....	38
5.4	DORMANT ACCOUNTS .....	39
5.5	TRANSACTION MONITORING .....	39
5.5.1	Monitoring Transactions for Account Holders - Non Cash Remittances & transactions.....	39
5.5.2	Monitoring Transactions for Account Holders - Cash Remittances & transactions.....	40
5.5.3	Monitoring Transactions - Cash Remittances for Non Account Holders .....	40
5.6	THRESHOLD LIMITS.....	41
5.7	EXCEPTION REPORTS.....	41
5.7.1	Income / Salary / Turnover Exceptions Report .....	41
5.7.2	High Value Transactions Report.....	41
5.8	CUSTOMER LOANS AND ADVANCES.....	42
5.8.1	Granting of Advance .....	42
5.8.2	Settlement of the advance .....	42
5.8.3	Monitoring the advance .....	42
5.9	LETTERS OF CREDIT AND OTHER CONTINGENCIES .....	43
<b>6</b>	<b>RECORD KEEPING .....</b>	<b>44</b>
6.1	DOCUMENT RETENTION .....	44
6.2	RETRIEVAL OF DOCUMENTS.....	44
<b>7</b>	<b>RECOGNISING SUSPICIONS OF MONEY LAUNDERING .....</b>	<b>45</b>
7.1	WHAT IS SUSPICION?.....	45
7.2	EXAMPLES OF SUSPICIOUS TRANSACTIONS QUOTED BY SBP .....	45
7.2.1	Transactions which do not make economic sense .....	46
7.2.2	Transactions inconsistent with the customer’s business .....	47
7.2.3	Transactions involving large amounts of cash .....	47
7.2.4	Transactions involving structuring to avoid reporting or identification requirement .....	48
7.2.5	Transactions involving accounts .....	49
7.2.6	Transactions involving transfers to and from abroad .....	50
7.2.7	Investment related transactions .....	51
7.2.8	Transactions involving unidentified parties .....	51
7.2.9	Transitions involving insurance .....	53
7.2.10	Transactions involving embassy and foreign consulate accounts .....	53
7.2.11	Miscellaneous Transactions .....	53
7.2.12	Potential Indicators of money laundering/terrorist financing .....	55
<b>8</b>	<b>REPORTING SUSPICIONS.....</b>	<b>57</b>
8.1	OVERVIEW .....	57
8.2	REPORTING PROCEDURES FOR STAFF AND MANAGEMENT .....	59
8.3	ACTIONS AFTER REPORTING .....	59
<b>9</b>	<b>SPECIMEN FORMS / LISTS.....</b>	<b>60</b>
9.1	SUSPICIOUS TRANSACTION REPORT (STR) FORM.....	61
9.2	CURRENCY TRANSACTION REPORT (CTR) FORM .....	65
9.3	KYC FORM (INDIVIDUALS IN PAKISTAN), FAQs AND RISK RATING SHEET .....	67
9.4	KYC FORM (BUSINESS / LEGAL ENTITIES), RISK RATING SHEET .....	74

9.5	KYC FORM (INDIVIDUALS IN SRI LANKA), FAQs AND RISK RATING SHEET .....	78
9.6	HALF YEARLY REVIEW OF CERTIFICATION FOR CDD / EDD – REVIEW OF ACCOUNTS .....	87
9.7	MEMBER COUNTRIES AND TERRITORIES OF THE FATF INCLUDE: .....	89
<b>10</b>	<b>SBP PRUDENTIAL REGULATIONS.....</b>	<b>91</b>
10.1	REGULATION M-1 CUSTOMER DUE DILIGENCE (CDD) .....	91
10.2	REGULATION M-2 ANTI MONEY LAUNDERING MEASURES .....	95
10.3	REGULATION M-3 RECORD RETENTION .....	96
10.4	REGULATION M- 4 CORRESPONDENT BANKING .....	97
10.5	REGULATION M-5 SUSPICIOUS TRANSACTIONS .....	97
10.6	ANNEXURE-X (AS PER STATE BANK OF PAKISTAN BPD CIRCULAR NO. 5 DATED JULY 08, 2006) ...	100
<b>11</b>	<b>SUMMARY OF CHANGES IN PREVIOUS KYC / AML PROCEDURES HANDBOOK .....</b>	<b>103</b>



# 1 INTRODUCTION

## **1.1 BACKGROUND & PURPOSE:**

The purpose of this Hand Book is to ensure the identification and appropriate management of money laundering risks, ensure compliance with local laws and regulations to ensure the full and accurate implementation of MCB Anti-Money Laundering Policy. The procedures established in this hand book reflect the minimum principles and standards to protect MCB from being used for money laundering and related activities and must not let MCB to be used for funding Terrorism, Drug Trafficking and other illegal professions **etc.**

Together with the policies and procedures designed by the Management, Compliance and Control Group will ensure that the steps taken are translated in such a way that they result into an outcome in line with Laws of the land in vogue and SBP Prudential Regulations. In this regard CCG expects unconditional support from all the Groups.

In adherence to these Guidelines, and every aspect of its business, the Bank expects that all the employees will conduct themselves in accordance with the highest ethical standards. Bank also expects its employees to conduct business while remaining in the framework of guidelines as defined in Anti Money Laundering laws and regulations. Employees shall not knowingly provide advice or any other form of assistance to individuals, who attempt to either violate or avoid money laundering laws or the guidelines provided in this Hand Book.

Failure to adhere to the defined Guidelines may subject to disciplinary action and other serious pecuniary punishment. (Circular No.Compliance/GEN/35 of Feb 18, 2010)

Guidelines include adoption of specific procedures for customer identification, account opening and know your customer / due diligence and enhanced due diligence, compliance with obligation to identify and report unusual / suspicious activities. These Guidelines apply to all products, services and businesses. Any queries in relation to the Guidelines should be directed to CCG through respective controlling offices of the Area.

(Add HotScan/Mantas/World Check salient features and the purpose of OFAC List provided to branches/offices) (Answered below please remove line)

Compliance Group went through a restructuring during the year 2010 and group was renamed as Compliance and Control Group (CCG) with added responsibilities of strengthening Internal Controls and Proof and Verification of various outstanding entries lying unattended at Front Offices.

Compliance Group also embraced various internal changes to further strengthen role of Compliance Function for Prevention of Money Laundering Activities and Combating Terrorist Financing, In line with MCB's slogan of Being the Most compliant Bank, Group implemented a Centralized Transaction Monitoring System called MANTAS to monitor account activities and identify various patterns of transactions as demonstrated by Customers and Field Offices to Highlight Suspicious Ones.

In Continuation to the above, Group also deployed a Separate Name Filtering Solution, called HOTSCAN Online to monitor all the remittances, which are routed through SWIFT; Solution's main purpose is to capture any transaction, in which either remitter or beneficiary's name matches with the Names sanctioned by international regulatory bodies operating under the instructions of United Nations.

To ensure a desired participation by financial Institutions in an effort to stop any illegal Individual or entity from Using a Banking Channel, List of such Individuals / Entities are updated by Office of Foreign Asset Control, Bank of England, and European Union from time to time. MCB Bank Ltd through Its HOTSCAN System Updates all those list on timely basis to promptly monitor all SWIFT transactions and Hold if either remitter or beneficiary's name Matches with the names in the Sanctioned Lists.

In an effort to further improve role of compliance, World-Check Online is an Internet-based risk screening service was made fully operational which enable us to instantly check individual or entity names against the full World-Check data set. It is updated in real-time basis. It also covers Politically Exposed Persons PEP(s), their family members and potentially high-risk associates worldwide, thus making World-Check risk intelligence the ideal solution for Politically Exposed Foreign Person (PEFP) and PEP screening.

**A change to CDD/AML Guidelines is an ongoing process subject to changes as instructed by the Regulator from time to time. Such changes shall be notified to all the stakeholders through internal communication / Circulars and they are directed to incorporate the amendments / changes in their practices till the Hand Book is revised.**

**In addition of the above, this Handbook is to understand:**

- a) The legal requirements and the different penalties for non-compliance.
- b) What the Bank requires of you.
- c) How to recognize money laundering and the action you must take to prevent the risk.
- d) All members of the Bank's management and staff are expected to:

- Be aware of their personal legal obligations and the legal obligations of the Bank. (See Section 2).
- Be aware of the Bank's Policy and follow the Bank's procedures defined by external as well as internal requirements. (See Sections 3 - 6).
- Be alert for anything suspicious related to customers and transactions. (See Section 7).
- Report suspicions as per internal procedures developed in line with State Bank of Pakistan (SBP) and Financial Monitoring Unit (FMU) regulations. (See Section 8).

## **1.2 WHAT IS MONEY LAUNDERING**

Anti-Money Laundering Ordinance 2009 has been promulgated thus equipping a financial system with legal backing for controlling the menace of money laundering. The act of money laundering would be a serious offence punishable under the provisions of the Ordinance. The Ordinance has specified the role of different government departments, banks, regulatory bodies and investigating agencies for keeping a strict track on movement of illegal funds through the financial systems. The Ordinance has also elaborated the procedures to identify and highlight the suspicious account transactions through the banking system. As Defined in the AML Act 2010, the Federal Government by notification through official gazette established a Financial Monitoring Unit (FMU) which is housed in the State Bank of Pakistan's Building as an independent monitoring body.

Money laundering is referred to methods criminals use to hide and disguise the true nature and origin of the money they make from their crimes.

The term "laundering" is used because criminals need to turn their "dirty" criminal money into clean funds that they can use without arousing suspicion. Getting the criminal money into the financial system means that it becomes harder to trace and confiscate. Drug traffickers, armed robbers, terrorists, illegal arms dealers, fraudsters, and tax evaders all need to launder the proceeds of their crimes.

Money laundering is a global problem. All financial centres are vulnerable and all financial institutions within those centres need to play their part in preventing the criminals from successfully laundering their criminal money.

## **1.3 THE BANK'S ROLE IN PREVENTING MONEY LAUNDERING**

The prevention of money laundering from MCB point of view has three objectives:

**Ethical** - taking part in the fight against crime.

**Professional** - ensuring that the Bank is not involved in recycling the proceeds of crime that would call into question its reputation, integrity and, if fraud is involved, its solvency.

**Legal** - complying with SBP Regulations that impose a series of specific obligations on financial institutions and their employees

It is important that the Bank and its staff fully understand and comply with these increased responsibilities. The penalties for non-compliance could be of very serious nature, both for the Bank and individual members of staff. The Bank's licence and the jobs of all concerned could be at stake. In addition, there are criminal penalties for assisting money launderers. However, increased vigilance by the Bank in this area will also protect us from the under mentioned risks:-

Adverse publicity, loss of public confidence, and loss of business caused by inadvertent association with criminals.

Losses arising from inadvertent business relationships with criminals who may themselves defraud the Bank or undermine the integrity of the Bank's employees.

Confiscation of the assets of drug traffickers by the court, including deposits and other properties held by banks as collateral or comfort for loans.

Criminal prosecution and severe penalties.

#### **1.4 STAGES OF MONEY LAUNDERING**

The first step in the laundering process is for criminals to attempt to get the proceeds of their crimes into a bank or other financial institution, sometimes using a false identity. They can then transfer the proceeds to other accounts, here or abroad, or use it to buy other goods or services.

It eventually appears to be like any legally earned money and becomes difficult to trace back to its criminal past. The criminals can then invest or spend it or, as is often the case, use it to fund more crimes.

The Money Laundering process is often taken place in three stages:-

a) **Placement** - (Injection or Pre-washing)

Placement, being the first stage is the means by which funds derived from a criminal activity are introduced into the financial system, either directly or through using other retail businesses. This can be in the form of large sums of cash or a series of smaller sums. Initial proceeds of drug trafficking or street sales of drugs are always in cash.

b) **Layering** - (Stacking or Washing)

The aim of the second stage is to disguise the transaction through a succession of complex financial transactions with the purpose of erasing as quickly as possible all links with its unlawful origin. The funds may be converted into shares, bonds or any other easily negotiable asset or may be transferred to other accounts in other jurisdictions.

c) **Integration** - (Recycling)

Complex integration schemes then place the laundered funds back into the economy through real estate, business assets, securities and equities, in such a way that they re-enter the financial system appearing as normal business funds that have been legitimately earned.

The largest amount of criminal money that needs to be laundered comes from the sale of illegal drugs, primarily heroin, cocaine and cannabis.

## **1.5 THE BANK'S VULNERABILITIES**

Money launderers need the world's banking systems to launder the proceeds of their crimes and all banks in all countries are vulnerable. Cash based societies and countries without fully comprehensive anti-money laundering programmes (comprising legislation, regulation and financial sector procedures) are especially attractive to the launderers.

Thus, our own degree of vigilance must reflect to counter these potential vulnerabilities. Cash payments arising from drug related crimes are by no means the only risk. Fraud, for example, does not generate any cash, but the extensive proceeds still need to be laundered. Corruption by various individuals and companies including public officials inevitably involve fraud or theft and handling the proceeds of large scale corruption can produce a serious reputational risk for the bank. In addition, preventative measures put in place by International Financial Institutions over the past decade have resulted in the need for criminals to use more complex routes to gain access to the financial system, rather than placing their cash directly into the bank. It must be stressed therefore that all of the bank's products and services are at risk from being used by criminals to launder the proceeds of their crime.

## **1.6 OVERSEAS NETWORK**

These guidelines are equally applicable to our Overseas Network; however the regulations on Anti Money Laundering and Know Your Customer of the host country will be followed. SBP Prudential Regulation M5 Section 4 states that, "In case of foreign branches of the Banks / DFIs and subsidiaries of the banks / DFIs in foreign countries undertaking banking business, the banks / DFIs would ensure compliance with the regulations (relating to Anti Money Laundering and KYC) of SBP or the relevant regulations of the host country, whichever are most exhaustive."

## **2. THE CURRENT LEGAL POSITION AND PENALTIES**

### **2.1 POSITION**

Banks and Financial Institutions are required to take immediate notice and report to State Bank of Pakistan all unusual or large transactions in a account which apparently have no genuine economic, commercial or lawful purpose provided that the Bank (s) after complete investigation / enquiry come to a conclusion that such transactions are not for economic, commercial or lawful business purpose and relate to illegal or illicit activities, corruption or corrupt practices and narcotic activities.

Prudential Regulations (PR) M1, M2, M3, M4 and M5 issued by State Bank of Pakistan on money laundering make it mandatory for every Commercial Bank / Financial Institution to put in place procedures to combat Money Laundering. A Commercial Bank would render itself liable for imposition of heavy penalties by SBP if these regulations are not strictly complied with. It is obligatory on MCB, its management and staff to follow the procedures strictly as outlined in these prudential regulations as well as Anti-Money Laundering Regulations 2008 under SRO No. 02 (KE) 2009 dated November 22, 2008.

#### **There are personal obligations on every member of management and staff that:**

It is an offence to assist anyone whom you know, or suspect to be, laundering money generated illegally. In the financial sector, assistance can be provided by, for example, opening a bank account, accepting deposits, making transfers/payments, advancing a loan, issuing/accepting letters of credit.

If you know or suspect that a transaction is related to any illegal activity, you must report it in order to get protection against a charge of knowingly assisting a criminal to launder the proceeds of his/her or their crime (see Sections 7 and 8).

In the case of drug trafficking or terrorist financing, if you form a suspicion of money laundering in the course of your employment or business activity, you must report it, even if you are not directly handling the transaction or funds in question, otherwise you will be alleged for the offence of collusion.

Field is categorically advised that unless it is established upon investigation / enquiry that the transactions in question are for unlawful purposes and have no economic, commercial or lawful business purposes, such transactions must not be reported as suspicious transactions. Otherwise, the Bank might be involved in damage suit by such account-holder(s). Staff is strictly advised that under no circumstances they should talk to non relevant people including customer / account

holder about transaction which is to be reported as suspicious transactions otherwise this could be treated as “tipping off” offence.

The procedures bank has developed to combat Money Laundering include:

1. Awareness raising and training of staff. (See Section 3).
2. The verification of new client identification and customer due diligence and his business. (See Sections 4 and 5).
3. Retention of records. (See Section 6).
4. Recognition and reporting suspicions of money laundering. (See Sections 7 and 8).

## **2.2 WHAT DOES THIS MEAN IN PRACTICE?**

You are not committing an offence if you **do not know or suspect** that funds relate to drugs, terrorism or other serious crime.

You are committing an offence if **knowing or suspecting** that someone is involved in any serious crime you:

- a) assist them to obtain control or retain their proceeds, or
- b) give them any help in investing or transferring those proceeds, or
- c) Advise them that you, or another colleague at the Bank, are suspicious of their activities.

In practice, of course, you are generally not likely to know and may not realise or suspect that there was anything suspicious about a transaction until it is all over and the customer has gone away. If that happens, your duty is clear; you must report your suspicion by raising STR (Suspicious Transaction Report); you will not be criticised that you were not suspicious immediately.

If you do not report your suspicion and the funds are related to drugs or terrorism, you will have committed an offence of failure to report. If you do not report your suspicion concerning any criminal money, whether relating to drugs, terrorism, tax evasion or any other serious crime, you may also need to defend an action against you for deliberately assisting the criminal.

If you are suspicious, you discuss it with your Branch Manager (BM) and Operations Manager (BOM) who will follow the procedure as laid down in Section 4.2.4 and Section 8.1. If they agree that the transaction is suspicious, they must report it by following process described in Section 4.2.4 under reporting of Suspicious Transactions.

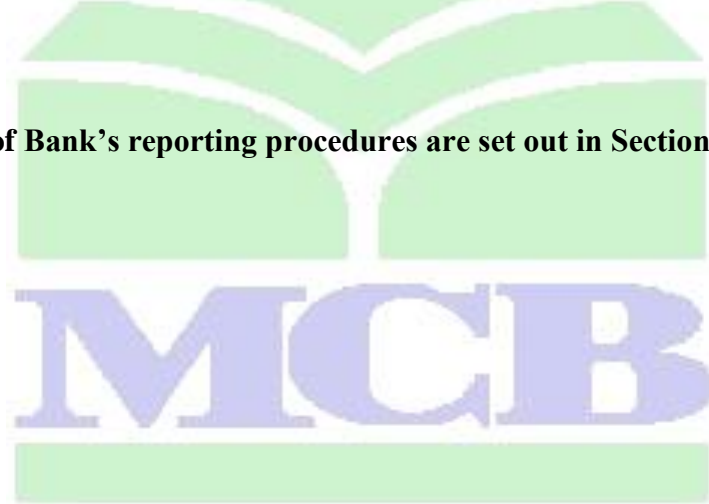
### **2.3 Procedure and manner of providing information to FMU (Financial Monitoring Unit).**

Compliance group / Field Offices shall file with the FMU, to the extent and in the manner prescribed by the FMU, Suspicious Transaction Report conducted or attempted by, at or through Bank if the Bank knows, suspects, or has reason to suspect that the transaction or a pattern of transactions of which is being carried out through proceeds of some crime or is informed about the intent of breaking Money Laundering Act.

All CTR shall to the extent and in the manner prescribed by the FMU be filed by Compliance group or Branch office to FMU immediately but not later than seven working days after the respective currency transactions.

Bank shall keep and maintain all record related to Suspicious Transaction Report and Cash Transaction Report filed by it for a period of at least five years from the date of reporting that transaction

**The Process Flow of Bank's reporting procedures are set out in Section 8.**



### **3 THE BANK'S POLICY**

It is the Policy of MCB BANK LTD. that:

- a) Local statutory and regulatory obligations to prevent money laundering are to be met in full.
- b) Positive management action will be exercised in order to minimize the risk of the Bank's services being abused for the purposes of laundering funds associated with drug trafficking, terrorism and other serious crimes, as defined by SBP and FMU.
- c) The Bank will not continue established relationships with customers, whose conduct gives rise to suspicion of involvement with illegal activities. Any customer relationship where the customer's conduct gives the Bank reasonable cause to believe or suspect involvement with illegal activities will be reported by the Head of Compliance Group to the FMU after proper scrutiny / enquiry in consultation with the respective Business Head(s). Thereafter, action will be undertaken in conjunction with the law enforcement agencies.
- d) The Bank's policy and procedures will be based upon the requirements of the Anti Money Laundering Regulations and AML Act 2010 issued by FMU.

#### **3.1 PROCEDURES WILL BE MAINTAINED TO ENSURE:**

- a) That the identities of all persons conducting business with the Bank are properly verified and sufficient information gathered and recorded to permit the Bank to "know its customer" for Customers Due Diligence and predict the expected pattern of business. (See Sections 4 and 5).
- b) Prospective business where all of the required information cannot be obtained without a justifiable reason is declined. (See Section 4).
- c) Potential new relationships that do not appear to be legitimate are declined. (See Section 4).
- d) In case where Bank is not able to satisfactorily complete required Customer Due Diligence (CDD) / Know Your Customer (KYC) measures including verification of identity, beneficial ownership or information on purpose and intended nature of business relationship, account should neither be opened nor any service be provided and instead reporting of suspicion should be considered. Similarly, relationship with existing customers should be terminated after reporting of suspicious transaction, if CDD / KYC

are found unsatisfactory. (See Section 4). [Refer Section 13 of BPRD Circular Letter No. 07 dated March 09, 2009]. Transactions conducted by non-account holders or by counter-parties that do not appear legitimate should be declined. (See Section 4).

- e) Cash remittances for Walk in Customers are monitored and will be subject to additional controls that include identifying and verifying the Identity (**CNIC/Valid Passport/Valid Driving License**) and purpose of walk-in-customers conducting transactions above the limit prescribed by the bank.(This limit is Rs, 500,000/)
- f) Established relationships are regularly monitored [Normal Risk = once in 3 years (CDD); High Risk = once a year (EDD)]. (See Section 5).
- g) If turnover in account deviate significantly from the customer's declared thresholds (Dr/Cr Turn-Over in KYC Form), at the time of establishing a relationship. EDD will also be required to be conducted irrespective of EDD time frame. (See Section 5).
- h) Records are retained to provide an audit trail and adequate evidence to the law enforcement agencies in their investigations. (See Section 6).
- i) All suspicions are reported promptly to respective ROM/RH for onward advice to the Head of Compliance North / South after having investigated the transaction independently and full co-operation is extended to the FMU at SBP and other law enforcement authorities when required. (See Section 4.2.4, Section 7 and Section 8).

### **3.2 SENIOR MANAGEMENT IS RESPONSIBLE FOR:**

- a) The day to day compliance with anti money laundering obligations is the sole responsibility of respective business heads within all segments of the Bank in their respective jurisdiction.
- b) Ensuring that the RCO / Head of Compliance North / South are provided with prompt reporting of any unusual/suspicious transactions and other matters of significance.
- c) Seeking from the Compliance Group, at least annually, a report relating to the Bank's compliance with its anti-money laundering obligations and acting on the findings and recommendations.
- d) Internal Audit to report deviations to the respective GMs / RHs to ensure rectification of exceptions found during their audit.

### **3.3 THE RESPONSIBILITIES OF COMPLIANCE:**

#### **The Head of Compliance & Control Group (HCCG) North & South / Head of Compliance & Control Group is responsible for:**

- a) Developing and maintaining policy in line with evolving statutory and regulatory obligations. The Heads of Compliance & Control (South & North) / Group Head Compliance will have available copies of the current SBP / FMU regulations on Anti Money Laundering and the Head of Compliance & Control Group will ensure that he has all the required updated knowledge with respect to any amendments in Anti Money Laundering requirements
- b) Making out all efforts to ensure staff is aware of their obligations and the Bank's procedures, and that staff is trained with money laundering prevention tactics. Head of Compliance & Control (South / North) / Head of Compliance & Control Group will ensure that Staff Colleges are advised with the current changes so that training courses offered on anti money laundering are modified accordingly.
- c) Representing the Bank to all external agencies in Pakistan (SBP, FMU, NAB, FIA and Customs, ANF etc), and in any other 3<sup>rd</sup> party enquiries with relation to money laundering / Terrorist Financing prevention.
- d) Making all out efforts that all segments of the Bank are complying fully with the stated policy and therefore monitoring operations and development of the policy at this end.
- e) Preparing compliance reports for the Board and Senior Management.
- f) Ensuring that controlling offices complete and forward the "Half-Yearly Certification for CDD/EDD – Review of Accounts." (See Section 9.6)
- g) Ensuring that the established STRs raised by field staff and field management are reported to FMU. Undertaking the internal review of all suspicions so reported and determining whether or not such suspicions have substance and require disclosure to FMU at SBP.
- h) Obtaining and making use of national and international information as unveiled by FATF (Financial Action Task Force) and other sources concerning Countries with serious deficiencies.

### **3.4 ALL EMPLOYEES ARE RESPONSIBLE FOR:**

- a) Remaining vigilant to the possibility of money laundering / terrorist financing.

- b) Complying fully with all anti money laundering procedures in respect of customer identification, beneficial ownership, 3<sup>rd</sup> party mandates, transactions monitoring, and record keeping and reporting.
- c) Reporting all suspicions of money laundering to the Compliance Group by following detailed procedures in Section 4.2.4.
- d) Employees who violate any of the anti money laundering regulations or the policies and procedures outlined in this Handbook will be subject to disciplinary action
- e) **PUNISHMENT FOR MONEY LAUNDERING** - Whoever commits the offence of money laundering shall be punishable with rigorous imprisonment for a term which shall not be less than one year but may extend to ten years and shall also be liable to fine which may extend to one million PKR and shall also be liable to forfeiture of property involved in the money laundering. [Anti-Money Laundering Act, 2010].

### **3.5 COMPLIANCE & CONTROL GROUP IS RESPONSIBLE FOR:**

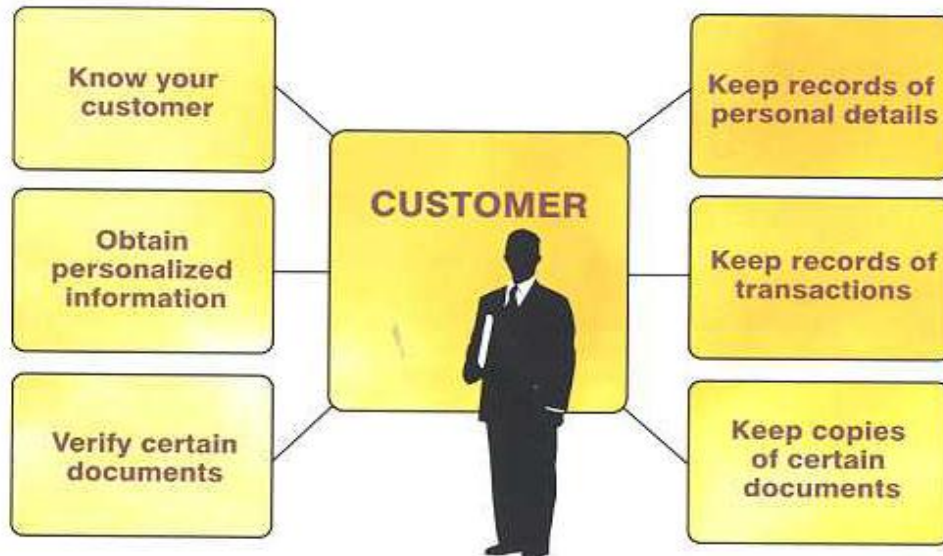
- a) Reviewing and ensuring compliance by the Bank with Anti Money Laundering statutory and regulatory obligations, in respect of Bank's Anti Money Laundering policy & procedures.
- b) Advising senior management of any deviations in business practices from the Bank's AML / CDD (KYC) policy and procedures that have been noted by the Compliance & Control Group.

### **3.6 PROVISION OF EDUCATION AND TRAINING**

All members of management and field staff are responsible to have training on anti money laundering at least once a year. Compliance Group will coordinate with Training Centers / HRD to ensure that respective directives from regulatory bodies are covered in these training sessions.

**All members of management and field staff will be given this Handbook in order for them to understand their obligations. All branch managers will sign the "Half-Yearly Review of Certification for CDD/EDD – Review of Accounts" (For details see Section 9.6)**

## 4 CUSTOMER IDENTIFICATION & ACCEPTANCE CRITERIA



### 4.1 FOUR KEY ELEMENTS OF CDD / KYC

Bank's CDD / KYC policy has four major elements:

**1- Customer Identification:** Establishing the identity of customers is central to the CDD / KYC policy both for the customer acceptance or rejection decision and for the on-going monitoring of customers' accounts and transactions. By identifying customers effectively, you are able to deal with them in the appropriate manner and comfortably.

**2- Customer Acceptance:** The point at which a new customer is accepted or rejected is the easiest point at which the risk of dealing with illegal money can be avoided. By following good customer acceptance policies, you can avoid dealing with entities and individuals who might engage in illegal transactions.

**3- Accounts & Transactions Monitoring:** In an effective CDD / KYC policy, customer accounts and transactions are properly classified in terms of risk and are regularly monitored. Through checks and thresholds, unusual activities or activities by high-risk customers are detected and reviewed.

**4- Risk Management:** To ensure that the risks posed by money laundering / terrorist financing and other criminal customer activities are consistently dealt with, good risk management practices are essential. In this way the Bank can 'scale' its operations by remaining vigilant about customer-driven risk.

#### **4.2 CUSTOMER DUE DILIGENCE & KNOW YOUR CUSTOMER (CDD / KYC)**

The general misperception of branch managers on CDD / (KYC) / AML policy is that SBP regulations make the new account opening difficult. On the contrary, proper account documentation and CDD / KYC procedures provide satisfaction and protection to the branch managers / staff against unforeseen events and assist in establishing relationship in accordance with the bank's policies. Getting maximum reliable information about the customer is the basic principle of good banking which enables the Bank to make correct decisions to meet with customer's genuine banking requirements promptly. Branch officers / staff must ensure that all the necessary documents have been obtained at the time of account opening or at the time of on-going reviews of CDD / KYC formalities.

The Bank has a statutory obligation to know its customers (which includes Customer Identification (CI), Customer Acceptance (CA), Assigned Risk Rating (Normal or High) and subsequent monitoring of transactions). It is also obligatory to understand the nature of the business to be conducted with us, beneficial ownership(s) and 3<sup>rd</sup> party mandates. This applies to all type of customers regardless of who they are, their personal status (For PEPs see Section 4.12), or the type of account or service that they require.

##### **Knowing your customer means:**

- a) Seeking evidence of identity and address and independently confirming that evidence at the start of a business relationship with the Bank. (See sub-sections 4.3-4.10);
- b) Seeking information regarding the nature of the business that the customer expects to conduct with the Bank, establishing sources of income and expected patterns of transactions, and keeping that information up to date, to show what might be regarded as normal activity for that customer.
- c) All resident prospective customers for accounts with MCB must be seen face to face except those customers who are living abroad and wants to open a non-face-to-face / on-line account; adequate measures in this regard should be taken, for example, independent verification by a reliable 3<sup>rd</sup> party, client report from the previous bank / DFI of the customer, etc.

**Branch Manager:** Will be responsible for reviewing all HR Accounts once in a year and NR accounts once in three years.

## **E-BANKING:**

**The impersonal and borderless nature of electronic banking combined with the speed of the transaction inevitably creates difficulty in customer identification and verification. Bank should proactively assess various risks posed by emerging technologies.**

There must be specific measures to mitigate the risk attached with non-face-to-face prospective customer such as:

- Certification of documents presented;
- Independent contact with the customer by the bank;
- Requiring the first payment to be carried out through an account in the customer's name with another bank subject to similar customer due diligence standards.
- Require an adequate verification of customer's previous banking relationships

### **4.2.1 THE NEED TO VERIFY IDENTITY AND ADDRESS**

The Bank must verify the credentials of every customer when an account is first opened. This applies to all types of accounts (personal customers; sole traders/proprietors; partnerships; private and public companies, trusts, Non Governmental Organizations (NGOs), Not-For-Profit Organizations (NPOs), government accounts, etc.)

#### **Proof of Identity of Walk-in-Customer**

Proof of identity must also be verified through original document, whenever a customer without an account with the Bank (i.e. a walk in customer) requires carrying out a cash-based remittance transaction of **Rs.500,000** or more. This limit is **Rs.1,000,000** if the cash remittance is to be credited to an account of Bank's Account Holder. The purpose of remittance column must also be completed in the remittance form.

Further to the above, In case customer does not have a valid CNIC, transaction can be processed on the strength of any other photo identity issued by Govt of Pakistan such as Passport, Driving license etc

Note: Any identity document without photo on it will not be sufficient for such transactions.

#### **4.2.2 COMPLETION OF ACCOUNT OPENING AND KNOW YOUR CUSTOMER FORMS**

All prospective customers must completely fill-in all the appropriate columns of Account Opening Form (AOF) and provide the necessary documentary evidence of identity and financial information. If any column on AOF is not applicable it should be stroked out as “N/A”; and no section should be left blank.

The customer must be interviewed by the Branch Manager (BM) and he **MUST** sign the KYC Form. Afterwards the AOF be handed over to Branch Operations Manager (BOM). The AOF must be signed by the BOM in order to keep intact the maker-checker policy of the Bank. The details of the AOF must invariably be input in the system by the BOM. The system generated report after this input **MUST** be checked by the BM.

Any additional information obtained during the interview about the customer’s background, country of origin, public or high profile position (PEP), nature of business and financial standing should be recorded by the branch manager and kept in customer’s file.

#### **4.2.3 COMPLETION OF ACCOUNT OPENING FORMALITIES AND AUTHORISATION**

No account will be opened until the account opening and relevant Know Your Customer forms have been completed and all documents have been received and examined to ensure that they are valid. For example:

- a) CNIC card has not been expired. [For further details see Section 4.5 Table]
- b) The documents (including CNIC) are originals and not copies.
- c) Specimen Signature Card (SSC) and mandate duly signed and completed and must be scanned instantly to enter it in the SSC module of the system.
- d) All documentary evidence, information and signatures are consistent. If signatures differ from CNIC; a file note on AOF must be recorded to this effect and undertaking from customer must be obtained.
- e) In case of giving a 3rd party mandate (SF-67); this form must be duly signed, completed and be backed by a written request giving therein the reasons/relationship amongst the account holder(s) and mandate holder. A separate KYC of Mandate Holder must be done and Relevant Identity Document must be obtained and filed.
- f) The Letter of Thanks (LOT) should be sent through registered post / courier to the customer on their given current mailing addresses in order to notify the customer that their account has been opened. If LOT is returned undelivered, a restraint of (WAN) where abouts unknown must be marked in the system.

- g) The cheque book should only be issued after the account opening form has been completed in all respects and the Letter of Thanks issued by the Bank has been received by the customer, to ensure the above, Branch must request customer to present a LOT before issuance of Cheque Book.

**In the absence of the Branch Manager the account opening will be approved by Branch Operations Manager.**

#### **4.2.4 REPORTING OF SUSPICIOUS CIRCUMSTANCES**

If there are any suspicious circumstances surrounding the opening or operation of any account, the Branch Manager or Operation Manager must report the matter immediately to the respective ROM / RH and an endorsed advance copy of STR to Head of Compliance & Control Group North / South. After making discreet inquiries, the respective ROM / RH together with LCO (posted at Circle Office) will send their detailed report to the Head of Compliance & Control Group (North / South), giving reason for the suspicion with their findings and shall endorse a copy thereof to the respective GM / Business Head. Respective GM / Business Head will send suspicious Report sent by RH / ROM & LCO to Head of Compliance & Control Group North / South. If it is established that the transaction under review is suspicious, the Head of Compliance North / South after due diligence and necessary checks will advise Head of Compliance Group, who will discuss it with President and subsequently the transaction will be reported to the FMU at SBP.

#### **4.3 CUSTOMER IDENTIFICATION – WHOSE IDENTITY MUST BE VERIFIED**

Establishing the identity of anyone who wishes to do business with the Bank is vital. For all applicants the Bank is required to be satisfied that:

- a) The genuineness of the person and his/her bona-fide address (current mailing address) is established.
- b) The sole traders/proprietors, partnership, company we are dealing with are a legitimate business with a known address and represents legitimate owners. Therefore, in respect of accounts for sole traders/proprietors, partnerships and companies, it is necessary to verify the identity of the business entity **PLUS** the key individuals who will be operating the account as well as those who are declared as investors to the business (beneficial owners). [For further details see Section 4.5 Table]

- c) Anonymous accounts or accounts in the name of fictitious persons (Benami Accounts) are not allowed to be opened.
- d) For joint accounts, the identity of each signatory in joint account must be established through separate KYC forms. This KYC requirement applies to 3<sup>rd</sup> parties also (e.g. power of attorney holders) who are permitted by the account holder to operate the account. If the customer gives a mandate to a 3<sup>rd</sup> party to operate the account, the Mandate Form (SF-67) should be signed by both parties i.e. the account holder and the 3<sup>rd</sup> party and must be backed by a written request giving the reasons / relationship by the account holder.

#### **4.4 CUSTOMER IDENTIFICATION - ACCOUNT OPENING DOCUMENTATION**

For each type of account, certain documentation must be obtained and sufficient information gathered for us to be certain that:

- a) We know our new customer, having verified identity and address and understood the customer's business and the expected level and pattern of transactions.
- b) The new customer has understood and accepted the Bank's terms and conditions for t account since Terms & Conditions Booklet is provided at the time of Account Opening.
- c) We are satisfied that the mandated individuals do have the authority of the account holder(s) to control the account; and.
- d) We are satisfied that the account holder(s) and their business are legitimate and the Bank is not exposed to financial, reputational and regulatory risk

**Original identification documents** must be seen, photocopied and retained in the customer's file. Care must be taken to ensure that the copies are clear and legible and that the copies are stamped, signed and dated to show that the originals have been seen by the authorised officer of MCB. If there is any doubt about the legality or acceptability of any document, immediate reference must be made to the ROM / RH or GM.

When a prospective customer's mailing address provided on AOF differs from the address on CNIC of customer, documentary evidence of the temporary address such as Copy of latest Utility Bill(s), tenancy agreement or letter from the landlord should be obtained. In case any such evidence is not produced, undertaking/vernacular from the customer along with endorsement by two witnesses must be obtained.

Documentary evidence could be a copy of the lease / tenancy agreement or a letter from the landlord stating that the person wishes to open account lives in his or her property as a tenant etc. This should be obtained together with a copy of landlord's CNIC and utility bill.

Care must be taken to ensure that the information presented / collected makes sense on a cumulative basis and does indeed relate to the applicant.

**Accounts must not be opened on the strength of faxed documentation**, even from within the Client Group. Only original or certified photocopy documentation is acceptable.

#### **4.5 MINIMUM DOCUMENTATION REQUIREMENTS TO OPEN AN ACCOUNT**

The following documentation requirements have been issued by the State Bank of Pakistan under Regulation M-1 for the Banks to obtain when they open various types of accounts along with KYC form.

#### **DOCUMENTS TO BE OBTAINED FROM VARIOUS TYPES OF CUSTOMERS/ACCOUNT HOLDER(S) UNDER REGULATION M-1**

SR.	NATURE OF ACCOUNT	DOCUMENTS/PAPERS TO BE OBTAINED
I	Individuals	<ol style="list-style-type: none"> <li>1. Attested photo copy of valid Computerized National Identity Card* (CNIC) or Passport of the individual by an Officer of the Bank.</li> <li>2. In case the CNIC does not contain a photograph, the Bank should also obtain, in addition to CNIC, any other document such as Driving License etc. that contains a photograph. However, if the individual does not have any other valid document which bears photograph, following documents should be obtained:               <ol style="list-style-type: none"> <li>i. A copy of the photograph duly attested by gazetted officer/Nazim</li> <li>ii. A copy of CNIC without photograph duly attested by the same person who has attested the photograph as per Sr. No (i) above.</li> <li>iii. A confirmation in writing to the effect that the individual has no other document bearing photograph.</li> </ol> <p>Bank shall ensure that the CNIC and the photograph are of the same person whose account is being opened with them. The particulars/CNIC of such persons must be confirmed from NADRA in writing or through its "Verisys" system by the Bank.</p> </li> <li>3. In case of a salaried person, attested copy of his service card, or any other acceptable evidence of service, including, but not limited to a certificate from the employer.</li> <li>4. In case of illiterate person, a passport size photograph of the new account</li> </ol>

SR.	NATURE OF ACCOUNT	DOCUMENTS/PAPERS TO BE OBTAINED
		<p>holder besides taking his right and left thumb impression on the specimen signature card.</p> <p><b>Note:</b> Senior Citizen having the age of 65 years or more will not be required to renew their expired CNICs and banks shall be allowed to open account on expired CNICs. (Compliance Memo GEN/ 146 dated June 10, 2009 and SBP Letter BPRD/BLRD-09/2009-3867 dated June 9, 2009)</p>
II	Sole Trader / Proprietorship	<p>Bank should exercise extra care in view of the fact that constituent documents are not available in such cases to confirm existence or otherwise of the proprietorships. All out efforts should be made to obtain relevant document(s) in order to establish the existence of the sole trader/proprietorship concern and following documents must be obtained:</p> <ol style="list-style-type: none"> <li>1. Attested photo copy of a valid Computerized National Identity Card (CNIC) or Passport of the individual by an Officer of the Bank. Same must also be verified through NADRA on-line VERISYS system.</li> <li>2. In case the CNIC does not contain a photograph, the Bank should also obtain, in addition to CNIC, any other document such as Driving License etc. that contains a photograph. However, if the individual does not have any other valid document which bears photograph, following documents should be obtained:               <ol style="list-style-type: none"> <li>(1) A copy of the photograph duly attested by gazetted officer/Nazim</li> <li>(2) A copy of CNIC without photograph duly attested by the same person who has attested the photograph as per Sr. No (i) above.</li> <li>(3) A confirmation in writing to the effect that the individual have no other document bearing photograph.</li> </ol> </li> </ol> <p>Bank shall ensure that the CNIC and the photograph are of the same person whose account is being opened with them. The particulars/CNIC of such persons must be confirmed from NADRA in writing or through its “Verisys” system by the Bank.</p>
III	Partnership	<ul style="list-style-type: none"> <li>- Attested photo copy of a valid Computerized National Identity Card (CNIC) of all partners.</li> <li>- Attested copy of ‘Partnership Deed’ duly signed by all partners of the firm.</li> <li>- Attested copy of Registration Certificate with Registrar of Firms. <b>In case the partnership is unregistered, this fact should be clearly mentioned on the Account Opening Form.</b></li> <li>- Authority Letter, in original, in favour of the person authorized to operate the account of the firm.</li> <li>- Purpose, source of funds, operation in account and how the Partnership will</li> </ul>

SR.	NATURE OF ACCOUNT	DOCUMENTS/PAPERS TO BE OBTAINED
		dissolve must be ascertained.
IV	<b>**Joint Stock Companies Whether Private or Public</b>	<p>Certified Copies of:</p> <ul style="list-style-type: none"> <li>(a) Resolution of Board of Directors for opening of account specifying the person(s) authorized to operate the company account with embossed seal of the company.</li> <li>(b) Memorandum and Articles of Association.</li> <li>(c) Certificate of Incorporation</li> <li>(d) Certificate of Commencement of Business in case of Public Limited Companies only (original required for inspection and return).</li> <li>(e) List of Directors on <b>Form 29</b> issued by the Registrar SECP.</li> <li>(f) Attested photo copies of CNIC of all the directors.</li> </ul> <p>Documents referred in point B, C, D &amp; E must be attested by SECP.</p> <p><b>**In case of Joint Stock Companies of Foreign Origin</b></p> <p>The condition of obtaining Board Resolution and Certificate of Commencement of Business for opening bank account has been relaxed for only such foreign companies / entities belonging to countries where said requirements are not enforced under their laws / regulations. However, such foreign companies will have to furnish the following documents in lieu of resolution passed by BOD for opening of account and Certificate of Commencement of Business to the satisfaction of their banks.</p> <ul style="list-style-type: none"> <li>a. Power of Attorney from the competent authority for opening bank accounts.</li> <li>b. A certificate from the company Secretary, duly authorized by the Board, that the entity started its business from certain date and that certificate of Commencement of Business is not issued in that country.</li> </ul> <p><b>All other instructions on the subject shall, however, remain unchanged.</b></p>
V	<b>Clubs, Societies and Associations</b>	<p>Certified copies of :</p> <ul style="list-style-type: none"> <li>a) Certificate of Registration by Registrar of Co-operative Societies/ Registration Authority.</li> <li>b) By-laws / Memorandum &amp; Articles of Association / Rules &amp; Regulations of the society containing official seal of the registration authority on each page thereof.</li> <li>c) Resolution of the Governing Body/Executive committee for opening of account authorizing the person(s) to operate the account and attested copy of a valid CNIC of the authorized person(s). It must be ensured that mandate for operation of account given in the resolution is not in violation of the provision of By-laws / Memorandum &amp; Articles of Associations.</li> <li>d) List of the members of the Managing Committee duly certified by the</li> </ul>

SR.	NATURE OF ACCOUNT	DOCUMENTS/PAPERS TO BE OBTAINED
		<p>registrar of co-operative societies should be obtained.</p> <p>e) Permission of the Registrar Co-operative Societies for opening of account in the name of society is required under Section 37 (d) of Co-operative Societies Act 1925</p> <p>f) In case of Associations, permission of the Registration Authority for opening of account in the name of Association as required under Section 7 (c) of Voluntary Social Welfare (Registration &amp; Control) Ordinance 1961.</p> <p>g) An undertaking signed by all the authorized persons on behalf of the institution mentioning that when any change takes place in the persons authorized to operate on the account, the banker will be informed immediately.</p> <p>h) Bank should obtain copies of valid CNICs of all the members of Governing and Executive Bodies of DHA etc or ask for delegation of power to Administrator under section (7) &amp; (8) of the Pakistan Defence Housing Authority Order, 1980 and accept copy of a valid CNIC of Administrator as well as authorized signatories for the purpose of opening accounts of DHA or similar other authorities subject to the condition that all other requirements laid down under PR-M1 shall be complied with in letter and spirit.</p>
VI	<b>Agents Accounts</b>	<ul style="list-style-type: none"> <li>• Certified copy of 'Power of Attorney'.</li> <li>• Attested photo copy of their valid CNIC / Passport / ID of the agent.</li> </ul>
VII	<b>Trust Account</b>	<p>A. Attested copy of Certificate of Registration.</p> <p>B. Certified copy of the 'Instrument of Trust / Trust Deed'.</p> <p>C. Attested photo copy of valid CNIC of all the trustees.</p> <p>D. Resolution duly passed by the Trustees in their meeting regarding opening &amp; operation of account in the Bank in the name of Trust. It must be ensured that mandate for operation of account given in the resolution is not in violation of the provision of Trust Deed.</p> <p>E. List of Trustees duly certified at least by Two Trustees should be obtained.</p> <p><b><u>Documents referred in Point A &amp; B will be attested by the Registrar of Trust.</u></b></p> <p>Bank can open accounts of trust covered under section 227 of Companies ordinance 1984 including Provident Fund, Gratuity Fund and pension funds after obtaining evidence of registration from any Govt Authority.</p> <p><b>Bank has to ensure that the opening of Trust Account &amp; subsequent operation in the account are in accordance with the spirit of KYC,</b></p>

SR.	NATURE OF ACCOUNT	DOCUMENTS/PAPERS TO BE OBTAINED
		<b>customers due diligence and other Anti Money Laundering / Combating Financing of terrorism (AML/CFT) safeguards.</b>
VIII	<b>Executors / Administrators</b>	Attested photo copy of CNIC of the Executor / Administrator. Certified copy of Letter of Administration or Probate.
IX	<b>Government Accounts</b>	It must be ensured that government accounts are not opened in the personal names of the government officials(s). Any such account, which is to be operated by an officer of the Federal / Provincial / Local Government in his / her official capacity, shall be opened only on production of a special resolution / authority from the concerned administrative department duly endorsed by the Ministry of Finance or Finance Department of the concerned provincial or Local Government.

**Note:** \* In case where the depositor / borrower has not yet got renewed the Computerized National Identity Card (CNIC), the Bank may obtain photocopies of expired CNIC as verified from NADRA and receipt of NADRA (evidencing that the client has applied for renewal of CNIC) along with an undertaking in writing that a copy of CNIC will be submitted within 15 days of the issuance of the CNIC as evidenced by the Receipt. Further, Bank may accept a copy of valid “Alien Registration Card” issued by National Aliens Registration Authority (NARA) instead of CNIC in case of registered aliens who wish to open a bank account in Pakistan in Pak. Rupees only. Likewise, Bank may also accept copy of National Identity Card for Overseas Pakistani (NICOP) and Pakistan Origin Card (POC) issued by NADRA from their holders for opening Bank accounts in Pakistan both in local and foreign currency in lieu of CNIC. **In terms of SBP guidelines; the CNICs of old aged persons having the age of 65 and above does not require the renewal of their CNICs by NADRA for opening a bank account.**

All the documents mentioned above must be seen in original and notation (original seen) thereof must be made on the photocopies of these documents by an authorized MCB Officer with signatures and stamp to this effect.

**Proof of Registration (PoR) issued by NADRA to Afghan Refugees is not acceptable for opening of account.**

#### 4.6 PROCEDURES WHERE IDENTIFICATION CANNOT BE COMPLETED

Business where all of the required information cannot be obtained will be declined. Exceptions will only be permitted on the decision of the respective Business Head, who will determine whether there are genuine reasons for the information or documentation not being available. In cases where there are no valid explanations for the absence of the information or documentation, the circumstances must be reported as a possible suspicion.

In the event that funds are being held on behalf of the prospective customer, the written approval of the respective Business Head must be obtained before funds are returned to the customer. In these circumstances, funds must never be paid away to a 3<sup>rd</sup> party.

#### **4.6.1 CIRCUMSTANCES FOR DECLINING NEW ACCOUNTS**

New relationship that do not appear to be legitimate including those where the applicant does not supply essential documentation as required in accordance with section 4.5 or proof of identity and address must be declined.

### **4.7 CUSTOMER IDENTIFICATION FOR NON ACCOUNT HOLDERS (WALK-IN-CUSTOMERS)**

#### **4.7.1 CASH REMITTANCES / PAYMENTS**

Cash remittances for non account holders present a high risk for the Bank and increase the Bank's vulnerability to money laundering. The additional measures listed below have therefore been introduced to mitigate those risks.

##### **4.7.1.1 OUTWARD REMITTANCES**

- a) Whenever there is any doubt in respect of the documentation, reference must be made to the Branch Manager or Operations Manager before acceptance of the transaction. Copies of the documentary evidence are to be retained with the remittance advice. Further, the Funds Transfer Form (SF-100) should be attached with the photocopy of CNIC and the bank staff must make the notation '**Original Seen**' with signatures on photocopy of CNIC.

The Branch Manager must authorise any cash remittance of **Rs. 500,000** or above; obtain Walk-in-Customer Information Form duly filled-in by the customer and make notation on the remittance form and sign the form to confirm that all of the procedures and evidence is satisfactory.

##### **4.7.1.2 INWARD REMITTANCES (FOR NON-ACCOUNT HOLDERS)**

- a) Cash payment (irrespective of amount) to non-account holders will require proper evidence of identity by showing original CNIC and the bank staff must make the notation '**Original Seen**' with signatures on photocopy of CNIC.

## 4.8 CUSTOMER IDENTIFICATION - SPECIAL CIRCUMSTANCES

### 4.8.1 3<sup>RD</sup> PARTY MANDATE HOLDER(S)

An account holder may choose to grant a mandate to 3<sup>rd</sup> party (another person individual or corporate) to operate an account on behalf of customer for the purpose mentioned in KYC form at the time of start of relationship. It is necessary to establish / verify the relationship between account holder and the mandate holder(s) along with the reasons for the mandate. The identity of the mandate holder(s) should be verified and the 3<sup>rd</sup> Party Mandate Form (SF-67) along with Authority Letter (AL) / Written Request should be signed and placed in the Customer File.

Any change in the address of the account holder(s) / 3<sup>rd</sup> Party Mandate Holder(s) must be notified to the bank directly by the account holder(s).

Where a Power of Attorney (POA) exists, the original POA must be seen and copied by the branch for the file. A 3<sup>rd</sup> Party Mandate must also be completed with complete supporting documents as mentioned above.

**Attorney's Profile must be maintained on following lines:**

#### RELATIONSHIP DETAILS.

Date POA accepted By the branch.	A/C No of Principal.	Title of account.	Date of account Opened.	Purpose of Account	Mandate Holder's relationship with Principal.

#### POA Details.

CNIC NO	Address.(If differs from CNIC get evidence of Present address)	PEP		Any Relationship with PEP.
		YES	NO	

Resident/Non Resident.	If Non Resident, Country of Residence.
NATIONALITY.	
OCCUPATION.	JOB TITLE.

EXISTING RELATIONSHIP WITH THE BANK, IF SO, ACCOUNT NO WITH BRANCH NAME.	DETAILS OF OTHER BANKING RELATIONSHIP.(Other than MCB)

#### **4.9 MAINTAINING RECORD FOR THE ACCOUNTS OPENED AND CLOSED**

Branches will keep a record of all accounts opened and closed. AOF and record of accounts opened and closed must be retained for a minimum period of 5 years after the relationship has ended.

#### **4.10 KNOWING THE CUSTOMER'S BUSINESS**

It is not sufficient only to identify the customer, it is also necessary to understand the customer's business and the use of the account or other banking services.

Knowing the customer obviously includes knowing who the customer is and where he / she lives or conduct their business, but KYC is also about what the customer does, his/her/their financial circumstances and how the account will be used.

#### **For all account holders' information is required on:**

- a) The purpose of the account
- b) The customer's occupation profession and source(s) of income. (At times, it could be difficult for the bank to verify individual's source of income. Under such circumstances, the branch manager or account opening officer will satisfy himself / herself when interviewing customer at the time of account opening about his / her income. However, for corporate and commercial customers source of income will be determined from their financials).
- c) **The turn-over thresholds as per relevant KYC form must be asked from the customer and this information should be populated in the banking core system.**
- d) Other bank accounts, credit cards, etc held by the customer.

*Unemployed customers* or other customers whose income can not be ascertained must state whether they have any other source of income.

*Customers in business* should clearly state the nature of their business or profession, e.g. “importers and dealers in watches” or “accountant in private practice”. Similarly, customers in employment should state their position and the employer’s name and address. Vague words or phrases (e.g. “in business” or “in service”), should not be used.

*Directors of Private Companies* must confirm whether they are the principal shareholders and, if not, the beneficial owners of the company must be identified. KYC information is needed to establish a pattern of expected activity by clearly mentioning the thresholds and can assist the Bank:

**No account should be opened until a satisfactory understanding of the customer’s Profile / business has been obtained and documented on the Know Your Customer Form.**

#### **4.11 CUSTOMER ACCEPTANCE**

Customer Acceptance: involves understanding the following minimum criteria on which the acceptance must be based upon:

- a) The type of customer (individual, company, bank, public or high profile position, linked account, business activities, etc).
- b) The type of account (individual, sole-proprietorship, business, trust, NGO, NPO, PEP. etc).
- c) Sources of income / legitimate source of funds.
- d) The country of origin / incorporation, etc.

#### **4.12 POLITICALLY EXPOSED PERSON (PEP)**

What is PEP?

PEP stands for politically Exposed Person. Business relationships with individuals holding important public positions and with persons or companies clearly related to them may expose a bank to significant reputational and / or legal risks. Such politically exposed person (“PEPs”) are individuals who are/or have been entrusted with prominent public functions, including heads of state or of government , senior politicians, senior government, judicial or military officials, senior executives of publicly owned corporations and important political party officials. Senior personnel from judiciary, executive, armed forces, administration etc should be reviewed with respect to the possibility of being PEP Branch / controlling office investigate the source of funds before accepting a PEP.

**“Politically Exposed Person”** also means a person who holds or has ever held one of the following offices or positions in or on behalf of state:

- a. head of state or head of government;
- b. member of the executive council of government or member of legislature;
- c. deputy minister or equivalent rank;
- d. Ambassador or attaché or counsellors of an ambassador;
- e. military officer with a rank of a Brigadier or above;
- f. President of a state-owned company or a state-owned bank;
- g. Head of government agency;
- h. Judge; (all categories of judges e.g. Civil Court (Magistrates of all classes), Additional District Judge (ADJ), District Judge (DJ), High Court Judges, Supreme Court Judges). Also Tribunals, Anti - Corruption Service Tribunals, Environmental Committee Judges.
- i. leader or president of a politically party represented in a legislature; or
- j. Holder of any prescribed office or position.” The definition also includes any prescribed family member of such a person.

PEP will continue to be identified as PEP even though the individual no longer holds the position which basically means that once PEP, always PEP.

The decision to open an account for PEP should be escalated to a senior level (GM). Government official of grade 20 and above must be reviewed against their possibility of being PEP. Prudence should also be exercised for government officials ranking below grade 20, having influential public positions. For Sri Lanka equivalent grades should be considered in this regard.

#### PROCEDURE FOR OPENING BANK ACCOUNT OF Politically Exposed Persons (PEP)

“As per Compliance Policy approved by BOD our objective is to identify, assess, monitor and control compliance risks across the bank. In terms of CDD/KYC/AML Procedures Handbook, GMs are presently empowered to take business decision on PEP accounts after obtaining consent from Compliance Group. In line with the management’s vision to make MCB a most Compliant Bank and focusing on compliance as our responsibility, there is a dire need to determine and mitigate the risks on a timely manner through effective systems and efficient controls. HotScan (Name-Filtering Solution) implemented by IBM has been deployed and is working effectively. Additionally the AML Solution namely MANTAS is also finalized and is in the implementation phase.

Politically Exposed Person (PEP) accounts possess **HIGH RISK** as they are high profile, constitute political influence and holders of important public / controlling positions. Enhanced due diligence is to be carried out while dealing with PEPs for establishing business relationship or transactions. Further, monitoring of sources of wealth / funds and beneficial owners has also to be done on regular basis for appropriate risk management.

In order to further establish the present monitoring system for PEP accounts it is suggested that all the cases falling under this category should be referred to CCG for name filtering, prudence and authentication. After having clearance from CCG, the decision to open an account for PEP is to be taken at the General Manager / Controlling Office level. The gist of proposed changes in the procedure for opening of PEP accounts are as under:-“

**Procedure**

The field will forward the requests for opening of PEP accounts through their respective General Managers to CCG. Proper due diligence will be carried out by CCG and respective GM will be informed accordingly. They will then take business decision at their end.

4.

Transactions conducted through correspondent relationships can present an additional risk for all banks unless sufficient know your customer procedures have been undertaken by the remitting bank on the underlying client and the origin of the funds. Consequently to comply with new regulatory guidance, additional measures will be required to ensure that we “know our correspondent banks”.

**The accounts of correspondents should only be opened once clearance is obtained from the Compliance Group who will consider the following factors:**

- 1- Information about the correspondent bank’s management
- 2- Major business activities and where they are located
- 3- Money-laundering prevention and detection efforts
- 4- Purpose of the account
- 5- The condition of bank regulation and supervision in the respondent’s country
- 6- The identity of any third party that will use the correspondent banking services (i.e. in case of payable through accounts). The Payment chain needs to be established from meaningful originator to the actual beneficiary

MCB would only establish correspondent relationships with foreign banks that are effectively supervised by the relevant authorities. For their part, respondent banks should have effective customer acceptance and KYC/ CDD policies.

MCB should refuse to enter into or continue a correspondent banking relationship with a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group (i.e. shell banks). MCB would pay particular attention when continuing relationships with respondent banks located in jurisdictions that have poor KYC Standards.

**Further, the reviews of the correspondents / Money Service Businesses (MSBs) and their accounts are to be carried out at regular intervals through Compliance Group.**

Particular attention should be paid when continuing relationship with Correspondent Banks located in jurisdictions that have poor KYC standards or have been identified by Financial Action Task Force (FATF) as being non co-operative. The purpose will be to ascertain whether the correspondent bank is itself regulated for Anti money laundering. In such circumstances, the banks / DFIs must satisfy themselves that the correspondent bank has verified the identity of and performed on-going due diligence on the customers having direct access to accounts of the correspondent bank / DFI and that it is able to provide relevant customer identification data upon request to the correspondent bank / DFI (PR M4, Section 5)

The volume and nature of transactions flowing through correspondent accounts with banks that do not have equivalent anti-money laundering procedures will need to be monitored against expected levels and destinations. Any material variances or unusual circumstances (whether isolated transactions or trends) will be subject to additional enquiries.

The Bank will consider terminating the accounts of correspondents who fail to provide satisfactory answers to such enquiries including, where appropriate, confirming the identity of customers featuring in unusual or suspicious circumstances.

Approval should be obtained from senior management, preferably at the level of Executive Vice President or equivalent, before establishing new correspondent banking relationships

**4.14 NEW REQUIREMENT FOR SWIFT MT 103**

A new requirement for the purpose of prevention, investigation, and detection of money laundering and terrorist financing new regulation requires that all international payments/funds transferred through SWIFT MT103 (Single Customer Credit Transfer) must now need to include the following:

<b>1- Sender's / Payer's</b>
(a) <b>Full Name</b>
(b) <b>Account Number or unique ID</b> (Passport No. or CNIC No. for Walk-in-Customers)
(c) <b>Full Address</b> (i.e. street/city, etc)
<b>2- Beneficiary's Details</b>
<b>3- Purpose of Remittance</b>

These should be clearly mentioned in specific SWIFT message fields as per SWIFT standards.

**4.15 COMBATING THE TERRORIST FINANCING**

**What is Terrorist Financing?**

United Nations 1999 International Convention for the Suppression of the Financing of Terrorism explains terrorist financing in the following way: "Any person commits an offence within the meaning of this Convention if that person by any means, directly or indirectly, unlawfully and wilfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out:

Any act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act."

The Convention also indicates that a person still commits an offence even if:

- the funds are not used to carry out an offence in (a) and (b) above;
- a person attempts to commit an offence as described above;
- a person participates as an accomplice in an offence as above; and
- a person organizes or directs others to commit an offence as above, or contributes to the commission of one or more offences as above by a group of persons acting with a common purpose, where the contribution is intentional and is made with the aim of furthering the criminal activity or criminal purpose of the group, where such activity involves the commission of an offence as above, or is made in the knowledge of the intention of the group to commit an offence as above

**Terrorists use techniques like those of money launderers to evade authorities' attention and to protect the identity of their sponsors and of the ultimate beneficiaries of the funds.**

However, financial transactions associated with terrorist financing tend to be in smaller amounts than is the case with money laundering, and when terrorists raise funds from legitimate sources, the detection and tracking of these funds becomes more difficult.

To move their funds, terrorists use the formal banking system, informal value-transfer systems, Hawalas and Hundis and, the oldest method of asset-transfer, the physical transportation of cash, gold and other valuables through smuggling routes.

### **Terrorist Activities**

The FATF has published a paper called Guidelines for Financial Institutions in Detecting Terrorist Financing; this could be downloaded from [www.fatf-gafi.org](http://www.fatf-gafi.org). All staff members are strongly encouraged to read a copy of this paper to be fully familiar with the nature of terrorist financing and some of the indicators which should raise concerns about whether a transaction is suspicious or not in order to prevent terrorist financing.

### **Terrorist Financing Legislation in Pakistan**

The following laws have been promulgated in Pakistan:

Anti Terrorism Act 1997

Anti Terrorism (Amendment) Ordinance 2001

Apart from reviewing suspicious transactions over accounts, it is also fundamentally important for Branch Managers in general and Operation Managers in particular to watch out all remittances taking place through on-line or through international means, i.e. SWIFT. The SDN list must be checked to ensure both remitters and beneficiary's names are not included in the list.

In case remitter or beneficiary's name is found on the list, STR must be generated immediately. For outward remittance, in case beneficiary's name is on SDN list, transaction must be stopped and respective RH / GM should be advised for their instructions.



## **5 REVIEWING AND MONITORING CUSTOMER ACCOUNTS**

### **5.1 THE NEED FOR VIGILANCE, MONITORING OF RECENTLY OPENED ACCOUNTS**

The foundation of any monitoring procedure lies in the initial collection of identification and “know your customer” information and the ongoing updating of that information. Updating arises from regular contact with the customer and the results of regular monitoring procedures.

The nature of the business that a customer expects to conduct must be ascertained when the account is opened and regularly updated. This will enable management and staff to judge whether the customer’s transactions are in line with expectations or whether unusual transactions give cause for concern and possible suspicion that criminal money be involved.

The initial period (at least 6 months) of any new customer relationship presents the greatest vulnerability and therefore warrants additional monitoring procedures. Once the initial period is over, ongoing routine monitoring covering all transactions becomes the norm.

Accounts that have been opened within the previous six months should be closely monitored:

- a) To establish a normal pattern of activity.
- b) To ensure that the activity is in line with the customer's expected profile on account opening.
- c) To ensure that the verified identification information remains unchanged, e.g. no early notifications of change of address or account signatories.
- d) To check and review the source of funds.
- e) To ensure that there are no unexplained large transactions.

### **5.2 UPDATING KNOWLEDGE OF THE CUSTOMER**

All managers and staff must recognise the need to keep up to date the Bank’s knowledge of the customers through Customer Due Diligence (CDD) / Enhanced Due Diligence (EDD) while updating KYC forms at specified intervals with particular reference to:

- a) Documenting the customer's banking habits and patterns of transactions through KYC.
- b) Documenting events or changes that are considered important for a sound knowledge of customers and their activities.
- c) Noting customers with particularly large sums being credited/debited to/from their accounts if their transactions amounts exceed the threshold values declared by them on KYC form.
- d) Providing immediate access to customers' KYC information to the CCG and Head of Compliance North / South; and
- e) Ensuring that the true beneficial owner and source of all funds is known to the Bank.
- f) A file note must be completed by recording every meeting and telephone conversation with the customer and filed in the customer file.

Accounts where there is little personal contact with the customer should be subject to review on a regular basis as per CDD or EDD rules set out in KYC form/ with assigned ratings of Normal or High Risks respectively. Also to ensure that any change of address or changes in circumstances that have been notified are recorded in the shape of fresh KYC form taken from the customer as well as populated in the system. Particular attention should be paid to any new sources of income or unexpected use of the account.

If at any time any member of staff believes that the level and nature of activity in an account is not consistent with the known business or profession of the customer, or if the transactions otherwise appear to be unusual or suspicious, a report should be made to the CCG and Head of Compliance North / South in accordance with the procedure laid down on Page 9 (last para) and in Section 8.

### **5.3 HALF YEARLY CERTIFICATION FOR CDD / EDD - REVIEW OF ACCOUNTS**

All Branch Managers are responsible for monitoring the activity in their customers' accounts in accordance with their knowledge of the customer's business and the expected activity as per their declared Turnover on KYC Form. **Managers should certify on half-yearly basis that they have undertaken CDD / EDD of all customers as per the frequencies set for Normal Risk (3 years) and High Risk (1 year) in KYC form.** During the review, Managers should check that all transactions are in line with expected activity and that new information has been recorded. Attention should be paid to any new sources of income or unexpected use of the account. A file note confirming the date of the review should be placed on the respective accounts KYC Forms [See 9.6]

## **5.4 DORMANT ACCOUNTS**

Dormant and inactive (including inoperative and unclaimed) accounts need to be monitored to respond to any transaction which because of the 'dormant' nature of the account, is unexpected or unusual and warrants particular review or approval.

Branches must adhere with Sections I.05.01, I.05.02, I.05.03 & I.10.07 of Branch Operations Manual (Version 1.0, December 31, 2007; also available on MCB Intranet Portal) on Dormant and Unclaimed Accounts. In case where the operation of dormant account is activated, branch manager must ensure that account holder has fulfilled all KYC requirements and the transaction in question is in line with the information provided previously.

Further the dormancy can only be activated from the parent branch where the account is being maintained or from any other branch with the consent of the parent branch through email, where account is being maintained. (Circular No POK/COD/GEN/2010-34 dated February 18, 2010).

For customers whose accounts are dormant and an attested copy of account holder's Computerized National Identity Card (CNIC) is not available in Bank's record, Bank shall not allow operation in such accounts until the account holder produces an attested copy of his / her CNIC and fulfil all other formalities for activation of the account.

## **5.5 TRANSACTION MONITORING**

The most important safeguard against money laundering is the ability to detect suspicious transactions and to take further action to prevent recurrence of such transactions. A number of monitoring procedures have therefore been introduced for cash and non cash transactions for account and non account holders based on CDD / EDD and thresholds defined accordingly. These procedures are set out below:

### **5.5.1 MONITORING TRANSACTIONS FOR ACCOUNT HOLDERS - NON CASH REMITTANCES & TRANSACTIONS**

Wire transfer remittances are a high-risk area warranting special attention. Although most wire transfers involve legitimate business transactions, the speed and anonymity they afford have made the system attractive to drug traffickers and money launderers who can swiftly move their money from bank to bank and country to country, and thus, conceal their source and ownership.

Information on the purpose, identity of the originator and the ultimate beneficiary must be available for all foreign remittances. Further enquiries should be made if these details are not included in inward remittances to ascertain whether there is a reportable suspicion.

### **5.5.2 MONITORING TRANSACTIONS FOR ACCOUNT HOLDERS - CASH REMITTANCES & TRANSACTIONS**

Cash transactions leave the Bank particularly vulnerable because of the bearer nature and universal acceptability of currency notes and the fact that there is little or no audit trail. Special care is required in handling cash transactions of large amounts. The KYC procedure should identify customers who use cash as an integral part of their business, e.g. retail outlets, grocery stores, or restaurants. For such customers, the normal cash amount and frequency of cash deposits withdrawals should be established and accordingly KYC and system parameters be updated.

The basic principle to be followed is that the size and frequency of cash transactions should have relevance to the nature and size of the customer's business and portion of sales generated on a cash basis. Further examples of what constitute suspicious transactions appear in Section 7 should be estimated on the basis of discussions with the customer and the monitoring of account transactions.

Currency Transaction Report (CTR) are required to be submitted to FMU but this is deferred until National Executive Committee (NEC) ratifies and describes the threshold value. Format is attached in the Annexure Section 9.2 for future reference.

### **5.5.3 MONITORING TRANSACTIONS - CASH REMITTANCES FOR NON ACCOUNT HOLDERS**

Non account holders can only deal with the Bank provided CDD. KYC is carried out and attested copy of CNIC by branch manager is obtained from the non account holder if the amount is up to Rs.500, 000. For amounts exceeding this threshold requires obtaining the filled-in Walk-in-Customer Information Form (WICIF) in addition to original CNIC's attested copy and must be kept with the vouchers.

In the case of requests for multiple cash remittance transactions by the same non-account holder, enquiries should be made to assess whether there are reasons to suspect criminal activity. Any suspicions should be reported promptly by following procedure given under section 4.2.4.

In cases where source of funds has not been verified satisfactorily e.g. because the remitter claims that the funds represent cash savings over a number of years, any subsequent transactions for that customer should be the subject of further enquiries.

In general terms, staff should not hesitate to withhold their services to non account holders who do not provide proper identification, give evasive answers to simple questions, or otherwise arouse suspicion of involvement in questionable activities or if the staff are not satisfied with the transaction.

## 5.6 THRESHOLD LIMITS

All transactions across accounts, above the following specified financial thresholds, will be reviewed and signed off in line with CDD / KYC information retrospectively by the respective branch managers. System generated reports will be produced for accounts with a debit or credit transactions or turnover above the following threshold limits:

<b>High Value Transactions Limit</b>	<b>Rs. 1,000,000 and above</b>
--------------------------------------	--------------------------------

**Personal and Business Accounts:** Thresholds will be input into the system as per the account holder's profile. For Sole Traders / Partnership accounts branch managers will decide the expected debit and credit turnover in the account after a thorough interview with the prospective customer, and in case of personal accounts, individual's monthly income / salary will be referred to decide on input as threshold limits in the system.

**Corporate Accounts & All Other Accounts:** In line with the financials or expected turnovers in corporate accounts, Branch Managers / Regional Manager will decide the respective parameters to be used as threshold limits for accounts falling into this category.

The above limit has been put in place to monitor the accounts' activities and by no means suggest that any transaction exceeding the limits will constitute a "Suspicious Transaction". Branch managers should use their judgment when they review such transactions and must refer to their respective RH / GMs or Business Heads when in doubt.

## 5.7 EXCEPTION REPORTS

### 5.7.1 INCOME / SALARY / TURNOVER EXCEPTIONS REPORT

This will show all the accounts where income / salary or Dr / Cr Turnover exceed the financial profile set in the account. This report will be basic tool for monitoring KYC. The parameters will be updated as and when the KYC is updated as per the CDD / EDD criteria of the Bank.

### 5.7.2 HIGH VALUE TRANSACTIONS REPORT

In order to monitor the exceptions, the above report is generated by Knowledge Manager Team (KM) and forwarded to respective branches on very next day; which will be a vital tool for monitoring customer transactions:

This report will include the high value transaction for Rs. 1,000,000 and above.

**It will be the responsibility of the Branch Manager** to review these reports and take actions where necessary and update KYC profile of customer as per CDD / EDD procedures as well as make notation on the above mentioned reports as to what action has been taken. These reports will be checked / audited by the respective compliance officer during the visit of the branch.

## **5.8 CUSTOMER LOANS AND ADVANCES**

### **5.8.1 GRANTING OF ADVANCE**

All lines of credit must have appropriate approval. It is the responsibility of Credit Administration Division to monitor the drawdown and settlement of customer loans and other facilities. If any of the following concerns are identified, they should be referred to the Head of Compliance North / South for his review:

- a) The legitimacy of the customer during the ‘normal due diligence’ procedure is in doubt.
- b) The use of loan is unusual for the customers’ business.
- c) The origin of the assets being offered for security is unclear.

### **5.8.2 SETTLEMENT OF THE ADVANCE**

The following situations must be referred to Credit Administration Division for review:

- a) any settlement out-of-line with the original agreement, e.g. early settlement;
- b) any unexpected settlement of an overdue position;
- c) Any settlement from a previously unknown and apparently unrelated source/account.
- d) Any suspicion of Money Laundering must be reported to the CCG with copy to the Head of Compliance North / South.

### **5.8.3 MONITORING THE ADVANCE**

On a day-to-day basis, any unusual transactions should be immediately obvious. The transaction monitoring reports should highlight any exceptional lodgements or fluctuations which should be referred to Head of Compliance North / South.

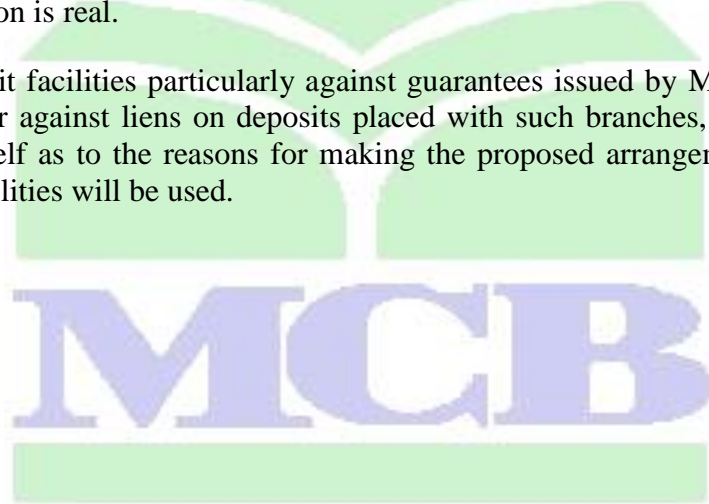
## **5.9 LETTERS OF CREDIT AND OTHER CONTINGENCIES**

Management and staff should be aware that other credit facilities, e.g. Documentary Credits, Guarantees and Indemnities may be used to launder the proceeds of crime. Funds may be surreptitiously moved by careful manipulation of such facilities and the use of such facilities should be reviewed from time to time.

Special scrutiny must be done to facilities being requested by customers who may be borrowing from, or who have apparently considerable funds in other institutions.

Letters of Credit may be used to move money around the world under the guise of international trade, but without any physical movement of goods. They may also be used to help disguise shipments of drugs or shipments of money in containers (purporting to be shipments of some legitimate commodity/machinery). Routine due diligence at the issue and confirmation stages is therefore vital. It is also necessary to carry out sufficient enquiries to be comfortable that the underlying transaction is real.

When granting credit facilities particularly against guarantees issued by MCB branches located in other countries or against liens on deposits placed with such branches, the Branch Manager should satisfy himself as to the reasons for making the proposed arrangement, the purpose for which the credit facilities will be used.



## **6 RECORD KEEPING**

### **6.1 DOCUMENT RETENTION**

Records are to be retained to provide an audit trail for all funds and adequate evidence for the law enforcement agencies in their investigations;

The minimum retention periods to comply with SBP Anti Money Laundering Regulations are:

- a) Account opening records and documentary evidence of identity - at least 5 years after the account is closed.
- b) Account ledger records - at least 5 years.
- c) Individual transaction records - at least 5 years.
- d) Records of suspicious reports received and reported to FMU at SBP will be kept by the bank indefinitely, till the bank gets permission from SBP to destroy such records. (PR3, Section 3)

#### **HOWEVER**

If it is known that a Police or tax investigation is under way, all records relating to the account and customer under investigation must be retained until Police / Tax Authorities advise otherwise. The Branch Manager is responsible for managing such situations for the Branch.

Transaction documents must be capable of distinguishing between the transactions relating to different customers and of identifying where the transaction took place and in what form.

### **6.2 RETRIEVAL OF DOCUMENTS**

Subject to the minimum retention periods specified under section 6.1 above, documents that are required under court order must be capable of being retrieved and produced **within 7 calendar days** of the date when the order was served. However if Branch Manager thinks that the required documents will not be able to retrieve within 7 days, he/ she will immediately advise Head of Compliance North / South to request for extension in producing these documents.

## **7 RECOGNISING SUSPICION OF MONEY LAUNDERING**

### **7.1 WHAT IS SUSPICION?**

As the types of transactions that may be used by a money launderer are almost unlimited, it is difficult to define a suspicious transaction. Suspicion is personal and subjective and falls far short of proof based on firm evidence. However, the suspicion must at least have some foundation and not just be based on mere speculation.

A suspicious transaction will often be:

- a) Any transaction where the amount, duration or other specific feature is inconsistent with the customer's professional or business activities, standard of living or normal movements on the account.
- b) A transaction that is not logical from an economic, financial or banking point of view.
- c) Activities involving high-risk customers, accounts or countries.

The key to recognising suspicion is based on having enough knowledge about a customer's normal expected transactions and financial circumstances to be able to recognise the unusual, what might be suspicious. For example, a customer who is unemployed or working in a junior position but is making frequent large cash deposits may be involved in money laundering frauds.

### **7.2 EXAMPLES OF SUSPICIOUS TRANSACTIONS QUOTED BY SBP**

The following are examples of potential suspicious transactions for both money laundering and terrorist financing. The lists of situations given below are intended mainly as a means of highlighting the basic ways in which money may be laundered. Although these lists are not all-inclusive, they may help financial institutions and NFBPs recognize possible money laundering and terrorist financing schemes.

While each individual situation may not be sufficient to suggest that money laundering or a criminal activity is taking place, a combination of such situations may be indicative of such transactions. A customer's declarations regarding the

background of such transactions should be checked for plausibility. Not every explanation offered by the customer can be accepted without additional scrutiny. Closer scrutiny should help to determine whether the activity is suspicious or one for which there does not appear to be a reasonable business or legal purpose.

It is justifiable to suspect any customer who is reluctant to provide normal information and documents required routinely by the financial institutions in the course of the business relationship. Financial Institutions should pay attention to customers who provide minimal, false or misleading information or, when applying to open an account, provide information that is difficult or expensive to verify.

### **7.2.1 TRANSACTIONS WHICH DO NOT MAKE ECONOMIC SENSE**

- (1) A customer-relationship that does not appear to make economic sense, for example, a customer having a large number of accounts with the same financial institution, frequently transfers money between different accounts or exaggeratedly high liquidity.
- (2) Transactions in which assets are withdrawn immediately after being deposited, unless the customer's business activities furnish a genuine reason for immediate withdrawal.
- (3) Transactions that cannot be reconciled with the usual activities of the customer, for example, the use of Letter of Credit and other methods of trade finance to move money between countries where such trade is not consistent with the customer's usual business.
- (4) Transactions which, without genuine reason, result in the intensive use of what was previously a relatively inactive account, such as customer's account which shows virtually no normal personal or business related activities but is used to receive or disburse unusually large sums which have no obvious purpose or relationship to the customer and / or his business.
- (5) Provision of bank guarantees or indemnities as collateral for loans between 3<sup>rd</sup> parties that are not in conformity with market conditions.
- (6) Unexpected payment of an overdue credit without any proper explanation.
- (7) Back-to-bank loans without any identifiable and legally admissible purpose.

### **7.2.2 TRANSACTIONS INCONSISTENT WITH THE CUSTOMER'S BUSINESS**

- (1) The currency transactions patterns of a business show a sudden change inconsistent with normal activities.
- (2) A large volume of cashier's cheques, money orders, or funds transfers is deposited into, or purchased through, an account when the nature of the account holder's business would not appear to justify such activity.
- (3) A retail business has dramatically different patterns of currency deposits of similar businesses in the same general location.
- (4) Unusual transfers of funds occur among related accounts or among accounts that involve the same or related principals.
- (5) Goods or services purchased by the business do not match the customer's stated line of business.

### **7.2.3 TRANSACTIONS INVOLVING LARGE AMOUNTS OF CASH**

- (1) Exchanging an unusually large amount of small – denominated notes for those of higher denomination.
- (2) Purchasing or selling of foreign currencies in substantial amounts by cash settlement despite the customer having an account with the financial institution.
- (3) Frequent withdrawal of large amounts in cash by means of cheques, including traveller's cheques.
- (4) Frequent withdrawal of large cash amounts that do not appear to be justified by the customer's business activity.
- (5) Large cash withdrawals from a previously dormant / inactive account, or from an account which has just received an unexpected large credit from abroad.
- (6) Company transactions, both deposits and withdrawal, that were denominated by unusually large amounts of cash, rather than by way of debits and credits associated with the normal commercial operations of the company, e.g. Cheques, letters of credit, bills of exchange, etc.

- (7) Depositing cash by means of numerous credit slips by a customer such that the amount of each deposit is not substantial, but the total of which is substantial.
- (8) The deposit of unusually large amounts of cash by a customer to cover requests for bankers' drafts, money transfers or other negotiable and readily marketable money instruments.
- (9) Customers whose deposits contain counterfeit notes or forged instruments.
- (10) Customers making large and frequent cash deposits but cheques drawn on the accounts are mostly to individuals and firms not normally associated with their business.
- (11) Customers who together, and simultaneously, use separate tellers to conduct large cash transactions or foreign exchange transactions.
- (12) The size and frequency of currency deposits increases rapidly with no corresponding increase in non-currency deposits.

#### **7.2.4 TRANSACTIONS INVOLVING STRUCTURING TO AVOID REPORTING OR IDENTIFICATION REQUIREMENT**

Structuring transactions are conducted to evade reporting and identification requirements. A person structures transactions by breaking down a single currency sum exceeding the specified threshold into smaller amounts that may be conducted as a series of transactions at or less than specified amount. Money launderers and criminals have developed many ways to structure large amounts of currency to evade the reporting and identification requirements. Unless currency smuggled out of country or commingled with the deposits of an otherwise legitimate business, any money laundering scheme that begins with a need to convert the currency proceeds of criminal activity into more legitimate-looking forms of financial instruments, accounts or investments, will likely involve some form of structuring. Financial institutions' employees should be aware of and alert to the following structuring schemes, namely:-

- (a) A customer makes currency deposit or withdrawal transactions, so that each is less than the CTR filling threshold.
- (b) a customer uses currency to purchase official bank cheques, money orders, or traveller's cheques with currency – in amounts less than the specified amount to avoid having to produce identification in the process;
- (c) deposits are structured through multiple branches of the same financial institution or by groups of people who enter a single branch at the same time; or
- (d) A person customarily uses the automated teller machine to make several deposits below a specified threshold.

In addition, structuring may occur before a customer brings the funds to a financial institution. In these instances, a financial institution may be able to identify the aftermath of structuring. Deposits of money instruments that may have been purchased elsewhere might be structured to evade the reporting and record keeping requirements. These instruments are often numbered sequentially in groups totalling less than the specified amount; bear the same handwriting (for the most part) and often the same small mark, stamp, or initials, or appear to have been purchased at numerous places on the same or different days.

#### **7.2.5 TRANSACTIONS INVOLVING ACCOUNTS**

- (1) Matching of payments out with credit paid in by cash on the same or previous day.
- (2) Paying in large 3<sup>rd</sup> party cheques endorsed in favour of the customer.
- (3) Substantial increases in deposits of cash or negotiable instruments by a professional firm or company, using client accounts or in-house company or trust accounts, especially, if the deposits are promptly transferred between other client company and trust accounts.
- (4) High velocity of funds through an account, *i.e.* low beginning and ending daily balances, which do not reflect the large volume of funds flowing through an account.
- (5) An account opened operated in the name of an exchange company that receives structured deposits.

- (6) An account operated in the name of an off shore company with structured movement of funds.

#### **7.2.6 TRANSACTIONS INVOLVING TRANSFERS TO AND FROM ABROAD**

- (1) Transfer of money abroad by an interim customer in the absence of any legitimate reason. An interim customer is one who is not a regular customer of the financial institution in question, or does not maintain an account, deposit account, safe deposit box, etc.
- (2) A customer which appears to have accounts with several financial intuitions in the same locality, especially when the financial institution is aware of a regular consolidated process from such accounts prior to a request for onward transmission of the funds elsewhere.
- (3) Requested transfers of large amounts of money abroad accompanied by the instruction to pay the beneficiary in cash.
- (4) Large and regular payments that cannot be clearly identified as bona fide transactions, from and to countries associated with (i) the production, processing or marketing of narcotics or other illegal drugs or (ii) criminal conduct.
- (5) Substantial increase in cash deposits by a customer without apparent cause, especially if such deposits are subsequently transferred within a short period out of the account and/or to a destination not normally associated with the customer.
- (6) Building up large balances, not consistent with the known turnover of the customer's business, and subsequent transfer to account (s) held overseas.
- (7) Cash payments remitted to a signal account by a large number of different persons without an adequate explanation.
- (8) Funds transfer activity occurs to or from a financial secrecy haven without an apparent business reason or when the activity is inconsistent with the customer's business or history.
- (9) Many small, incoming transfers of funds are received, or deposits are made using cheques and money orders. Almost immediately, all or most

of the transfers or deposits are wired to another city or country in a manner inconsistent with the customer's business or history.

- (10) Incoming funds transfers with limited content and lack of remitter's information.
- (11) Unusually large number and variety of beneficiaries are receiving funds transfers from one company.

### **7.2.7 INVESTMENT RELATED TRANSACTIONS**

- (1) Purchasing of securities to be held by the financial institution in safe custody, where this does not appear appropriate given the customer's apparent standing.
- (2) Requests by a customer for investment management services where the source of funds is unclear or not consistent with the customer's apparent standing.
- (3) Larger or unusual settlements of securities transactions in cash form.
- (4) Buying and selling of a security with no discernible purpose or in circumstances which appear unusual.

### **7.2.8 TRANSACTIONS INVOLVING UNIDENTIFIED PARTIES**

- (1) Provision of collateral by way of pledge or guarantee without any discernible plausible reason by 3<sup>rd</sup> parties unknown to the financial institution and who have no identifiable close relationship with the customers.
- (2) Transfer of money to another financial institution without indication of the beneficiary.
- (3) Payment orders with inaccurate information concerning the person placing the orders.
- (4) Use of (false name) pseudonyms or numbered accounts for affecting commercial transactions by enterprises active in trade and industry.

- (5) Holding in trust of shares in an unlisted company whose activities cannot be ascertained by the financial institution.
- (6) Customers who wish to maintain a number of trustee or clients account that does not appear consistent with their type of business, including transitions that involve nominee names.



### **7.2.9 TRANSITIONS INVOLVING INSURANCE**

- (1) A customer purchases products with termination features without concern for the product's investment performance.
- (2) A customer purchases insurance products using a single, large premium payment, particularly when payment is made through unusual methods such as currency or currency equivalents.
- (3) A customer purchases product that appears outside the customer's normal range of financial wealth or estate planning needs.
- (4) A customer borrows against the cash surrender value of permanent life insurance policies, particularly when payments are made to apparently unrelated 3<sup>rd</sup> parties.
- (5) Policies are purchased that allow for the transfer of beneficial ownership interests without the knowledge and consent of the insurance issuer. This would include second hand endowment and bearer insurance policies.
- (6) A customer is known to purchase several insurance products and uses the proceeds from an early policy surrender to purchase other financial assets.

### **7.2.10 TRANSACTIONS INVOLVING EMBASSY AND FOREIGN CONSULATE ACCOUNTS**

- (1) Official embassy business is conducted through personal accounts
- (2) Account activity is not consistent with the purpose of the account, such as pouch activity or payable upon proper identification transitions.
- (3) Accounts are funded through substantial currency transitions.
- (4) Accounts directly fund personal expenses of foreign national without appropriate controls, including, but not limited to, expenses for college students.

### **7.2.11 MISCELLANEOUS TRANSACTIONS**

- (1) Purchase or sale of large amounts of precious metals by an interim customer.
- (2) Purchase of bank cheques on a large scale by an interim customer.
- (3) Extensive or an increased use of safe deposit facilities that do not appear to be justified by the customer's personal or business activities.
- (4) Safe deposit boxes are used by individuals who do not reside or work in the institution's service area despite the availability of such services at an institution closer to them;
- (5) Unusual traffic patterns in the safe deposit box area or unusual use of safe custody accounts. For example, more individuals may enter more frequently, or carry bags or other containers that could conceal large amounts of currency, monetary instruments, or small valuable items.
- (6) A customer rents multiple safe deposit boxes to park large amounts of currency, monetary instruments, or high-value assets awaiting conversion to currency, for placement into the financial system. Similarly, a customer establishes multiple safe custody accounts to park large amounts of securities awaiting sale and conversion into currency, monetary instruments, outgoing funds transfers, or a combination thereof, for placement into the financial system.
- (7) Loans are made for, or are paid on behalf of, a 3<sup>rd</sup> party with no reasonable explanation.
- (8) To secure a loan, the customer purchases a certificate of deposit using an unknown source of funds, particularly when funds are provided via currency or multiple monetary instruments.
- (9) A customer purchases a number of open-end stored value cards for large amounts. Purchases of stored value cards are not commensurate with normal business activities.
- (10) Suspicious movements of funds occur from one financial institution to another, and then funds are moved back to the first financial institution.
- (11) Purchase of real estate on price higher than the determinable value.
- (12) A series of purchases of real estate within relatively short span of time.

### **7.2.12 POTENTIAL INDICATORS OF MONEY LAUNDERING/TERRORIST FINANCING**

The following examples of potentially suspicious activity that may involve money laundering or terrorist financing threat, are primarily based on guidance note provided by the Financial Action Force (FATF) in the name of “Guidance for Financial Institutions in Detecting Terrorist Financing” FATF is an intergovernmental body whose purpose is the development and promotion of polices, both national and international levels, to combat money laundering and terrorist financing in the world.

**(a) Activity Inconsistent with Customers Business:**

- I. Funds are generated by business owned by individuals of the same origin or involvement of multiple individuals of the same origin from high-risk countries (e.g. non-cooperative countries and territories identified by international authorities such as FATF)
- II. The stated occupation of the customer does not commensurate with the type or level of activity.
- III. Persons involved in currency transactions share an address or phone number, particularly when the address is also a business location or does not seem to correspond to the stated occupation ( e.g. student , unemployed, or self employed);
- IV. In nonprofit or charitable organization , financial transactions occur for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organization and the other parties in the transaction; and
- V. A safe deposit box opened on behalf of commercial entity when the business activity of the customer is unknown or such activity does appear to justify the use of safe box deposit box.

**(b) Funds Transfer:**

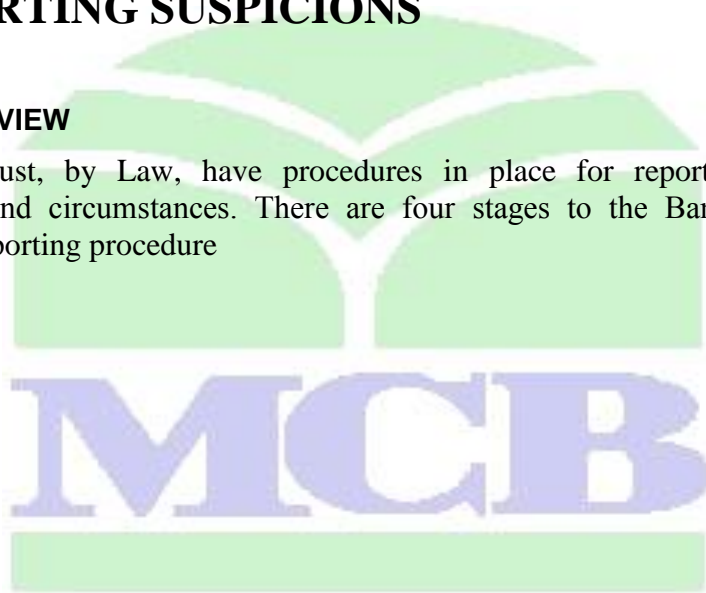
- I. Large number of incoming outgoing funds transfer take place through business account and there appear to be no logical or other economic purpose for the transfer, particularly when this activity involve high risk locations;
  - II. Fund transfers are ordered in small amounts in an apparent effort to avoid triggering identification or reporting requirements.
  - III. Funds transfer do not include information on the originator, or the person on whose behalf the transaction is conducted, when the inclusion of such information would be expected;
  - IV. Multiple personal and business accounts or the accounts of non profit organizations or charities are used to collect and funnel funds to a small number of foreign beneficiaries; and
  - V. Foreign exchange transactions are performed on behalf of customer by a 3<sup>rd</sup> party, followed by funds transfers to locations having no apparent business connection with the customer or to high risk countries.
- (c) **Other Transactions that Appear Unusual or Suspicious:**
- I. Transactions involving foreign currency exchange are followed; within a short time by funds transfer to high risk locations;
  - II. Multiple accounts are used to collect and funnel funds to a small number of foreign beneficiaries, both persons and business, particularly in high risk locations;
  - III. A customer obtains a credit instrument on engages in commercial financial transaction involving the movement of funds to or from the high-risk locations when there appear to be no logical business reasons for dealing with those locations;

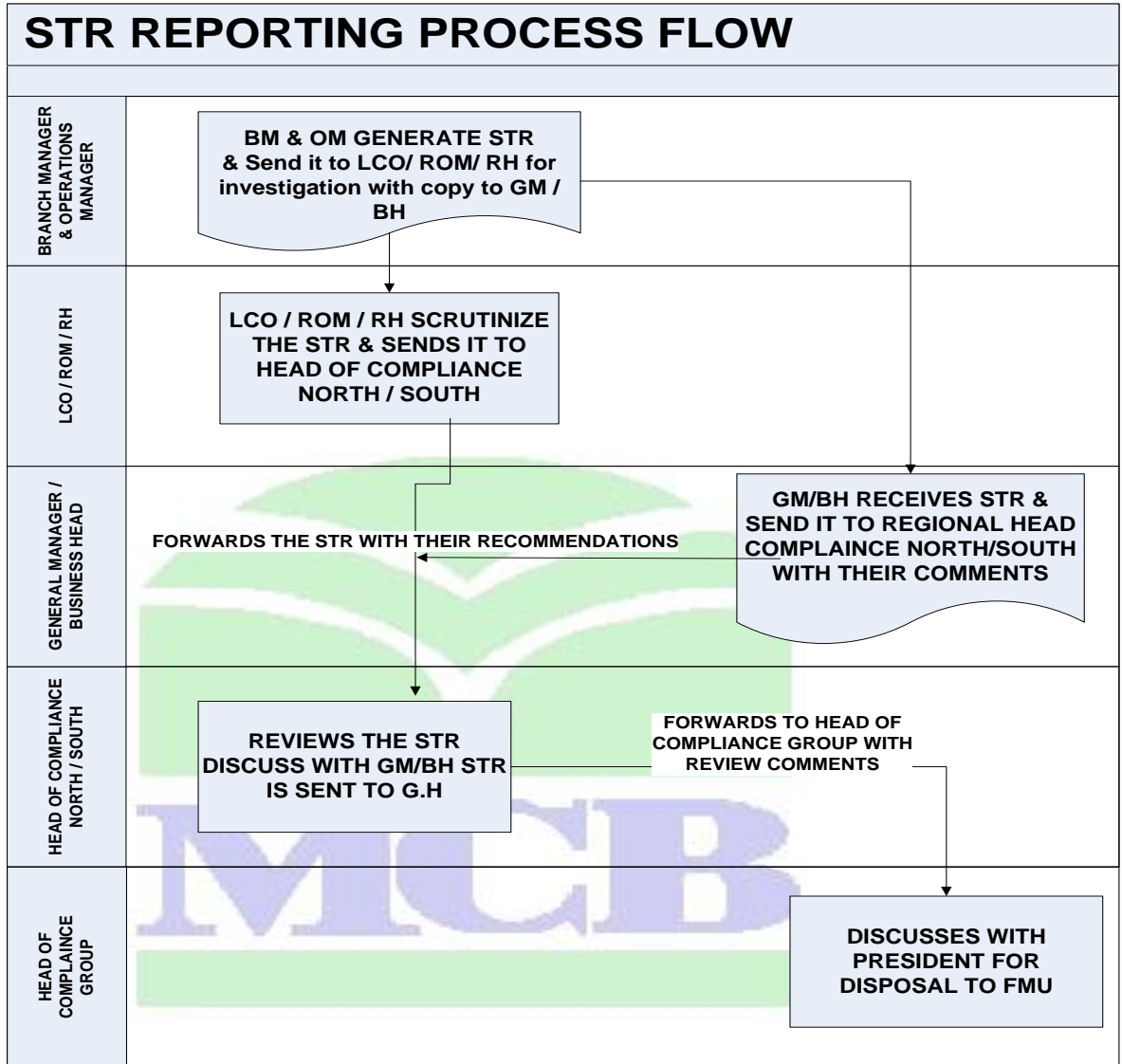
- IV. The opening of Accounts of Financial Institutions from locations of specific concern (High Risk Locations)
- V. Funds are sent or received via international transfer from or to high risk locations; and
- VI. Insurance policy loans or policy surrender values that are subject to substantial surrender charge.

## **8 REPORTING SUSPICIONS**

### **8.1 OVERVIEW**

The Bank must, by Law, have procedures in place for reporting suspicious transactions and circumstances. There are four stages to the Bank's suspicious transaction reporting procedure





The above process flow represents procedure described in Section 4.2.4 (Reporting of Suspicious Transactions / circumstances).

Head of Compliance Group will discuss the matter with the President and accordingly raise it with Financial Monitoring Unit (FMU). If the suspicion is not established and STR is not to be raised, the Internal Suspicious Report Form will remain on file within the Bank and the initiator branch will be advised accordingly. The name of the individual member of staff who made the report will not be revealed.

Once a report has been made in line with these procedures, all personal legal obligations have been met. All reports submitted to FMU are treated in the strictest confidence. The customer is never informed and whoever do so would be subject to a criminal offence.

## **8.2 REPORTING PROCEDURES FOR STAFF AND MANAGEMENT**

Staff with any suspicion must report immediately on the Suspicious Transaction Report Form a copy of which is set out in Section 9.1.

It is important that the reason for the suspicion is explained fully. It is of critical importance that such suspicions must not be discussed with anyone outside the Bank. Care must be taken in discussing a suspicion, even with other colleagues, and if this is considered not to be appropriate, then discussion must only be held with CCG or Head of Compliance North / South.

**It is vital that no mention of such suspicion is made to the customer. Any discussion of this nature would risk a “tipping-off” offence being committed, if the customer becomes aware that a report had been submitted.**

All staff must note that once the reporting process has commenced, it must be followed through and completed, even if the original suspicion might appear to have been resolved.

This procedure must be followed and repeated every time there is an unusual transaction, even if the bank has already notified FMU of previous unusual transactions relating to that customer/account.

All reports will be retained by the Head of Compliance North / South for reference purposes whether or not the transaction is reported to FMU.

MCB will not hesitate to report STR to Financial Monitoring Unit, because by failing to make a report, we will commit an offence as per AML Ordinance 2007. Branch managers will give top priority to queries raised by Head of Compliance North / South regarding any account which is under suspicion, as the delays could cause serious problems.

## **8.3 ACTIONS AFTER REPORTING**

When the investigators need to use the information from the Bank, they will contact the Bank with an appropriate Court Order and it is this information that may be used

in Court. It is possible that FMU or an investigator might approach the Bank for additional explanation of the initial report, or for other information. No member of management or staff should provide any explanation or information and the enquirer must be referred to the Compliance Group.

## **9 SPECIMEN FORMS / LISTS**

- 9.1 SUSPICIOUS TRANSACTION REPORT (STR) FORM<sup>1</sup>
- 9.2 CURRENCY TRANSACTIONS REPORT (CTR) FORM<sup>2</sup>
- 9.3 KYC FORM (INDIVIDUALS IN PAKISTAN), FAQs AND RISK RATING SHEET<sup>3</sup>
- 9.4 KYC FORM (BUSINESS / LEGAL ENTITIES), FAQs AND RISK RATING SHEET<sup>3</sup>
- 9.5 KYC FORM (INDIVIDUALS IN SRI LANKA), FAQs AND RISK RATING SHEET<sup>3</sup>
- 9.6 HALF-YEARLY REVIEW OF CERTIFICATION FOR CDD / EDD  
REVIEW OF ACCOUNTS
- 9.7 LIST OF FATF MEMBER COUNTRIES

- 
- 1. FORMAT OF STR IS AVAILABLE ON MCB INTRANET PORTAL
  - 2. CURRENCY TRANSACTION REPORT (CTR) IS REQUIRED TO BE SUBMITTED TO FMU BUT THIS IS DEFERRED UNTIL NATIONAL EXECUTIVE COMMITTEE (NEC) RATIFIES AND DESCRIBES THE THRESHOLD VALUE

3. KYC FORMS FOR CORPORATE / BUSINESS & LEGAL ENTITIES FOR PAKISTAN AND SRI LANKA WILL BE PROVIDED LATER ON ONCE THEY ARE APPROVED BY THE MANAGEMENT

### 9.1 SUSPICIOUS TRANSACTION REPORT (STR) FORM

20. ( Part II ) THE GAZETTE OF PAKISTAN EXTRA , JANUARY 6 ,2009										
SUSPICIOUS TRANSACTION REPORT										
[ See Regulation 4 ( 2 ) ]										
(Check appropriate box)										
1 )	Date	09-04-2009		( dd/mm/yyyy )						
2 )	<input checked="" type="checkbox"/>	Initial Report	<input type="checkbox"/>	Corrected Report	<input type="checkbox"/>	Supplemental Report				
<b>Part I Reporting Financial Institution System</b>										
3 )	Name of Institution	MCB BANK LIMITED								
4 )	NIFT Code	0062								
5 )	Address of Financial Institution	Compliance Group , MCB TOWER , 10 <sup>TH</sup> Level I.I. Chundrigar Road , Karachi								
6 )	Name of Branch where transaction activity occurred									
7 )	Branch Code									
8 )	Address of Branch									
9 )	Primary Regulator	<input checked="" type="checkbox"/>	SBP	<input type="checkbox"/>	SECP	Other ( Please Specify )				
<b>Reporting Officer</b>										
10 )	Name									
11 )	Designation									
12 )	Phone Number(s) ( Include area code )						13 )	Fax Number(s) ( Include area code )		
14 )	Email Address						15 )	Cell Number (s)		
<b>Contact for Assistance ( if different from Reporting Officer )</b>										
16 )	Name									
17 )	Designation									
18 )	Phone Number(s) ( Include area code )						19 )	Fax Number(s) ( Include area code )		
20 )	Email Address						21 )	Cell Number (s)		

Part II	Suspect Information									
22)	Name									
23)	Father / Husband's Name									
24)	Address ( permanent )									
25)	Address ( present )									
26)	Other Known Address									
27)	Phone Number(s) Residence ( Include area code )									
28)	Phone Number(s) Office ( Include area code )									
29)	Fax Number ( s )									
30)	Cell Number ( s )									
31)	CNIC Number									
32)	NIC Number ( In case CNIC Number is not available )									
33)	Any other Identification Number									
34)	National Tax Number (NTN) if available									
35)	Date of Birth								( dd/mm/yyyy )	
36)	Nationality									
37)	Occupation / Type of Business									
38)	Relationship with Financial Institution									
	<input checked="" type="checkbox"/>	A/C Holder	<input type="checkbox"/>	Employee	<input type="checkbox"/>	Agent	<input type="checkbox"/>	Walk In Customer		
	Other Please Specify									
39)	Business relation with Suspect ( if any )									
40)	Is relationship still maintained with person ?							Yes		Not
41)	In case No. Mention date of termination of relationship									( dd/mm/yyyy )
42)	Capacity in which the person is performing the transactions/acts									
	<input type="checkbox"/>	Individual	<input type="checkbox"/>	Company	<input type="checkbox"/>	Agent	<input type="checkbox"/>	Broker		
	Other Please Specify									
43)	Identities of other persons known to be involved in reported activity									

<b>Part III</b>	<b>Suspicious Transaction Information</b>										
44)	Date of Suspicious Transaction								( dd/mm/yyyy)		
45)	Amount involved ( Please Specify Currency )										
46)	<b>Suspicious Transactions :</b>										
	Date		Amount			Description of Transaction					
47)	<b>Brief Narrative ( Reasons for Suspicion )</b>										
	( Include Suspicious activity information, explanation/description and background details )										
48)	<b>Characterization of Suspicious Transaction i.e. Nature of Suspected predicate Schedule Offence</b>										
49)	<b>Has the transaction already been reported to any law Enforcement Agency? If so list the agency</b>										
	a										
	b										
	c										
	d										


Part IV		Account Information						
50)	Account number (s) effected , if any							
	a)		b)		c)		d)	
51)	Account Opened on dd/mm/yyyy							
	a)		b)		c)		d)	
52)	Current Status of the Account(s)							
	a)		b)		c)		d)	
53)	Purpose of the Account(s)							
	a)						b)	
54)	Average Monthly Turnover of the Account(s)							
	a)		b)		c)		d)	
55)	Aggregate Credits/Debits for Last 3 Years							
	a)		b)		c)		d)	
56)	Peak Balance(s) of last 3 years							
	a)		b)		c)		d)	
57)	Nature of Account(s)							
		Individual		Partnership		Company		Trust
		Other Please Specify						
58)	Transaction Mean / Method							
		Cash		Cheque		Remittance		Pay Order
		Credit Card		Debit Card		Deposit		Fixed Deposit
		Draft		Transfer		LC		Online Transfer
59)	Copies of Following Documents are attached							
		Customer Identification documents/ Accounts Opening Form						
		KYC /CDD of customer or Suspect						
		Other Documents obtained at the time of Opening Account/Relationship						
	Related Documents Supporting the STR.							
60)	Other Relevant information ( Information linked to STR or action taken by the reporting entity.							
							Seal & Signature of Reporting Officer	

## 9.2 CURRENCY TRANSACTION REPORT (CTR) FORM

<b>Annexure - II</b>	
[See Regulation 5]	
<b>Currency Transaction Report</b>	
(Under Section 7 of the Anti Money Laundering Ordinance 2007)	
(Check appropriate box)	
1) Date	_____ / _____ / _____ dd/mm/yyyy
2)	<input type="checkbox"/> Initial Report <input type="checkbox"/> Corrected Report <input type="checkbox"/> Supplemental Report
<b>Part I</b>	Person(s) Involved in Transaction(s)
<b>Section A-</b>	Person(s) on Whose Behalf Transaction(s) Is Conducted
3)	Name _____
4)	Father / Husband's name _____
5)	Address (permanent) _____
6)	Address (present) _____
7)	Other Known Address _____
8)	Phone Number - Residence (include area code) _____
9)	Phone Number - Office (include area code) _____
10)	Fax Number _____
11)	Cell Number _____
12)	CNIC Number _____
13)	NIC Number (in case CNIC number is not available) _____
14)	Any other Identification Number _____
15)	National Tax Number (NTN), If available _____
16)	Date of Birth: _____ / _____ / _____ dd/mm/yyyy
17)	Nationality _____
18)	Occupation / Type of Business _____
19)	Relationship with Financial Institution <input type="checkbox"/> Customer <input type="checkbox"/> Employee <input type="checkbox"/> Agent <input type="checkbox"/> Walk in Customer <input type="checkbox"/> Other (Please specify) _____
20)	Business Relation with Suspect (if any) _____
<b>Section B-</b>	Individuals Conducting Transaction(s) (if other than above)
21)	Name _____
22)	Father / Husband's name _____
23)	Address (permanent) _____
24)	Address (present) _____
25)	Contact Numbers (include area code) _____
26)	CNIC Number _____
27)	Any other Identification Number _____



### 9.3 KYC FORM (INDIVIDUALS IN PAKISTAN), FAQs AND RISK RATING SHEET

 <span style="float: right;">CONFIDENTIAL</span>			
<b>KNOW YOUR CUSTOMER (KYC) FORM</b> (For Individual Clients)			
<b>Branch</b>	<b>Name</b>		<b>Account Number/s:</b>
	<b>Code</b>		<b>Date Account/s Opened:</b>
<b>ACCOUNT TITLE</b>			
<b>1-ACCOUNT TYPE</b>	Saving Account <input type="checkbox"/> Current Account <input type="checkbox"/> Collection A/c <input type="checkbox"/> BBA <input type="checkbox"/> KBA <input type="checkbox"/> CBG Product Account <input type="checkbox"/> Bancassurance Account <input type="checkbox"/> Others (please specify) _____		
<b>2-ACCOUNT STATUS</b>		<b>3-ACCOUNT NATURE</b>	
<b>Resident</b> <input type="checkbox"/> <input type="checkbox"/> Pakistani <input type="checkbox"/> Foreigner Country of Citizenship _____ <b>Non - Resident</b> <input type="checkbox"/> <input type="checkbox"/> Pakistani Country of Residence _____ <input type="checkbox"/> Foreigner Country of Residence _____ Country of Citizenship _____		<b>Individual</b> <input type="checkbox"/> <b>Joint</b> <input type="checkbox"/> Nature of Relation Family Business Other <small>(In case of joint a/c KYC Form of each client will be filled separately)</small>	
<b>4-Politically Exposed Person (PEP)</b> Yes <input type="checkbox"/> No <input type="checkbox"/>			
Politician <input type="checkbox"/> Judiciary <input type="checkbox"/> Armed Forces <input type="checkbox"/> Executives (Govt) <input type="checkbox"/> Administration (Local/Municipal etc) <input type="checkbox"/> Journalist <input type="checkbox"/> Others (Please specify) _____			
<b>5-PERSONAL INFORMATION</b>			
CNIC/ PASSPORT # _____		Issued Date _____	Verification (Dated) <input type="checkbox"/> _____
Expiry Date / Validity _____		Issued By _____	
Permanent Address (as per CNIC) _____			
Present Address(as per CNIC) _____			
Mention Address (permanenet/current) if different from as given in CNIC _____			
Signature if vary from as given in CNIC <input type="checkbox"/> NO <input type="checkbox"/> YES (If yes then undertaking/file-note to be obtained)			
Telephone (Res) _____		Telephone (Off) _____	Mobile Number _____
Email _____		Fax Number _____	
Occupation: Govt. Service <input type="checkbox"/> Private Service <input type="checkbox"/> Self Employed <input type="checkbox"/> Agriculture <input type="checkbox"/> Student <input type="checkbox"/> House Wife <input type="checkbox"/> (For House Wife, the source of funds should be identified) Others (specify) _____			
Name & Address of Employer _____		Source of funds/Nature of Business/Industry _____	
Monthly Salary/Income _____		Education Level _____	
<b>6-PURPOSE OF ACCOUNT</b>			
Receipts and Payments <input type="checkbox"/> Savings and Investments <input type="checkbox"/> Others (Specify) _____			
<b>7-BANKING HISTORY</b>			
Name of Bank/s _____		Relationship since _____	
Ever Refused Banking Facility by any Bank/Financial Institution? YES <input type="checkbox"/> NO <input type="checkbox"/>			
Does the client appear in known suspected terrorist list/s or any other alert list? (In case of YES, account should not be opened) YES <input type="checkbox"/> NO <input type="checkbox"/>			

8-BUSINESS INFORMATION										
Name of Business _____										
Place and Date of Incorporation/Formation: _____										
Related concerns _____										
Nature of Business (e.g. Jeweler, Electronics, Textile etc) _____										
Type of Business:	Wholesale/Supplies	<input type="checkbox"/>	Retailing	<input type="checkbox"/>	Trading	<input type="checkbox"/>	Manufacturing	<input type="checkbox"/>		
	Import/Export	<input type="checkbox"/>	Other ( please specify) _____							
Commodities/Products Sold: _____										
Commodities/Products Purchased: _____										
Years in current business: _____										
Total Assets during the last year (To include Fixed Assests/Stocks/Receiveables/Cash in hand etc)	Year	Amount (Rs.)		Gross Profit during the last year	Year	Amount (Rs.)				
Note any significant expected or recent (<12 months) changes in product mix or business activities (i-e. opened new selling location in recent year etc.) _____										
Description of Business Operations: Including size of business & number of employees: _____										
Names and Locations of Major Suppliers: _____										
Names and Locations of Major Customers: _____										
Please indicate the nature of activity to be undertaken with the bank:										
Payment to Suppliers/Vendors	<input type="checkbox"/>	Payment from/to Customers	<input type="checkbox"/>	Payroll Payments	<input type="checkbox"/>	Inter-Company Payments	<input type="checkbox"/>	Others (specify) _____		
9-OTHER SOURCES OF WEALTH/FUNDS										
Specify other sources & amount of Income _____										
10-TRANSACTION PROFILE										
Expected Aggregate Daily Turnover (in the account)	Debit	Average		Maximum		Credit	Average		Maximum	
Expected Monthly Turnover										
11-Volume (on daily basis)	Cash	Transfer / Clearing	Foreign Remittances		Trade Products		RTCs			
Upto Rs 100,000	<input type="checkbox"/>	<input type="checkbox"/>	Originating Countries		Letters of Credit	<input type="checkbox"/>	Facility required? Yes <input type="checkbox"/>			
Rs 100,001 to Rs 250,000	<input type="checkbox"/>	<input type="checkbox"/>			Foreign Bill Purchased	<input type="checkbox"/>				
Rs 250,001 to Rs 500,000	<input type="checkbox"/>	<input type="checkbox"/>	Destination Countries		Bank Guarantees	<input type="checkbox"/>	No <input type="checkbox"/>			
Rs 500,001 to Rs 1 million	<input type="checkbox"/>	<input type="checkbox"/>			Others (specify)	<input type="checkbox"/>				
Rs 1 million to Rs 10 million	<input type="checkbox"/>	<input type="checkbox"/>								
Over and above Rs 10 million	<input type="checkbox"/>	<input type="checkbox"/>								
12-OVERALL LEVEL OF RISK			Normal Risk (NR) <input type="checkbox"/>		High Risk (HR) <input type="checkbox"/>					
THIS KYC FORM IS REVIEWED BY:		NAME	ASSESSMENT				SIGNATURES/ Date			
Account Opening Officer										
Branch Manager (Having verified/authenticated all the necessary documents for KYC)										

## KYC RISK RATING SHEET (INDIVIDUALS IN PAKISTAN)

SR.	RISK FACTOR	HIGH RISK (HR)	NORMAL RISK (NR)	RISK RATING
1	<b>Citizenship Status</b>	(1) <i>Non-resident foreigner</i> (2) <i>Resident foreigner</i> (3) Citizen of country of concern/high risk area	Pakistani Citizen and/or not a resident of high risk area within Pakistan	
2	<b>Geographical Address</b>	(1) Non-Local address the credentials of which could not be ascertained or linked to tax/corruption haven. (2) Present Address in the CNIC varies from the present address provided in the form. (3) Local address within Pakistan with area of concern where the account activity needs to be observed with regard to likely suspicious/terrorist activity	Local/non-local address within our normal market / bankable areas	
3	<b>Occupation</b>			
	<b>Service</b>	(1) Employed nationally/internationally with high risk businesses/firms	Employed / Retired from Banking industry are not considered high risk	
	<b>Business</b>	(2) Business falls in any of the high risk category as defined in the <i>FAQ Sheet</i>	Businesses other than the high risk category as defined in the <i>FAQ Sheet</i>	
4	<b>Politically Exposed Person</b>	(3) Politically Exposed Person (or prominent public figure / person as defined in attached <i>FAQ Sheet</i> )		
5	<b>Length of Relationship/ Banking History</b>		Existing banking customer with relationship is greater than 1 year No prior relationship with any bank Existing banking customer with relationship is less than 1 year	
6	<b>Transaction Profile</b>			
	<b>Cash/Clearing / Transfer</b>	Rs 1 million and above (Aggregate Daily)	Less than Rs 1 million	
	<b>Transaction Profile - Foreign Remittances</b>	Rs 1 million and above (Aggregate Daily)	Less than Rs 1 million	

	<b>Transaction Profile - Rupee</b> <i>Travellers</i> <i>Cheques</i>	More than Rs 100,000/- (Aggregate Daily)	Less than Rs 100,000	
--	---	--	----------------------	--

**Note:** If any of the above risk factors is rated as high, client/s' risk rating will be categorized in the High Risk Category in the section of *Overall Level of Risk* in KYC Form.

In case of any material change in the clients' profile; the same should be promptly noted in the ongoing review section of the KYC Form. This means, the branch manager shall not wait for the next review but shall immediately change the risk category accordingly.



## FREQUENTLY ASKED QUESTIONS

### 1-What is PEP?

PEP stands for Politically Exposed Person. Business relationships with individuals holding important public positions and with persons or companies clearly related to them may expose a bank to significant reputational and/or legal risks. Such politically exposed persons (“PEPs”) are individuals who are/or have been entrusted with prominent public functions, including heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of publicly owned corporations and important political party officials. Senior personnel from judiciary, executive, armed forces, administration etc should be reviewed with respect to the possibility of being PEP

The definition of PEP also includes entity for which PEP is a beneficial owner of an entity if the PEP exercises actual or effective control over the entity. Entities that are 20% or more owned by PEP are defined as PEP. Wherever we have knowledge that PEP owns less than 20% of an entity but still exercises effective control, or if we know that an entity has been formed for the benefit of PEP, that entity must also be defined as PEP.

PEP will continue to be identified as PEP even though the individual no longer holds the position which basically means that once PEP, always PEP.

Branch/controlling office should investigate the source of funds before accepting a PEP. The decision to open an account for PEP should be taken at a senior level (GM). Government officials of grade 20 and above

must be reviewed against their possibility of being PEP. Prudence should also be exercised for government officials ranking below grade 20, having influential public positions.

**Politically exposed person or PEP or in other words Senior Public Figure** is a term that describes a person who has been entrusted with a prominent public function, or is closely related to such a person. By virtue of this position and the influence it holds, PEPs present a higher risk for potential involvement in bribery and corruption.

The process of screening for PEPs is usually performed at the beginning of account opening, called enhanced due diligence, and screening of accounts periodically is performed as part of ongoing due diligence. Since September 11, 2001, more than 100 countries have changed their laws related to financial services regulation, with the fight against political corruption playing a foundational role.

Although there is no global definition of PEP, most countries based their definition on the Financial Action Task Force (FATF) definition:

- current or former senior official in the executive, legislative, administrative, military, or judicial branch of a foreign government (elected or not)
- a senior official of a major foreign political party
- a senior executive of a foreign government-owned commercial enterprise, being a corporation,

business or other entity formed by or for the benefit of any such individual

- an immediate family member of such individual; meaning spouse, parents, siblings, children, and spouse's parents or siblings
- Any individual publicly known (or actually known by the relevant financial institution) to be a close personal or professional associate.

The definition is not intended to cover middle ranking or more junior individuals in the foregoing categories.

Canadian PEFP definition is:

"Politically exposed foreign person - means a person who holds or has ever held one of the following offices or positions in or on behalf of a foreign state:

- (a) head of state or head of government;
- (b) member of the executive council of government or member of a legislature;
- (c) deputy minister or equivalent rank;
- (d) ambassador or attaché or counselors of an ambassador;
- (e) military officer with a rank of a Brigadier or above;
- (f) president of a state-owned company or a state-owned bank;
- (g) head of a government agency;
- (h) judge;
- (i) leader or president of a political party represented in a legislature; or
- (j) holder of any prescribed office or position."

The definition includes any prescribed family member of such a person.

**Close Associates** means Agent / Representative, Business Associate, Senior Employee, Adviser (including, but not limited to financial, political, and legal)

**Immediate family Members** means Husband, Wife, Partner, Mother, Father, Brother, Sister, Son, Daughter, Son-in-law, Daughter-in-law, Father-in-law, Brother-in-law, Step relative listed above e.g. step-Son, Step-Mother, etc.

### **2-Why KYC is necessary?**

To determine the **true identity** of the beneficial owner(s), the real party in interest, controlling person or entity of the accounts (M-1)

### **3-Is KYC one time exercise?**

No. KYC would be an ongoing exercise for prudent banking practices. With each material change in the profile of client, KYC needs to be reviewed in the light of changed scenario.

### **4-What are Due Diligence (DD) and Enhanced Due Diligence (EDD) of a customer?**

For each customer bank is required to undertake the normal due diligence process. And where the level of risk from the customer to the bank is high, staff will be *legally required* to perform the enhanced due diligence as required under the Prudential Regulations (M1-5), other instructions of State Bank of Pakistan and Anti-Money Laundering Ordinance 2007 (AML Regulations 2008, AML Rules 2008). Failing the implementation of these requirements will be source of concern for the bank.

**5-Which are the major countries that are of concern with respect to AML?**

Afghanistan, Nigeria, Iran, Iraq, Syria, Myanmar (Burma), North Korea, Sudan, Zimbabwe, Cuba, Ivory Cost, Congo, Belarus, British Virgin Islands, Israel, India, Turkmenistan, Uzbekistan, Sao Tomi & Principe should be placed in the high risk countries.

**6-Ever refused banking facility?**

If the customer has been refused banking facility, by any banking company, staff should take extra care in handling the transactions on behalf of such accounts.

**7 -Which are high risk businesses?**

Following business should be dealt with extra care while continuing business relationship with the entrepreneurs:

1. Precious Metals/Stones
2. Arms Dealers
3. Jewellers
4. Artefacts/Antiques/ Art Dealers
5. Real estate Company
6. Religious organizations and trusts.
7. NGOs/ Non Profit Organization (NPOs) /Charities, societies with cross border donations.
8. Concerns/Associations closely related with Politically exposed persons (PEPs)
9. All accounts of Exchange Companies & /Franchisees of Exchange Companies.
10. International correspondent bank
11. Unregulated Hedge fund
12. Un-regulated law firm or accounting company
13. Travel agent
14. Leather goods stores (prohibited items)
15. Import/export companies
16. Casinos

17. Offshore corporations and banks located in tax/banking havens

18. Scrap dealers

19. Other cash-intensive businesses

**8- Assessment of account opening and authorizing officer/executive.**

Assessment must be based on the available material information about the client. For this matter, sound judgment and good understanding of businesses would be appreciated to establish true-identity of the existing and prospective clients.

**09-One view of the Client**


A client of the bank can have multiple accounts in the bank with different branches, so the transactions in all of his accounts should be reviewed to assess the clients' profile.

*For further clarification contact:*

AML Division

Compliance Group, MCB Tower, 10<sup>th</sup> Level, Karachi, Ph. 021-2270121

### 9.4 KYC FORM (BUSINESS / LEGAL ENTITIES), RISK RATING SHEET

 <span style="float: right; border: 1px solid black; padding: 2px;">CONFIDENTIAL</span>						
<b>KNOW YOUR CUSTOMER (KYC) FORM</b> (For Business/Legal Entities)						
<b>Branch</b>	Name			Account Number/s:		
	Code			Date Account/s Opened:		
<b>ACCOUNT TITLE</b>						
<b>ACCOUNT TYPE</b>	Current Account	<input type="checkbox"/>	Collection Account	<input type="checkbox"/>	Others (Pls specify) _____	
<b>ACCOUNT NATURE</b>						
Sole-proprietorship		Registered/Unregistered	<input type="checkbox"/>	Partnership	<input type="checkbox"/>	
Private Ltd Co			<input type="checkbox"/>	Registered	<input type="checkbox"/>	
Government Body			<input type="checkbox"/>	Unregistered	<input type="checkbox"/>	
Others (NGOs/ TruStOs/ Societies/Clubs/NPOs etc)			<input type="checkbox"/>	Listed	<input type="checkbox"/>	
			<input type="checkbox"/>	Unlisted	<input type="checkbox"/>	
			<input type="checkbox"/>	Exchange Company	<input type="checkbox"/>	
			<input type="checkbox"/>	Financial Institution	<input type="checkbox"/>	
			<input type="checkbox"/>	AML Program (Copy to be obtained)		
			<input type="checkbox"/>	Compliance Policy & Procedures (Obtain Copy)		
			<input type="checkbox"/>	<input type="checkbox"/>		
<b>BUSINESS INFORMATION</b>						
Business Address			Registration No. _____			
_____			Registering Authority _____			
_____			Licensing Authority _____			
_____			Country of incorporation _____			
Place & Date of Incorporation/Formation:			<b>Authority to Operate A/c granted to:</b>			
Related/sister concerns			1- _____			
Nature of Business (e.g. Jeweler, Electronics, Textile etc)			2- _____			
_____			3- _____			
_____			4- _____			
<b>Type of Business:</b>	Wholesale/Supplies	<input type="checkbox"/>	Retailing	<input type="checkbox"/>	Trading	<input type="checkbox"/>
	Import/Export	<input type="checkbox"/>	Services	<input type="checkbox"/>	Manufacturing	<input type="checkbox"/>
Other ( please specify) _____						
Commodities/Products Sold (Pls specify): _____						
Commodities/Products Purchased (Pls specify): _____						
Years in current business: _____						
National Tax Number (NTN) _____						
Total Assets during the last year (To include Fixed Assets/Stocks/Receiveables/Cash in hand etc)		Year	Amount (Rs.)	Gross Profit during the last year	Year	Amount (Rs.)
Attach copy of Financial Statements						
Description of Business Operations: _____						
Names and Locations of Major Suppliers (Pls specify): _____						
Names and Locations of Major Customers/Buyers (Pls specify): _____						
Please indicate the nature of activity to be undertaken with the bank:						
Payment to Suppliers/Vendors		<input type="checkbox"/>	Payment from/to Customers	<input type="checkbox"/>	Payroll Payments	<input type="checkbox"/>
		<input type="checkbox"/>		<input type="checkbox"/>	Inter-Company Payments	<input type="checkbox"/>
		<input type="checkbox"/>		<input type="checkbox"/>	Others (specify)	_____
<b>Concern closely related to Politically Exposed Person (PEP)</b> Yes <input type="checkbox"/> No <input type="checkbox"/>						
<b>Shareholders (PARTNERS/DIRECTORS/TRUSTEES)</b>						
Particulars	Name & Father Name	Citizenship Status	CNIC/Passport No Issued By, Issue Date & Valid Till	Address Permanent Present Mailing	Share-holding (Percentage)	Beneficial Owners/Controlling Interest with ultimate effective control over the legal person or arrangement
<small>(For all directors holding more than 20 % share, separate KYC Form of each such director should be got filled) (Attach additional sheet in case of need)</small>						
Does any of the owner appear in known suspected terrorist list/s or any other alert list? (In case of YES, account should not be opened)						YES <input type="checkbox"/> NO <input type="checkbox"/>

TRANSACTION PROFILE						
		Average		Maximum		
Debit						Credit
Expected Daily Turnover						Average
Expected Monthly Turnover						Maximum
Volume (on daily basis)	Cash	Transfer / Clearing	Foreign Remittances		Trade Products	
Upto Rs 100,000			Originating Countries		Letters of Credit	
Rs 100,001 to Rs 250,000					Foreign Bill Purchased	
Rs 250,001 to Rs 500,000			Destination Countries		Bank Guarantees	
Rs 500,001 to Rs 1 million					Others (specify)	
Rs 1 million to Rs 10 million						
Over and above Rs 10 million						
OVERALL LEVEL OF RISK		Normal Risk (NR)		High Risk (HR)		
THIS KYC FORM IS REVIEWED BY:		NAME	ASSESSMENT			SIGNATURES/ Date
Account Opening Officer						
Branch Manager (Having verified/authenticated all the necessary documents for KYC)						
ONGOING REVIEW OF KYC FORM				Account Title		
				Account Number/s		
(FOR HIGH RISK CUSTOMERS ONCE IN A YEAR AND FOR NORMAL RISK CUSTOMERS ONCE IN TWO YEARS)						
PERIOD	HIGH RISK		NORMAL RISK			SIGNATURES/ REVIEW DATE



### KYC RISK RATING SHEET (Business/Legal Entities)

SR.	RISK FACTOR	HIGH RISK (HR)	NORMAL RISK (NR)	RISK RATING
1	<b>Citizenship Status of Owners</b>	<ul style="list-style-type: none"> <li>• Citizen of a country of concern/high-risk/tax haven/with weak AML regime and not sufficiently following FATF recommendations</li> <li>• Non resident Customer</li> <li>• Foreigner</li> </ul>	Resident Pakistani	
2	<b>Geographical Address of the business concern</b>	i) Business Address the credentials of which could partially be ascertained j) Possibility of linked to tax/corruption haven k) Temporary address provided	Address within our normal market / bankable areas	
3	<b>Ownership Structure/Effective Controlling Interest</b>	l) Where the information regarding the beneficial ownership/controlling interest is not fully/publicly available requiring further review. m) Where there is a Politically Exposed Person in the owners of the entity n) High net worth customer with no clearly identifiable source of income	Where the information regarding the controlling interest is adequate, accurate and timely leading to clear understanding of ownership structure.	
4	<b>Nature of Business</b>	Business falls in any of the high risk category as defined in the <i>FAQ Sheet</i>	Businesses other than the high risk category as defined in the <i>FAQ Sheet</i>	
5	<b>Disclosure Status</b>	Where the disclosure of financial position of the client is not in keeping with transactional profile of the client esp. Sole proprietorship, Partnerships, Private/Public Ltd Companies, NGOs/NPOs/Clubs/Societies etc.	<ul style="list-style-type: none"> <li>• Makes adequate financial/regulatory disclosures</li> <li>• Listed on the stock exchanges</li> <li>• Government entities</li> </ul>	
6	<b>Transaction Profile (On aggregate daily basis)</b>			
	<b>Cash/Clearing / Remittances</b>	Sole Proprietorship Rs.1million & above Partnership Rs.1million & above NGOs/NPOs/Trusts/ Societies, Clubs etc Rs.1million & above Private Ltd Companies Rs.1million & above	Public Limited Companies Government Bodies etc	

	<b>Transactional Analysis/ Behaviour</b>	Where unusually large, complex and unusual patterns of transactions are observed.	Where there are usual patterns of transactions are observed which are conducted in line with the apparent economic or visible lawful purpose	
--	--	---	--	--

**Note:**

- If any of the above risk factors is rated as high, client/s' risk rating will be categorized in the High Risk Category in the section of *Overall Level of Risk* in KYC Form.
- In case of any material change in the clients' profile, the same should be promptly noted in the ongoing review section of the KYC Form. This means, the branch manager shall not wait for the next review but shall immediately change the risk category accordingly.
- AML Department should be consulted regarding information about country of concern/tax haven etc.






9.5 KYC FORM (INDIVIDUALS IN SRI LANKA), FAQs AND RISK RATING SHEET

<span style="float: right;">CONFIDENTIAL</span>			
<b>KNOW YOUR CUSTOMER (KYC) FORM</b> (For Individual Clients-Sri Lanka)			
<b>Branch</b>	Name		Account Number/s:
	Code		Date Account/s Opened:
<b>ACCOUNT TITLE</b>			
<b>ACCOUNT TYPE</b>	Saving Account <input type="checkbox"/> Current Account <input type="checkbox"/> Collection Account <input type="checkbox"/> Fixed Deposit <input type="checkbox"/> Certificate of Dep: <input type="checkbox"/> Treasury Product <input type="checkbox"/> Others (please specify) <input type="checkbox"/>		
<b>ACCOUNT STATUS</b>		<b>ACCOUNT NATURE</b>	
<b>Resident</b> <input type="checkbox"/>  <input type="checkbox"/> Sri Lankan  <input type="checkbox"/> Foreigner Country of Citizenship _____  <b>Non - Resident</b> <input type="checkbox"/>  <input type="checkbox"/> Sri Lankan Country of Residence _____  <input type="checkbox"/> Foreigner Country of Residence _____  Country of Citizenship _____		<b>Individual</b> <input type="checkbox"/>  <b>Joint</b> <input type="checkbox"/> <small>(In case of joint a/c KYC Form of each client will be filled separately)</small>  Nature of Relation <input type="checkbox"/> Family <input type="checkbox"/> Business <input type="checkbox"/> Other <input type="checkbox"/>	
<b>Politically Exposed Person (PEP)</b> Yes <input type="checkbox"/> No <input type="checkbox"/>			
Politician <input type="checkbox"/> Judiciary <input type="checkbox"/> Armed Forces <input type="checkbox"/> Executives (Govt) <input type="checkbox"/> Administration (Local/Municipal etc) <input type="checkbox"/> Journalist <input type="checkbox"/> Others (Please specify) _____ <input type="checkbox"/>			
<b>PERSONAL INFORMATION</b>			
NIC/ PASSPORT # _____		Issued Date _____	
Expiry Date / Validity _____		Verification (Dated) <input type="checkbox"/> _____	
Permanent Address (as per NIC) _____		Issued By _____	
Present Address(as per NIC) _____			
Mention Address (permanenet/current) if different from as given in NIC _____			
Signature if vary from as given in NIC <input type="checkbox"/> NO <input type="checkbox"/> YES (If yes then undertaking/file note to be obtained)			
Telephone (Res) _____		Telephone (Off) _____	
Email _____		Mobile Number _____	
Fax Number _____			
Occupation: Gov. Service <input type="checkbox"/> Private Service <input type="checkbox"/> Self Employed <input type="checkbox"/> Agriculture <input type="checkbox"/> Student <input type="checkbox"/> House Wife <input type="checkbox"/> (For House Wife, the source of funds should be identified) <input type="checkbox"/> Others (specify) _____			
Name & Address of Employer: _____			
Monthly Salary _____		Education Level _____	
<b>PURPOSE OF ACCOUNT</b>			
Receipts and Payments <input type="checkbox"/>		Savings and Investments <input type="checkbox"/>	
		Others (Specify) _____	
<b>BANKING HISTORY</b>			
Name of Bank/s _____		Relationship since _____	
Ever Refused Banking Facility by any Bank/Financial Institution? YES <input type="checkbox"/> NO <input type="checkbox"/>			
Does the client appear in known suspected terrorist list/s or any other alert list? (In case of YES, account should not be opened) YES <input type="checkbox"/> NO <input type="checkbox"/>			



BUSINESS INFORMATION					
Name of Business _____					
Place and Date of Incorporation/Formation: _____					
Related concerns					
Nature of Business (e.g. Jeweler, Electronics, Textile etc) _____					
Type of Business: Wholesale/Supplies <input type="checkbox"/> Retailing <input type="checkbox"/> Trading <input type="checkbox"/> Manufacturing <input type="checkbox"/>					
Import/Export <input type="checkbox"/> Other ( please specify) _____					
Commodities/Products Sold: _____					
Commodities/Products Purchased: _____					
Years in current business: _____					
Total Assets during the last year (To include Fixed Assests/Stocks/Receivables/Cash in hand etc)		Year	Amount (Rs.)	Gross Profit during the last year	
				Year	Amount (Rs.)
Note any significant expected or recent (<12 months) changes in product mix or business activities (i-e. opened new selling location in recent year etc.) _____					
Description of Business Operations: Including size of business & number of employees: _____					
Names and Locations of Major Suppliers: _____					
Names and Locations of Major Customers: _____					
Please indicate the nature of activity to be undertaken with the bank:					
Payment to Suppliers/ Vendors <input type="checkbox"/> Payment from/to Customers <input type="checkbox"/> Payroll Payments <input type="checkbox"/> Inter-Company Payments <input type="checkbox"/> Others (specify) _____					
OTHER SOURCES OF WEALTH/FUNDS					
Specify other sources of income _____					
TRANSACTION PROFILE					
Expected Daily Turnover (in the account)		Average		Maximum	
		Debit		Credit	
Expected Monthly Turnover					
Volume (on daily basis)	Cash	Transfer / Clearing	Foreign Remittances	Trade Products	Rupees Travellers Cheques
Upto Rs 100,000	<input type="checkbox"/>	<input type="checkbox"/>	<b>Originating Countries</b>	Letters of Credit <input type="checkbox"/>	<b>Facility required?</b>
Rs 100,001 to Rs 250,000	<input type="checkbox"/>	<input type="checkbox"/>		Foreign Bill Purchased <input type="checkbox"/>	<b>Yes</b> <input type="checkbox"/>
Rs 250,001 to Rs 500,000	<input type="checkbox"/>	<input type="checkbox"/>		Bank Guarantees <input type="checkbox"/>	<b>No</b> <input type="checkbox"/>
Rs 500,001 to Rs 1 million	<input type="checkbox"/>	<input type="checkbox"/>	<b>Destinantion Countries</b>	Others (specify) <input type="checkbox"/>	
Rs 1 million to Rs 10 million	<input type="checkbox"/>	<input type="checkbox"/>			
Over and above Rs 10 million	<input type="checkbox"/>	<input type="checkbox"/>			
OVERALL LEVEL OF RISK			Normal Risk (NR) <input type="checkbox"/> High Risk (HR) <input type="checkbox"/>		
THIS KYC FORM IS REVIEWED BY:	NAME	ASSESSMENT		SIGNATURES/ Date	
Account Opening Officer					
Branch Manager (Having verified/authenticated all the necessary documents for KYC)					

<b>ONGOING REVIEW OF KYC FORM</b>		<b>Account Title</b>	
		<b>Account Number/s</b>	
<b>(FOR HIGH RISK CUSTOMERS ONCE IN A YEAR AND FOR NORMAL RISK CUSTOMERS ONCE IN THREE YEARS)</b>			
<b>PERIOD</b>	<b>HIGH RISK</b>	<b>NORMAL RISK</b>	<b>SIGNATURES/ REVIEW DATE</b>
			



8-BUSINESS INFORMATION							
Name of Business _____							
Place and Date of Incorporation/Formation: _____							
Related concerns _____							
Nature of Business (e.g. Jeweler, Electronics, Textile etc) _____							
Type of Business: Wholesale/Supplies <input type="checkbox"/> Retailing <input type="checkbox"/> Trading <input type="checkbox"/> Manufacturing <input type="checkbox"/>							
Import/Export <input type="checkbox"/> Other ( please specify) _____							
Commodities/Products Sold: _____							
Commodities/Products Purchased: _____							
Years in current business: _____							
Total Assets during the last year (To include Fixed Assests/Stocks/Receivables/Cash in hand etc)		Year	Amount (Rs.)	Gross Profit during the last year			
				Year	Amount (Rs.)		
Note any significant expected or recent (<12 months) changes in product mix or business activities (i-e. opened new selling location in recent year etc.) _____							
Description of Business Operations: Including size of business & number of employees: _____							
Names and Locations of Major Suppliers: _____							
Names and Locations of Major Customers: _____							
Please indicate the nature of activity to be undertaken with the bank:							
Payment to Suppliers/Vendors <input type="checkbox"/>		Payment from/to Customers <input type="checkbox"/>		Payroll Payments <input type="checkbox"/>			
				Inter-Company Payments <input type="checkbox"/>			
				Others (specify) _____			
9-OTHER SOURCES OF WEALTH/FUNDS							
Specify other sources & amount of Income _____							
10-TRANSACTION PROFILE							
Expected Aggregate Daily Turnover (in the account)		Average		Maximum			
Debit				Credit			
Expected Monthly Turnover							
11-Volume (on daily basis)		Cash	Transfer / Clearing	Foreign Remittances	Trade Products	RTCs	
Upto Rs 100,000		<input type="checkbox"/>	<input type="checkbox"/>	<b>Originating Countries</b>	Letters of Credit <input type="checkbox"/>	Facility required?	
Rs 100,001 to Rs 250,000		<input type="checkbox"/>	<input type="checkbox"/>		Foreign Bill Purchased <input type="checkbox"/>	Yes <input type="checkbox"/>	No <input type="checkbox"/>
Rs 250,001 to Rs 500,000		<input type="checkbox"/>	<input type="checkbox"/>	<b>Destinantion Countries</b>	Bank Guarantees <input type="checkbox"/>	No <input type="checkbox"/>	
Rs 500,001 to Rs 1 million		<input type="checkbox"/>	<input type="checkbox"/>		Others (specify) <input type="checkbox"/>		
Rs 1 million to Rs 10 million		<input type="checkbox"/>	<input type="checkbox"/>				
Over and above Rs 10 million		<input type="checkbox"/>	<input type="checkbox"/>				
12-OVERALL LEVEL OF RISK		Normal Risk (NR) <input type="checkbox"/> High Risk (HR) <input type="checkbox"/>					
THIS KYC FORM IS REVIEWED BY:		NAME	ASSESSMENT		SIGNATURES/ Date		
Account Opening Officer							
Branch Manager <small>(Having verified/authenticated all the necessary documents for KYC)</small>							

### KYC RISK RATING SHEET (INDIVIDUALS IN SRI LANKA)

SR.	RISK FACTOR	HIGH RISK (HR)	NORMAL RISK (NR)	RISK RATING
1	<b>Citizenship Status</b>	(4) <i>Non-resident foreigner</i> (5) <i>Resident foreigner</i> (6) Citizen of country of concern/high risk area	Sri Lankan Citizen and/or not a citizen of high risk area within Sri Lanka	
2	<b>Geographical Address</b>	(4) Non-Local address the credential of which could not be ascertained or linked to tax/corruption haven.  (5) Present Address in the NIC varies from the present address provided in the form.  (6) Local address within Sri Lanka with area of concern where the account activity need to be observed with regard to likely suspicious/terrorist activity	Local address within our normal market / bankable areas	
3	<b>Occupation Service</b>	(4) Employed internationally with high risk businesses/firms	Employed locally or Retired from industry not considered high risk or unemployed	
	<b>Business</b>	(5) Business falls in any of the high risk category as defined in the <i>FAQ Sheet</i>	Businesses other than the high risk category as defined in the <i>FAQ Sheet</i>	
4	<b>Politically Exposed Person</b>	(6) Politically Exposed Person  (or prominent public figure / person as defined in attached <i>FAQ Sheet</i> )		
5	<b>Length of Relationship/ Banking History</b>		Existing banking customer with relationship is greater than 1 year No prior relationship with any bank Existing banking customer with relationship is less than 1 year	
6	<b>Transaction Profile</b>			
	<b>Cash/Clearing / Transfer</b>	Rs 1 million and above	Less than Rs 1 million	
	<b>Transaction Profile - Foreign Remittances</b>	Rs 1 million and above	Less than Rs 1 million	
	<b>Transaction Profile -Bearer Certificats of Deposits</b>	More than Rs 100,000/-		

**Note:** If any of the above risk factors is rated as high, client/s will be categorized in the High Risk Category in the section of *Overall Level of Risk* in KYC Form  
In case of any material change in the clients' profile; the same should be promptly noted in the Ongoing review section of the Form this means, the branch manager shall not wait for the next review but shall immediately change the risk category accordingly.



## FREQUENTLY ASKED QUESTIONS

### 1-What is PEP?

PEP stands for Politically Exposed Person. Business relationships with individuals holding important public positions and with persons or companies clearly related to them may expose a bank to significant reputational and/or legal risks. Such politically exposed persons (“PEPs”) are individuals who are/or have been entrusted with prominent public functions, including heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of publicly owned corporations and important political party officials. Senior personnel from judiciary, executive, armed forces, administration etc should be reviewed with respect to the possibility of being PEP

The definition of PEP also includes entity for which PEP is a beneficial owner of an entity if the PEP exercises actual or effective control over the entity. Entities that are 20% or more owned by PEP are defined as PEP. Wherever we have knowledge that PEP owns less than 20% of an entity but still exercises effective control, or if we know that an entity has been formed for the benefit of PEP, that entity must also be defined as PEP.

PEP will continue to be identified as PEP even though the individual no longer holds the position which basically means that once PEP, always PEP.

Branch/controlling office should investigate the source of funds before accepting a PEP. The decision to open an account for PEP should be taken at a senior level (GM). Government officials of grade 20 and above

must be reviewed against their possibility of being PEP. Prudence should also be exercised for government officials ranking below grade 20, having influential public positions.

**Politically exposed person or PEP or in other words Senior Public Figure** is a term that describes a person who has been entrusted with a prominent public function, or is closely related to such a person. By virtue of this position and the influence it holds, PEPs present a higher risk for potential involvement in bribery and corruption.

The process of screening for PEPs is usually performed at the beginning of account opening, called enhanced due diligence, and screening of accounts periodically is performed as part of ongoing due diligence. Since September 11, 2001, more than 100 countries have changed their laws related to financial services regulation, with the fight against political corruption playing a foundational role.

Although there is no global definition of PEP, most countries based their definition on the Financial Action Task Force (FATF) definition:

- current or former senior official in the executive, legislative, administrative, military, or judicial branch of a foreign government (elected or not)
- a senior official of a major foreign political party
- a senior executive of a foreign government-owned commercial enterprise, being a corporation,

business or other entity formed by or for the benefit of any such individual

- an immediate family member of such individual; meaning spouse, parents, siblings, children, and spouse's parents or siblings
- Any individual publicly known (or actually known by the relevant financial institution) to be a close personal or professional associate.

The definition is not intended to cover middle ranking or more junior individuals in the foregoing categories.

Canadian PEFP definition is:

"Politically exposed foreign person - means a person who holds or has ever held one of the following offices or positions in or on behalf of a foreign state:

- (a) head of state or head of government;
- (b) member of the executive council of government or member of a legislature;
- (c) deputy minister or equivalent rank;
- (d) ambassador or attaché or counselors of an ambassador;
- (e) military officer with a rank of a Brigadier or above;
- (f) president of a state-owned company or a state-owned bank;
- (g) head of a government agency;
- (h) judge;
- (i) leader or president of a political party represented in a legislature; or
- (j) holder of any prescribed office or position."

The definition includes any prescribed family member of such a person.

**Close Associates** means Agent / Representative, Business Associate, Senior Employee, Adviser (including, but not limited to financial, political, and legal)

**Immediate family Members** means Husband, Wife, Partner, Mother, Father, Brother, Sister, Son, Daughter, Son-in-law, Daughter-in-law, Father-in-law, Brother-in-law, Step relative listed above e.g. step-Son, Step-Mother, etc.

### 2-Why KYC is necessary?

To determine the **true identity** of the beneficial owner(s), the real party in interest, controlling person(s) and entity of the accounts (M-1)

### 3-Is KYC one time exercise?

No. KYC would be an ongoing exercise for prudent banking practices. With each material change in the profile of client, KYC needs to be reviewed in the light of changed scenario.

### 4-What are Due Diligence (DD) and Enhanced Due Diligence (EDD) of a customer?

For each customer bank is required to undertake the normal due diligence process. And where the level of risk from the customer to the bank is high, staff will be *legally required* to perform the enhanced due diligence as required under the Prudential Regulations (M1-5), other instructions of State Bank of Pakistan and Anti-Money Laundering Ordinance 2007 (AML Regulations 2008, AML Rules 2008). Failing the implementation of these requirements will be source of concern for the bank.

**5-Which are the major countries that are of concern with respect to AML?**

Afghanistan, Nigeria, Iran, Iraq, Syria, Myanmar (Burma), North Korea, Sudan, Zimbabwe, Cuba, Ivory Cost, Congo, Belarus, British Virgin Islands, Israel, India, Turkmenistan, Uzbekistan, Sao Tomi & Principe should be placed in the high risk countries.

**6-Ever refused banking facility?**

If the customer has been refused banking facility, by any banking company, staff should take extra care in handling the transactions on behalf of such accounts.

**7 -Which are high risk businesses?**

Following business should be dealt with extra care while continuing business relationship with the entrepreneurs:

1. Precious Metals/Stones
2. Arms Dealers
3. Jewellers
4. Artefacts/Antiques/ Art Dealers
5. Real estate Company
6. Religious organizations and trusts.
7. NGOs/ Non Profit Organization (NPOs) /Charities, societies with cross border donations.
8. Concerns/Associations closely related with Politically exposed persons (PEPs)
9. All accounts of Exchange Companies & /Franchisees of Exchange Companies.
10. International correspondent bank
11. Unregulated Hedge fund
12. Un-regulated law firm or accounting company
13. Travel agent
14. Leather goods stores (prohibited items)
15. Import/export companies
16. Casinos

17. Offshore corporations and banks located in tax/banking havens

18. Scrap dealers

19. Other cash-intensive businesses

**8- Assessment of account opening and authorizing officer/executive.**

Assessment must be based on the available material information about the client. For this matter, sound judgment and good understanding of businesses would be appreciated to establish true-identity of the existing and prospective clients.

**09-One view of the Client**

A client of the bank can have multiple accounts in the bank with different branches, so the transactions in all of his accounts should be reviewed to assess the clients' profile.

*For further clarification contact:*

AML Division

Compliance Group, MCB Tower, 10<sup>th</sup> Level, Karachi, Ph. 021-2270121

### 9.6 HALF - YEARLY REVIEW OF CERTIFICATION FOR CDD / EDD – REVIEW OF ACCOUNTS

Compliance report for the PERIOD FROM: \_\_\_\_\_ TO: \_\_\_\_\_ 20.....

**Branch Name & Code:** ..... **City:** .....

**Name of Managers/Chief Managers:** .....

**To: COMPLIANCE GROUP (SOUTH / NORTH)**

S. No.	MEASURES & PROCEDURES	Relevant Circulars
1	Account Opening Forms of all new accounts opened during the period under review have been checked and required documents are held by us. All formalities relating to Account Opening including obtaining of Computerized National Identity Cards (CNIC), carrying out of proper Due diligence etc. have been fully complied with.	Circular No. POK/CM & C/GEN/113 dated April, 14, 2003. Circular No.POK/OD/COMP/2003/GEN/405 dated November 6, 2003 Circular No .POK/O & MW/PI/940 dated March 17, 2004 Circular No POK/Comp/ GEN/ 271dated October 0-1, 2007.
2	CDD / Client Profile (KYC) of every new customer have been properly filled in and all related documents have been obtained and attached. Accounts of existing customers are being updated on the basis of Annual Meetings as well as HVT reports generated at our branch and fresh / new KYC have been obtained from the customer.	Circular No.POK/COMPLIANCE/GEN/237 dated July 02, 2003 Circular No.POK/COMPLIANCE/GEN/317 dated December 23, 2008 Circular No.POK/COMPLIANCE/GEN/19 dated January 22, 2009
3	We have ensured that no Benami Transactions have taken place at our Branch.	Circular No.POK/COMPLIANCE/GEN/279 dated August 5, 2003
4	No transaction has been carried out by our branch for Countries/Individuals/Clients who are on the list of Office of Foreign Assets Control (OFAC) of US Government, SBP, NAB and High Risk Clients/Countries as per lists provided by Compliance Group.	Circular No.POK/Compliance/GEN/332 dated September 9, 2003 Circular No.POK/Compliance/GEN/196 dated June 26, 2004 Circular No.POK/Compliance/GEN/215 dated July 07, 2003
5	We have ensured that formalities relating to opening & operation of accounts by Blind Persons have been fully complied with.	Circular No.POK/Compliance/GEN/333 dated September 9, 2003
6,	We have ensured that procedure prescribed for handling Term Deposit Receipts (TDR) has been strictly followed.	Circular No.POK/Compliance/GEN/384 dated October 18, 2003
7	Suspicious transactions observed during the period under report have been referred to the respective Head of Compliance under a copy to respective GM / BH for necessary action.	Circular No.POK/Compliance/GEN/189 dated June 24, 2004
8	We have undertaken required due diligence including identifying and verifying the identity of walk-in-customers and followed the procedures prescribed for dealing with walk-in customers and the proper use of Walk-in-customer-information-form (WICIF). Procedure prescribed for On-Line Cross Branch Transactions above Rs.0.500 M strictly followed.	Circular No.POK/Compliance/GEN/189 dated June 24, 2004 Circular No.POK/Compliance/CL/84 dated March 21, 2005. Circular No. POK/OPS OD/2004/0501 dated May 11, 2004

S. No.	MEASURES & PROCEDURES	Relevant Circulars
9	We have carried required due diligence regarding Monitoring of Hundi / Hawala Transactions in Un-Authorized Money Changers Accounts and ensured that neither any account is being maintained nor any transaction relating to them pertains to our branch.	Circular No. POK/ Compliance/GEN/306 dated December 11, 2008
10	Circulars (internal & external) and Guidelines for Anti Money Laundering AML/ Know Your Customer KYC procedures Handbook including Compliance News Letters have been received by us, circulated amongst Branch's staff members and they have understood the procedures for its implementation and same are kept in a separate file accessible to all staff.	POK/Comp/GEN/121 Dated May 09, 2008
11	All Accounts Opened during the year 2009 till date under High Risk (HR) Category must be reviewed & proper EDD be Carried out.	Refer: CDD/KYC & AML Handbook <ul style="list-style-type: none"> <li>• Para 5.3 on page # 38/105</li> <li>• Para 3.1 (f) on Page # 14/87</li> </ul>

**Exceptions (if any)**


---

Name, Signature & Stamp of Branch Manager

---

Name, Counter Signature & Stamp of Local Compliance Officer / ROM / RH

**9.7 MEMBER COUNTRIES AND TERRITORIES OF THE FATF INCLUDE:**

**FATF Members**

1. Argentina	2. Germany	3. New Zealand
4. Australia	5. Greece	6. Norway
7. Austria	8. Hong Kong, China	9. Portugal
10. Belgium	11. Iceland	12. Republic of Korea
13. Brazil	14. India	15. Russian Federation
16. Canada	17. Ireland	18. Singapore
19. China	20. Italy	21. South Africa
22. Denmark	23. Japan Netherlands*	24. Spain
25. European Commission	26. Kingdom of the Netherlands	27. Gulf Co-operation Council
28. Finland	29. Luxembourg	30. Switzerland
31. France	32. Mexico	33. Turkey
34. Sweden	35. United Kingdom	36. United States

\* *The Kingdom of Netherlands: The Netherlands, The Netherlands Antilles and Aruba*

**Countries with Observer Status**

India

Republic of Korea

(Source: FATF, 2009)

There are **NO** Non-Cooperative Countries and Territories (NCCTs).

(Source: Annual Review of Non-Cooperative Countries and Territories 2006-2007: Eighth NCCT Review  
12 October 2007)

**PAKISTAN IS MEMBER OF ASIA PACIFIC GROUP (APG):** *which is an FATF Style Regional Body (FSRB). The regional FATF-style bodies have similar form and functions to those of the FATF, and some FATF members are also members of these bodies.*

**LEGAL FRAMEWORK**  
**SBP PRUDENTIAL REGULATIONS**  
**M1 – M5**



## **10 SBP PRUDENTIAL REGULATIONS**

### **10.1 REGULATION M-1 KNOW YOUR CUSTOMER (KYC) CUSTOMER DUE DILIGENCE (CDD)**

With the view to preserve integrity and safety of the financial system, it is expedient to prevent the possible use of the banking sector for money laundering and terrorist financing, transfer of illegal/ill-gotten monies, and as conduit for white collar crime etc. To this end, Customer Due Diligence / Know Your Customer (CDD / KYC) has increased, which requires special attention and concrete implementation. In the line with the international best practices, as also to ensure transparency/prudence in banking transactions while starting relationship with a new customer and maintaining and continuing relationship with existing customers, the following **minimum** STEPS.....are required to be followed by banks / DFIs to avert the risks posed by the money laundering and terrorist financing. However, banks / DFIs are free to take additional measures in line with Financial Action Task Force Recommendations.

SBP Focus Areas are:

2. Banks / DFIs shall have formulate and put in place, a comprehensive and approved CDD / KYC & AML policy (((duly approved by their Board of Directors and in case of branches of foreign banks, approved by their head office, and cascade the same down the line to each and every business location / concerned officers for strict compliance))).
3. CDD / KYC policy of the banks / DFIs shall interalia include a description of the types of customers that are likely to pose a higher than average risk to the bank / DFI and guidelines for conducting Enhanced Customer Due Diligence depending upon the customers' background, country of origin, public or high profile position, nature of business, etc.
4. Banks / DFIs should undertake customer due diligence measures when:
  - (a) establishing business relationship;
  - (b) conducting occasional transactions above rupees one million whether carried out in a single operation or in multiple operations that appear to be linked;
  - (c) carrying out occasional wire transfers (domestic / cross border) regardless of any threshold;
  - (d) there is suspicion of money laundering / terrorist financing; and
  - (e) there is a doubt about the veracity or adequacy of available identification data on the customer.
5. Banks / DFIs shall undertake at least following Customer due diligence measures:
  - (a) Banks / DFIs should not open and maintain anonymous accounts or accounts in the name of fictitious persons.
  - (b) All reasonable efforts shall be made to determine identity of every prospective customer. For this purpose, minimum set of documents to be obtained by the banks / DFIs from various types of customers / account holder(s), at the time of opening account, as prescribed in Annexure-VIII of

the Prudential Regulations for Corporate / Commercial Banking. While opening bank account of “proprietorships”, the requirements laid down for individuals at Serial No. (1) of Annexure-VIII shall apply except the requirement mentioned at No. (3) of the Annexure. Banks / DFIs should exercise extra care in view of the fact that constituent documents are not available in such cases to confirm existence or otherwise of the proprietorships.

(c) Banks / DFIs shall identify the true beneficial ownership of accounts/ transactions by taking all reasonable measures.

(d) For all customers, banks / DFIs should determine whether the customer is acting on behalf of another person, and should then take reasonable steps to obtain sufficient identification data to verify the identity of that other person (remitter).

(e) For customers that are legal persons or for legal arrangements, banks / DFIs are required to take reasonable measures to (i) understand the ownership and control structure of the customer (ii) determine that the natural persons who ultimately own or control the customer. This includes those persons who exercise ultimate effective control over a legal person or arrangement.

(f) Government accounts should not be opened in the personal names of the government official(s). Any such account, which is to be operated by an officer of the Federal / Provincial / Local Government in his / her official capacity, shall be opened only on production of a special resolution / authority from the concerned administrative department duly endorsed by the Ministry of Finance or Finance Department of the concerned Government.

(g) Precaution should be taken while opening of account of prospective customer engaged in the business of Lottery Schemes, Employment Schemes, Real Estate Schemes, Deposit and Loan Schemes, Multi Level Marketing Ponzi & Pyramid Schemes and Introducing Brokers of Foreign Brokerage Houses. (Circular NO. F&FCD/PO/GEN/319 of December 18, 2009)

6. Verification is an integral part of CDD / KYC measures for which banks / DFIs shall ensure that;

(a) copies of CNIC wherever required in Annexure-VIII are invariably verified, before opening the account, from NADRA through utilizing on-line facility or where the banks / DFIs or their branches do not have such facility from the regional office(s) of NADRA.

(b) the identity of the beneficial owner is verified using reliable information/ satisfactory sources.

(c) the cost of verification of CNIC from NADRA should not be passed on to their account holder(s) (either existing or prospective).

7. Banks / DFIs shall note that:

(a) For customers / clients whose accounts are dormant and an attested copy of account holder's Computerized National Identity Card (CNIC) is not available in bank's / DFIs record, banks / DFIs shall not allow operation in such accounts until the account holder produces an attested copy of his / her CNIC and fulfill all other formalities for activation of the account.

(b) For all other customers / clients including depositors and borrowers, banks / DFIs shall obtain the attested copies of CNICs by June 30, 2009. Banks / DFIs shall discontinue

relationship with such customers who fail to submit a copy of their CNIC by the above deadline. Existing accounts whether active/dormant or inactive without CNIC, block option should be exercised for all debit transaction/withdrawals, irrespective of mode of payment. One month prior notice is served upon such customers who have not submitted copies of their CNICs. **Joint accounts/Partnership accounts:** It is necessary to obtain copies of CNIC of all individual joint account holders and partners. **Joint stock companies:** It is necessary to obtain CNIC of all directors. However for a **public limited company** which is subject to regulatory disclosure requirement, partial availability of CNIC i.e. CNIC of any of the Directors, is available. **Government accounts:** Debit block option should not be exercised in case of government account if bank has any documentary proof and is otherwise satisfied with identity of the authorized signatory. Any kind of transaction requested by a walk-in customer having old or expired CNIC must be denied. (SBP Circular No. BPRD/30 of September 30, 2009.)

Banks / DFIs are encouraged to carry on public campaign through print / electronic media individually as well as through Pakistan Banks Association for creating public awareness on requirement of CNIC for banking purposes. They are also advised to confirm compliance with the subject instructions by the above extended timelines.

8. Banks / DFIs are also advised that CDD/KYC is not a one time exercise to be conducted at the time of entering into a formal relationship with customer / account holder. This is an on-going process for prudent banking practices. To this end, banks / DFIs are required to:
  - (a) Set up a compliance unit with a full time Head.
  - (b) Put in place a system to monitor the accounts and transactions on regular basis.
  - (c) Update customer information and records, if any, at reasonable intervals.
  - (d) Install an effective MIS to monitor the activity of the customers' accounts.
  - (e) Chalk out plan of imparting suitable training to the staff of bank / DFI periodically.
  - (f) Maintain proper records of customer identifications and clearly indicate, in writing, if any exception is made in fulfilling the CDD / KYC measures.
  
9. Banks / DFIs shall conduct enhanced due diligence when:
  - (a) Dealing with high-risk customers, business relationship or transaction including the following;
    - i) Non-resident customers;
    - ii) Private banking customers/Non Banking Financial Institutions;
    - iii) Legal persons or arrangements including non-governmental organizations (NGOs) / not-for-profit organizations (NPOs) and trusts / charities;
    - iv) Customer(s) belonging to countries where CDD / KYC and anti-money laundering regulations are lax;
    - v) Customer(s) with links to offshore tax havens;
    - vi) Customer(s) in cash intensive businesses;

- vii) High net worth customers with no clearly identifiable source of income; and
  - viii) Customers in high-value items etc.
- (b) There is reason to believe that the customer has been refused banking facilities by another bank / DFI.
- (c) Opening correspondent banks' accounts.
- (d) Dealing with non-face-to-face / on-line customers. Adequate measures in this regard should be put in place, e.g. independent verification by a reliable 3<sup>rd</sup> party, client report from the previous bank / DFI of the customer etc.
- (e) Establishing business relationship or transactions with counterparts from or in countries not sufficiently applying FATF recommendations.
- (f) Dealing with politically exposed persons (PEP) or customers holding public or high profile positions.
10. For politically exposed persons or holders of public or high profile positions, enhanced due diligence should include the following:
- (a) Relationship should be established and or maintained with the approval of senior management including when an existing customer becomes holder of public or high profile position.
  - (b) Appropriate risk management systems to determine whether a potential customer, a customer or the beneficial owner is a politically exposed person/ holder of public or high profile position and sources of wealth /funds of customers, beneficial owners for on going monitoring on regular basis.
11. Where there are low risks and information on the identity of the customer and the beneficial owner of a customer is publicly available, or where adequate checks and controls exist, banks / DFIs may apply simplified or reduced CDD / KYC measures. Following cases may be considered for application of simplified or reduced CDD / KYC:
- (a) Financial institutions provided they are subject to requirements to combat money laundering and terrorist financing consistent with the FATF recommendations and are supervised for compliance with those requirements.
  - (b) Public companies that are subject to regulatory disclosure requirements and such companies are listed on a stock exchange or similar situations.
  - (c) Government administrations or entities.
12. Reduced CDD / KYC measures shall not be applied where there is risk of money laundering or terrorist financing or when a customer resides in a country, which does not comply with FATF recommendations.
13. In case banks / DFIs are not able to satisfactorily complete required CDD / KYC measures including identity, beneficial ownership or information on purpose and intended nature of business

relationship, account should not be opened or any service provided and instead reporting of suspicious transaction be considered. Similarly, relationship with existing customers should be terminated and reporting of suspicious transaction be considered if CDD / KYC is found unsatisfactory.

14. State Bank of Pakistan, during the course of inspection, would particularly check the efficacy of the CDD / KYC policies and system of the banks / DFIs and its compliance by all the branches and the staff members. Appropriate action shall be taken against the bank / DFI and the concerned staff members for non-compliance and negligence in this area, under the provisions of Banking Companies Ordinance, 1962.

## **10.2 REGULATION M-2 ANTI MONEY LAUNDERING MEASURES**

Banks / DFIs are advised to follow the following guidelines to safeguard themselves against their involvement in money laundering activities, and other unlawful trades. These will add to or reinforce the precautions, Banks / DFIs may have been taking on their own in this regard:

1. Banks / DFIs shall ensure that their business is conducted in conformity with high ethical standards and that banking laws and regulations are adhered to. It is accepted that banks/DFIs normally do not have effective means of knowing whether a transaction stems from or forms part of wrongful activity. Similarly, in an international context, it may be difficult to ensure that cross border transactions on behalf of customers are in compliance with the regulations of another country. Nevertheless banks/DFIs should not set out to offer services or provide active assistance in transactions, which in their opinion, are associated with money derived from illegal activities.
2. Specific procedures are established for ascertaining customer's status and his source of earnings, for monitoring of accounts on a regular basis, for checking identities and bona fides of remitters and beneficiaries, for retaining internal record of transactions for future reference. The transactions, which are out of character/inconsistent with the history, pattern, or normal operation of the account involving heavy deposits / withdrawals / transfers, should be viewed with suspicion and properly investigated.
3. Banks / DFIs are required to include accurate and meaningful originator information (name, address and account number) on funds transfers including wire transfers and related messages that are sent, and the information should remain with the transfer or related message throughout the payment chain. However, Banks / DFIs may, if satisfied, substitute the requirement of mentioning address with CNIC, passport, driving license or similar identification number for this purpose.
4. Beneficiary financial institutions shall adopt effective risk-based procedures for identifying and handling wire transfers that are not accompanied by complete originator information. Wire transfers with incomplete originator information may be seen with suspicion which may require reporting to FMU or termination of the transaction. Banks/ DFIs should remain careful from financial institutions which do not comply with aforesaid requirements by limiting or terminating business relationship.

5. Banks/ DFIs shall not allow personal accounts to be used for business purposes. except proprietorship, small businesses and professions where constituent documents are not available and banks / DFIs are satisfied with KYC profile of the account holder, purpose of relationship and expected turnover of the account keeping in view financial status & nature of business of that customer. (SBP BPRD Circular Letter No. 42 of 2009 issued on December 31, 2009.)
6. For an effective implementation of banks' / DFIs' policy and procedures relating to anti money laundering / other unlawful trades, suitable training be imparted to members of staff and they be informed of their responsibility in this regard.
7. Bank shall not allow personal accounts to be used for business purposes except proprietorship, small businesses and professions where documents constitute are not available and banks are satisfied with KYC profile of the account holder, purpose of relationship and expected turn-over of the account keeping in view the financial status and nature of business of that customer. (BPRD Circular Letter No. 42 of 2009 dated December 31, 2009.)

Keeping in view the above principles, banks / DFIs shall issue necessary instructions for guidance and implementation by all concerned.

### **10.3 REGULATION M-3 RECORD RETENTION**

- i. The records of transactions and identification data etc. maintained by banks/DFIs occupy critical importance as far as legal proceedings are concerned. The prudence demands that such records may be maintained in systematic manner with exactness of period of preservation to avoid any set back on legal and reputational fronts. Banks/DFIs shall therefore, maintain, for a minimum period of five years, all necessary records on transactions, both domestic and international. The records so maintained must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide, if necessary, to SBP or law enforcement agencies for investigation or as an evidence in legal proceedings. Banks /DFIs shall, however, retain those records for longer period where transactions relate to litigation or are required by the Court of law or by any other competent authority.
- ii. The Banks / DFIs shall keep records on the identification data obtained through the customer due diligence process (e.g. copies or records of official identification documents like passports identity cards, driving licenses or similar documents), account files and business correspondence for at least five years after the business relationship is ended.
- iii. The records relating to the suspicious transactions reported by the bank / DFI will be retained by the bank / DFI, even after the lapse of the period prescribed above, till such time the bank / DFI gets permission from State Bank of Pakistan to destroy such record.

#### **10.4 REGULATION M- 4 CORRESPONDENT BANKING**

1. The banks /DFIs shall gather sufficient information about their correspondent banks to understand fully the nature of their business. Factors to consider include:
  - Know your customer policy (KYC)
  - Information about the correspondent bank's management and ownership.
  - Major business activities
  - Their location
  - Money Laundering prevention and detection measures
  - The purpose of the account
  - The identity of any 3<sup>rd</sup> party that will use the correspondent banking services (i.e. in case of payable through accounts)
  - Condition of the bank regulation and supervision in the correspondent's country
2. The banks/DFIs should establish correspondent relationships with only those foreign banks that have effective customer acceptance and KYC policies and are effectively supervised by the relevant authorities.
3. The banks /DFIs should refuse to enter into or continue a correspondent banking relationship with a bank incorporated in a jurisdiction in which it (the correspondent bank) has no physical presence and which is unaffiliated with a regulated financial group (i.e. shell banks). The Banks / DFIs should also guard against establishing relations with correspondent foreign financial institutions that permit their accounts to be used by shell banks.
4. The Banks / DFIs should pay particular attention when continuing relationships with correspondent banks located in jurisdictions that have poor KYC standards or have been identified by Financial Action Task Force as being non cooperative in the fight against money laundering.
5. The Banks / DFIs should be particularly alert to the risk that correspondent accounts might be used directly by 3<sup>rd</sup> parties to transact business on their own behalf (e.g. payable- through-accounts). In such circumstances, the banks / DFIs must satisfy themselves that the correspondent bank has verified the identity of and performed on-going due diligence on the customers having direct access to accounts of the correspondent bank / DFI and that it is able to provide relevant customer identification data upon request to the correspondent bank/DFIs.
6. Approval should be obtained from senior management, preferably at the level of Executive Vice President or equivalent before establishing new correspondent banking relationship.

#### **10.5 REGULATION M-5 SUSPICIOUS TRANSACTIONS**

1. The Banks / DFIs should pay special attention to all complex, unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. Examples of such suspicious transactions are listed at Annexure-IX to this Circular. However, these are not intended to be exhaustive and only provide examples of the most

basic ways in which money may be laundered. The background and purpose of such transactions should, as far as possible, be examined, the findings established in writing, and be available to help the relevant authorities in inspection and investigation.

2. If the bank / DFI suspects, or has reasonable grounds to suspect, that funds are the proceeds of a criminal activity or terrorist's financing, it should report promptly, its suspicions, through Compliance Officer of the bank / DFI to banking policy department of the State Bank of Pakistan. The report should contain, at a minimum, the following information:
  - a) Title, type and number of the accounts.
  - b) Amounts involved.
  - c) Detail of the transactions.
  - d) Reasons for suspicion.

State Bank has been encouraging Banks / DFIs to make use of technology and upgrade their systems and procedures in accordance with the changing profile of various risks. Accordingly, all Banks / DFIs are advised to implement systems which could flag out of pattern transactions for reporting suspicious transactions

The existing list of examples of suspicious transactions as Annexure-IX is supplemented with the enclosed list of characteristics of financial transactions that may be a cause for increased scrutiny as Annexure-X."

3. The employees of the banks / DFIs are strictly prohibited to disclose the fact to the customer or any irrelevant quarter that a suspicious transaction or related information is being reported for investigation.
4. In cases of foreign branches of the banks/DFIs and subsidiaries of the banks/DFIs in foreign countries undertaking banking business, the banks/DFIs would ensure compliance with the regulations (relating to Anti Money Laundering and KYC) of State Bank of Pakistan or the relevant regulations of the host country, whichever are more exhaustive".

#### **Termination of Business with customer**

Once business has decided to close the accounts of a customer who has been subject to a suspicious activity report, the business must follow up and track the matter to ensure that all accounts are closed on a timely basis.

In addition, once a business has decided to terminate a relationship because of Compliance concern, it should add the customer to the Local Negative list maintained by CCG to be used while opening of new accounts. If such a customer is later flagged as a prospective customer, businesses should ensure that CCG is contacted before relationship initiation.

Similarly, where a business decides to terminate a customer relationship and it learns during the course of its suspicious activity investigation that the same customer has relationship with another MCB branch; it should immediately advise the other business of the suspicious activity that was detected and its decision to terminate the customer relationship.

If Business files a suspicious activity report and decides either to keep the account involved in suspicious activity open or to keep an account open, the business should continue to monitor the account. Filing a suspicious activity report does not end the need to monitor transactions involving an account. Filing a suspicious activity report heightens the need to scrutinize customer activity to determine whether additional action is appropriate including, among other things:

Whether additional suspicious activity report should be filed in accordance with local law or the customer relationship should be terminated, if the business has not already decided to do so.



**10.6 Annexure-x (As per State Bank of Pakistan bpd Circular No. 5 DATED JULY 08, 2006)**

**CHARACTERISTICS OF FINANCIAL TRANSACTIONS  
THAT MAY BE A CAUSE FOR INCREASED SCRUTINY**

**A. Accounts:**

(1) Accounts that receive relevant periodical deposits and are dormant at other periods. These accounts are then used in creating a legitimate appearing financial background through which additional fraudulent activities may be carried out.

(2) A dormant account containing a minimal sum suddenly receives a deposit or series of deposits followed by daily cash withdrawals that continue until the sum so received has been removed.

(3) When opening an account, the customer refuses to provide information required by the financial institution, attempts to reduce the level of information provided to the minimum or provides information that is misleading or difficult to verify.

(4) An account for which several persons have signature authority, yet these persons appear to have no relation among each other (either family ties or business relationship).

(5) An account opened by a legal entity or an organization that has the same address as other legal entities or organizations but for which the same person or persons have signature authority, when there is no apparent economic or legal reason for such an arrangement (for example, individuals serving as company directors for multiple companies headquartered at the same location, etc.).

(6) An account opened in the name of a recently formed legal entity and in which a higher than expected level of deposits are made in comparison with the income of the promoter of the entity.

(7) The opening by the same person of multiple accounts into which numerous small deposits are made that in aggregate are not commensurate with the expected income of the customer.

(8) An account opened in the name of a legal entity that is involved in the activities of an association or foundation whose aims are related to the claims or demands of a terrorist organization.

(9) An account opened in the name of a legal entity, a foundation or an association, which may be linked to a terrorist organization and that shows movements of funds above the expected level of income.

**B. Deposits and Withdrawals:**

(1) Deposits for a business entity in combinations of monetary instruments that are a typical of the activity normally associated with such a business.

- (2) Large cash withdrawals made from a business account not normally associated with cash transactions.
- (3) Large cash deposits made to the account of an individual or legal entity when the apparent business activity of the individual or entity would normally be conducted in cheques or other payment instruments.
- (4) Mixing of cash deposits and monetary instruments in an account in which such transactions do not appear to have any relation to the normal use of the account.
- (5) Multiple transactions carried out on the same day at the same branch of a financial institution but with an apparent attempt to use different tellers.
- (6) The structuring of deposits through multiple branches of the same financial institution or by groups of individuals who enter a single branch at the same time.
- (7) The deposit or withdrawal of cash in amounts which fall consistently just below identification or reporting thresholds.
- (8) The presentation of uncounted funds for a transaction. Upon counting, the transaction is reduced to an amount just below that which would trigger reporting or identification requirements.
- (9) The deposit or withdrawal of multiple monetary instruments at amounts which fall consistently just below identification or reporting thresholds, if any, particularly if the instruments are sequentially numbered.

**C. Wire Transfers:**

- (1) Wire transfers ordered in small amounts in an apparent effort to avoid triggering identification or reporting requirements.
- (2) Wire transfers to or for an individual where information on the originator, or the person on whose behalf the transaction is conducted, is not provided with the wire transfer, when the inclusion of such information would be expected.
- (3) Use of multiple personal and business accounts or the accounts of non-profit organizations or charities to collect and then funnel funds immediately or after a short time to a small number of foreign beneficiaries.
- (4) Foreign exchange transactions that are performed on behalf of a customer by a 3<sup>rd</sup> party followed by wire transfers of the funds to locations having no apparent business connection with the customer or to countries of specific concern.

**D. Characteristics of the Customer or His/Her Business Activity:**

- (1) Funds generated by a business owned by individuals of the same origin or involvement of multiple individuals of the same origin from countries of specific concern acting on behalf of similar business types.

- (2) Shared address for individuals involved in cash transactions, particularly when the address is also a business location and/or does not seem to correspond to the stated occupation (for example student, unemployed, self-employed, etc.).
- (3) Stated occupation of the transactor is not commensurate with the level or type of activity (for example, a student or an unemployed individual who receives or sends large numbers of wire transfers, or who makes daily maximum cash withdrawals at multiple locations over a wide geographic area).
- (4) Regarding non-profit or charitable organizations, financial transactions for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organization and the other parties in the transaction.
- (5) A safe deposit box is opened on behalf of a commercial entity when the business activity of the customer is unknown or such activity does not appear to justify the use of a safe deposit box.
- (6) Unexplained inconsistencies arising from the process of identifying or verifying the customer (for example, regarding previous or current country of residence, country of issue of the passport, countries visited according to the passport, and documents furnished to confirm name, address and date of birth).

#### **E. Transactions Linked to Locations of Concern:**

- (1) Transactions involving foreign currency exchanges that are followed within a short time by wire transfers to locations of specific concern (for example, countries designated by national authorities, FATF non-cooperative countries and territories, etc.).
- (2) Deposits are followed within a short time by wire transfers of funds, particularly to or through a location of specific concern (for example, countries designated by national authorities, FATF non-cooperative countries and territories, etc.).
- (3) A business account through which a large number of incoming or outgoing wire transfers take place and for which there appears to be no logical business or other economic purpose, particularly when this activity is to, through or from locations of specific concern.
- (4) The use of multiple accounts to collect and then funnel funds to a small number of foreign beneficiaries, both individuals and businesses, particularly when these are in locations of specific concern.
- (5) A customer obtains a credit instrument or engages in commercial financial transactions involving movement of funds to or from locations of specific concern when there appears to be no logical business reasons for dealing with those locations.
- (6) The opening of accounts of financial institutions from locations of specific concern.
- (7) Sending or receiving funds by international transfers from and/or to locations of specific concern.

## 11 SUMMARY OF CHANGES IN PREVIOUS KYC / AML PROCEDURES HANDBOOK

The following is the gist of changes incorporated in the previous KYC / AML Procedures Handbook yielding the current CDD/KYC & AML Procedures Handbook.

No.	Section	Section Amended in Handbook	Page No.	Reason for Change	Remarks
1	1.1 (Old- Nil)	Background & Purpose of this Handbook	5	To familiarize the staff in a more explanatory manner. This will also include the introduction to HotScan (name-filtering solution) and MANTAS (AML solution) as well as the background of OFAC lists used for CDD/AML compliance.	
2	1.2 (Old- 1.1)	What is Money Laundering? Anti-Money Laundering Act 2010 has been promulgated thus introducing a financial system with legal backing for controlling the menace of money laundering. The act of money laundering would be a serious offence punishable under the provisions of the Ordinance. The Ordinance has specified the role of different government department, banks, regulatory bodies and investigating agencies for checking movement of illegal funds through the financial systems. The Act has also elaborated the procedure to check the suspicious accounts transactions through the banking system. In the line with the AML Act, the Federal Government has established a Financial Monitoring Unit (FMU) which is housed in the State Bank of Pakistan.	6	This new para is being added in the light of AML Act 2010 passed in March 2010.	
3	1.3 (Old- 1.2)	The Bank's Role in Preventing Money Laundering Since August 2001, when the SBP regulations on Anti Money Laundering took effect, all Pakistani Banks and DFIs providing financial services, have had to put procedures in place to prevent criminals from using them to launder their "dirty" money. Similar responsibilities are placed on banks all over the world.	7	This has become redundant due to inclusion of above mentioned paragraphs.	



4	Old-1.3	Purpose of This Handbook (This heading is being deleted and its contents are added in Section 1.1.	6	This has become redundant due to inclusion of above mentioned paragraphs.	
5	2.2	What Does This Mean in Practice? Time-lines for STR Reports to FMU will be mentioned.	10	An addition in Handbook to let users know the time lines of this regulatory requirement.	FMU Regulations 2008
6	3.1	Point (f) HR Accounts will be reviewed once a year and NR accounts once in three years	14	Change in internal policy	
7	4.2	<b>Knowing Your Customer means:</b> Designation of Branch Manager as responsible person for reviewing all the high risk accounts once a year and all the normal risk accounts once in three years	18	To Ensure abidance by policy it was necessary to give ownership.	
8	4.8 4.8.1	<b>4.8 CUSTOMER IDENTIFICATION - SPECIAL CIRCUMSTANCES</b>  <b>4.8.1 3<sup>RD</sup> PARTY MANDATE HOLDER(S)</b>  Addition of details of Mandate Holder (Power of Attorney).	29	These are mandatory additions in order to establish the group accounts.	
9	4.12	<b>Politically Exposed Persons (PEP)</b> The following procedure needs to be added besides a few changes for the explanation of the definition of PEP.  <u>PROCEDURE FOR Politically Exposed Persons (PEP)</u>  <b>Present Procedure</b>  The PEP accounts are opened with the permission of respective General Managers  <b>Proposed Procedure</b>  The field will forward the requests for opening of PEP accounts through their respective General Managers to CCG. GM will inform accordingly for name clearance for PEP and same will be carried out by CCG through Name-Filtering Solution and against existing Negative- / Watch-Lists and GM will then take business decision	32	PEP requires Enhanced Due Diligence (EDD) and use of Name-Filtering Solution which is not available with the business; therefore CCG will do the name clearance.	

		accordingly.			
<b>10</b>		Business accounts are to be opened on the strength of NTN No / BRN (Business Registration No.) and CNIC N0s.of all directors are to be entered in the core banking system.  Details of attorney holders are to be reported in the system.	<b>N-A</b>	This is necessitated in order to tag the business accounts on CNIC.  In order to ascertain the ownership of accounts having operated through attorneys.	
<b>11</b>		KYC Forms developed first time previous year now requires some further additions of fields such as “Source of Funds” for Business KYC Form. Amendment is required for “Accounts Opened First Time” which should fall under “Normal Risk” (NR) instead of “High Risk” (HR).	<b>N-A</b>	Updation/Additions/Deletions are required.	
<b>12</b>		Some nomenclature changes such as terminologies of RCO, Compliance & Controls Group instead of Compliance Group, etc needs to be changed.	<b>N-A</b>	This is due to merger of ICD in Compliance Group, changes in Bank’s organizational changes, etc.	
<b>13</b>	<b>9.6</b>	<b>HALF-YEARLY REVIEW OF CERTIFICATION FOR CDD / EDD – REVIEW OF ACCOUNTS</b>  Point No. 11 is being inserted as following:  “All Accounts opened during the year 2009 till date under High Risk (HR) category must be reviewed & proper EDD carried out.”	<b>86</b>	This is a new addition to ensure carrying out Enhanced Due Diligence (EDD) at branch level.	
<b>14</b>	<b>10.2</b>	Amendment in Regulation M-2 (Anti-Money Laundering Measures)  A new point is to be inserted as Point 7. “Bank shall not allow personal accounts to be used for business purposes except proprietorship, small businesses and professions where documents constitute are not available and banks are satisfied with KYC profile of the account holder, purpose of relationship and expected turn-over of the account keeping in view the financial status and nature of business of that customer.”	<b>94</b>	SBP has issued fresh directives as per BPRD Circular Letter No. 42 of 2009 dated December 31, 2009.	

