MANAGING CORE RISKS IN BANKING:

GUIDANCE NOTES ON PREVENTION OF MONEY LAUNDERING

BANGLADESH BANK

Focus Group on Prevention of Money Laundering

Coordinator

Md. Atiqur Rahman
Deputy General Manager
Anti-Money Laundering Department
Bangladesh Bank

Members

Chowdhury M.A.Q. Sarwar
Head of Compliance and Human Resources
Citibank N.A., Bangladesh

Iqbal U. Ahmed, Managing Director (CC)
Trust Bank Limited

Md. Anwar Hossain
Executive Vice President
Prime Bank Limited

Debasish Choudhury
Senior Principal Officer
Rupali Bank Limited

Md.Abdullah Al-Mamun
Manager
Compliance & Control
HSBC, Bangladesh

Table of Contents

CHAPTER I : BACKGROUND

Introduction..... 1
What is Money Laundering..... 2
Why Money Laundering is done..... 3
Why we must combat Money Laundering..... 4
Stages of Money Laundering..... 5
Vulnerability of the Financial System to Money Laundering..... 6
How Financial Institutions Can Combat Money Laundering..... 8
International Anti-Money Laundering Initiatives..... 8

CHAPTER II: WHAT THE LAW REQUIRES

Requirements under the Money Laundering Prevention Act 2002…….. 15
The Offence of Money Laundering…….. 15
Penalties for Money Laundering…….. 16
Responsibilities of Bangladesh Bank……... 17

CHAPTER III: ANTI MONEY LAUNDERING POLICY

Senior Management Commitment……... 18
Written Anti-Money Laundering Compliance Policy……. 18

CHAPTER IV: ORGANIZATIONAL STRUCTURE

Designation of Anti-Money Laundering Compliance Officers……... 20
Organization Structure……. 23

CHAPTER V : IDENTIFICATION PROCEDURES

Introduction…….. 26
Know Your Customer (KYC) Policies And Procedures……. 27
Customer Acceptance Policy……... 28
Customer Identification…… 28
What Constitutes a Person's Identity……... 29
Individual Customers……... 30
Persons without Standard Identification Documentation…… 32
Corporate Bodies and other Entities…… 32
Partnerships and Unincorporated Businesses…….. 34
Powers of Attorney/ Mandates to Operate Accounts…….. 34
Requirements in respect of Accounts Commenced Prior to 30 April 2002…… 34
Internet or Online Banking…….. 35
Provision of Safe Custody and Safety Deposit Boxes……. 36
Timing and Duration of Verification……... 36

CHAPTER VI: ANTI MONEY LAUNDERING PROCESSES

Know Your Customer Procedures……... 37
Risk categorization – Based on Activity/KYC Profile…… 38
Transaction Monitoring Process…….. 38
Suspicious Activity Reporting Process…… 39
Self-Assessment Process…….. 40
System of Independent Procedures Testing……. 40

CHAPTER VII: RECORD KEEPING

Statutory Requirements…… 41
Documents Verifying Evidence of Identity and Transaction Records……. 41
Formats and Retrieval of Records…… 42
Wire Transfer Transactions…….. 42
Investigations…… 43

Training Records…….. 43
CHAPTER VIII: RECOGNITION AND REPORTING OF SUSPICIOUS TRANSACTIONS
Recognition of Suspicious Transactions…….. 44
Reporting of Suspicious Transactions…….. 44
Internal Reporting Procedures and Records……. 46
Reporting Procedures……... 47
CHAPTER IX: TRAINING AND AWARENESS
Statutory Requirements…… 48
The Need for Staff Awareness……. 48
Education and Training Programs…… 48
New Employees…… 49
Customer Service/Relationship Managers/Tellers/Foreign Exchange Dealers…… 49
Processing (Back Office) Staff……. 49
Senior Management/Operations Supervisors and Managers…… 50
Anti Money Laundering Compliance Officer…….. 50
Refresher Training…… 50
ANNEXURES
Annexure A: Model Account Application Form for Individual Accounts…….. 51
Annexure B: Model Account Application Form for Corporate Accounts……... 54
Annexure C: Model Transaction Profile…….. 56
Annexure D: KYC Profile Form…….. 58
Annexure E: Identification of Directors & Authorized Signatories……. 64
Annexure F: Explanation to Walk-in / One-off Customers……. 65
Annexure G: Examples of Potentially Suspicious Transactions…….. 66
Annexure H: Internal Suspicious Activity Report Form……. 72
Annexure I: Internal Control Checklist…… 74
Annexure J: Money Laundering Prevention Act, 2002 (English version with amendment))…… 76
Annexure K: Money Laundering Prevention Act, 2003 (Bangla with amendment)…… 81

CHAPTER I: BACKGROUND

1.1 Introduction

1.1.1 These Guidance Notes have been prepared by the Focus Group on Prevention of Money Laundering, which was established under the aegis of the Bangladesh Bank to oversee the issue of guidelines to facilitate the implementation of the Prevention of Money Laundering Act 2002, the Rules and Directives of the Bangladesh Bank. These guidelines are recommendations as to good practice but do not constitute a legal interpretation of the Act. The Focus Group on Prevention of Money Laundering included representatives from Bangladesh Bank, nationalized commercial banks, private commercial banks and foreign banks operating in Bangladesh.

1.1.2 In recognition of the fact that financial institutions may be particularly vulnerable to being used by money launderers, Bangladesh Bank as part of its supervisory process, will assess the adequacy of procedures adopted to counter money laundering and the degree of compliance with such procedures.

1.1.3 These Guidance Notes are designed to assist *Banks and other Financial Institutions in* complying with the Bangladesh's money laundering regulations. The Central Bank intends to use these Guidance Notes as criteria against which it will assess the adequacy of the internal controls, policies and procedures to counter money laundering of institutions subject to its supervision.

1.1.4 It is recognized that *Banks and other Financial Institutions* may have systems and procedures in place which, whilst not identical to those outlined in these Guidance Notes, nevertheless impose controls and procedures which are at least equal to, if not higher than, those contained in these Guidance Notes. This will be taken into account by the Bangladesh Bank in the assessment of a *Banks and other Financial Institutions* systems and controls and compliance with the Regulations.

1.1.5 An overriding aim of the Money Laundering Regulations and these Guidance Notes is to ensure that appropriate identification information is obtained in relation to the customers of *Banks and other Financial Institutions* and the payments made between them. This is both to assist the detection of suspect transactions and to create an effective "audit trail" in the event of an investigation subsequently proving necessary.

1.1.6 In some respects, these Guidance Notes go beyond the requirements of the Money Laundering Regulations. Nonetheless, it is expected that all institutions conducting *relevant financial business* pay due regard to these Guidance Notes in developing responsible anti-money laundering procedures suitable to their situation. If a *Bank or other Financial Institution* appears not to be doing so then Bangladesh Bank may seek an explanation and may conclude that the *Bank or other Financial Institution* is carrying on business in a manner that may give rise to sanctions under the applicable legislation.

1.1.7 It is important that the management of *Banks and other Financial Institutions* view money-laundering prevention as part of their risk management strategies and not simply as a stand-alone requirement that is being imposed by the legislation. Money laundering prevention should not be viewed in isolation from an institution's other business systems and needs.

1.1.8 Throughout these Guidance Notes there is reference to an 'account' or 'accounts' and procedures to be adopted in relation to them. This is a matter of convenience and has been done for illustrative purposes. It is recognized that these references may not always be appropriate to all types of *relevant financial business* covered by the Regulations.

1.1.9 Where there are provisions in these guidelines relating to an account or accounts these will have relevance to mainstream banking activity but should, by analogy, be adapted appropriately to the situations covered by other relevant business. For example 'account' could refer to bank accounts, fixed deposits or other investment product, trusts or a business relationship etc.

1.2 What is Money Laundering?

1.2.1 A definition of what constitutes the offence of money laundering under Bangladesh law is set out in Section 2 (Tha) of the Prevention of Money Laundering Act 2002 (Act No. 7 of 2002) which is reads as follows: "Money Laundering means -
(Au) Properties acquired or earned directly or indirectly through illegal means;
(Aa) Illegal transfer, conversion, concealment of location or assistance in the above act of the properties acquired or earned directly of indirectly through legal or illegal means; "

1.2.3 Properties has been defined in section 2(Da) of the Act as "Properties means movable or immovable properties of any nature and description.

1.2.4 "The U.S. Customs Service, an arm of the Department of the Treasury, provides a lengthy definition of money laundering as "the process whereby proceeds, reasonably believed to have been derived from criminal activity, are transported, transferred, transformed, converted or intermingled with legitimate funds for the purpose of concealing or disguising the true nature, source, disposition, movement or ownership of those proceeds. The goal of the money-laundering process is to make funds derived from, or associated with, illicit activity appear legitimate."

1.2.5 Another definition of Money Laundering under U.S Law is, "… the involvement in any one transaction or series of transactions that assists a criminal in keeping, concealing or disposing of proceeds derived from illegal activities."

1.2.6 The EU defines it as "the conversion or transfer of property, knowing that such property is derived from serious crime, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in committing such an offence or offences to evade the legal consequences of his action, and the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from serious crime."

1.2.7 A concise working definition was adopted by Interpol General Secretariat Assembly in 1995, which defines money laundering as: "Any act or attempted act to conceal or disguise the identity of illegally obtained proceeds so that they appear to have originated from legitimate sources".

1.2.8 The Joint Money Laundering Sterling Group (JMLSG) of the U.K. defines it as "the process whereby criminals attempt to hide and disguise the true origin and ownership of the proceeds

of their criminal activities, thereby avoiding prosecutions, conviction and confiscation of their criminal funds".

1.2.9 In lay terms Money Laundering is most often described as the “turning of dirty or black money into clean or white money”. If undertaken successfully, money laundering allows criminals to legitimize "dirty" money by mingling it with "clean" money, ultimately providing a legitimate cover for the source of their income. Generally, the act of conversion and concealment is considered crucial to the laundering process.

1.3 Why Money Laundering is done?

Criminals engage in money laundering for three main reasons:

1.3.1 First, money represents the lifeblood of the organization that engages in criminal conduct for financial gain because it covers operating expenses, replenishes inventories, purchases the services of corrupt officials to escape detection and further the interests of the illegal enterprise, and pays for an extravagant lifestyle. To spend money in these ways, criminals must make the money they derived illegally appear legitimate.

1.3.2 Second, a trail of money from an offense to criminals can become incriminating evidence. Criminals must obscure or hide the source of their wealth or alternatively disguise ownership or control to ensure that illicit proceeds are not used to prosecute them.

1.3.3 Third, the proceeds from crime often become the target of investigation and seizure. To shield ill-gotten gains from suspicion and protect them from seizure, criminals must conceal their existence or, alternatively, make them look legitimate.

1.4 Why we must combat Money Laundering

1.4.1 Money laundering has potentially devastating economic, security, and social consequences. Money laundering is a process vital to making crime worthwhile. It provides the fuel for drug dealers, smugglers, terrorists, illegal arms dealers, corrupt public officials, and others to operate and expand their criminal enterprises. This drives up the cost of government due to the need for increased law enforcement and health care expenditures (for example, for treatment of drug addicts) to combat the serious consequences that result. Crime has become increasingly international in scope, and the financial aspects of crime have become more complex due to rapid advances in technology and the globalization of the financial services industry.

1.4.2 Money laundering diminishes government tax revenue and therefore indirectly harms honest taxpayers. It also makes government tax collection more difficult. This loss of revenue generally means higher tax rates than would normally be the case if the untaxed proceeds of crime were legitimate. We also pay more taxes for public works expenditures inflated by corruption. And those of us who pay taxes pay more because of those who evade taxes. So we all experience higher costs of living than we would if financial crime—including money laundering—were prevented.

1.4.3 Money laundering distorts asset and commodity prices and leads to misallocation of resources. For financial institutions it can lead to an unstable liability base and to unsound asset structures thereby creating risks of monetary instability and even systemic crises. The loss of credibility and investor confidence that such crises can bring has the potential of destabilizing financial systems, particularly in smaller economies.

1.4.4 One of the most serious microeconomic effects of money laundering is felt in the private sector. Money launderers often use front companies, which co-mingle the proceeds of illicit activity with legitimate funds, to hide the ill-gotten gains. These front companies have access to substantial illicit funds, allowing them to subsidize front company products and services at levels well below market rates. This makes it difficult, if not impossible, for legitimate business to compete against front companies with subsidized funding, a situation that can result in the crowding out of private sector business by criminal organizations.

1.4.5 No one knows exactly how much "dirty" money flows through the world's financial system every year, but the amounts involved are undoubtedly huge. The International Money Fund has estimated that the magnitude of money laundering is between 2 and 5 percent of world gross domestic product, or at least USD 800 billion to USD1.5 trillion. In some countries, these illicit proceeds dwarf government budgets, resulting in a loss of control of economic policy by governments. Indeed, in some cases, the sheer magnitude of the accumulated asset base of laundered proceeds can be used to corner markets -- or even small economies.

1.4.6 Among its other negative socioeconomic effects, money laundering transfers economic power from the market, government, and citizens to criminals. Furthermore, the sheer magnitude of the economic power that accrues to criminals from money laundering has a corrupting effect on all elements of society.

1.4.7 The social and political costs of laundered money are also serious as laundered money may be used to corrupt national institutions. Bribing of officials and governments undermines the moral fabric in society, and, by weakening collective ethical standards, corrupts our democratic institutions. When money laundering goes unchecked, it encourages the underlying criminal activity from which such money is generated.

1.4.8 Nations cannot afford to have their reputations and financial institutions tarnished by an association with money laundering, especially in today's global economy. Money laundering erodes confidence in financial institutions and the underlying criminal activity -- fraud, counterfeiting, narcotics trafficking, and corruption -- weaken the reputation and standing of any financial institution. Actions by banks to prevent money laundering are not only a regulatory requirement, but also an act of self-interest. A bank tainted by money laundering accusations from regulators, law enforcement agencies, or the press risk likely prosecution, the loss of their good market reputation, and damaging the reputation of the country. It is very difficult and requires significant resources to rectify a problem that could be prevented with proper anti-money-laundering controls.

1.4.9 It is generally recognized that effective efforts to combat money laundering cannot be carried out without the co-operation of financial institutions, their supervisory authorities and the law enforcement agencies. Accordingly, in order to address the concerns and obligations of these three parties, these Guidance Notes were drawn up.

1.5 Stages of Money Laundering

1.5.1 There is no single method of laundering money. Methods can range from the purchase and resale of a luxury item (e.g. a house, car or jewellery) to passing money through a complex international web of legitimate businesses and 'shell' companies (i.e. those companies that primarily exist only as named legal entities without any trading or business activities). There are a number of crimes where the initial proceeds usually take the form of cash that needs to enter the financial system by some means. Bribery, extortion, robbery and street level purchases of drugs are almost always made with cash. This has a need to enter the financial system by some means so that it can be converted into a form which can be more easily transformed, concealed or transported. The methods of achieving this are limited only by the ingenuity of the launderer and these methods have become increasingly sophisticated.

1.5.2 Despite the variety of methods employed, the laundering is not a single act but a process accomplished in 3 basic stages which may comprise numerous transactions by the launderers that could alert a financial institution to criminal activity -

Placement - the physical disposal of the initial proceeds derived from illegal activity.

Layering - separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity.

Integration - the provision of apparent legitimacy to wealth derived criminally. If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing as normal business funds.

1.5.3 The three basic steps may occur as separate and distinct phases. They may also occur simultaneously or, more commonly, may overlap. How the basic steps are used depends on the available laundering mechanisms and the requirements of the criminal organisations. The table below provides some typical examples.

Placement stage	**Layering stage**	**Integration stage**
Cash paid into bank (sometimes with staff complicity or mixed with proceeds of legitimate business).	Sale or switch to other forms of investment.	Redemption of contract or switch to other forms of investment.
Cash exported.	Money transferred to assets of legitimate financial institutions.	False loan repayments or forged invoices used as cover for laundered money.
Cash used to buy high value goods, property or business assets.	Telegraphic transfers (often using fictitious names or funds disguised as proceeds of legitimate business).	Complex web of transfers (both domestic and international) makes tracing original source of funds virtually impossible.
Cash purchase of single premium life insurance or other investment.	Cash deposited in outstation branches and even overseas banking system.	

	Resale of goods/assets.	

1.6 Vulnerability of the Financial System to Money Laundering

1.6.1 Money laundering is often thought to be associated solely with banks and moneychangers. All financial institutions, both banks and non-banks, are susceptible to money laundering activities. Whilst the traditional banking processes of deposit taking, money transfer systems and lending do offer a vital laundering mechanism, particularly in the initial conversion from cash, it should be recognised that products and services offered by other types of financial and non-financial sector businesses are also attractive to the launderer. The sophisticated launderer often involves many other unwitting accomplices such as currency exchange houses, stock brokerage houses, gold dealers, real estate dealers, insurance companies, trading companies and others selling high value commodities and luxury goods.

1.6.2 Certain points of vulnerability have been identified in the laundering process, which the money launderer finds difficult to avoid, and where his activities are therefore more susceptible to being recognized. These are:

- entry of cash into the financial system;
- cross-border flows of cash; and
- Transfers within and from the financial system.

1.6.3 Financial institutions should consider the money laundering risks posed by the products and services they offer, particularly where there is no face-to-face contact with the customer, and devise their procedures with due regard to that risk.

1.6.4 Although it may not appear obvious that the products might be used for money laundering purposes, vigilance is necessary throughout the financial system to ensure that weaknesses cannot be exploited.

1.6.5 *Banks and other Financial Institutions* conducting relevant financial business in liquid products are clearly most vulnerable to use by money launderers, particularly where they are of high value. The liquidity of some products may attract money launderers since it allows them quickly and easily to move their money from one product to another, mixing lawful and illicit proceeds and integrating them into the legitimate economy.

1.6.6 All banks and non-banking financial institutions, as providers of a wide range of money transmission and lending services, are vulnerable to being used in the layering and integration stages of money laundering as well as the placement stage.

1.6.7 Electronic funds transfer systems increase the vulnerability by enabling the cash deposits to be switched rapidly between accounts in different names and different jurisdictions.

1.6.8 However, in addition, banks and non-banking financial institutions, as providers of a wide range of services, are vulnerable to being used in the layering and integration stages. Other loan accounts may be used as part of this process to create complex layers of transactions.

1.6.9 Some banks and non-banking financial institutions may additionally be susceptible to the attention of the more sophisticated criminal organizations and their "professional money launderers". Such organizations, possibly under the disguise of front companies and nominees, may create large scale but false international trading activities in order to move their illicit monies from one country to another. They may create the illusion of international trade using false/inflated invoices to generate apparently legitimate international wire transfers, and may use falsified/bogus letters of credit to confuse the trail further. Many of the front companies may even approach their bankers for credit to find the business activity. Banks and non-banking financial institutions offering international trade services should be on their guard for laundering by these means.

1.6.10 Investment and merchant banking businesses are less likely than banks and money changers to be at risk during the initial placement stage.

1.6.11 Investment and merchant banking businesses are more likely to find them being used at the layering and integration stages of money laundering. The liquidity of many investment products particularly attracts sophisticated money laundering since it allows them quickly and easily to move their money from one product to another, mixing lawful and illicit proceeds and integrating them into the legitimate economy.

1.6.12 Although it may not appear obvious that insurance and retail investment products might be used for money laundering purposes, vigilance is necessary throughout the financial system to ensure that non traditional banking products and services are not exploited.

1.6.13 Intermediaries and product providers who deal direct with the public may be used at the initial placement stage of money laundering, particularly if they receive cash. Premiums on insurance policies may be paid in cash, with the policy subsequently being cancelled in order to obtain a return of premium (e.g. by cheque), or an insured event may occur resulting in a claim being paid out. Retail investment products are, however, more likely to be used at the layering and integration stages. The liquidity of a mutual funds may attract money launderers since it allows them quickly and easily to move their money from one product to another, mixing lawful and illicit proceeds and integrating them into the legitimate economy.

1.6.14 Lump sum investments in liquid products are clearly most vulnerable to use by money launderers, particularly where they are of high value. Payment in cash should merit further investigation, particularly where it cannot be supported by evidence of a cash-based business as the source of funds.

1.6.15 Insurance and investment product providers and intermediaries should therefore keep transaction records that are comprehensive enough to establish an audit trail. Such records can also provide useful information on the people and organizations involved in laundering schemes.

1.6.16 Corporate vehicles trust structures and nominees are firm favorites with money launderers as a method of layering their proceeds. Providers of these services can find themselves much in demand from criminals.

1.6.17 The facility with which currency exchanges can be effected through a bureau is of particular attraction especially when such changes are effected in favor of a cheque or gold bullion.

1.7 How Financial Institutions Can Combat Money Laundering

1.7.1 The prevention of laundering the proceeds of crime has become a major priority for all jurisdictions from which financial activities are carried out. One of the best methods of preventing and deterring money laundering is a sound knowledge of a customer's business and pattern of financial transactions and commitments. The adoption of procedures by which Banks and other Financial Institutions "know their customer" is not only a principle of good business but is also an essential tool to avoid involvement in money laundering. For the purposes of these guidance notes the term Banks and other Financial Institutions refer to businesses carrying on relevant financial business as defined under the legislation.

1.7.2 Thus efforts to combat money laundering largely focus on those points in the process where the launderer's activities are more susceptible to recognition and have therefore to a large extent concentrated on the deposit taking procedures of banks i.e. the placement stage.

1.7.3 Institutions and intermediaries must keep transaction records that are comprehensive enough to establish an audit trail. Such records can also provide useful information on the people and organizations involved in laundering schemes.

1.7.4 In complying with the requirements of the Act and in following these Guidance Notes, financial institutions should at all times pay particular attention to the fundamental principle of good business practice - 'know your customer'. Having a sound knowledge of a customer's business and pattern of financial transactions and commitments is one of the best methods by which financial institutions and their staff will recognize attempts at money laundering. This aspect is referred to in Chapter VIII of these Guidance Notes - Recognition and Reporting of Suspicious Transactions. It will also be dealt with in staff training programs which are a fundamental part of the procedures designed to recognize and combat money laundering and which are referred to in Chapter IX – Training and Awareness.

1.8 International Anti-Money Laundering Initiatives

1.8.1. Money laundering has become a global problem as a result of the confluence of several remarkable changes in world markets (i.e., the globalization of markets). The growth in international trade, the expansion of the global financial system, the lowering of barriers to international travel, and the surge in the internationalization of organized crime have combined to provide the source, opportunity, and means for converting illegal proceeds into what appears to be legitimate funds.

1.8.2. In 1986, the U.S. became the first country in the world to criminalize the "laundering" of the proceeds of criminal activity with the enactment of the Money Laundering Control Act of 1986. Since enacting the law, the U.S. Congress has increased its coverage, reach and scope, making it the broadest, strongest and most far-reaching money laundering law in the world.

1.8.3. The U.S. law is a weapon of enormous breadth and power wielded by U.S. prosecutors in that country. Those convicted under the law face a maximum prison term of 20 years and a fine of $500,000 per violation. A legal entity such as a bank or business that is convicted under the law faces fines and forfeitures. In addition, a bank that is convicted of money laundering can lose its charter and federal deposit insurance. Persons and entities also face civil money penalties

1.8.4. Concerted efforts by governments to fight money laundering have been going on for the past fifteen years. The main international agreements addressing money laundering are the 1988 United Nations Vienna Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (the Vienna Convention) and the 1990 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds of Crime. And the role of financial institutions in preventing and detecting money laundering has been the subject of pronouncements by the Basle Committee on Banking Supervision, the European Union, and the International Organization of Securities Commissions.

1.8.5. The Vienna Convention, adopted in December 1988, laid the groundwork for efforts to combat money laundering by creating an obligation for signatory states (including Bangladesh) to criminalize the laundering of money from drug trafficking. It promotes international cooperation in investigations and makes extradition between signatory states applicable to money laundering. It also establishes the principle that domestic bank secrecy provisions should not interfere with international criminal investigations.

1.8.6. During the past twenty years there have been a number of resolutions passed by the ICPO-Interpol General Assembly, which have called on member countries to concentrate their investigative resources in identifying, tracing and seizing the assets of criminal enterprises. These resolutions have also called on member countries to increase the exchange of information in this field and encourage governments to adopt laws and regulations that would allow access, by police, to financial records of criminal organizations and the confiscation of proceeds gained by criminal activity.

1.8.7. In December 1988, the G-10's Basle Committee on Banking Supervision issued a "statement of principles" with which the international banks of member states are expected to comply. These principles cover identifying customers, avoiding suspicious transactions, and cooperating with law enforcement agencies. In issuing these principles, the committee noted the risk to public confidence in banks, and thus to their stability, that can arise if they inadvertently become associated with money laundering.

1.8.8. Over the past few years, the Basle Committee has moved more aggressively to promote sound supervisory standards worldwide. In close collaboration with many non-G-10 supervisory authorities, the Committee in 1997 developed a set of "*Core Principles for Effective Banking Supervision*". Many important guidelines issued by Basle Committee for worldwide implementation for all banks among which, "*Prevention of the Criminal Use of the Banking System for the Purpose of Money Laundering*", December 1988 "*Customer Due Diligence for Banks*", October 2001"*Sound Practices for the Management and Supervision of Operational Risk*", February 2003; *Shell banks and booking offices*", January 2003; relate to money laundering controls.

1.8.9. In 1989, the G-7 countries recognized that money laundering had become a global problem, not least due to the increase in drug trafficking. The G-7 Summit in Paris in 1989 took a great step forward in combating international money laundering with the creation of the Financial Action Task Force (FATF) to develop a coordinated international response to mounting concern over money laundering. One of the first tasks of the FATF was to develop steps national governments should take to implement effective anti-money laundering programs.

1.8.10. The experts within FATF came up with a list of 40 Recommendations, built on the firm foundations of the 1988 UN Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances and the Statement of Principles of the Basle Committee on Banking Regulations.

1.8.11. The FATF 40 Recommendations set out the basic framework on what countries need to do -- in terms of laws, regulations and enforcement -- to combat money laundering effectively and were designed with universal application in mind. Over time, they have been revised to reflect new developments in money laundering and experience. The 40 Recommendations have now become the global blueprint in anti-money laundering best practice and set the international standards for money laundering controls. Setting those standards meant that all participating governments committed to moving in the same direction at the same pace, a requirement for success. Through FATF's peer-review process, the participants have pushed each other into implementing the standards. Even the IMF regards the anti-money laundering actions advocated by the FATF as crucial for the smooth functioning of financial markets.

1.8.12. In joining FATF, every member nation makes a political commitment to adopt the recommendations and allows itself to be evaluated by the other member nations on whether it has fulfilled that commitment. Today FATF has grown to an organization of thirty-one member countries and has representatives from the Gulf Cooperation Council and the European Commission. Participants include representatives from members' financial regulatory authorities, law enforcement agencies, and ministries of finance, justice, and external affairs. Representatives of international and regional organizations concerned with combating money laundering also attend FATF meetings as observers. This top-down, cooperative approach has been greatly successful in encouraging FATF member nations to improve their money laundering regimes.

1.8.13. With expanded membership, FATF has now achieved agreement on money laundering standards and implementation among 31 governments. More than that, FATF has encouraged development of regional groups to adhere to the same standards. By the last count, about 130 jurisdictions -- representing about 85 percent of world population and about 90 to 95 percent of global economic output -- have made political commitments to implementing "The Forty Recommendations."

1.8.14. Another, more controversial initiative that FATF has developed to enhance international cooperation is publication of a list of non-cooperative countries and territories (NCCT) -- jurisdictions that lack a commitment to fight money laundering. Following the June 2000 publication of the first such list, a number of the 15 NCCT jurisdictions have acted quickly to implement FATF standards.

1.8.15. Other UN initiatives, such as the 2000 UN Convention against Transnational Organized Crime, have assisted in complementing the work undertaken by the FATF. However, it was the FATF's exercise on Non-Cooperating Countries and Territories which brought about a sea change in thinking at the highest political levels. The exercise, which identifies and evaluates the legal, judicial and regulatory framework of countries whose regulatory systems do not appear to meet international standards, has been a success, despite its unpopularity in many quarters.

1.8.16. After 11 September 2001, the tragedy in New York highlighted to all civilized nations the need to look at the finances of terrorists and the methods used to transfer funds around the

world. The FATF expanded its mission beyond money laundering and agreed to focus its expertise on the worldwide effort to combat terrorist financing.

1.8.17. The FATF, at its Washington meeting in October 2001, came up with 8 Special Recommendations to tackle this threat. Terrorists use similar systems to money launderers and the 8 Special Recommendations complement the 40 existing Recommendations.

1.8.18. The United Kingdom was one of the first countries in the world to have signed and ratified the UN International Convention on the Suppression of the Financing of Terrorists through the Terrorism Act 2000. In fact the UK was unique in meeting the requirements of all 8 FATF Special Recommendations immediately.

1.8.19. Several regional or international bodies such as the APG (Asia/Pacific Group on Money Laundering), CFATF (Caribbean Financial Action Task Force), the ESAAMLG (Eastern and Southern Africa Anti-Money Laundering Group), GAFISUD (Financial Action Task Force for South America), the MONEYVAL Committee of the Council of Europe (the Select Committee of experts on the evaluation of anti-money laundering measures) and the OGBS (Offshore Group of Banking Supervisors), either exclusively or as part of their work, perform similar tasks for their members as the FATF does for its own membership. Bangladesh is a member of APG.

1.8.20. This co-operation forms a critical part of the FATF's strategy to ensure that all countries in the world implement effective counter-measures against money laundering. Thus the APG, the CFATF, GAFISUD, the MONEYVAL Committee and OGBS carry out mutual evaluations for their members, which assess the progress they have made in implementing the necessary anti-money laundering measures. In the same vein, APG, CFATF and the MONEYVAL also review regional money laundering trends.

1.8.21. During the past decade, a number of countries have created specialized government agencies as part of their systems for dealing with the problem of money laundering. These entities are commonly referred to as "Financial Intelligence Units" or "FIUs". These units increasingly serve as the focal point for national anti-money laundering programs because they provide the possibility of rapidly exchanging information (between financial institutions and law enforcement / prosecutorial authorities, as well as between jurisdictions), while protecting the interests of the innocent individuals contained in their data.

1.8.22. Since 1995, another forum for international cooperation has developed among a number of national financial intelligence units (FIUs), who began working together in an informal organization known as the Egmont Group (named for the location of the first meeting in the Egmont-Arenberg Palace in Brussels). The goal of the group is to provide a forum for FIUs to improve support to their respective national anti-money laundering programs. This support includes expanding and systematizing the exchange of financial intelligence, improving expertise and capabilities of the personnel of such organizations, and fostering better communication among FIUs through the application of new technologies. The Egmont Secretariat, currently hosted by the UK, is the ideal vehicle for FIUs from various countries to talk to one another once they reach the required standard.

1.8.23. Financial Crimes Enforcement Network (FinCEN), the U.S. financial intelligence unit led by the Department of the Treasury, provides training and technical assistance to a broad spectrum of foreign government officials, financial regulators, law enforcement personnel,

and bankers. This training covers a variety of topics, including money laundering typologies, the creation and operation of FIUs, the establishment of comprehensive anti-money-laundering regimes, computer systems architecture and operations, and country-specific anti-money-laundering regimes and regulations. FinCEN also works closely with the informal Egmont Group of more than 50 FIUs to assist various jurisdictions in establishing and operating their own FIUs.

1.8.24. Additionally, FinCEN has provided FIU and money laundering briefings and training in many jurisdictions, including Argentina, Armenia, Australia, the Bahamas, Brazil, Canada, China, Costa Rica, Dominican Republic, El Salvador, Germany, Greece, Hong Kong, India, Indonesia, Isle of Man, Jamaica, Jersey, Kazakhstan, Lebanon, Italy, Liechtenstein, Nauru, Nigeria, Netherlands, Palau, Paraguay, Russia, Seychelles, South Africa, Switzerland, St. Vincent and the Grenadines, Taiwan, Tanzania, Thailand, Tonga, and the United Kingdom. FinCEN has also conducted personnel exchanges with the Korean and Belgian FIUs.

1.8.25. The U.S. Department of State's Bureau for International Narcotics and Law Enforcement Affairs (INL) develops assistance programs to combat global money laundering. INL participates in and supports international anti-money-laundering bodies and provides policy recommendations regarding international money laundering activities.

1.8.26. The U.S. State Department has developed a programmatic approach to assist jurisdictions in developing anti-money-laundering regimes to protect their economies and governments from abuse by financial criminals and stem the growth of international money laundering. This approach integrates training, technical assistance, and money laundering assessments on specific money laundering problems or deficiencies to achieve concrete, operational, institution-building objectives.

1.8.27. The International Organization of Securities Commissions (IOSCO) adopted, in October 1992, a report and resolution encouraging its members to take necessary steps to combat money laundering in securities and futures markets. A working group of IOSCO's Consultative Committee has been set up to collect information from IOSCO members' self-regulatory organizations and exchanges on their efforts to encourage their own members to fight money laundering.

1.8.28. Other international instruments such as the Council of Europe's 1990 Convention on Laundering, Search, Seizure and Confiscation of the Proceeds of Crime, which is open for signature by non-Council of Europe members, has been another useful method by which countries have attracted the expertise of the international community to join in and help countries to identify and rectify the imbalances within their systems. It established a common criminal policy on money laundering. It adopted a common definition of money laundering and common measures for dealing with it. The convention laid down the principles for international cooperation among the contracting parties, which may include states outside the Council of Europe.

1.8.29. In June 1991, the Council of the European Communities adopted a directive on the "Prevention of the Use of the Financial System for the Purpose of Money Laundering." This directive was issued in response to the new opportunities for money laundering opened up by the liberalization of capital movements and cross-border financial services in the European Union. The directive obligates member states to outlaw money laundering. They must require financial institutions to establish and maintain internal systems to prevent laundering, to

obtain the identification of customers with whom they enter into transactions of more than ECU 15,000, and to keep proper records for at least five years. Member states must also require financial institutions to report suspicious transactions and must ensure that such reporting does not result in liability for the institution or its employees.

1.8.30. In March 2000 the US. Department of Treasury unveiled the National Money Laundering Strategy for 2000, the most comprehensive plan ever put forth on the subject. It included literally scores of specific action items to combat money laundering. For each item, goals for the year are laid out and specific government officials are listed who are personally responsible for meeting those goals.

1.8.31. The National Money Laundering Strategy for 2002 identified four critical fronts for efforts to combat money laundering: to attack financing networks of terrorist entities; focus attention on the use of charities and other NGOs to raise, collect, and distribute funds to terrorist groups; establish an interagency targeting team to help focus efforts and resources against the most significant money laundering organizations and systems; and work with the international financial institutions to improve and monitor anti-money laundering compliance efforts throughout the world..

1.8.32. The IMF is contributing to the FATF's efforts in several important ways, consistent with its core areas of competence. As a collaborative institution with near universal membership, the IMF is a natural forum for sharing information, developing common approaches to issues, and promoting desirable policies and standards-all of which is critical in the fight against money laundering and the financing of terrorism. In addition, the Fund has expertise based on its broad experience in conducting financial sector assessments, providing technical assistance in the financial sector, and exercising surveillance over member's exchange systems.

1.8.33. After 11 September 2001 the IMF identified new ways to advance its contribution to international efforts to combat money laundering and the financing of terrorism.

1.8.34. In October 2002 a group of the world's largest banks jointly with Transparency International (TI), the global anti-corruption organization, drew up a set of global anti-money laundering guidelines for international private banks. The new guidelines were formulated in working sessions held in Wolfsberg, Switzerland, and, accordingly the new guidelines came to be known as the "Wolfsberg Anti-Money Laundering Principles" which declared, “Bank policy will be to prevent the use of its world-wide operations for criminal purposes. The bank will endeavor to accept only those clients whose source of wealth and funds can be reasonably established to be legitimate."

1.8.35. The principles represent the Wolfsberg Group’s effort to establish anti-money laundering guidelines that were viewed as appropriate when dealing with clients in the global marketplace. The principles dealt with diverse aspects of "know your customer" policies that pertain to relationships between high net worth individuals and the private banking departments of financial institutions. They also dealt with the identification and follow-up of unusual or suspicious activities.

1.8.36. The participating institutions of the Wolfsberg Group were ABN AMRO Bank, Barclays Bank, Banco Santander Central Hispano, S.A., The Chase Manhattan Private Bank, Citibank, N.A., Credit Suisse Group, Deutsche Bank AG, HSBC, J.P. Morgan, Inc., Société Générale, and UBS AG.

1.8.37. In support of efforts to suppress the financing of terrorism the Wolfsberg Group together with Transparency International held a meeting at Wolfsberg from January 9 - 11, 2002 attended by key regulators of the financial industry, representatives of national law enforcement and judicial agencies and international organizations who contributed to the discussions and welcomed the initiative taken by the Wolfsberg Group.

1.8.38. The meeting issued a Statement describing the role that financial institutions could play in the fight against terrorism which presented new challenges as funds used in the financing of terrorism do not necessarily derive from criminal activity, which is a requisite element of most existing money laundering offences. Successful participation in this fight by the financial sector requires global cooperation by governments with the financial institutions to an unprecedented degree.

1.8.39. The provision of official lists of suspected terrorists and terrorist organizations on a globally coordinated basis by the relevant competent authority in each jurisdiction providing appropriate details and information had been identified as a crucial element in the Statement.

CHAPTER II: WHAT THE LAW REQUIRES

2.1 Requirements under the Money Laundering Prevention Act 2002

2.1.1 The legislation specifically relating to money laundering is contained in the Money Laundering Prevention Act 2002 (Act No. 7 of 2002) the provisions of which supercedes whatever may contain in any other Act in force in Bangladesh. So far as financial service providers are concerned, the Act:

- defines the circumstances, which constitute the offence of money laundering and provides penalties for the commission of the offence (See Section 2 Tha of the Act),

- requires banks, financial institutions and other institutions engaged in financial activities to establish the identity of their customers (See Section 19 Ka of the Act),

- requires banks, financial institutions and other institutions engaged in financial activities to retain correct and full information used to identify their customers and transaction records at least for five years after termination of relationships with the customers (See Section 19 Ka of the Act), and

- imposes an obligation on banks, financial institutions and other institutions engaged in financial activities and their employees to make a report to the Bangladesh Bank where:

- they suspect that a money laundering offence has been or is being committed (See Section 19 Ga of the Act) and;

- provide customer identification and transaction records to Bangladesh Bank from time to time on demand (See Section 19 Kha of the Act).

2.2 The Offence of Money Laundering

The money laundering offences are, in summary:

2.2.1 It is an offence for any person to obtain, retain, transfer, remit, conceal or invest moveable or immovable property acquired directly or indirectly through illegal means. (See Section 2 Tha). Concealing or disguising the property includes concealing or disguising its nature, source, location, disposition, movement, ownership or any rights with respect to it.

2.2.2 It is an offence for any person to illegally conceal, retain transfer, remit, or invest moveable or immovable property even when it is earned through perfectly legitimate means. (See Section 2 Tha). It is a defense if the person concerned can prove that the offence was committed without his knowledge or it has occurred despite his despite his best efforts to prevent it. (See Section 20 (1) of the Act).

2.2.3 It is also an offence for any individual or entity to provide assistance to a criminal to obtain, retain, transfer, remit, conceal or invest moveable or immovable property if that person knows or suspects that those properties are the proceeds of criminal conduct.

2.2.4 It is an offence for banks, financial institutions and other institutions engaged in financial activities not to retain identification and transaction records of their customers.

2.2.5 It is an offence for banks, financial institutions and other institutions engaged in financial activities not to report the knowledge or suspicion of money laundering to Bangladesh Bank as soon as it is reasonably practicable after the information came to light.

2.2.6 It is also an offence for anyone to prejudice an investigation by informing i.e. tipping off the person who is the subject of a suspicion, or any third party, that a report has been made, or that the authorities are acting, or are proposing to act, in connection with an investigation into money laundering. Preliminary enquiries of a customer to verify identity or to ascertain the source of funds or the precise nature of the transaction being undertaken will not trigger a tipping off offence before a suspicions report has been submitted in respect of that customer unless the enquirer knows that an investigation is underway or that the enquiries are likely to prejudice an investigation. Where it is known or suspected that a suspicions report has already been disclosed to the authorities and it becomes necessary to make further enquiries, great care should be taken to ensure that customers do not become aware that their names have been brought to the attention of the law enforcement agencies.

2.2.7 It is an offence for any person to violate any freezing order issued by the Court on the basis of application made by Bangladesh Bank.

2.2.8 It is an offence for any person to express unwillingness, without reasonable grounds to assist any enquiry officer in connection with an investigation into money laundering.

2.3 Penalties for Money Laundering

All offences under the Act are non-bailable and the penalties for the commission of the offences all have prison terms and/or fines as prescribed in the Act as follows:

2.3.1 The offence of money laundering is punishable by terms of a minimum imprisonment for six months and a maximum of up to seven years plus a fine amounting to double the money laundered (See Section 13 of the Act).

2.3.2 The punishment for violation of Seizure Orders is a minimum imprisonment for one year or a fine of at least Taka ten thousand, or both. (See Section 14 of the Act).

2.3.3 The punishment for violation of Freezing Orders is a minimum imprisonment for one year or a fine of at least Taka five thousand, or both. (See Section 15 of the Act).

2.3.4 The offence of divulging information by informing i.e. tipping off the person who is the subject of a suspicion, or any third party is punishable by a minimum imprisonment for one year or a fine of at least Taka ten thousand, or both. (See Section 14 of the Act).

2.3.5 The offence of obstructing investigations or failure to assist any enquiry officer in connection with an investigation into money laundering is punishable by a minimum imprisonment for one year or a fine of at least Taka ten thousand, or both. (See Section 17 of the Act).

2.3.6 If any bank, financial institution and other institutions engaged in financial activities fail to retain customer identification and transaction records or fail to furnish required information as per the Act, Bangladesh Bank will report such failure to the licensing authority of the defaulting institution so that the concerned authority can take proper action for such negligence and failure (See Section 19 (3) of the Act)

2.3.7 Bangladesh Bank is empowered to impose fines of not less than Taka ten thousand and not more than Taka one lac on any bank, financial institution and other institutions engaged in financial activities for the failure or negligence to retain customer identification and transaction records or fail to furnish required information to Bangladesh Bank (See Section 19 (4) of the Act)

2.3.8 If any Company, Partnership Firm, Society, or Association violates any provisions of the Act, it will be deemed that every owner, partner, directors, employees and officers have individually violated such provisions.

2.4 Responsibilities of Bangladesh Bank

The Act gives Bangladesh Bank broad responsibility for prevention of money laundering and wide-ranging powers to take adequate measures to prevent money laundering, facilitate its detection, monitor its incidence, enforce rules and to act as the prosecuting agency for breaches of the Act. The responsibilities and powers of Bangladesh Bank are, in summary (See Section 4 and 5 of the Act):

2.4.1 To investigate into all money-laundering offences.

2.4.2 Supervise and monitor the activities of banks, financial institutions and other institutions engaged in financial activities.

2.4.3 Call for reports relating to money laundering from banks, financial institutions and other institutions engaged in financial activities, analyze such reports and take appropriate actions.

2.4.4 Provide training to employees of banks, financial institutions and other institutions engaged in financial activities on prevention of money laundering.

2.4.5 To authorize any person to enter into any premises for conducting investigations into money laundering offences.

2.4.6 Persons authorized by Bangladesh Bank to investigate offences can exercise the same powers as the Officer in Charge of Police Station can exercise under the Code of Criminal Procedure.

2.4.7 To do all other acts in attaining the objectives of the Act.

2.4.8 The Courts will not accept any offence under the Act for trial unless a complaint is lodged by Bangladesh Bank or any person authorized by Bangladesh Bank in this behalf.

CHAPTER III: ANTI MONEY LAUNDERING POLICY

3.1 Senior Management Commitment

3.1.1 The most important element of a successful anti-money-laundering program is the commitment of senior management, including the chief executive officer and the board of directors, to the development and enforcement of the anti-money-laundering objectives which can deter criminals from using their facilities for money laundering, thus ensuring that they comply with their obligations under the law.

3.1.2 Senior management must send the signal that the corporate culture is as concerned about its reputation as it is about profits, marketing, and customer service. As part of its anti- money laundering policy an institution should communicate clearly to all employees on an annual basis a statement from the chief executive officer that clearly sets forth its policy against money laundering and any activity which facilitates money laundering or the funding of terrorist or criminal activities. Such a statement should evidence the strong commitment of the institution and its senior management to comply with all laws and regulations designed to combat money laundering.

3.1.3 The statement of compliance policy should at a minimum include:

- A statement that all employees are required to comply with applicable laws and regulations and corporate ethical standards.
- A statement that all activities carried on by the financial institution must comply with applicable governing laws and regulations.
- A statement that complying with rules and regulations is the responsibility of each individual in the financial institution in the normal course of their assignments. It is the responsibility of the individual to become familiar with the rules and regulations that relate to his or her assignment. Ignorance of the rules and regulations is no excuse for non-compliance.
- The statement should direct staff to a compliance officer or other knowledgeable individuals when there is a question regarding compliance matters.
- A statement that employees will be held accountable for carrying out their compliance responsibilities.

3.2. Written Anti-Money Laundering Compliance Policy

3.2.1 At a minimum, the board of directors of each bank and other financial institution must develop, administer, and maintain an anti-money-laundering compliance policy that ensures and monitors compliance with the Act, including record keeping and reporting requirements. Such a compliance policy must be written, approved by the board of directors, and noted as such in the board meeting minutes.

3.2.2 The written anti-money-laundering compliance policy at a minimum should establish clear responsibilities and accountabilities within their organizations to ensure that policies, procedures, and controls are introduced and maintained which can deter criminals from using their facilities for money laundering and the financing of terrorist activities, thus ensuring that they comply with their obligations under the law.

3.2.3 The Policies should be tailored to the institution and would have to be based upon an assessment of the money laundering risks, taking into account the Financial institution's business structure and factors such as its size, location, activities, methods of payment, and risks or vulnerabilities to money laundering.

3.2.4 It should include standards and procedures to comply with applicable laws and regulations to reduce the prospect of criminal abuse. Procedures should address its Know Your Customer ("KYC") policy and identification procedures before opening new accounts, monitoring existing accounts for unusual or suspicious activities, information flows, reporting suspicious transactions, hiring and training employees and a separate audit or internal control function to regularly test the program's effectiveness.

3.2.5 It should also include a description of the roles the Anti-Money Laundering Compliance Officers(s)/Unit and other appropriate personnel will play in monitoring compliance with and effectiveness of money laundering policies and procedures.

3.2.6 The anti-money laundering policies should be reviewed regularly and updated as necessary and at least annually based on any legal/regulatory or business/ operational changes, such as additions or amendments to existing anti-money laundering rules and regulations or business.

3.2.7 In addition the policy should emphasize the responsibility of every employee to protect the institution from exploitation by money launderers, and should set forth the consequence of non-compliance with the applicable laws and the institution's policy, including the criminal, civil and disciplinary penalties and reputational harm that could ensue from any association with money laundering activity.

CHAPTER IV: ORGANIZATIONAL STRUCTURE

4.1 Designation of Anti-Money Laundering Compliance Officers (AMLCO)

4.1.1 All financial institutions must designate a Chief Anti-Money Laundering Compliance Officer (CAMLCO) at its head office who has sufficient authority to implement and enforce corporate-wide anti-money laundering policies, procedures and measures and who will report directly to senior management and the board of directors. This provides evidence of senior management's commitment to efforts to combat money laundering and, more importantly, provides added assurance that the officer will have sufficient clout to investigate potentially suspicious activities.

4.1.2 The position within the organization of the person appointed as CAMLCO will vary according to the size of the financial institution and the nature of its business, but he or she should be sufficiently senior to command the necessary authority. Each financial institution should prepare a detailed specification of the role and obligations of the CAMLCO. Larger financial institutions may choose to appoint a senior member of their compliance, internal audit or inspection departments. In small institutions it may be appropriate to designate the Head of Operations.

4.1.3 The CAMLCO may effect his or her responsibilities through a specific department, unit, group, or committee. Depending on the size, structure, business and resources of a financial institution, the designated department, unit, group, or committee or officer may be dedicated solely to the financial institution‘s anti-money laundering responsibilities or perform the compliance functions in addition to existing duties.

4.1.4 The designated CAMLCO, directly or through the designated department, unit, group, or committee, should be a central point of contact for communicating with the regulatory agencies regarding issues related to the financial institution’s anti-money laundering program.

4.1.5 Depending on the scale and nature of the institution the designated CAMLCO may choose to delegate duties or rely on suitably qualified staff for their practical performance whilst remaining responsible and accountable for the operation of the designated functions. In larger institutions, because of their and complexity the appointment of one or more permanent Deputy CAMLCO of suitable seniority may be necessary.

4.1.6 The designated CAMLCO must ensure that at each division, region, branch or unit of the financial unit that deals directly with the public, a senior level officer is appointed as Anti Money Laundering Compliance Officer (AMLCO) to ensure that each division, region, branch or unit is carrying out policies and procedures as required. These officers should report to the CAMLCO regularly on compliance issues and the need for any revisions to policies and procedures. This division, regional, branch or unit level officers may be dedicated solely to the financial institution‘s anti-money laundering responsibilities or perform the compliance functions in addition to existing duties.

4.1.7 All staff engaged in the *Financial Institution* at all levels must be made aware of the identity of the C*AMLCO*, his Deputy and the staff's branch/unit level AMLCO, and the procedure to follow when making a suspicious activity report. All relevant staff must be aware of the chain through which suspicious activity reports should be passed to the C*AMLCO*. A suggested format of an internal report form is set out in Annexure H.

4.1.8 A sample job description of the Chief Anti-Money Laundering Compliance Officers (CAMLCO) is appended below which may be adapted for creating a suitable job description of the Regional/Branch/ Unit Anti-Money Laundering Compliance Officers (AMLCO):

POSITION TITLE: Chief Anti-Money Laundering Compliance Officer

FUNCTION: The Chief Anti-Money Laundering Compliance Officer (CAMLCO), who will report to the Chief Executive Officer for this responsibility, coordinates and monitors day to day compliance with: applicable money laundering laws, rules and regulations; the Institution's AML Policy (the "Policy"); and the practices, procedures and controls implemented by the Institution.

POSITION RESPONSIBILITIES:

1) Monitor, review and coordinate application and enforcement of the Bank's/ Institution's compliance policies including Anti-Money Laundering Compliance Policy. This will include: an AML risk assessment; and practices, procedures and controls for account opening, KYC procedures and ongoing account/transaction monitoring for detecting suspicious transactions/account activity, and a written AML training plan (refer to Chapter IX);

2) To monitor changes of laws/regulations and directives of Bangladesh Bank that may require revisions to the Policy, and making these revisions;

3) Respond to compliance questions and concerns of the staff and advise regions/branches/units and assist in providing solutions to potential issues involving compliance and money laundering risk;

4) Ensure the Bank's/Institution's AML Policy is complete and up-to-date; maintain ongoing awareness of new and changing business activities and products and identify potential compliance issues that should be considered by the Bank/Institution;

5) Actively develop the compliance knowledge of all staff, especially the compliance personnel. Develop and conduct training courses in the Bank/Institution to raise the level of awareness of compliance in the Bank;

6) Develop and maintain ongoing relationships with regulatory authorities, external and internal auditors, Regional/ Branch/Unit Heads and Compliance resources to assist in early identification of compliance issues;

7) Assist in review of control procedures in the Bank/Institution to ensure legal and regulatory compliance and in the development of adequate and sufficient testing procedures to prevent and detect compliance lapses;

8) To monitor the business' self-testing for AML compliance and any corrective action;

9) To manage the Suspicious Activity Reporting Process:

- Reviewing transactions referred by divisional, regional, branch or unit compliance officers as suspicious;
- Reviewing the Transaction Monitoring reports (directly or together with account management personnel);
- Ensuring that internal Suspicious Activity Reports ("internal SARs"):
  - are prepared when appropriate;
  - reflect the uniform standard for "suspicious activity involving possible money laundering" established in the Policy;
  - are accompanied by documentation of the branch's decision to retain or terminate the account as required under the Policy;
  - are advised to other branches of the institution who are known to have a relationship with the customer;
  - are reported to the Chief Executive Officer, and the Board of Directors of the institution when the suspicious activity is judged to represent significant risk to the institution, including reputation risk .
- Ensuring that a documented plan of corrective action, appropriate for the seriousness of the suspicious activity, be prepared and approved by the Branch Manager;
- Maintaining a review and follow up process to ensure that planned corrective action, including possible termination of an account, be taken in a timely manner;
- Manage the process for reporting suspicious activity to Bangladesh Bank authorities after appropriate internal consultation;

JOB CHARACTERISTICS AND REQUIREMENTS

The Chief Anti-Money Laundering Compliance Officer (CAMLCO) should possess:

- Proven leadership and organizational skills and ability to exert managerial control;

- Excellent communication skills, with an ability to clearly and diplomatically articulate issues, solutions and rationale; an effective trainer to raise the level of awareness of the control and compliance culture;

- Solid understanding of AML regulatory issues and product knowledge associated with a broad range of relevant financial services, banking activities;

- High degree of judgment, good problem solving skills and be results oriented to ensure sound implementation of control and compliance processes and procedures;

- High personal standard of ethics, integrity and commitment to fulfilling the objectives of the position and protecting the interest of the Bank.

The Chief Anti-Money Laundering Compliance Officer (CAMLCO):

- Must be familiar with the ways in which any of their respective business's products and services may be abused by money launderers;

- Must be able to assist their respective Institutions develop effective AML policies, including programs to provide AML training to all personnel;

- Must be able to assist their respective business assess the ways in which products under development may be abused by money launderers in order to establish appropriate AML controls before product is rolled out into the marketplace.

- Must be capable of assisting their respective business evaluate whether questionable activity is suspicious under the standard set forth in the AML Policy and under any applicable law and regulation;

- Must attend each year at least one formal AML training program, either internal or external;

EDUCATION (OR EQUIVALENT TRAINING)

The Chief Anti-Money Laundering Compliance Officer (CAMLCO) should have a working knowledge of the diverse banking products offered by the Institution. The person could have obtained relevant banking and compliance experience as an internal auditor or regulatory examiner, with exposure to different banking products and businesses. Product and banking knowledge could be obtained from being an external or internal auditor, or as an experienced Operations staff.

EXPERIENCE

The Chief Anti-Money Laundering Compliance Officer (CAMLCO) should have a minimum of ten years of experience, with a minimum of three years at a managerial/administrative level.

4.2 Organisation Structure

4.2.1 Whilst complying with rules and regulations is the responsibility of each individual in the financial institution in the normal course of their assignments, the following individuals and functions all play a vital role in the effectiveness of the Institutions AML program:

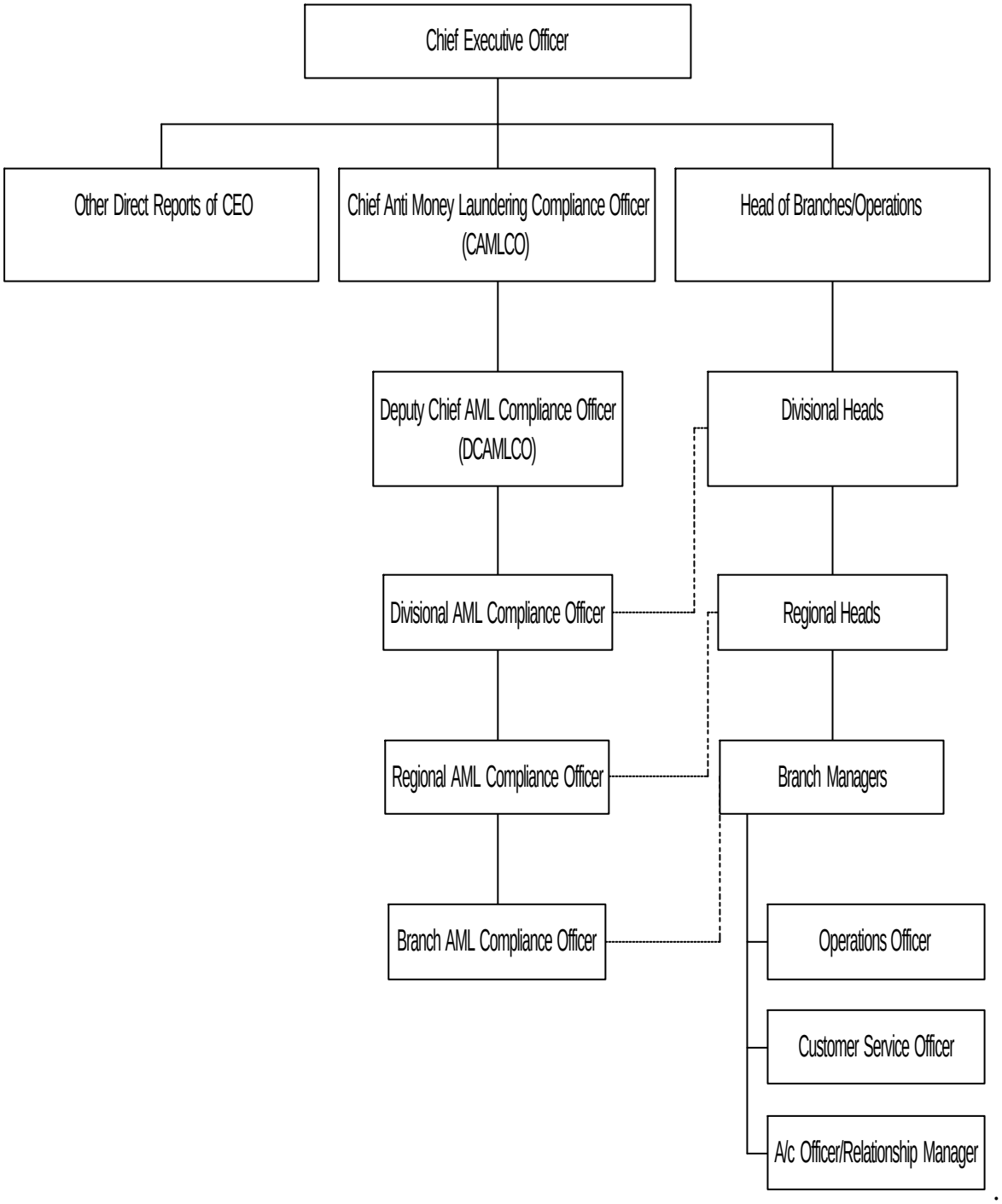
Account Officer/Relationship Manager
Customer Service Officer
Operations Staff
Anti Money Laundering Compliance Officer (AMLCO)
Branch Manager (Unit Head)
Risk Management /Credit Officer
Internal Control Officer
Operations & Technology Manager
Controller of Branches
Chief Anti Money Laundering Compliance Officer (CAMLCO)
Chief Executive Officer (CEO)

4.2.2 The Grid below details the individual responsibilities of the above functions:-

Function	**Role / Responsibilities**
Account Officer/ Relationship Manager/ Staff Responsible for account opening	▪ Perform due diligence on prospective clients prior opening an account ▪ Be diligent regarding the identification (s) of account holder and the transactions relating to the account ▪ Ensure all required documentation is completed satisfactorily ▪ Complete the KYC Profile for the new customer ▪ Ongoing monitoring of customer's KYC profile and transaction activity ▪ Obtain documentary evidence of large cash deposits ▪ Escalate any suspicion to the Supervisor, Branch Manager and AMLCO
Customer Service Officer	▪ Support the Account Officer in any of the above roles ▪ Perform the Account Officer roles in their absence
Operations Staff	▪ Ensuring that all control points are completed prior to transaction monitoring ▪ Ongoing diligence on transaction trends for clients ▪ Update customer transaction profiles in the ledger/system
AMLCO	▪ Manages the transaction monitoring process ▪ Reports any suspicious activity to Branch Manager, and if necessary the CAMLCO ▪ Provide AML training to Branch staff ▪ Update policy with local AML regulations and communicate to all staff ▪ Submit Branch returns to CAMLCO on Bi-monthly basis (MIS)
Branch Manager (Unit Head)	▪ Ensures that the AML program is effective within the branch/unit ▪ First point of contact for any AML issues
Risk Management /Credit Officer/ Internal Control Officer	▪ Perform AML Risk Assessment for the Business ▪ Perform periodic Quality Assurance on the AML program in the unit ▪ Communicate updates in AML laws and internal policies
Operations & Technology Manager Controller of Branches	▪ Ensures that the required reports and systems are in place to maintain an effective AML program ▪ Overall responsibility to ensure that the branches have an AML program in place and that it is working effectively
CAMLCO	▪ Implements and enforces Institution's anti-money laundering policies ▪ Reports suspicious clients to Bangladesh Bank on Institution's behalf ▪ Informs Controller of Branches/AMLCOs of required actions (if any)
Chief Executive	▪ Overall responsibility to ensure that the Business has an

Officer (CEO)	AML program in place and that it is working effectively

4.2.3 A sample organization chart is given below:



CHAPTER V IDENTIFICATION PROCEDURES

5.1 Introduction

5.1.1 Sound Know Your Customer (KYC) procedures are critical elements in the effective management of banking risks. KYC safeguards go beyond simple account opening and record-keeping and require banks to formulate a customer acceptance policy and a tiered customer identification program that involves more extensive due diligence for higher risk accounts, and includes proactive account monitoring for suspicious activities.

5.1.2 Sound KYC procedures have particular relevance to the safety and soundness of financial institutions, in that:

- they help to protect financial institution's reputation and the integrity of banking systems by reducing the likelihood of banks becoming a vehicle for or a victim of financial crime and suffering consequential reputational damage;
- they constitute an essential part of sound risk management (e.g. by providing the basis for identifying, limiting and controlling risk exposures in assets and liabilities, including assets under management).

5.1.3 The inadequacy or absence of KYC standards can subject banks to serious customer and counterparty risks, especially reputational, operational, legal and concentration risks. It is worth noting that all these risks are interrelated. However, any one of them can result in significant financial cost to banks (e.g. through the withdrawal of funds by depositors, the termination of inter-bank facilities, claims against the bank, investigation costs, asset seizures and freezes, and loan losses), as well as the need to divert considerable management time and energy to resolving problems that arise.

5.1.4 **Reputational risk** poses a major threat to banks, since the nature of their business requires maintaining the confidence of depositors, creditors and the general marketplace. Reputational risk is defined as the potential that adverse publicity regarding a bank's business practices and associations, whether accurate or not, will cause a loss of confidence in the integrity of the institution. Banks are especially vulnerable to reputational risk because they can so easily become a vehicle for or a victim of illegal activities perpetrated by their customers. They need to protect themselves by means of continuous vigilance through an effective KYC program. Assets under management, or held on a fiduciary basis, can pose particular reputational dangers.

5.1.5 **Operational risk** can be defined as the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events. Most operational risk in the KYC context relates to weaknesses in the implementation of banks' programs, ineffective control procedures and failure to practice due diligence. A public perception that a bank is not able to manage its operational risk effectively can disrupt or adversely affect the business of the bank.

5.1.6 **Legal risk** is the possibility that lawsuits, adverse judgments or contracts that turn out to be unenforceable can disrupt or adversely affect the operations or condition of a bank. Banks may become subject to lawsuits resulting from the failure to observe mandatory KYC standards or from the failure to practice due diligence. Consequently, banks can, for example, suffer fines,

criminal liabilities and special penalties imposed by regulators. Indeed, a court case involving a bank may have far greater cost implications for its business than just the legal costs. Banks will be unable to protect themselves effectively from such legal risks if they do not engage in due diligence in identifying their customers and understanding their business.

5.1.7 On the liabilities side, concentration risk is closely associated with funding risk, particularly the risk of early and sudden withdrawal of funds by large depositors, with potentially damaging consequences for the bank's liquidity. Funding risk is more likely to be higher in the case of small banks and those that are less active in the wholesale markets than large banks. Analyzing deposit concentrations requires banks to understand the characteristics of their depositors, including not only their identities but also the extent to which their actions may be linked with those of other depositors. It is essential that liabilities managers in small banks not only know but also maintain a close relationship with large depositors, or they will run the risk of losing their funds at critical times.

5.1.8 Customers frequently have multiple accounts with the same bank, but in offices located in different areas. To effectively manage the reputational, compliance and legal risk arising from such accounts, banks should be able to aggregate and monitor significant balances and activity in these accounts on a fully consolidated countrywide basis.

5.2 Know Your Customer (KYC) Policies and Procedures

5.2.1 Having sufficient information about your customer - "knowing your customer" (KYC) - and making use of that information underpins all anti-money laundering efforts, and is the most effective defense against being used to launder the proceeds of crime. If a customer has established an account using a false identity, s/he may be doing so to defraud the institution itself, or to ensure that s/he cannot be traced or linked to the crime the proceeds of which the institution is being used to launder. A false name, address or date of birth will usually mean that law enforcement agencies cannot trace the customer if s/he is needed for interview as part of an investigation.

5.2.2 Section 19 Ka of the Prevention of Money Laundering Act 2002 requires all institutions to seek satisfactory evidence of the identity of those with whom they deal (referred to in these Guidance Notes as verification of identity). Unless satisfactory evidence of the identity of potential customers is obtained in good time, the business relationship must not proceed.

5.2.3 When a business relationship is being established, the nature of the business that the customer expects to conduct with the institution should be ascertained at the outset to establish what might be expected later as normal activity. This information should be updated as appropriate, and as opportunities arise. **In order to be able to judge whether a transaction is or is not suspicious, institutions need to have a clear understanding of the business carried on by their customers.**

5.2.4 An institution must establish to its satisfaction that it is dealing with a real person (natural, corporate or legal), and must verify the identity of persons who are authorized to operate any bank or investment account, or transact business for the customer. Whenever possible, the prospective customer should be interviewed personally.

5.2.5 The verification procedures needed to establish the identity of a prospective customer should basically be the same whatever type of account or service is required. The best identification documents possible should be obtained from the prospective customer i.e. those that are the most difficult to obtain illicitly. No single piece of identification can be fully guaranteed as genuine, or as being sufficient to establish identity so verification will generally be a cumulative process. **The overriding principle is that every institution must know who their customers are, and have the necessary documentary evidence to verify this.**

Section19 Ka of the Act requires that records of the verification of identity must be retained for five years after an account is closed or the business relationship ended (see Chapter V - Record Keeping).

5.2.6 Financial institutions in the design of KYC programs should include certain key elements. Such essential elements should start from the banks' risk management and control procedures and should include (1) customer acceptance policy, (2) customer identification, (3) on-going monitoring of high risk accounts and (4) identification of suspicious transactions. Banks should not only establish the identity of their customers, but should also monitor account activity to determine those transactions that do not conform with the normal or expected transactions for that customer or type of account. KYC should be a core feature of banks' risk management and control procedures, and be complemented by regular compliance reviews and internal audit. The intensity of KYC programs beyond these essential elements should be tailored to the degree of risk.

5.3 Customer Acceptance Policy

5.3.1 Financial Institutions should develop clear customer acceptance policies and procedures, including a description of the types of customer that are likely to pose a higher than average risk to a bank. In preparing such policies, factors such as customers' background, country of origin, public or high profile position, linked accounts, business activities or other risk indicators should be considered.

5.3.2 Financial Institutions should develop graduated customer acceptance policies and procedures that require more extensive due diligence for higher risk customers. For example, the policies may require the most basic account-opening requirements for a working individual with a small account balance. It is important that the customer acceptance policy is not so restrictive that it results in a denial of access by the general public to banking services, especially for people who are financially or socially disadvantaged. On the other hand, quite extensive due diligence would be essential for an individual with a high net worth whose source of funds is unclear. Decisions to enter into business relationships with higher risk customers, such as public figures or politically exposed persons (see section 5.11 below), should be taken exclusively at senior management level.

5.4 Customer Identification

5.4.1 Customer identification is an essential element of KYC standards. For the purposes of this Guidance Notes, a customer includes:

- the person or entity that maintains an account with the bank or those on whose behalf an account is maintained (i.e. beneficial owners);
- the beneficiaries of transactions conducted by professional intermediaries; and
- any person or entity connected with a financial transaction who can pose a significant reputational or other risk to the bank.

5.4.2 The customer identification process applies naturally at the outset of the relationship. To ensure that records remain up-to-date and relevant, there is a need for banks to undertake regular reviews of existing records. An appropriate time to do so is when a transaction of significance takes place, when customer documentation standards change substantially, or when there is a material change in the way that the account is operated. However, if a bank becomes aware at any time that it lacks sufficient information about an existing customer, it should take steps to ensure that all relevant information is obtained as quickly as possible.

5.4.3 Whenever the opening of an account or business relationship is being considered, or a one-off transaction or series of linked transactions of Tk.5,000 or more is to be undertaken, identification procedures must be followed. Identity must also be verified in all cases where money laundering is known, or suspected.

5.4.4 Once verification of identity has been satisfactorily completed, no further evidence is needed when other transactions are subsequently undertaken. Records must be maintained as set out Chapter VII, and information should be updated or reviewed as appropriate.

5.5 What Constitutes a Person's Identity

5.5.1 Identity generally means a set of attributes which uniquely define a natural or legal person. There are two main constituents of a person's identity, remembering that a person may be any one of a range of legal persons (an individual, body corporate, partnership, etc). For the purposes of this guidance, the two elements are:

- the physical identity (e.g. name, date of birth, TIN/voter registration/passport/ID number, etc.); and
- the activity undertaken.

5.5.2 Confirmation of a person's address is also useful in determining whether a customer is resident in a high-risk country. Knowledge of both residence and nationality may also be necessary, in a non money-laundering context, to avoid breaches of UN or other international sanctions to which Bangladesh is a party. Where a passport is taken as evidence, the number, date and place of issue should be recorded.

5.5.3 The other main element in a person's identity is sufficient information about the nature of the business that the customer expects to undertake, and any expected or predictable, pattern of transactions. For some business these may be obvious, however, for more complex businesses this may not be the case. The extent of the description required will depend on the institution's own understanding of the applicant's business.

5.5.4 When commencing a business relationship, institutions should consider recording the purpose and reason for establishing the business relationship, and the anticipated level and nature of activity to be undertaken. Documentation about the nature of the applicant's business should

also cover the origin of funds to be used during the relationship. For example, funds may be transferred from a bank or the applicant's employer, or be the proceeds of a matured insurance policy, etc.

5.5.5 Once account relationship has been established, reasonable steps should be taken by the institution to ensure that descriptive information is kept up to date as opportunities arise. It is important to emphasize that the customer identification process do not end at the point of application. The need to confirm and update information about identity, such as changes of address, and the extent of additional KYC information to be collected over time will differ from sector to sector and between institutions within any sector. It will also depend on the nature of the product or service being offered, and whether personal contact is maintained enabling file notes of discussion to be made or whether all contact with the customer is remote.

5.6 Individual Customers

5.6.1 Where verification of identity is required, the following information should be obtained from all individual applicants for opening accounts or other relationships, and should be independently verified by the institution itself:

- true name and/or names used;
- parent's names;
- date of birth;
- current and permanent address;
- details of occupation/employment and sources of wealth or income

5.6.2 One or more of the following steps is recommended to verify addresses:

- provision of a recent utility bill, tax assessment or bank statement containing details of the address (to guard against forged copies it is strongly recommended that original documents are examined);
- checking the Voter lists;
- checking the telephone directory;
- record of home/office visit.

The information obtained should demonstrate that a person of that name exists at the address given, and that the applicant is that person.

5.6.3 The date of birth is important as an identifier in support of the name, and is helpful to assist law enforcement. Although there is no obligation to verify the date of birth, this provides an additional safeguard. It is also helpful for residence/nationality to be ascertained to assist risk assessment procedures and to ensure that an institution does not breach UN or other international financial sanctions.

5.6.4 Identification documents, either originals or certified copies, should be pre-signed and bear a photograph of the applicant, e.g.:-

(i) Current valid passport;
(ii) Valid driving license;

(iii) Voter ID Card;
(iv) Armed Forces ID card;
(v) A Bangladeshi employer ID card bearing the photograph and signature of the applicant; or
(vi) A certificate from any local government organs such as Union Council chairman, Ward Commissioner, etc. or any respectable person acceptable to the institution.

5.6.5 Identification documents which do not bear photographs or signatures, or are easy to obtain, are normally not appropriate as **sole** evidence of identity, e.g. birth certificate, credit cards, non-Bangladeshi driving license. Any photocopies of documents showing photographs and signatures should be plainly legible. Where applicants put forward documents with which an institution is unfamiliar, either because of origin, format or language, the institution must take reasonable steps to verify that the document is indeed genuine, which may include contacting the relevant authorities or obtaining a notarized translation. *Financial Institutions* should also be aware of the authenticity of passports.

5.6.6 Where there is no face-to-face contact, and photographic identification would clearly be inappropriate, procedures to identify and authenticate the customer should ensure that there is sufficient evidence, either documentary or electronic, to confirm address and personal identity. At least one additional check should be undertaken to guard against impersonation. In the event that internal procedures require sight of a current passport or ID Card where there is no face-to-face contact, then a certified true copy should be obtained.

5.6.7 There is obviously a wide range of documents which might be provided as evidence of identity. It is for each institution to decide the appropriateness of any document in the light of other procedures adopted. However, particular care should be taken in accepting documents which are easily forged or which can be easily obtained using false identities.

5.6.8 In respect of joint accounts where the surname and/or address of the account holders differ, the name and address of all account holders, not only the first named, should normally be verified in accordance with the procedures set out above.

5.6.9 Any subsequent change to the customer's name, address, or employment details of which the financial institution becomes aware should be recorded as part of the know your customer process. Generally this would be undertaken as part of good business practice and due diligence but also serves for money laundering prevention.

5.6.10 **File copies of supporting evidence should be retained.** Where this is not possible, the relevant details should be recorded on the applicant's file. Institutions which regularly conduct one-off transactions, should record the details in a manner which allows cross reference to transaction records. Such institutions may find it convenient to record identification details on a separate form, similar to the example in Annexure F, to be retained with copies of any supporting material obtained.

5.6.11 An introduction from a respected customer personally known to the management, or from a trusted member of staff, may assist the verification procedure but does not replace the need for verification of address as set out above. Details of the introduction should be recorded on the customer's file. However, personal introductions without full verification should not become the norm, and directors/senior managers must not require or request staff to breach account opening procedures as a favor to an applicant

5.7 Persons without Standard Identification Documentation

5.7.1 Most people need to make use of the financial system at some point in their lives. It is important, therefore, that the socially or financially disadvantaged such as the elderly, the disabled, students and minors should not be precluded from obtaining financial services just because they do not possess evidence of identity or address where they cannot reasonably be expected to do so. In these circumstances, a common sense approach and some flexibility without compromising sufficiently rigorous anti-money laundering procedures is recommended. Internal procedures must allow for this, and must provide appropriate advice to staff on how identity can be confirmed in these exceptional circumstances. The important point is that a person's identity can be verified from an original or certified copy of another document, preferably one with a photograph.

5.7.2 A certifier must be a suitable person, such as for instance a lawyer, accountant, director or manager of a regulated institution, a notary public, a member of the judiciary or a senior civil servant. The certifier should sign the copy document (printing his name clearly underneath) and clearly indicate his position or capacity on it together with a contact address and phone number.

5.7.3 In these cases it may be possible for the institution to accept confirmation from a professional (e.g. doctor, lawyer, directors or managers of a regulated institution, etc) who knows the person. Where the individual lives in accommodation for which he or she is not financially responsible, or for which there would not be documentary evidence of his/her address, it may be acceptable to accept a letter from the guardian or a similar professional as confirmation of a person's address. A manager may authorize the opening of a business relationship if s/he is satisfied with confirmation of identity circumstances but must record his/her authorization on the customer's file, and must also retain this information in the same manner and for the same period of time as other identification records.

5.7.4 For students or other young people, the normal identification procedures set out above should be followed as far as possible. Where such procedures would not be relevant, or do not provide satisfactory evidence of identity, verification might be obtained in the form of the home address of parent(s), or by making enquiries of the applicant's educational institution.

5.7.5 Under normal circumstances, a family member or guardian who has an existing relationship with the institution concerned would introduce a minor. In cases where the person opening the account is not already known, the identity of that person, and any other person who will have control of the account, should be verified.

5.8 Corporate Bodies and other Entities

5.8.1 Because of the difficulties of identifying beneficial ownership, and the possible complexity of organization and structures, corporate entities and trusts are the most likely vehicles to be used for money laundering, particularly when a legitimate trading company is involved. Particular care should be taken to verify the legal existence of the applicant and to ensure that any person purporting to act on behalf of the applicant is authorized to do so. **The principal requirement is to look behind a corporate entity to identify those who have ultimate control over the business and the company's assets, with particular attention being paid to any shareholders or others who exercise a significant influence over the affairs of the**

company. Enquiries should be made to confirm that the company exists for a legitimate trading or economic purpose, and that it is not merely a "brass plate company" where the controlling principals cannot be identified.

5.8.2 Before a business relationship is established, measures should be taken by way of company search and/or other commercial enquiries to ensure that the applicant company has not been, or is not in the process of being, dissolved, struck off, wound-up or terminated. In addition, if the institution becomes aware of changes in the company structure or ownership, or suspicions are aroused by a change in the nature of business transacted, further checks should be made.

5.8.3 Particular care should be exercised when establishing business relationships with companies incorporated or registered abroad, or companies with no direct business link to Bangladesh. Such companies may be attempting to use geographic or legal complication to interpose a layer of opacity between the source of funds and their final destination. In such circumstances, institutions should carry out effective checks on the source of funds and the nature of the activity to be undertaken during the proposed business relationship. This is particularly important if the corporate body is registered or has known links to countries without anti-money laundering legislation and procedures equivalent to Bangladesh's. In the case of a trading company, a visit to the place of business may also be made to confirm the true nature of the business.

5.8.4 No further steps to verify identity over and above usual commercial practice will normally be required where the applicant for business is known to be a company, or a subsidiary of a company, quoted on a recognized stock exchange.

5.8.5 The following documents should normally be obtained from companies:

- Certified true copy of Certificate of Incorporation or equivalent, details of the registered office, and place of business;
- Certified true copy of the Memorandum and Articles of Association, or by-laws of the client.
- Copy of the board resolution to open the account relationship and the empowering authority for those who will operate any accounts;
- Explanation of the nature of the applicant's business, the reason for the relationship being established, an indication of the expected turnover, the source of funds, and a copy of the last available financial statements where appropriate;
- Satisfactory evidence of the identity of each of the principal beneficial owners being any person holding 10% interest or more or with principal control over the company's assets and any person (or persons) on whose instructions the signatories on the account are to act or may act where such persons are not full time employees, officers or directors of the company;
- Satisfactory evidence of the identity of the account signatories, details of their relationship with the company and if they are not employees an explanation of the relationship. Subsequent changes to signatories must be verified;
- Copies of the list/register of directors.

5.8.6 Where the business relationship is being opened in a different name from that of the applicant, the institution should also satisfy itself that the reason for using the second name makes sense.

5.8.7 The following persons (i.e. individuals or legal entities) must also be identified in line with this part of the notes:

- All of the directors who will be responsible for the operation of the account / transaction.
- All the authorized signatories for the account/transaction.
- All holders of powers of attorney to operate the account/transaction.
- The beneficial owner(s) of the company
- The majority shareholders of a private limited company.

A letter issued by a corporate customer similar to Annexure E is acceptable in lieu of passport or other photo identification documents of their shareholders, directors and authorized signatories. Where the institution already knows their identities and identification records already accord with the requirements of these notes, there is no need to verify identity again.

5.8.8 When authorized signatories change, care should be taken to ensure that the identities of all current signatories have been verified. In addition, it may be appropriate to make periodic enquiries to establish whether there have been any changes in directors/shareholders, or the nature of the business/activity being undertaken. Such changes could be significant in relation to potential money laundering activity, even though authorized signatories have not changed.

5.9 Partnerships and Unincorporated Businesses

5.9.1 In the case of partnerships and other unincorporated businesses whose partners/directors are not known to the institution, the identity of all the partners or equivalent should be verified in line with the requirements for personal customers. Where a formal partnership agreement exists, a mandate from the partnership authorizing the opening of an account and conferring authority on those who will operate it should be obtained.

5.9.2 Evidence of the trading address of the business or partnership should be obtained and a copy of the latest report and accounts (audited where applicable).

5.9.3 An explanation of the nature of the business or partnership should be ascertained (but not necessarily verified from a partnership deed) to ensure that it has a legitimate purpose.

5.10 Powers of Attorney/ Mandates to Operate Accounts

The authority to deal with assets under a power of attorney constitutes a business relationship and therefore, where appropriate, it may be advisable to establish the identities of holders of powers of attorney, the grantor of the power of attorney and third party mandates. Records of all transactions undertaken in accordance with a power of attorney should be kept in accordance with Chapter VII.

5.12 Requirements in respect of Accounts Commenced Prior to 30 April 2002

5.12.1 Anti-money laundering legislation and requirements in respect of KYC procedures for business relationships did not apply prior to 30th April 2002. It is therefore reasonable to assume that business relationships commenced before that date may not satisfy the requirements

of these guidance notes in terms of supporting documentary evidence. In some circumstances, the lack of up to date documentary evidence to support existing business relationships may pose operational and other risks to the institution. Consequently, all relevant financial businesses must review existing business relationships commenced prior to 30th April 2002 (referred to in this section as "pre 2002 accounts") to establish whether any documentary evidence required by their current KYC procedures is lacking. **The review must be completed by 31st January 2010.**

5.12.2 When an institution's management reviews a pre-2002 account, the form in Annexure E should be used. Two senior managers who must also sign the form should conduct the review. **This form must be retained with client records, and will be treated as a constituent element of the institution's KYC documentation for a pre-2002 account.**

5.12.3 In carrying out their review of pre-2002 accounts, management must decide whether to obtain any missing elements of the documentary evidence, or to decide that, in light of the existing nature of the business relationship, it is unnecessary to do so. Each business relationship must be treated in one-way or the other. A decision must not be taken on the basis of categories or groups of clients.

5.12.4 When reviewing the nature of a business relationship, management should take into account a number of considerations, such as the length of time the relationship has been in place, the frequency with which the institution has contact with the client, and the volumes and numbers of transactions. Such factors will help determine whether it is necessary to update or supplement KYC documentation already held.

5.12.5 Where it is decided to seek missing documentation, the institution must do so at the earliest possible opportunity and persist until the information is received, or the original decision revised. Where missing information is not obtained within a reasonable period of time, the institution should consider termination of the business relationship

5.13 Internet or Online Banking

5.13.1 Banking and investment business on the Internet add a new dimension to *Financial Institutions*' activities. The unregulated nature of the Internet is attractive to criminals, opening up alternative possibilities for money laundering, and fraud.

5.13.2 It is recognized that on-line transactions and services are convenient. However, it is not appropriate that *Financial Institutions* should offer on-line live account opening allowing full immediate operation of the account in a way which would dispense with or bypass normal identification procedures.

5.13.3 However, initial application forms could be completed on-line and then followed up with appropriate identification checks. The account, in common with accounts opened through more traditional methods, should not be put into full operation until the relevant account opening provisions have been satisfied in accordance with these Guidance Notes.

5.13.4 The development of technologies such as encryption, digital signatures, etc., and the development of new financial services and products, makes the Internet a dynamic environment offering significant business opportunities. The fast pace of technological and product

development has significant regulatory and legal implications, and Bangladesh Bank is committed to keeping up to date with any developments on these issues through future revisions to its Guidance Notes.

5.14 Provision of Safe Custody and Safety Deposit Boxes

Where facilities to hold boxes, parcels and sealed envelopes in safe custody are made available, it is expected that *Financial Institutions* will follow the identification procedures set out in these Guidance Notes. In addition such facilities should only be made available to account holders.

5.15 Timing and Duration of Verification

5.15.1 The best time to undertake verification is *prior to entry* into the account relationship. Verification of identity should, as soon as is reasonably practicable, be completed before any transaction is completed.

5.15.2 However, if it is necessary for sound business reasons to open an account or carry out a significant one-off transaction before verification can be completed, this should be subject to stringent controls which should ensure that any funds received are not passed to third parties. Alternatively, a senior member of staff may give appropriate authority.

5.15.3 This authority should not be delegated, and should only be done in exceptional circumstances. Any such decision should be recorded in writing.

5.15.4 Verification, once begun, should normally be pursued either to a satisfactory conclusion or to the point of refusal. If a prospective customer does not pursue an application, staff may (or may not) consider that this is in itself suspicious.

CHAPTER VI: ANTI MONEY LAUNDERING PROCESSES

6.1 Know Your Customer Procedures

6.1.1 Each *Financial Institution* is required to perform due diligence on all prospective clients prior to opening an account. This process is completed by fulfilling the documentation requirements (Account Application, Bank References, Source of funds and Identification for example) and also a 'Know Your Customer' profile which is used to record a client's source of wealth, expected transaction activity at it's most basic level.

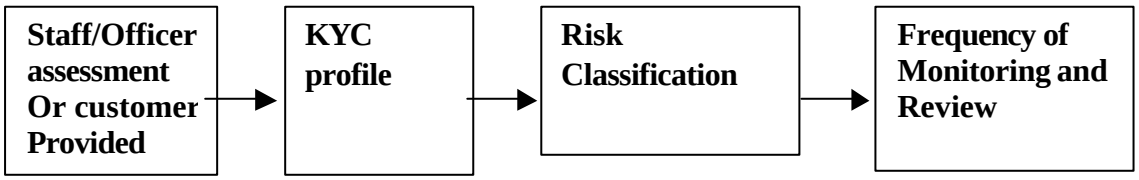
6.1.2 Once the identification procedures have been completed and the client relationship is established, *Financial Institutions* should monitor the conduct of the relationship/account to ensure that it is consistent with the nature of business stated when the relationship/account was opened. *Financial Institutions* do this firstly by the their staff being diligent, reporting suspicious transactions undertaken by the customer, updating the client's KYC profile for any significant changes in their lifestyle (e.g., change of employment status, increase in net worth) and by monitoring the transaction activity over the client's account on a periodic basis.

6.1.3 KYC profile gives the basic information about the customer like, Name, Address, Tel/Fax Numbers, line of business, Annual sales. If the customer is a Public Figure, the account will become automatically a High Risk Account.

6.1.4 The KYC Profile information will also include the observations of the Institution's Staff/Officer when they visit the customer's business place like, the business place is owned or rented, the type of clients visited, by what method is the client paid (cheque or cash). The Staff/Officer will record his observations and sign the KYC Profile form.

6.1.5 In the case of high net worth Accounts, the information will include net worth of the customer, source of funds etc

6.1.6 The KYC Profile leads to Risk Classification of the Account as High/Low Risk.



6.2 Risk categorization – Based on Activity/KYC Profile

6.2.1 When opening accounts, the concerned staff/Officer must assess the risk that the accounts could be used for "money laundering", and must classify the accounts as either High Risk or Low Risk. The risk assessment may be made using the KYC Profile Form given in Annexure D in which following seven risk categories are scored using a scale of 1 to 5 where scale 4-5 denotes High Risk, 3- Medium Risk and 1-2 Low Risk:

- Occupation or nature of customer's business
- Net worth / sales turnover of the customer
- Mode of opening the account

- Expected value of monthly transactions
- Expected number of monthly transactions
- Expected value of monthly cash transactions
- Expected number of monthly cash transactions

6.2.2 The risk scoring of less than 14 indicates low risk and more than 14 would indicate high risk. The risk assessment scores are to be documented in the KYC Profile Form (see Annexure D). However, management may judgmentally override this automatic risk assessment to "Low Risk" if it believes that there are appropriate mitigants to the risk. This override decision must be documented (reasons why) and approved by the Branch Manager, and Branch AML Compliance Officer.

6.2.3 KYC Profiles and Transaction Profiles must be updated and re-approved at least annually for "High Risk" accounts (as defined above). There is no requirement for periodic updating of profiles for "Low Risk" transactional accounts. These should, of course, be updated if and when an account is reclassified to "High Risk", or as needed in the event of investigations of suspicious transactions or other concern.

6.3 Transaction Monitoring Process

6.3.1 Financial Institutions are expected to have systems and controls in place to monitor on an ongoing basis the relevant activities in the course of the business relationship. The nature of this monitoring will depend on the nature of the business. The purpose of this monitoring is for Financial Institutions to be vigilant for any significant changes or inconsistencies in the pattern of transactions. Inconsistency is measured against the stated original purpose of the accounts i.e. the declared Transaction Profile (TP) of the Customer. Possible areas to monitor could be: -

a. transaction type
b. frequency
c. unusually large amounts
d. geographical origin/destination
e. changes in account signatories

6.3.2. It is recognized that the most effective method of monitoring of accounts is achieved through a combination of computerized and human manual solutions. A corporate compliance culture, and properly trained, vigilant staff through their day-to-day dealing with customers, will form an effective monitoring method as a matter of course. Computerized approaches may include the setting of "floor levels" for monitoring by amount. Different "floor levels" or limits may be set for different categories of customers.

6.3.3. Whilst some Financial Institutions may wish to invest in expert computer systems specifically designed to assist the detection of fraud and money laundering, it is recognized that this may not be a practical option for many Financial Institutions for the reasons of cost, the nature of their business, or difficulties of systems integration, in such circumstances institutions will need to ensure they have alternative systems in place.

6.3.4. Every Business and every individual will have normally certain kind of transaction in line with their business/individual needs. This will be declared in a Transaction Profile (TP) at the time of opening account from the customer. Ideally any deviation from the normally expected TP

should be reviewed with human judgment and interaction with customer. Such reviews may result in changing the expected profile or closing the customer account.

6.3.5. It may not be feasible for some institutions or specific branches of institutions having very large number of customers to track every single account against the TP where a risk based approach should be taken for monitoring transactions based on use of "Customer Categories" and "Transaction Limits" (individual and aggregate) established within the branch. The Customer Category is assigned at account inception - and may be periodically revised - and is documented on the Transaction Profile. Transaction Limits are established by the business subject to agreement by Branch AMLCO. The Customer Categories and Transaction Limits are maintained in the manual ledgers or computer systems.

6.3.6. On a monthly basis Branch/ Unit of the financial institution must prepare an exception report of customers whose accounts showed one or more individual account transaction during the period that exceeded the "transaction limit" established for that category of customer based on Anti-Money Laundering risk assessment exercise.

6.3.7. Account Officers/Relationship Managers or other designated staff will review and sign-off on such exception report of customers whose accounts showed one or more individual account transaction during the period that exceeded the "transaction limit" established for that category of customer. The concerned staff will document their review by initial on the report, and where necessary will prepare internal Suspicious Activity Reports (SARs) with action plans for approval by the relevant Branch Manager and review with the Branch AMLCO. A copy of the transaction identified will be attached to the SARs.

6.3.8. AMLCO will review the SARs and responses from the Account Officers /Relationship Managers or other concerned staff. If the explanation for the exception does not appear reasonable then the Branch/Unit Head should review the transactions prior to considering submitting them to the regional AMLCO or CAMLCO.

6.3.9. If the Branch/Unit Head and / or AMLCO believe the transaction should be reported then the AMLCO will supply the relevant details to the RAMLCO or the CAMLCO.

6.3.10. The RAMLCO and CAMLCO will investigate any reported accounts and will send a status report on any of the accounts reported. No further action should be taken on the account until notification has been received.

6.3.11. If, after confirming with the client, the transaction trend is to continue the Account Officer is responsible for documenting the reasons why the transaction profile has changed and should amend the KYC profile accordingly.

6.4 Suspicious Activity Reporting Process

6.4.1 *Financial Institutions* must establish written internal procedures so that, in the event of a suspicious activity being discovered, all staff is aware of the reporting chain and the procedures to follow. Such procedures should be periodically updated to reflect any regulatory changes.

6.4.2 *Financial Institutions* should ensure that staff report all suspicious activities to their Branch/Unit level AMLCO, and that any such report be considered in the light of all other

relevant information by the AMLCO, or by another designated person, for the purpose of determining whether or not the information or other matter contained in the report does give rise to a knowledge or suspicion (See section 2 Umah of the AML Circular #2).

6.4.3 Where staff continues to encounter suspicious activities on an account, which they have previously reported to the *AMLCO*, they should continue to make reports to the *AMLCO* whenever a further suspicious transaction occurs, and the *AMLCO* should determine whether a disclosure in accordance with the regulations is appropriate.

6.4.4 All reports of suspicious activities must reach the CAMLCO and only the CAMLCO should have the authority to determine whether a disclosure in accordance with the regulation is appropriate. However the line/relationship manager can be permitted to add his comments to the suspicion report indicating any evidence as to why he/she believes the suspicion is not justified.

6.4.5 Detailed procedures on reporting of suspicious activities are given in Chapter VIII of this Guidance Notes.

6.5 Self-Assessment Process

Each financial institution should establish an annual self-assessment process that will assess how effectively the financial institution's anti-money laundering procedures enable management to identify areas of risk or to assess the need for additional control mechanisms. The self-assessment should conclude with a report documenting the work performed, who performed it, how it was controlled and supervised and the resulting findings, conclusions and recommendations. The self-assessment should advise management whether the internal procedures and statutory obligations of the financial institution have been properly discharged. The report should provide conclusions to three key questions:

- Are anti-money laundering procedures in place?
- Are anti-money laundering procedures being adhered to?
- Do anti-money laundering procedures comply with all policies, controls and statutory requirements?

6.6 System of Independent Procedures Testing

Testing is to be conducted at least annually by the financial institution's internal audit personnel, compliance department, and by an outside party such as the institution's external auditors. The tests include:

- interviews with employees handling transactions and interviews with their supervisors to determine their knowledge and compliance with the financial institution's anti-money laundering procedures;
- a sampling of large transactions followed by a review of transaction record retention forms and suspicious transaction referral forms;
- a test of the validity and reasonableness of any exemptions granted by the financial institution; and
- a test of the record keeping system according to the provisions of the *Act*.

Any deficiencies should be identified and reported to senior management together with a request for a response indicating corrective action taken or to be taken and a deadline

CHAPTER VII: RECORD KEEPING

7.1. Statutory Requirements

7.1.1 The requirement contained in Section 19 Ka of the Act to retain correct and full records of customers' identification and transactions at least for five years after termination of relationships with the customers is an essential constituent of the audit trail that the law seek to establish.

7.1.2 If the law enforcement agencies investigating a money laundering case cannot link funds passing through the financial system with the original criminal money, then confiscation of those funds cannot be made. Often the only valid role required of a financial institution in a money laundering investigation is as a provider of relevant records, particularly where the money launderer has used a complex web of transactions specifically for the purpose of confusing the audit trail.

7.1.3 The records prepared and maintained by any financial institution on its customer relationships and transactions should be such that:

- requirements of legislation and Bangladesh Bank directives are fully met;
- competent third parties will be able to assess the institution's observance of money laundering policies and procedures;
- any transactions effected via the institution can be reconstructed;
- any customer can be properly identified and located;
- all suspicious reports received internally and those made to Bangladesh Bank can be identified; and
- the institution can satisfy within a reasonable time any enquiries or court orders from the appropriate authorities as to disclosure of information.

7.1.4 Where there has been a report of a suspicious activity or the Institution is aware of a continuing investigation into money laundering relating to a client or a transaction, records relating to the transaction or the client should be retained until confirmation is received that the matter has been concluded.

7.2 Documents Verifying Evidence of Identity and Transaction Records

7.2.1 Records relating to verification of identity will generally comprise:

- a description of the nature of all the evidence received relating to the identity of the verification subject;
- the evidence itself or a copy of it or, if that is not readily available, information reasonably sufficient to obtain such a copy.

7.2.2 Records relating to transactions will generally comprise:

- details of personal identity, including the names and addresses, etc. as prescribed by Bangladesh Bank under AML Circular # 2 and subsequent directives pertaining to:
  (1) the customer;
  (2) the beneficial owner of the account or product;
  (3) the non-account holder conducting any significant one-off transaction;
  (4) any counter-party;
- details of transaction including:
  (5) the nature of such transactions;
  (6) Customer's instruction(s) and authority(ies);
  (7) source(s) and volume of funds;
  (8) destination(s) of funds;
  (9) book entries;
  (10) custody of documentation;
  (11) the date of the transaction;
  (12) the form (e.g. cash, cheque) in which funds are offered and paid out.

7.2.3 These records of identity must be kept for at least five years from the date when the relationship with the customer has ended. This is the date of:

i. the carrying out of the one-off transaction, or the last in a series of linked one-off transactions; or
ii. the ending of the business relationship; or
iii. the commencement of proceedings to recover debts payable on insolvency.

7.3 Formats and Retrieval of Records

7.3.1 To satisfy the requirements of the law, it is important that records are capable of retrieval without undue delay. It is not necessary to retain documents in their original hard copy form, provided that the firm has reliable procedures for holding records in microfiche or electronic form, as appropriate, and that these can be reproduced without undue delay. In addition, an institution may rely on the records of a third party, such as a bank or clearing house in respect of details of payments made by customers. However, the primary requirement is on the institution itself and the onus is thus on the business to ensure that the third party is willing and able to retain and, if asked to, produce copies of the records required.

7.3.2 However, the record requirements are the same regardless of the format in which they are kept or whether the transaction was undertaken by paper or electronic means. Documents held centrally must be capable of distinguishing between the transactions relating to different customers and of identifying where the transaction took place and in what form.

7.4 Wire Transfer Transactions

7.4.1 Investigations of major money laundering cases over the last few years have shown that criminals make extensive use of telegraphic transfers (TT) and electronic payment and message systems. The rapid movement of funds between accounts in different jurisdictions increases the complexity of investigations. In addition, investigations become even more difficult to pursue if the identity of the original ordering customer or the ultimate beneficiary is not clearly shown in a TT and electronic payment message instruction.

7.4.2 Following the recent focus on terrorist financing, relevant financial businesses are required to include accurate and meaningful originator (name, account number, and where possible address) and beneficiary information (account name and/or account number) on all outgoing funds transfers and related messages that are sent, and this information should remain with the transfer or related message throughout the payment chain. Institutions should conduct enhanced scrutiny of and monitor for suspicious incoming funds transfers which do not contain meaningful originator information.

7.4.3 The records of electronic payments and messages must be treated in the same way as any other records in support of entries in the account and kept for a minimum of five years.

7.5 Investigations

7.5.1 Where an institution has submitted a report of suspicious activity to Bangladesh Bank (see Chapters VI and VIII of these Guidance Notes) or where it knows that a client or transaction is under investigation, it should not destroy any relevant records without the agreement of the Bangladesh Bank even though the five-year limit may have been reached.

7.5.2 Financial Institutions should maintain a register or tabular records of all investigations made to it by the Bangladesh Bank and all disclosures to the Bangladesh Bank. The register should be kept separate from other records and contain as a minimum the following details:

i. the date and nature of the enquiry,
ii. details of the account(s) involved; and
iii. be maintained for a period of at least 5 years.

7.6 Training Records

So that *Financial Institutions* can demonstrate that they have complied with the regulations concerning staff training, they should maintain records which include:-

(i) details of the content of the training programs provided;
(ii) the names of staff who have received the training;
(iii) the date on which the training was delivered;
(iv) the results of any testing carried out to measure staff understanding of the money laundering requirements; and
(v) an on-going training plan.

CHAPTER VIII: RECOGNITION AND REPORTING OF SUSPICIOUS TRANSACTIONS

8.1 Recognition of Suspicious Transactions

8.1.1 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. It is more than the absence of certainty that someone is innocent. A person would not be expected to know the exact nature of the criminal offence or that the particular funds were definitely those arising from the crime. However, a suspicious transaction will often be one that is inconsistent with a customer's known, legitimate business or personal activities or with the normal business for that type of customer. Therefore, the first key to recognition is knowing enough about the customer's business to recognize that a transaction, or series of transactions, is unusual.

8.1.2 Questions that a financial Institution must consider when determining whether an established customer's transaction must be suspicious are:

- Is the size of the transaction consistent with the normal activities of the customer ?
- Is the transaction rational in the context of the customer's business or personal activities ?
- Has the pattern of transactions conducted by the customer changed ?
- Where the transaction is international in nature, does the customer have any obvious reason for conducting business with the other country involved ?

8.1.3 Examples of what might constitute suspicious transactions are given by types of business in Annexure G. **These are not intended to be exhaustive and only provide examples of the most basic way by which money may be laundered.** However, identification of any of the types of transactions listed in Annexure G should prompt further investigation and be a catalyst towards making at least initial enquiries about the source of funds.

8.2 Reporting of Suspicious Transactions

8.2.1 There is a statutory obligation on all staff to report suspicions of money laundering. Section 19 Ga of the Act contains the requirement to report to the Bangladesh Bank. Actual reporting should be made in accordance with an internal reporting procedure to be established by a financial institution for the purposes of facilitating the operation of the reporting obligation.

8.2.2 In line with accepted practice, some businesses may choose to require that such unusual or suspicious transactions be drawn initially to the attention of supervisory management to ensure that there are no known facts that will negate the suspicion before further reporting on to the Anti Money Laundering Compliance Officer or an appointed deputy.

8.2.3 Each institution has a clear obligation to ensure:

- that each relevant employee knows to which person they should report suspicions, and
- that there is a clear reporting chain under which those suspicions will be passed without delay to the Chief Anti Money Laundering Compliance Officer.

8.2.4 Once employees have reported their suspicions to the appropriate person in accordance with an established internal reporting procedure they have fully satisfied the statutory obligations.

8.2.5 Financial institutions must refrain from carrying out transactions which they know or suspect to be related to money laundering until they have apprised the Bangladesh Bank. Where it is impossible in the circumstances to refrain from executing a suspicious transaction before reporting to the Bangladesh Bank or where reporting it is likely to frustrate efforts to pursue the beneficiaries of a suspected money laundering operation, the financial institutions concerned shall apprise the Bangladesh Bank immediately afterwards. While it is impossible to spell out in advance how to deal with every possible contingency, in most cases common sense will suggest what course of action is most appropriate. Where there is doubt, the advice of the Anti Money Laundering Compliance Officers may be sought.

8.2.6 It is the Chief Anti Money Laundering Compliance Officer (CAMLCO) who will have the responsibility in financial institutions for communicating reports of suspicious transactions to the Anti-Money Laundering Department of Bangladesh Bank and who will provide the liaison between the financial institution and the Bangladesh Bank.

8.2.7 The CAMLCO has a significant degree of responsibility and should be familiar with all aspects of the legislation. He/she is required to determine whether the information or other matters contained in the transaction report he/she has received give rise to a knowledge or suspicion that a customer is engaged in money laundering.

8.2.8 S/he must take steps to validate the suspicion in order to judge whether or not a report should be submitted to Bangladesh Bank. In making this judgment, the CAMLCO should consider all other relevant information available within the financial institution concerning the person or business to which the initial report relates. This may include a review of other transaction patterns and volumes through the account or accounts in the same name, the length of the relationship, and referral to identification records held. If, after completing this review, the CAMLCO decides that there are no facts that would negate the suspicion, then he must disclose the information to Bangladesh Bank.

8.2.9 The determination of whether or not to report implies a process with at least some formality attached to it. It does not necessarily imply that the CAMLCO must give reasons for negating, and therefore not reporting any particular matter, but it clearly would be prudent for internal procedures to require that written reports are submitted and that he/she should record his/her determination in writing. Clearly in cases where there is a doubt it would be prudent for the CAMLCO to make a report to the Bangladesh Bank.

8.2.10 It is therefore imperative that the CAMLCO has reasonable access to information that will enable him/her to undertake his/her responsibility. In addition, the reference in the above sub-section 8.2.9 to "determination" implies a process with some formality. It is important therefore that the CAMLCO should keep a written record of every matter reported to him, of whether or not the suggestion was negated or reported, and of his reasons for his decision.

8.2.11 The CAMLCO will be expected to act honestly and reasonably and to make his determinations in good faith. Provided the CAMLCO or an authorized deputy does act in good faith in deciding not to pass on any suspicions report, there will be no liability for non-reporting if the judgment is later found to be wrong.

8.2.12 Care should be taken to guard against a report being submitted as a matter of routine to Bangladesh Bank without undertaking reasonable internal enquiries to determine that all available information has been taken into account.

8.3 Internal Reporting Procedures and Records

8.3.1 Reporting lines should be as short as possible, with the minimum number of people between the person with the suspicion and the CAMLCO. This ensures speed, confidentiality and accessibility to the CAMLCO. However, in line with accepted practice, some financial sector businesses may choose to require that such unusual or suspicious transactions be drawn initially to the attention of supervisory management to ensure that there are no known facts that will negate the suspicion before further reporting to the CAMLCO or an appointed deputy through the branch/unit level AMLCO.

8.3.2 **Supervisors** should also be aware of their own legal obligations. An additional fact which the supervisor supplies may negate the suspicion in the mind of the person making the initial report, but not in the mind of the supervisor. The supervisor then has a legal obligation to report to the AMLCO.

8.3.3 **Larger institutions** may choose to appoint deputy AMLCOs within divisions or branches, to enable the validity of the suspicion to be examined before being passed to CAMLCO. In such cases, the role of the deputy AMLCOs must be clearly specified and documented. All procedures should be documented in appropriate manual and job descriptions.

8.3.4 **All suspicions reported** to the AMLCO should be documented (in urgent cases this may follow an initial discussion by telephone). In some organizations it may be possible for the person with the suspicion to discuss it with the AMLCO and for the report to be prepared jointly. In other organizations the initial report should be prepared and sent to the AMLCO. The report should include the full details of the customer and as full a statement as possible of the information giving rise to the suspicion.

8.3.5 **The AMLCO should acknowledge receipt** of the report and at the same time provide a reminder of the obligation to do nothing that might prejudice enquiries, i.e. "tipping off". All internal enquiries made in relation to the report, and the reason behind whether or not to submit the report to the authorities, should be documented. This information may be required to supplement the initial report or as evidence of good practice and best endeavors if, at some future date, there is an investigation and the suspicions are confirmed

8.3.6 **On-going communication** between the AMLCO and the reporting person/department is important. The institution may wish to consider advising the reporting person, department or branch of the AMLCO's decision, particularly if the report is believed to be invalid. Likewise, at the end of an investigation, consideration should be given to advising all members of staff concerned of the outcome. It is particularly important that the AMLCO is informed of all communication between the investigating officer and the branch/unit concerned at all stages of the investigation.

8.3.7 **Records of suspicions**, which were raised internally with the CAMLCO but not disclosed to Bangladesh Bank, should be retained for five years from the date of the transaction. Records of suspicions which the Bangladesh Bank has advised are of no interest should be retained for a

similar period. Records of suspicions that assist with investigations should be retained until the financial institution is informed by the Bangladesh Bank that they are no longer needed.

8.4 Reporting Procedures

8.4.1 The national reception point for reporting of suspicions by the CAMLCO is:

The General Manager
Anti-Money Laundering Department
Bangladesh Bank
Head Office
Dhaka

8.4.2 The Anti Money Laundering Department of Bangladesh Bank can be contacted during office hours at the following numbers:

Telephone: (02) 7120659 and (02) 7120371
Fax: (02) 9566212
Email: gmamlbb@bangla.net

8.4.3 The use of a standard format in the reporting of suspicious activities is important and all institutions are required to use the unusual/suspicious transactions reporting form as per Annexure GA of the AML Circular No.2 dated 17th July 2002. Suspicious activity reports should be typed whenever possible or, if the standard layout is followed, generated on word-processing software. Institutions using popular commercial software packages may be able to take advantage of form-based document and template features. Further information and advice can be obtained from the Anti Money Laundering Department of Bangladesh Bank.

8.4.4 Sufficient information should be disclosed on the suspicious transaction, including the reason for the suspicion, to enable the investigating officer to conduct appropriate enquiries. If a particular offence is suspected, this should be stated so that the report may be passed to the appropriate investigation team with the minimum of delay. However, it is not necessary to complete all sections of the suspicious activity report form and its submission should not be delayed if particular details are not available.

8.4.5 Where additional relevant evidence is held which could be made available to the investigating officer, this should be noted on the form.

8.4.6 Following the submission of a suspicious activity report, an institution is not precluded from subsequently terminating its relationship with a customer, provided it does so for normal commercial reasons. It must not alert the customer to the fact of the disclosure as to do so would constitute a "tipping-off" offence. Close liaison with Anti Money Laundering Department of Bangladesh Bank and the investigating officer is encouraged in such circumstances so that the interests of all parties may be fully considered.

CHAPTER IX: TRAINING AND AWARENESS

9.1 Statutory Requirements

9.1.1 Section 4 (Umah) of the Act requires Bangladesh Bank to provide training to the staff/officers of banks, financial institutions and other institutions engaged in financial activities in order to combat money laundering.

9.1.2 Since financial institutions themselves have responsibilities under the Act in relation to identification, reporting and record retention, it follows that they must ensure that their staffs are adequately trained to discharge their responsibilities.

9.1.3 It is therefore imperative for all financial institutions to take appropriate measures to make employees aware of:

- policies and procedures to prevent money laundering and for identification, record keeping and internal reporting;
- the legal requirements; and
- to provide relevant employees with training in the recognition and handling of suspicious transactions.

9.1.4 The Act does not specify the nature of the training to be given and these Guidance Notes therefore set out what steps might be appropriate to enable institutions to fulfill this requirement.

9.2 The Need for Staff Awareness

9.2.1 The effectiveness of the procedures and recommendations contained in these Guidance Notes must depend on the extent to which staff in institutions appreciates the serious nature of the background against which the legislation has been enacted. Staff must be aware of their own personal statutory obligations and that they can be personally liable for failure to report information in accordance with internal procedures. All staff must be trained to co-operate fully and to provide a prompt report of any suspicious transactions.

9.2.2 It is, therefore, important that financial institutions introduce comprehensive measures to ensure that all staff and contractually appointed agents are fully aware of their responsibilities.

9.3 Education and Training Programs

9.3.1 Timing and content of training packages for various sectors of staff will need to be adapted by individual businesses for their own needs. However it is recommended that the following might be appropriate.

9.3.2 All relevant staff should be educated in the process of the "know your customer" requirements for money laundering prevention purposes. The training in this respect should cover not only the need to know the true identity of the customer but also, where a business relationship is being established, the need to know enough about the type of business activities expected in relation to that customer at the outset to know what might constitute suspicious activity at a

future date. Relevant staff should be alert to any change in the pattern of a customer's transactions or circumstances that might constitute criminal activity.

9.3.3 Although Directors and Senior Managers may not be involved in the day-to-day procedures, it is important that they understand the statutory duties placed on them, their staff and the institution itself. Some form of high-level general awareness raising training is therefore suggested.

9.4 New Employees

A general appreciation of the background to money laundering, and the subsequent need for reporting any suspicious transactions to the Anti Money Laundering Compliance Officer (AMLCO) should be provided to all new employees who are likely to be dealing with customers or their transactions, irrespective of the level of seniority. They should be made aware of the importance placed on the reporting of suspicions by the organization, that there is a legal requirement to report, and that there is a personal statutory obligation to do so.

9.5 Customer Service/Relationship Managers/Tellers/Foreign Exchange Dealers

9.5.1 Members of staff who are dealing directly with the public are the first point of contact with potential money launderers and their efforts are vital to the organization's strategy in the fight against money laundering. They must be made aware of their legal responsibilities and should be made aware of the organization's reporting system for such transactions. Training should be provided on factors that may give rise to suspicions and on the procedures to be adopted when a transaction is deemed to be suspicious.

9.5.2 It is vital that 'front-line' staffs are made aware of the organization's policy for dealing with non-regular (walk in) customers particularly where large transactions are involved, and the need for extra vigilance in these cases.

9.6 Processing (Back Office) Staff

Those members of staff who receive completed Account Opening, Payment Order/DD/TT/FDR application forms and cheques for deposit into customer's account or other investments must receive appropriate training in the processing and verification procedures. Those members of staff, who are in a position to deal with account opening, or to accept new customers, must receive the training given to cashiers and other front office staff above. In addition, the need to verify the identity of the customer must be understood, and training should be given in the organization's account opening and customer/client verification procedures. Such staff should be aware that the offer of suspicious funds or the request to undertake a suspicious transaction may need to be reported to the Anti Money Laundering Compliance Officer (or alternatively a line supervisor) whether or not the funds are accepted or the transactions proceeded with and must know what procedures to follow in these circumstances.

9.7 Senior Management/Operations Supervisors and Managers

A higher level of instruction covering all aspects of money laundering procedures should be provided to those with the responsibility for supervising or managing staff. This will include the offences and penalties arising from the Act for non-reporting and for assisting money launderers; internal reporting procedures and the requirements for verification of identity and the retention of records.

9.8 Anti Money Laundering Compliance Officer

In depth training on all aspects of the Money Laundering Legislation, Bangladesh Bank directives and internal policies will be required for the Anti Money Laundering Compliance Officer. In addition, the AMLCO will require extensive instructions on the validation and reporting of suspicious transactions and on the feedback arrangements, and on new trends and patterns of criminal activity.

9.9 Refresher Training

In addition to the above relatively standard requirements, training may have to be tailored to the needs of specialized areas of the institution's business. It will also be necessary to keep the content of training programs under review and to make arrangements for refresher training at regular intervals i.e. at least annually to ensure that staff does not forget their responsibilities. Some financial sector businesses may wish to provide such training on an annual basis; others may choose a shorter or longer period or wish to take a more flexible approach to reflect individual circumstances, possibly in conjunction with compliance monitoring.

ANNEXURES

Annexure A: Model Account Application Form for Individual Accounts

ACCOUNT APPLICATION FORM – INDIVIDUAL ACCOUNT

I / We apply to open account(s) with …….. (the "Bank") in the currency(s) mentioned below. I / We agree to provide any document requested by the Bank according to the type of Account(s) applied. I / We hereby confirm that I / We have gone through the Bank's Individual Account Conditions which I / We accept entirely and agree to be bound by such terms and conditions as amended and supplemented from time to time.

[Please tick (√) appropriately]

I / We hereby request the opening of an account with ……..in the following manner.

Capacity : Single Joint

Account Category Current Account Savings Account Fixed Deposit Account
Other, *(Please Specify)*:----------

Account Currency Bangladesh Taka United States Dollars
Other Foreign Currency, (Please Specify):----------

Customer Type **Bangladesh National** Resident in Bangladesh Non-Resident
Foreign National Resident in Bangladesh Non-Resident

Account Title *(Please Specify) :* ----------

CUSTOMER INFORMATION – PRIMARY APPLICANT

Name : Mr./Mrs./Ms./Dr./Other, *(Please Specify) :* ----------

Father's /Husband's Name : ----------

Mother's Name : ----------

Marital Status : Married Single Other, *(Please Specify)*:

Date of Birth : ---------- Passport No : ----------

Nationality : ---------- TIN : ----------

Permanent Address : ----------

Mailing Address : ----------

(if different from above) : ----------

Occupation : ---------- Income (Per month):----------

Employer : ----------

Employer's Address : ----------

Contact Details : Telephone *(Home)* : ---------- Telephone *(Office)* : ----------

: Telephone *(Mobile)* : ---------- E-mail : ----------

Existing Banker : ----------

(1) CUSTOMER INFORMATION – JOINT APPLICANT

Name : Mr./Mrs./Ms./Dr./Other, *(Please Specify) :* ----------

Father's / Husband's Name : ----------

Mother's Name : ----------

Marital Status : Married Single Other, *(Please Specify)*:

Date of Birth : ---------- Passport No : ----------

Nationality : ---------- TIN : ----------

Permanent Address : ----------

Mailing Address : ----------

(if different from above) : ----------

Occupation : ---------- Income (Per month):----------

Employer : ----------

Employer's Address : ----------

Contact Details: Telephone *(Home)* : ---------- Telephone *(Office)* : ----------

Telephone *(Mobile)* : ---------- - E-mail : ----------

Existing Banker : ----------

Signature(s) of Customer(s)

Primary Applicant		**Joint Applicant**		**Joint Applicant**	
Name		Name		Name	
Date		Date		Date	

Introduced by :

Name :	**Signature :**
Account No. :	**Address :**

For Bank Use Only

Initial Deposit		Account Number		Date	
Category A - Approver			Category B - Approver		

Annexure B: Model Account Application Form for Corporate Accounts

ACCOUNT APPLICATION FORM – CORPORATE ACCOUNT

We apply to open account(s) with …….. (the "Bank") in the currency(s) mentioned below. We agree to provide any document requested by the Bank according to the type of Account(s) applied. We hereby confirm receipt of the Bank's Account Conditions which we accept entirely.

[Please tick (√) appropriately]

We hereby request opening of account(s) with ……..

Residency	Resident	Non-Resident
Account Category	Current Account	Convertible Account
	Fixed Deposit Account	Special Notice Deposit Account
	Other, *(Please Specify)*:----------	
Account Currency	Bangladesh Taka	
	United States Dollars	
	Other Foreign Currency, (Please Specify):----------	
Customer Type	Limited Liability Company Incorporated in Bangladesh	
	Limited Liability Company Incorporated Overseas	
	Sole Proprietorship	
	Partnership	
	NGO / Unincor porated Association	
	Other, (Please Specify): ----------	

Account Title *(Please Specify) :* ----------

TAX INFORMATION ***[Applicable for Fixed Deposit(s) / Short Notice Deposit Account(s)***

Tax Not Exempt Tax Identification Number : ----------

Tax Exempt Approval Dated : ----------(Copy Enclosed)

DEPOSIT INFORMATION ***[Applicable for Fixed Deposits(s)***

Title of the Deposit : ----------
Amount : (in words):----------
(in figures):----------Interest Rate : ----------(%)

Tenor	Three Month	Six Month	Twelve Month
	Other, *(Please specify):* ----------		
Deposit by	Cash		
	Cheque Number ----------dated----------drawn on		

----------*(Bank Name)*

We authorize you to debit our Account Number ----------with you

DEPOSIT INFORMATION

Maturity Instructions :

Credit principal and interest to our Account Number----------with you

Renew principal Only and credit interest to our Account Number---------- ----with you

Renew principal Only and mail your cheque for the Interest to our address

Mail your cheque for the principal & Interest together to our address----------

Renew principal Only and mail your cheque for the Interest to our Account Number----------with----------*(Bank Name)*

Mail your cheque for the principal & Interest to our Account Number----------with ----------*(Bank Name)*

Authorized Signature(s) of the Customer with the Company Seal

Signature	
Name	
Title	

Signature	
Name	
Title	

Introduced by :

Name :	**Signature :**
Account No. :	**Address :**

For Bank Use Only

Initial Deposit		Account Number		Date	
Category A - Approver		Category B – Approver			

Annexure C: Model Transaction Profile

Transaction Profile

Bank Products Required	***No. of Transactions*** *(monthly)*	***Maximum Size*** *(per Transaction)*	***Total Value*** *(monthly)*
Outgoing FCY Transfers			
Outgoing LCY Transfers Drafts / Travelers Checks			
Cash Withdrawals			
Check Payment			
Pay Link Payments			
FX Products			
MM Products (Deposits)			
Letters of Credit / Guarantees			
Loan Facilities			
Investment Transactions			
Payroll Cards			
Other (Specify)			
Expected Sources of Funds			
Incoming FCY Transfers			
Incoming LCY Transfers			
Cash Deposits			
Check Deposits			
Cash Collection			
Outstation Cash Collections			
Outstation Check Collections			
FCY Check Collections			
Export Proceeds			
Other (Specify)			

Note: Please use additional sheets if required

I/We, the undersigned, hereby confirm that this Transaction Profile truly represents the transactions arising out of the normal course of business of our organization. I/We also confirm to revise our Transact Profile, if necessary, from time to time.

Signature		Signature

Name Title Date	

Name Title Date

Annexure D: KYC Profile Form

Customer/Account Name:

Account or Reference Number:

Name of Account Officer/Relationship Manager/ Officer Opening the Account:

Source of funds and nature of business

What is the nature of the business relationship and source of funds.

Describe how the source of funds have been verified and confirmation of whether or not the levels, types of amounts of transactions are commensurate with nature of the business described when the relationship was established.

1. Who is the actual owner of the account (*i.e. account holder acting as an agent/trustee*)?

……

……

2. Original Passport/ID sighted & photocopy obtained. YES NO
(*If no, obtain deferral*)

3. For non-resident & foreigners ensure the reason for opening the account in Bangladesh
(*i.e. why not in the country of residence/ origin*)

Type of visa (Resident / Work) ……..

……

……

……

4. What does the Customer Do?

Category	**Risk level**	**Rating**
Jewelry /Gems trade	High	5
Money transmitters/changers	High	5
Real Estate Agents	High	5
Construction promoters of projects	High	5
Offshore Corporation	High	5
Art/antique dealers	High	5
Restaurant/Bar/casino/night club owners	High	5
Traders with a turnover of more than 1 crore per annum	High	4

Import/Export agents	High	5
Cash Intensive business (cash deposit > 25 lacs in a month)	High	5
Share & Stock broker	High	5
Finance Companies (NBFI)	High	5
Travel agents	High	4
Transport Operators	Medium	3
Auto dealers (used/ reconditioned cars)	Medium	3
Auto Primary(new car)	Low	2
Shop owner (retail)	Low	2
Business – Agents, Franchisees	Low	2
Small trader (turnover less than 50 lacs per annum)	Low	2
Software business	Low	1
Manufacturers (other than arms)	Low	1
Retired from service	Low	0
Service	Low	0
Self employed professiona ls	Low	2
Operations in multiple locations	High	5
Corporate Customers of Repute (irrespective of the category)	Low	2

5. What is the net worth / sales turnover of the customer?

Amount (Tk.)	**Risk level**	**Risk rating**
1-50 Lacs	Low	0
50 L – 200 L	Medium	1
> 2 crores	High	3

6. How was the a/c opened?

Mode	**Risk level**	**Risk rating**
RM/Affiliate	Low	0
DSA	Medium	1
Internet	High	3
Walk-in / Unsolicited	High	3

7. Expected Value of transactions on a monthly basis.

Value for CA (Tk. Lacs)	**Value for SA (Tk. Lacs)**	**Risk level**	**Risk rating**
0 - 10	0 - 5	Low	0
10 – 50	5 - 20	Medium	1
> 50	> 20	High	3

8. Expected Number of transactions on a monthly basis

Number for CA	**Number for SA**	**Risk level**	**Risk rating**
0 – 100	0 - 20	Low	0
101 – 250	21 - 50	Medium	1
> 250	> 50	High	3

9. Expected Value of Cash Transactions on a monthly basis

Value for CA	**Value for SA**	**Risk level**	**Risk rating**

(Tk. Lacs)	(Tk. Lac)		
0 – 10	0 - 2	Low	0
11 - 25	3 - 7	Medium	1
> 25	> 7	High	3

10. Expected Number of Cash Transactions on a monthly basis

Number for CA	Number for SA	Risk level	Risk rating
0 - 15	0 - 5	Low	0
15 - 30	6 - 10	Medium	1
> 30	> 10	High	3

Overall Risk Assessment:

Risk rating	*Risk assessment*
>=14	**high**
<14	**low**

Comments:

……
……
……
……
……

Account Officer/RM's Signature: Approver's Signature:	Approver's Signature:
Special Approvals obtained: …… …… …… ……	

Complete the profile form for high net worth customers falling under the following criterion:

a) New Customers whose initial deposit is more than Tk. 50 Lacs (initial means within One month of A/c opening)
b) Existing customers whose total AUM (Asset under Management) grow to > Tk. 50 Lacs for 3 consecutive months

List of Questions to be used when obtaining source of wealth

KYC REQUIREMENT FOR HIGH NET WORTH CUSTOMERS.
APPENDIX I

A. Source of Wealth

Type of source of wealth:

❒ Business ownership	❒ Top executive	❒ Inheritance
❒ Profession *	❒ Investments *	❒ Other

Instructions: Please refer to the list of questions to be used when obtaining source of wealth
You may need to choose more than one category for a business owner with inherited wealth

B. Notes of Face-to-face meeting with customers.

C. Annual Review of Customer Profile

Profession – E.g. Physician, lawyer, engineer, accountants and sports professional etc.
Investments – Someone who buys and sells assets of any type: real estate, securities, companies, royalties and patents etc.

Prepared by:	**Account Officer/ Relationship Manager**	**Reviewed by:**	**Branch Manager/Branch Operations Head**
Name:		**Name:**	
Date:		**Date:**	

Note: This form must be renewed every year

List of Questions to be used when obtaining source of wealth

Wealth Generated From Business Ownership

- Description and nature of the business and its operations
- Ownership type: private or public?
- What kind of company?
- Percent of ownership?
- Estimated sales volume?
- Estimated net income?
- Estimated net worth?
- How long in business?
- How was the business established?
- Other owners or partners (yes/no)?
- Names of other owners or partners?
- Percent owned by other owners or partners?
- Number of employees
- Number of locations?
- Geographic trade areas of business
- Other family members in business?
- Significant revenues from government contract or licenses?

Wealth Derived From Being a Top Executive

- Estimate of compensation?
- What does the company do? (for example, manufacturer, service...)
- Position held (for example, President, CFO)
- Length of time with company?
- Area of expertise (for example, finance, production, etc...)
- Publicly or privately owned?
- Client's past experience (for example, CFO at another company...)

Primary Source of Wealth was Through Inheritance

- In what business was the wealth generated?
- Inherited from whom?
- Type of asset inherited (for example: land, securities, company trusts...)
- When were the assets inherited?
- How much was inherited?
- Percent ownership for a business that is inherited

Wealth Generated From a Profession (Physician, dentist, lawyer, engineer, entertainer, professional sports...)

- What is the profession, including area of specialty (ex: arts - singer, construction - engineer)
- Source of wealth (Ex: lawyer who derived wealth from real estate, Dr. running a clinic...)
- Estimate of income

Wealth Generated From Investments

- Where did the source of wealth come from? (example, invested in shares, bonds, etc.)
- What do they currently invest in? (for example, real estate, stock market...)

- What is the size of the investment?
- Cite notable public transactions if any
- What is the client's role in transaction (ex: takes positions, buy companies, middle man)
- Estimated annual income/capital appreciation?
- How long has the client been an investor?

Annexure E: Identification of Directors & Authorised Signatories

(Company letterhead)

The Manager
(Name & Address of Financial Institution)

Date: ……

Sub: Identification of Directors & Authorized signatories

This is to introduce the following directors of the company & authorized signatories of the account(s) of the company maintained with your bank.

Name **Designation**	**Father's Name** **Mother's Name**	**Date of birth** **Nationality** **TIN**	**Present Address**	**Permanent Address**

We certify that information provided above is true and correct. Please treat this letter together with duly attested photographs of the above individuals attached herewith on separate sheet, as Photo Identification document.

Sincerely

…….
Chairman/ Secretary (Name & Seal)

(Company Stamp)

Annexure F: Explanation to Walk-in / One-off Customers

The AML Circular # 2 requires us to obtain satisfactory evidence of identification of applicants who do not maintain accounts with us for conducting one off transactions. You are therefore kindly requested to provide the following details, together with appropriate documentary evidence, before this transaction may proceed.

Thank you for your co-operation.

NAME	
Date of birth	Nationality
Father's Name	Mother's Name
ADDRESS	
Other Identification (ID Card number, Passport details etc)	
Value of Transaction	
Date	Signed

Note:
This is an example document which institutions who are regularly engaged in one-off transactions may care to adapt to their own requirements for obtaining verification of identity in accordance with the regulations.

Annexure G: Examples of Potentially Suspicious Transactions

Financial Institutions may wish to make additional enquiries in the following circumstances

BANKING TRANSACTIONS

Cash transactions

- Unusually large cash deposits made by an individual or company whose ostensible business activities would normally be generated by cheques and other instruments.

- Substantial increases in cash deposits of any individual or business 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.

- Customers who deposit cash by means of numerous credit slips so that the total of each deposit is unremarkable, but the total of all the credits is significant.

- Company accounts whose transactions, both deposits and withdrawals, are denominated by cash rather than the forms of debit and credit normally associated with commercial operations (e.g. cheques, Letters of Credit, Bills of Exchange, etc.).

- Customers who constantly pay in or deposit cash to cover requests for payment order, bankers drafts, money transfers or other negotiable and readily marketable money instruments.

- Customers who seek to exchange large quantities of low denomination notes for those of higher denomination.

- Branches that have a great deal more cash transactions than usual. (Head Office statistics detect aberrations in cash transactions.)

- Customers whose deposits contain counterfeit notes or forged instruments.

- Customers transferring large sums of money to or from other locations with instructions for payment in cash.

- Large cash deposits using ATM facilities, thereby avoiding direct contact with bank or building society staff.

Accounts

- Customers who wish to maintain a number of trustee or client accounts which do not appear consistent with the type of business, including transactions which involve nominee names.

- Customers who have numerous accounts and pay in amounts of cash to each of them in circumstances in which the total of credits would be a large amount.

- Any individual or company whose account shows virtually no normal personal banking or business related activities, but is used to receive or disburse large sums which have no obvious purpose or relationship to the account holder and/or his business (e.g. a substantial increase in turnover on an account).

- Reluctance to provide normal information when opening an account, providing minimal or fictitious information or, when applying to open an account, providing information that is difficult or expensive for the financial institution to verify.

- Customer's reluctance or refusal to disclose other banking relationships.

- Home address or business location is far removed from the Branch where the account is being opened and the purpose of maintaining an account at your Branch cannot be adequately explained.

- Reluctance or refusal to provide business financial statements.

- Information provided by the customer in the Transaction Profile does not make sense for the customer's business.

- A visit to the place of business does not result in a comfortable feeling that the business is in the business they claim to be in.

- Customers who appear to have accounts with several financial institutions within the same locality, especially when the bank is aware of a regular consolidation process from such accounts prior to a request for onward transmission of the funds.

- Matching of payments out with credits paid in by cash on the same or previous day.

- Paying in large third party cheques endorsed in favor of the customer.

- Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit from abroad.

- Customers who together, and simultaneously, use separate tellers to conduct large cash transactions or foreign exchange transactions.

- Greater use of safe deposit facilities. Increased activity by individuals. The use of sealed packets deposited and withdrawn.

- Companies' representatives avoiding contact with the branch.

- 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.

- Customers who show an apparent disregard for accounts offering more favorable terms

- Customers who decline to provide information that in normal circumstances would make the customer eligible for credit or for other banking services that would be regarded as valuable.

- Insufficient use of normal banking facilities, e.g. avoidance of high interest rate facilities for large balances.

- Large number of individuals making payments into the same account without an adequate explanation.

International banking/trade finance

- Customer introduced by an overseas branch, affiliate or other bank based in countries where production of drugs or drug trafficking may be prevalent.

- Use of Letters 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.

- Customers who make regular and large payments, including wire transactions, that cannot be clearly identified as bona fide transactions to, or receive regular and large payments from: countries which are commonly associated with the production, processing or marketing of drugs; proscribed terrorist organizations; [tax haven countries].

- Building up of large balances, not consistent with the known turnover of the customer's business, and subsequent transfer to account(s) held in other locations.

- Unexplained electronic fund transfers by customers on an in and out basis or without passing through an account.

- Frequent requests for TCs, foreign currency drafts or other negotiable instruments to be issued.

- Frequent paying in of TCs or foreign currency drafts, particularly if originating from overseas.

- Customers who show apparent disregard for arrangements offering more favorable terms.

Institution employees and agents

- Changes in employee characteristics, e.g. lavish life styles or avoiding taking holidays.

- Changes in employee or agent performance, e.g. the salesman selling products for cash have a remarkable or unexpected increase in performance.

- Any dealing with an agent where the identity of the ultimate beneficiary or counterpart is undisclosed, contrary to normal procedure for the type of business concerned.

Secured and unsecured lending

- Customers who repay problem loans unexpectedly.

- Request to borrow against assets held by the financial institution or a third party, where the origin of the assets is not known or the assets are inconsistent with the customer's standing.

- Request by a customer for a financial institution to provide or arrange finance where the source of the customer's financial contribution to a deal is unclear, particularly where property is involved.

- Customers who unexpectedly repay in part or full a mortgage or other loan in a way inconsistent with their earnings capacity or asset base.

MERCHANT BANKING BUSINESS

New business

- A personal client for whom verification of identity proves unusually difficult and who is reluctant to provide details.

- A corporate/trust client where there are difficulties and delays in obtaining copies of the accounts or other documents of incorporation.

- A client with no discernible reason for using the firm's service, e.g. clients whose requirements are not in the normal pattern of the institution's business and could be more easily serviced elsewhere.

- An investor introduced by an overseas bank, affiliate or other investor, when both investor and introducer are based in countries where production of drugs or drug trafficking may be prevalent.

- Any transaction in which the counterparty to the transaction is unknown.

Dealing patterns and abnormal transactions

Dealing patterns

- A large number of security transactions across a number of jurisdictions.

- Transactions not in keeping with the investor's normal activity, the financial markets in which the investor is active and the business which the investor operates.

- Buying and selling of a security with no discernible purpose or in circumstances which appear unusual, e.g. churning at the client's request.

- Low grade securities purchases and sales, with the proceeds used to purchase high grade securities.

- Bearer securities held outside a recognized custodial system.

Abnormal transactions

- A number of transactions by the same counterparty in small amounts of the same security, each purchased for cash and then sold in one transaction, the proceeds being credited to an account different from the original account.

- Any transaction in which the nature, size or frequency appears unusual, e.g. early termination of packaged products at a loss due to front end loading, or early cancellation, especially where cash had been tendered and/or the refund cheque is to a third party.

- Transactions not in keeping with normal practice in the market to which they relate, e.g. with reference to market size and frequency, or at off-market prices.

- Other transactions linked to the transaction in question which could be designed to disguise money and divert it into other forms or to other destinations or beneficiaries.

Settlements

Payment

- A number of transactions by the same counterparty in small amounts of the same security, each purchased for cash and then sold in one transaction.

- Large transaction settlement by cash.

- Payment by way of third party cheque or money transfer where there is a variation between the account holder, the signatory and the prospective investor, must give rise to additional enquiries.

Delivery

- Settlement to be made by way of bearer securities from outside a recognized clearing system.

- Allotment letters for new issues in the name of persons other than the client.

Disposition

- Payment to a third party without any apparent connection with the investor.

- Settlement either by registration or delivery of securities to be made to an unverified third party.

- Abnormal settlement instructions including payment to apparently unconnected parties.

Annexure H: Internal Suspicious Activity Report Form

Strictly Private & confidential

To	Anti Money Laundering Compliance Officer	Date:
From	Name (Mr./ Ms)	Branch/Department
	Job Title	SAR Ref No.

***Note**: This form may be completed in **English**. For any queries, please contact AMLCO. Please provide full details of the transaction(s) and any other relevant data. Attach copies of relevant documents/transaction notes.*

Customer/ Business Name	Transaction Date(s)
Account Number(s)	Copies of Transactions and Account Details Attached ⬭ Yes ⬭ No
Description of Transaction(s). *(Nature of transaction, Origin & destination of Transaction etc)*	
Source of Funds and Purpose of Transaction (*If you can, try to tactfully ask the customer*)	
Reasons why you think the transaction is suspicious (*Give as much details as possible*) Signatures of Bank Staff.	
TO BE COMPLETED BY AMLCO.	

ACTION TAKEN TO VALIDATE

- Acknowledgement sent to the originator on _____.
- Reviewed account documentation
- Discuss with the relationship manager/ branch manager.
- Other.

AGREED SUSPICIOUS. Yes/No

COMMENTS / NOTES OF AMLCO

Signature
AMLCO Date.

Annexure I: Internal Control Checklist

	Yes	No
Have you carried out a review of processes in your business to identify where money laundering is most likely to occur?		
Is this review regularly updated?		
Have you established procedures and controls to prevent or detect money laundering?		
Is the effectiveness of such controls tested?		
Do online or electronic transactions circumvent these controls?		
Do you have a comprehensive written policy on money laundering?		
Is all staff aware of this policy?		
Does your money laundering policy include clear guidelines on accepting corporate hospitality and gifts?		
Is all staff aware of their responsibilities with regard to money laundering?		
Do they receive regular money laundering training?		
Are all members of staff sufficiently capable of identifying suspicious transactions?		
Are your systems capable of highlighting suspicious transactions (i.e. those not conforming to usual parameters)?		
Do all members of staff know the identity of their Anti Money Laundering Compliance Officer (AMLCO)?		
Are your systems capable of providing the AMLCO will all the information required for the Annual Management Report?		
Do you thoroughly check and verify the identity of all your clients?		
Do you have client accounts in the name of fictitious persons/ entities?		

Do you know the identity of the beneficial owner of all your corporate clients?

Is this identity verified?

Are all suspicious transactions reported to Bangladesh Bank?

Annexure J:

(The following is an English translation of the Act and incorporates its amendment (Act No. 3 of 2003). Strikethrough words mean that these were removed while those in italic mean that these were inserted by the amendment. In case of any dispute the official Bangla versions of the Acts shall prevail).

Money Laundering Prevention Act, 2002 (Act No.7 of 2002)

Whereas it is just and necessary to prepare rules with a view to preventing money laundering, Therefore, it is enacted as under :

First Chapter

Introduction

1. **Short Title and Introduction.-**(1) This Act will be called as 'Money Laundering Protirodh (Prevention) Ain (Act), 2002

(2) This Act will be in force on the date to be fixed through Government Gazette;

2. **Definition.-** If nothing is contrary to the subject and reference, in this Act-

(Ka) " Illegal means" will mean any means which is not recognized by any Act, Rules or Regulations;

(Kha) "Crime" means any crime under this Act,

(Ga) "Court" means Money Laundering Court";

(Gha) Financial Institution" means financial institution defined under Section 2 (Kha) of Financial Institution Act,1993 (Act No.-27of 1993);

~~(Umah) "Code of Civil Procedure" means Code of Civil Procedure, 1908 (Act V of 1908);~~

(Cha) " Court of Session" means Court of Session mentioned in Section 6 of Code of Criminal Procedure;

(Chaa) "Determined" means determined by rules;

(Ja) "Code of Criminal Procedure" means Code of Criminal Procedure, 1898 (Act V of 1898);

(Jha) "Rule" means rule prepared under this Act;

(Eionh) "Bangladesh Bank" means Bangladesh Bank established under the Bangladesh Bank Order, 1972 (P.O. No. 127 of 1972;

(Ta) "Bank" means the Bank Company defined by Section 5(Na) of Bank Company Ain (Act), 1991 (Act No. 14 of 1991);

(Tha) "Money Laundering" means

(Au) Properties acquired or earned directly or indirectly through illegal means;

(Aa) Illegal transfer, conversion, concealment of location or assistance in the above act of the properties acquired or earned directly of indirectly through legal or illegal means;

(Da) "Properties" means movable or immovable properties of any nature and description;

(Dha) "Supreme Court" means Bangladesh Supreme Court constituted under Paragraph 94 of the Constitution of the People's Republic of Bangladesh;

(Na) "High Court" means the High Court Division of the Supreme Court

3. **Supremacy of the Act.-** Not withstanding whatever may contain in any other Act in force, the provisions of this Act will remain in force.

Second Chapter

Responsibility and power of Bangladesh Bank in preventing Money Laundering

4 . **Responsibility of Bangladesh Bank in preventing Money Laundering.-** The responsibility of Bangladesh Bank will be to prevent and resist crime of money laundering and for resisting such criminal activities –

(Ka) To conduct enquiry about the crime of money laundering;

(Kha) Observe and supervise the activities of banks, financial institutions and other financial institutions engaged in financial activities;

(Ga) To invite statement from the banks, financial institutions and other institutions engaged in financial activities about any matter connected with money laundering;

(Gha) Examination of the statement received under (Ga) above and taking of proper action accordingly;

(Umah) To give training to the staff/officer of the bank, financial institutions and other institutions engaged in financial activities.

(Cha) To perform other work in fulfillment of the objective of this Act.

5 . **Power of enquiry, etc.—**(1) Bangladesh Bank or any person authorized by Bangladesh Bank can enquire into the crime committed under this Act and other related issues and for such enquiry if it is required to enter in to any place the same can be done after following the required system.

(2) In case of enquiry in to a matter the power which an Officer in Charge of a Police Station can exercise under the Code of Civil Procedure Bangladesh Bank or any person authorized by Bangladesh Bank will be able to exercise the same power while enquiring into the crime committed under this Act.

Third Chapter

Money Laundering Court

6. **Establishment of Money Laundering Court.** (1) In order to fulfill the objective of this Act all Courts of Sessions will be regarded as Money Laundering Court and all Session Judges will be the justice of Money Laundering Court.

(2) Session Judge will settle all cases under this Act himself or he can send the case to any Additional Session Judge under him for settlement.

7. **Jurisdiction of the Court.** (1) The Court will be able to impose the prescribed punishment for the crime committed under this Act and in applicable cases pass other orders including order for enquiry, confinement, seizure, fine and compensation.

(2) If the crime under other Act is associated with the crime under another Act in such a manner that in order to dispense justice it is necessary to proceed for trial for the both crimes together or cases are to be instituted together, then trial for the crime committed under this Act can be done at the same time under other Act in the same Court.

But the condition is this that if money laundering is associated with the schedule of crimes under such Act which is imprisonable for a period less than three years the same will not be treated as a punishment under this Act.

8. **Acceptance of the crime for trial etc.** (1) Notwithstanding what is contained in any other laws all crimes under this Act will be cognizable for trial under this Act.

(2) All crimes under this Act will be Non-bailable.

(3) Subject to other provisions of this Act, no accused or punishable person will be released on bail, if--

(Ka) no opportunity is given to the complainant party on the application for releasing him on bail.

(Kha) The Court is satisfied that there is reasonable ground to adjust him guilty on the charges brought against him; or

(Ga) The Court is satisfied that the justice will not be hindered if he is released on bail.

9. **Application of Code of ~~Civil and~~ Criminal Procedure, etc**.-(1) If nothing otherwise exists in this Act, provisions of the Code of ~~Civil and~~ Criminal Procedures will be applicable ~~as the case may be~~ in case of filing of complain, enquiry, seizure, attachment of property, trial and settlement for the crimes under this Act.

(2) Person conducting cases in the Court on behalf of the complainant will be called as Public Prosecutor.

(3) The Court will be able to order the enquiry officer to do further enquiry on the crime of the cases under trial and in such cases the Court will be able to fix up time limit for submission of the above enquiry report.

10. **Legal seizure of property.--** On the basis of written application from Bangladesh Bank or any person authorized by Bangladesh Bank the Court will issue legal seizure of property to this effect that the property of the accused in whatever condition it may remain will be banned from sale or transfer.

11. **Freezing of the property.--** (1) On the basis of written application of Bangladesh Bank or person authorized by Bangladesh Bank the Court will issue Freezing Order for the properties of the person who is accused under this Act.

(2) If the Freezing Order is issued as per Sub-section (1) above

(Ka) The Court will publish it in the form of Notification in the Bangladesh Gazette and national daily for information of general public.

(Kha)The concerned property will in no way can be transferred or the concerned property can not be made encumbered..

(3) In the Freezing Order under this Section, the name of the accused, designation, name of father and mother, address, profession etc should be mentioned as far as possible.

(4) If the bank account of the accused is under Freezing Order, if nothing contrary is mentioned in the above Order, all receivables of the accused will be credited in the frozen bank account.

~~12. **Appeal.**----- Whatever different may exist in the Code of Civil and Criminal Procedures, the aggrieved party aggrieved by order, judgment, decree or punishment imposed by the Court will be able to appeal in the High Court within 30 days of the date of the above order, judgment, decree or punishment order.~~

*12. **Appeal.**----- Whatever different may exist in the Code of Criminal Procedures, the party aggrieved by order, judgment or punishment imposed by the Court will be able to appeal in the High Court within 30 days of the date of the such order, judgment or punishment.*

Fourth Chapter

Crime and Punishment

13. **Punishment for Money Laundering**----(1) If any person is engaged in Money Laundering in any way he will be regarded as a person who has committed a crime.
(2) The concerned accused for the crime mentioned in Sub-section (1) will be sentenced to imprisonment for at least a period of six months and a maximum of seven years and will be fined for an amount not exceeding double the amount involved in the crime.

14 **Punishment for violation of seizure order.**- ~~(1)~~ If any person violates the seizure order under Section 10 he will be imprisoned for ~~at least~~ one year *maximum* or fined for ~~at least~~ Taka ten thousand *maximum* or he may be punished with both.

15 **Punishment for violation of the Freezing Order.**- ~~(1)~~ If any person violates the Freezing Order under Section 11 he will be imprisoned for ~~at least~~ one year *maximum* or fined for ~~at least~~ Taka five thousand *maximum* or he may be punished with both.

16 **Punishment for divulgation of information. –** (1) No person will obstruct the enquiry or divulge information relating to enquiry or relevant other information to other person with a view to casting adverse influence on the enquiry.
(2) If any person violates the provision of Sub-section (1) he will be imprisoned for ~~at least~~ one year *maximum* or fined for ~~at least~~ Taka ten thousand *maximum* or he may be punished with both.

17. **Punishment for obstruction in enquiry.**- (1) No person will express his unwillingness without any reasonable ground to assist the enquiry officer in his enquiry activities under this Act.
(2) If any person violates the provision of Sub-section (1) he will be imprisoned for ~~at least~~ one year *maximum* or fined for ~~at least~~ Taka ten thousand *maximum* or he may be punished with both

Fifth Chapter

Miscellaneous

18. **Agreement with the Foreign Country.—**(1) The government may enter in to agreement with any foreign country in order to fulfill the objective of this Act.
(2) If any agreement is entered into with a foreign country under Sub-section (1) above, the government will declare the name of such country as the 'country under agreement' in order to fulfill the objective of this Act by Notification in the Government Gazette.

19 **Responsibility of the banks, financial institutions and other institutions engaged in financial activities in preventing and identifying money laundering—**(1) In checking and identifying money laundering banks, financial institutions and other institutions engaged in financial activities—
(Ka) As a client of it , it should preserve the correct and full information of all of its clients and in the event of closing of transactions it should preserve records of transactions for at least five years from the date of closure;
(Kha) Will provide the records so preserved as per Sub-section (Ka) above to Bangladesh Bank from time to time on demand;
(Ga) Information regarding abnormal transactions and doubtful transactions which are likely to be related to money laundering should be informed to Bangladesh Bank.

(2) Bangladesh Bank will determine the information to be preserved as per Sub-section (1) and issue Circular or Gazette Notification from time to time.

(3) In the event of failure of providing and preserving the information as mentioned in Sub-section (1) Bangladesh Bank will inform the licensing authority of the defaulting bank, financial institution and other institutions engaged in financial activities so that the concerned authority can take proper action for negligence and failure against the concerned bank, financial institution and other institution engaged in financial activities as per their own rule or provision.

(4) Whatever may contain in Sub-section (3), Bangladesh Bank will be able to impose fine up to a maximum of Taka one lac and a minimum of Taka ten thousand to the defaulting bank, financial institution and other institution engaged in financial activities for failure to preserve and supply information as mentioned in Sun-section (3) and also for negligence.

20. **Crime committed by the Company etc.—**(1) If the violator of any provision of this Act is a company, it will be regarded that each proprietor, director, manager, secretary or any other officer or employee or representative of the company has violated the provision :

But the condition is this that the concerned person will not be responsible for the violation if he can prove that the above violation has been done beyond his knowledge or he has failed to check the violation despite his best effort.

Explanation :- In this section—

(Ka) "Company" will mean any company, statutory body, partnership concern, Association or institution formed with one or more than one person;

(Kha) "Director" will mean any partner or member of the Board of Director in whatever name it is called.

(2) Registration of the company which is engaged in money laundering directly or indirectly will be liable to be cancelled.

21. **Power to frame rules.—**Government by Notification in Government Gazette will be able to frame rules in order to fulfill the objective of this Act.

Schedule

[Reference - conditions of Section 7(2)]

(Ka) Penal Code, 1860 (XLV of 1860);
(Kha) Arms Act, 1878 (XL of 1878)
(Ga) Foreign Exchange Regulation Act, 1947 (VII of 1947);
(Gha) Anti-Corruption Act, 1957 (XXVI of 1957);
(Umah) Special Power Act, 1974 (XIV of 1974);
(Cha) Madak Drabwa Niatran Ain (Drugs Control Act), 1990 (Act No. 20 of 1990);
~~(Chaa) Jana Nirapatra (Bishesh Bidhan)Ain [Public Safety(Special power) Act], 2000 (Act No. 7 of 2000);~~
(Ja) Nari O Shishu Nirjatan Daman Ain (Women and Children Oppression Prevention Act), 2000 (Act No.-8 of 2000);
(Jha) Aain-sringkhola Bighnokari Aporadh (Druto Bichar) Aain, 2002. (Crimes obstructing law & order (speedy trial) Act), (Act No. 11 of 2002).

Annexure K:

সূচী

ধারা পৃষ্ঠা

বিষয়

প্রথম অধ্যায়
প্রারম্ভিক

১। সংক্ষিপ্ত শিরোনাম ও প্রবর্তন ২
২। সংজ্ঞা ২
৩। আইনের প্রাধান্য ৩

দ্বিতীয় অধ্যায়
মানি লন্ডারিং প্রতিরোধে বাংলাদেশ ব্যাংকের দায়িত্ব ও ক্ষমতা

৪। মানি লন্ডারিং প্রতিরোধে বাংলাদেশ ব্যাংকের দায়িত্ব ৪
৫। তদন্তের ক্ষমতা, ইত্যাদি ৪

তৃতীয় অধ্যায়
মানি লন্ডারিং আদালত

৬। মানি লন্ডারিং আদালত প্রতিষ্ঠা ৫
৭। আদালতের এখতিয়ার ৫
৮। অপরাধ বিচারার্থ গ্রহণ, ইত্যাদি ৫
৯। দেওয়ানী কার্যবিধি ও ফৌজদারী কার্যবিধির প্রয়োগ,ইত্যাদি ৬
১০। সম্পত্তির ক্রোকাদেশ ৬
১১। সম্পদ অবরুদ্ধকরণ ৬
১২। আপীল ৭

চতুর্থ অধ্যায়
অপরাধ ও দন্ড

১৩। মানি লন্ডারিং এর শাস্তি ৮
১৪। ক্রোকাদেশ লংঘনের শাস্তি ৮
১৫। অবরুদ্ধকরণ আদেশ লংঘনের শাস্তি ৮
১৬। তথ্য ফাঁসকরণের শাস্তি ৮
১৭। তদন্তে বাধা দেওয়ার শাস্তি ৮

পঞ্চম অধ্যায়
বিবিধ

১৮। বিদেশী রাষ্ট্রের সহিত চুক্তি ৯
১৯। মানি লন্ডারিং প্রতিরোধ ও সনাক্তকরণে ব্যাংক,আর্থিক প্রতিষ্ঠান এবং আর্থিক কর্মকান্ডের সহিত জড়িত অন্যান্য সংস্থার দায়-দায়িত্ব ৯
২০। কোম্পানী ইত্যাদি কর্তৃক অপরাধ সংঘটন ১০
২১। বিধি প্রণয়নের ক্ষমতা ১০

তফসিল ১১

(মানি লন্ডারিং প্রতিরোধ আইন, ২০০২ সংশোধনকল্পে প্রণীত আইন (২০০৩ সনের ৩ নং আইন) এর ধারাসমূহ ইহাতে সন্নিবেশিত হইয়াছে। বিলুপ্ত অংশ কাটা অক্ষরে এবং নতুন সংযোজিত অংশ বাঁকা অক্ষরে দেখানো হইয়াছে)।

রেজিষ্টার্ড নং ডি এ-১

বাংলাদেশ (মনোগ্রাম) **গেজেট**

অতিরিক্ত সংখ্যা
কর্তৃপক্ষ কর্তৃক প্রকাশিত

রবিবার, এপ্রিল ৭, ২০০২

বাংলাদেশ জাতীয় সংসদ

ধাকা, ৭ই এপ্রিল,২০০২/২৪শে চৈত্র,১৪০৮

সংসদ কর্তৃক গৃহীত নিম্নলিখিত আইনটি ৫ই এপ্রিল, ২০০২ (২২শে চৈত্র, ১৪০৮) তারিখে রাষ্ট্রপতির সম্মতি লাভ করিয়াছে এবং এতদ্বারা এই আইনটি সর্বসাধারণের অবগতির জন্য প্রকাশ করা যাইতেছে ঃ-

২০০২ সনের ৭নং আইন

মানি লন্ডারিং প্রতিরোধের উদ্দেশ্যে বিধান প্রণয়নকল্পে প্রণীত আইন

যেহেতু মানিলন্ডারিং প্রতিরোধের উদ্দেশ্যে বিধান প্রণয়ন করা সমীচীন ও প্রয়োজনীয়;

সেহেতু এতদ্‌দ্বারা নিম্নরূপ আইন করা হইলঃ

প্রথম অধ্যায়
প্রারম্ভিক

১। সংক্ষিপ্ত শিরোনাম ও প্রবর্তন ।- (১) এই আইন মানিলন্ডারিং প্রতিরোধ আইন, ২০০২ নামে অভিহিত হইবে ।

(২) সরকার, সরকারী গেজেটে প্রজ্ঞাপন দ্বারা, যেই তারিখ নির্ধারণ করিবে সেই তারিখে এই আইন বলবৎ হইবে ।

২। সংজ্ঞা । - বিষয় বা প্রসংগের পরিপন্থী কোন কিছু না থাকিলে, এই আইনে-

(ক) "অবৈধ পন্থা" অর্থ এই আইনের অধীন কোন অপরাধ;

(খ) "অপরাধ" অর্থ এই আইনের অধীন কোন অপরাধ;

(গ) "আদালত" অর্থ মানিলন্ডারিং আদালত ;

(ঘ) "আর্থিক প্রতিষ্ঠান" অর্থ আর্থিক প্রতিষ্ঠান আইন, ১৯৯৩ (১৯৯৩ সনের ২৭ নং আইন) এর ধারা ২ (খ)-তে সংজ্ঞায়িত আর্থিক প্রতিষ্ঠান;

~~(ঙ) "দেওয়ানী কার্যবিধি" অর্থ Code of Civil Procedure, 1908 (Act V of 1908);~~

(চ) "দায়রা আদালত" অর্থ ফৌজদারী কার্যবিধির section 6-এ উল্লিখিত Courts of Session;

(ছ) "নির্ধারিত" অর্থ বিধি দ্বারা নির্ধারিত;

(জ) "ফৌজদারী কার্যবিধি" অর্থ Code of Criminal Procedure, 1898 (Act V of 1898);

(ঝ) "বিধি" অর্থ এই আইনের অধীন প্রণীত বিধি;

(ঞ) "বাংলাদেশ ব্যাংক" অর্থ The Bangladesh Bank Order, 1972 (P.O.No. 127 of 1972) এর অধীন স্থাপিত Bangladesh Bank.

(ট) "ব্যাংক" অর্থ ব্যাংক কোম্পানী আইন, ১৯৯১ (১৯৯১ সনের ১৪ নং আইন) এর ধারা ৫(ণ)-তে সংজ্ঞায়িত ব্যাংক কোম্পানী;

(ঠ) "মানিলন্ডারিং" অর্থ-

(অ) অবৈধ পন্থায় প্রত্যক্ষ বা পরোক্ষভাবে আহরিত বা অর্জিত সম্পদ;

(আ) বৈধ বা অবৈধ পন্থায় প্রত্যক্ষ বা পরোক্ষভাবে আহরিত বা অর্জিত সম্পদের অবৈধ পন্থায় হস্তান্তর, রূপান্তর, অবস্থানের গোপনকরণ বা উক্ত কাজে সহায়তা করা;

(ড) "সম্পদ" অর্থ যে কোন প্রকৃতির ও বর্ণনার স্থাবর বা অস্থাবর সম্পদ;

(ধ) "সুপ্রীম কোর্ট" অর্থ গণপ্রজাতন্ত্রী বাংলাদেশের সংবিধানের ৯৪ অনুচ্ছেদ দ্বারা গঠিত বাংলাদেশ সুপ্রীম কোর্ট;

(ণ) "হাইকোর্ট বিভাগ" অর্থ সুপ্রীম কোর্টের হাইকোর্ট বিভাগ ।

৩। **আইনের প্রাধান্য** ।– আপাততঃ বলবৎ অন্য কোন আইনে যাহা কিছুই থাকুক না কেন, এই আইনের বিধানাবলী কার্যকর থাকিবে ।

দ্বিতীয় অধ্যায়
মানি লন্ডারিং প্রতিরোধে বাংলাদেশ ব্যাংকের দায়িত্ব ও ক্ষমতা

৪। **মানি লন্ডারিং প্রতিরোধে বাংলাদেশ ব্যাংকের দায়িত্ব** । - বাংলাদেশ ব্যাংকের দায়িত্ব হইবে মানিলন্ডারিং অপরাধ দমন ও প্রতিরোধ এবং উক্তরূপ অপরাধমূলক তৎপরতা রোধ করিবার উদ্দেশ্যে-

(ক) মানিলন্ডারিং অপরাধ সম্পর্কে তদন্ত পরিচালনা;

(খ) ব্যাংক, আর্থিক প্রতিষ্ঠান এবং আর্থিক কর্মকান্ডের সহিত জড়িত অন্যান্য সংস্থার কার্যতৎপরতা দাপ্তরিক এবং পর্যবেক্ষণ;

(গ) ব্যাংক, আর্থিক প্রতিষ্ঠান এবং আর্থিক কর্মকান্ডের সহিত জড়িত অন্যান্য সংস্থার নিকট হইতে মানিলন্ডারিং সম্পর্কিত কোন বিষয়ে প্রতিবেদন আহ্বান করা;

(ঘ) দফা (গ) এর অধীন প্রাপ্ত প্রতিবেদন পর্যালোচনা এবং তদনুযায়ী ব্যবস্থা গ্রহণ;

(ঙ) ব্যাংক, আর্থিক প্রতিষ্ঠান এবং আর্থিক কর্মকান্ডের সহিত অন্যান্য সংস্থার কর্মকর্তা ও কর্মচারীদের প্রশিক্ষণ প্রদান ;

(চ) এই আইনের উদ্দেশ্য পূরণকল্পে অন্যান্য কার্য সম্পাদন ।

৫। **তদন্তের ক্ষমতা, ইত্যাদি** ।- (১) বাংলাদেশ ব্যাংক অথবা বাংলাদেশ ব্যাংকের নিকট হইতে ক্ষমতাপ্রাপ্ত কোন ব্যক্তি এই আইনের অধীন কোন অপরাধ বা সংশ্লিষ্ট অন্যান্য বিষয়ে তদন্ত করিতে পারিবে এবং তদন্তের উদ্দেশ্যে কোন স্থানে প্রবেশের প্রয়োজন হইলে তিনি নির্ধারিত পদ্ধতি অনুসরণ করিয়া উক্ত স্থানে প্রবেশ করিতে পারিবেন ।

(২) কোন অপরাধ তদন্তের ক্ষেত্রে ধানার ভারপ্রাপ্ত কর্মকর্তা ফৌজদারী কার্যবিধির অধীনে যে ক্ষমতা প্রয়োগ করিতে পারেন, এই আইনের অধীন কোন অপরাধ তদন্তের ক্ষেত্রে বাংলাদেশ ব্যাংক অথবা বাংলাদেশ ব্যাংকের নিকট হইতে ক্ষমতাপ্রাপ্ত ব্যক্তি একইরূপ ক্ষমতা প্রয়োগ করিতে পারিবেন ।

৪

তৃতীয় অধ্যায়
মানিলন্ডারিং আদালত

৬। **মানিলন্ডারিং আদালত প্রতিষ্ঠা** ।- (১) এই আইনের উদ্দেশ্য পূরণকল্পে সকল দায়রা আদালত মানিলন্ডারিং আদালত বলিয়া গণ্য হইবে এবং সকল দায়রা জজ মানিলন্ডারিং আদালতের বিচারক হইবেন ।

(২) এই আইনের অধীন সকল মামলা দায়রা জজ নিজে নিষ্পত্তি করিবেন অধবা তাহার অধীনস্থ যে কোন অতিরিক্ত দায়রা জজের নিকট নিষ্পত্তির জন্য প্রেরণ করিতে পারিবেন ।

৭। **আদালতের এখতিয়ার** ।- (১) আদালত এই আইনের অধীন অপরাধের জন্য নির্ধারিত দন্ড আরোপ এবং উপযুক্ত ক্ষেত্রে তদন্তাদেশ, অবরুদ্ধকরণাদেশ, ক্রোকাদেশ, অর্ধদন্ড এবং ক্ষতিপূরণ আদেশসহ অন্যান্য আদেশ প্রদান করিতে পারিবে ।

(২) যদি এই আইনের অধীন কোন অপরাধের সহিত অন্য কোন আইনের কোন অপরাধ এমনভাবে জড়িত ধাকে যে, ন্যায়বিচারের স্বার্থে উভয় অপরাধের বিচার একই সংগে বা একই মামলায় করা প্রয়োজন, তাহা হইলে এই আইনের অধীন অপরাধের বিচার উক্ত অন্য আইনের অধীন অপরাধের সহিত একই সংগে উক্ত আদালতে করা যাইবে ঃ

তবে শর্ত ধাকে যে, এই আইনের তফসিলে বর্ণিত কোন আইনের অধীন অর্ধ্ব তিন বৎসর কারাদন্ডযোগ্য কোন অপরাধের সহিত মানিলন্ডারিং জড়িত ধাকিলে উহা এই আইনের অধীন অপরাধ বলিয়া গণ্য হইবে না ।

৮। **অপরাধ বিচারার্থ গ্রহ, ইত্যাদি** । - (১) অন্য কোন আইনে যাহা কিছুই ধাকুক না কেন, এই আইনের অধীন দন্ডনীয় সকল অপরাধ বিচারার্থ গ্রহনীয় (cognizable) হইবে ।

(২) বাংলাদেশ ব্যাংক অধবা বাংলাদেশ ব্যাংকের নিকট হইতে ক্ষমতাপ্রাপ্ত কোন ব্যক্তির লিখিত অভিযোগ ব্যতীত কোন আদালত এই আইনের অধীন কোন অপরাধ বিচারের জন্য গ্রহণ করিবে না ।

(৩) এই আইনের অধীন সকল অপরাধ অ-জামিনযোগ্য (Non-bailable) হইবে ।

৫

(৪) এই আইনের অন্যান্য বিধান সাপেক্ষে, অভিযুক্ত বা শাস্তিযোগ্য কোন ব্যক্তিকে জামিনে মুক্তি দেওয়া হইবে না, যদি-

(ক) তাহাকে জামিনে মুক্তি দেওয়ার আবেদনের উপর অভিযোগকারী পক্ষকে শুনানীর সুযোগ দেওয়া না হয়; এবং

(খ) তাহার বিরুদ্ধে আনীত অভিযোগে তিনি দোষী সাব্যস্ত হওয়ার যুক্তিসঙ্গত কারণ রহিয়াছে মর্মে আদালত সন্তুষ্ট হন; অথবা

(গ) তাহাকে জামিনে মুক্তি দেওয়ার কারণে ন্যায় বিচার বিঘ্নিত হইবে না মর্মে আদালত সন্তুষ্ট না হন ।

৯। **~~দেওয়ানী কার্যবিধি ও~~ ফৌজদারী কার্যবিধির প্রয়োগ, ইত্যাদি** ।- (১) এই আইনে ভিন্নতর কিছু না থাকিলে, এই আইনের অধীন কোন অপরাধের অভিযোগ দায়ের, তদন্ত, ক্রোক, সম্পদ অবরুদ্ধকরণ, বিচার ও নিষ্পত্তির ক্ষেত্রে ~~, ক্ষেত্রমত দেওয়ানী কার্যবিধি ও~~ ফৌজদারী কার্যবিধির বিধানাবলী প্রযোজ্য হইবে ।

(২) আদালতে অভিযোগকারীর পক্ষে মামলা পরিচালনাকারী ব্যক্তি পাবলিক প্রসিকিউটর বলিয়া গণ্য হইবেন ।

(৩) আদালত উহার বিচারাধীন কোন মামলা সংক্রান্ত অপরাধ সম্পর্কে অধিকতর তদন্তের জন্য তদন্তকারী ব্যক্তিকে নির্দেশ দিতে পারিবে এবং উক্ত নির্দেশে তদন্তের প্রতিবেদন দাখিলের জন্য সময়সীমা নির্ধারণ করিয়া দিতে পারিবে ।

১০। **সম্পত্তির ক্রোকাদেশ** । - বাংলাদেশ ব্যাংক বা ইহার নিকট হইতে ক্ষমতাপ্রাপ্ত ব্যক্তির লিখিত আবেদনের ভিত্তিতে আদালত এই মর্মে ক্রোকাদেশ প্রদান করিতে পারিবে যে, অভিযুক্ত ব্যক্তির সম্পদ, যেখানে যে অবস্থায় থাকুক না কেন বিক্রয় বা হস্তান্তর নিষিদ্ধ থাকিবে ।

১১। **সম্পদ অবরুদ্ধকরণ** ।- (১) এই আইনের অধীন অভিযুক্ত ব্যক্তির সম্পদের বিষয়ে বাংলাদেশ ব্যাংক অথবা বাংলাদেশ ব্যাংকের নিকট হইতে ক্ষমতাপ্রাপ্ত ব্যক্তির লিখিত আবেদনের ভিত্তিতে আদালত উক্ত সম্পদ অবরুদ্ধকরণের জন্য আদেশ (Freezing order) প্রদান করিতে পারিবে ।

(২) উপ-ধারা (১) এর অধীন কোন অবরুদ্ধকরণ আদেশ প্রদান করা হইলে-

(ক) আদালত বিষয়টি সর্বসাধারণের অবগতির জন্য বাংলাদেশ গেজেট এবং জাতীয় দৈনিক পত্রিকায় বিজ্ঞপ্তি আকারে প্রচার করিবে;

(খ) সংশ্লিষ্ট সম্পদ হস্তান্তর বা উক্ত সম্পদকে কোনভাবে দায়যুক্ত করা যাইবে না ।

(৩) এই ধারার অধীন অবরুদ্ধকরণ আদেশে অভিযুক্ত ব্যক্তির নাম, পদবী, পিতা-মাতার নাম, ঠিকানা, পেশা ইত্যাদি যতদূর সম্ভব উল্লেখ থাকিবে ।

(৪) কোন ব্যক্তির ব্যাংক একাউন্ট অবরুদ্ধকরণের আদেশ কার্যকর থাকা অবস্থায়, উক্ত আদেশে ভিন্নরূপ উল্লেখ না থাকিলে, উক্ত ব্যক্তি প্রাপ্ত হইয়াছে এইরূপ সমুদয় অর্থ তাহার অবরুদ্ধ ব্যাংক একাউন্টে জমা হইবে ।

~~**১২। আপীল** ।- দেওয়ানী কার্যবিধি বা ফৌজদারী কার্যবিধিতে ভিন্নতর যাহা কিছুই থাকুক না কেন, আদালত কর্তৃক প্রদত্ত আদেশ, রায়, ডিক্রি বা আরোপিত দন্ড দ্বারা সংক্ষুব্ধ পক্ষ, উক্ত আদেশ, রায়, ডিক্রি বা দন্ডাদেশ প্রদানের তারিখ হইতে ত্রিশ দিনের মধ্যে হাইকোর্ট বিভাগে আপীল করিতে পারিবেন ।~~

১২। **আপীল** ।- ফৌজদারী কার্যবিধিতে ভিন্নতর যাহা কিছুই থাকুক না কেন, আদালত কর্তৃক প্রদত্ত আদেশ, রায় বা আরোপিত দন্ড দ্বারা সংক্ষুব্ধ পক্ষ, উক্ত আদেশ, রায় বা দন্ডাদেশ প্রদানের তারিখ হইতে ত্রিশ দিনের মধ্যে হাইকোর্ট বিভাগে আপীল করিতে পারিবেন ।

৭

চতুর্থ অধ্যায়
অপরাধ ও দন্ড

১৩। **মানিলন্ডারিং এর শাস্তি** ।- (১) কোন ব্যক্তি মানিলন্ডারিং এর সাথে কোনভাবে জড়িত থাকিলে তিনি অপরাধ করিয়াছেন বলিয়া গণ্য হইবেন ।

(২) উপ-ধারা (১) এর অধীন অপরাধের জন্য সংশ্লিষ্ট অপরাধী অন্যূন ছয় মাস এবং অনধিক সাত বৎসর কারাদন্ডে দন্ডনীয় হইবেন এবং অপরাধের সহিত জড়িত অর্থের অনধিক দ্বিগুন অর্থদন্ডে দন্ডনীয় হইবেন

১৪। **ক্রোকাদেশ লংঘনের শাস্তি** ।- ~~(১)~~ কোন ব্যক্তি ধারা ১০ এর অধীন ক্রোকাদেশ লংঘন করিলে তিনি ~~অন্যূন~~ অনূর্ধ্ব এক বৎসর কারাদন্ড বা ~~অন্যূন~~ অনূর্ধ্ব দশ হাজার টাকা অর্থদন্ড অথবা উভয় দন্ডে দন্ডনীয় হইবেন ।

১৫। **অবরুদ্ধকরণ আদেশ লংঘনের শাস্তি** ।- (১) কোন ব্যক্তি ধারা ১১ এর অধীন অবরুদ্ধকরণ আদেশ লংঘন করিলে তিনি ~~অন্যূন~~ অনূর্ধ্ব এক বৎসর কারাদন্ড বা ~~অন্যূন~~ অনূর্ধ্ব পাঁচ হাজার টাকা অর্থদন্ড বা উভয় দন্ডে দন্ডনীয় হইবেন

১৬। **তথ্য ফাঁসকরণের শাস্তি**।- (১) কোন ব্যক্তি এই আইনের অধীন কোন তদন্ত কার্যক্রম ব্যাহতকরণ বা উহাতে কোন বিরূপ প্রভাব বিস্তারের উদ্দেশ্যে তদন্ত সম্পর্কিত কোন তথ্য বা প্রাসংগিক অন্য কোন তথ্যঅন্য কোন ব্যক্তির নিকট ফাঁস করিবেন না ।

(২) কোন ব্যক্তি উপ-ধারা (১) এর বিধান লংঘন করিলে তিনি ~~অন্যূন~~ অনূর্ধ্ব এক বৎসর কারাদন্ড বা ~~অন্যূন~~ অনূর্ধ্ব দশ হাজার টাকা অর্থদন্ড বা উভয় দন্ডে দন্ডনীয় হইবেন ।

১৭। **তদন্তে বাধা দেওয়ার শাস্তি** ।- (১) এই আইনের অধীন কোন তদন্ত কার্যক্রমে সংশ্লিষ্ট কর্মকর্তাকে সহযোগিতা প্রদানে, কোন যুক্তিসংগত কারণ ব্যতিরেকে, কোন ব্যক্তি অস্বীকৃতি জ্ঞাপন করিবেন না ।

(২) কোন ব্যক্তি উপ-ধারা (১) এর বিধান লংঘন করিলে তিনি ~~অন্যূন~~ অনূর্ধ্ব এক বৎসর কারাদন্ড বা ~~অন্যূন~~ অনূর্ধ্ব দশ হাজার টাকা অর্থদন্ড বা উভয় দন্ডে দন্ডনীয় হইবেন ।

পঞ্চম অধ্যায়
বিবিধ

১৮। **বিদেশী রাষ্ট্রের সহিত চুক্তি** ।- (১) আইনের উদ্দেশ্য পূরণকল্পে সরকার কোন বিদেশী রাষ্ট্রের সহিত চুক্তি সম্পাদন করিতে পারিবে ।

(২) উপ-ধারা (১) এর অধীন কোন বিদেশী রাষ্ট্রের সহিত চুক্তি সম্পাদন করা হইলে সরকার, সরকারী গেজেটে প্রজ্ঞাপন দ্বারা, উক্ত বিদেশী রাষ্ট্রকে এই আইনের উদ্দেশ্য পূরণকল্পে চুক্তিবদ্ধ রাষ্ট্র হিসাবে ঘোষণা করিবে ।

১৯। **মানিলন্ডারিং প্রতিরোধ ও সনাক্তকরণে ব্যাংক, আর্থিক প্রতিষ্ঠান এবং আর্থিক কর্মকান্ডের সহিত জড়িত অন্যান্য সংস্থার দায়-দায়িত্ব** ।- (১) মানিলন্ডারিং প্রতিরোধ ও সনাক্তকরণে ব্যাংক, আর্থিক প্রতিষ্ঠান এবং আর্থিক কর্মকান্ডের সহিত জড়িত অন্যান্য সংস্থা-

(ক) উহার গ্রাহকের হিসাব পরিচালনাকালে সকল গ্রাহকের পরিচিতির সঠিক ও পূর্ণাঙ্গ তথ্য সংরক্ষণ করিবে এবং কোন গ্রাহকের হিসাবের লেনদেন বন্ধ হওয়ার ক্ষেত্রে উক্তরূপ বন্ধ হওয়ার দিন হইতে অন্যূন পাঁচ বৎসরকাল বিগত সময়ের লেনদেনের হিসাব সংরক্ষণ করিবে ;

(খ) দফা (ক) এর অধীন সংরক্ষিত তথ্যাদি সময় সময় বাংলাদেশ ব্যাংকে ইহার চাহিদা মোতাবেক সরবরাহ করিবে;

(গ) অস্বাভাবিক লেনদেন এবং মানিলন্ডারিং এর সহিত সংশ্লিষ্ট থাকিতে পারে এইরূপ সন্দেহজনক লেনদেন সম্পর্কিত তথ্য বাংলাদেশ ব্যাংকে সময় সময় অবহিত করিবে ।

(২) উপ-ধারা (১) এর অধীন সংরক্ষণযোগ্য তথ্যাদি নির্ধারণ করিয়া বাংলাদেশ ব্যাংক, সময় সময় পরিপত্র বা গেজেট বিজ্ঞপ্তি প্রকাশ করিবে ।

(৩) বাংলাদেশ ব্যাংক উপ-ধারা (১)-এ উল্লিখিত তথ্যাদি সংরক্ষণ ও সরবরাহে ব্যর্থতা বা অবহেলার জন্য দায়ী সংশ্লিষ্ট ব্যাংক, আর্থিক প্রতিষ্ঠান এবং আর্থিক কর্মকান্ডের সহিত জড়িত অন্যান্য সংস্থার ব্যবসায়িক কার্যক্রমের অনুমতি বা লাইসেন্স প্রদানকারী কর্তৃপক্ষকে অবহিত করিবে, যাহাতে সংশ্লিষ্ট কর্তৃপক্ষ স্ব-স্ব আইন বা বিধি বিধান মোতাবেক সংশ্লিষ্ট ব্যাংক, আর্থিক প্রতিষ্ঠান এবং আর্থিক কর্মকান্ডের সহিত জড়িত অন্যান্য সংস্থার অবহেলা বা ব্যর্থতার জন্য যথাযথ ব্যবস্থা গ্রহণ করিতে পারে ।

(৪) বাংলাদেশ ব্যাংক উপ-ধারা (৩)-এ যাহাই থাকুক না কেন, উপ-ধারা (১)-এ উল্লিখিত তথ্যাদি সংরক্ষণ ও সরবরাহে ব্যর্থতা বা অবহেলার জন্য দায়ী সংশ্লিষ্ট ব্যাংক, আর্থিক প্রতিষ্ঠান এবং আর্থিক কর্মকান্ডের সহিত জড়িত অন্যান্য সংস্থাকে অনূর্ধ্ব এক লক্ষ টাকা কিন্তু দশ হাজার টাকার কম নয় জরিমানা করিতে পারিবে ।

২০। **কোম্পানী ইত্যাদি কর্তৃক অপরাধ সংঘটন** ।-(১) এই আইনের অধীন কোন বিধান লংঘনকারী ব্যক্তি যদি কোম্পানী হয়, তাহা হইলে উক্ত কোম্পানীর প্রত্যেক মালিক, পরিচালক, ম্যানেজার, সচিব বা অন্য কোন কর্মকর্তা বা কর্মচারী বা প্রতিনিধি বিধানটি লংঘন করিয়াছেন বলিয়া গণ্য হইবেন ঃ

তবে শর্ত থাকে যে, সংশ্লিষ্ট ব্যক্তি যদি এইরূপ প্রমাণ করিতে সক্ষম হন যে, উক্ত লংঘন তাহার অজ্ঞাতসারে হইয়াছে অথবা উহার লংঘন রোধ করিবার জন্য তিনি যথাসাধ্য চেষ্টা করিয়া ব্যর্থ হইয়াছেন, তাহা হইলে উক্ত লংঘনের জন্য সংশ্লিষ্ট ব্যক্তি দায়ী হইবেন না ।

ব্যাখ্যা ।- এ ধারায়-

(ক) "কোম্পানী" বলিতে কোন কোম্পানী, সংবিধিবদ্ধ সংস্থা, অংশীদারী কারবার, সমিতি বা এক বা একাধিক ব্যক্তির সমন্বয়ে গঠিত সংগঠনকে বুঝাইবে ;

(খ) "পরিচালক" বলিতে কোন অংশীদার বা পরিচালনা বোর্ডে, যে নামেই অভিহিত হউক, এর সদস্যকেও বুঝাইবে ।

(২) কোন কোম্পানী প্রত্যক্ষ বা পরোক্ষভাবে মানিলন্ডারিং এর সাথে জড়িত থাকিলে উক্ত কোম্পানীর নিবন্ধন বাতিলযোগ্য হইবে ।

২১। **বিধি প্রণয়নের ক্ষমতা** ।- সরকার, সরকারী গেজেটে প্রজ্ঞাপন দ্বারা, এই আইনের উদ্দেশ্য পূরণকল্পে বিধি প্রণয়ন করিতে পারিবে ।

১০

তফসিল
[ধারা ৭(২) এর শর্তাংশ দ্রষ্টব্য]

(ক) Penal code, 1860 (XLV of 1860);
(খ) Arms Act, 1878 (XL of 1878);
(গ) Foreign Exchange Regulation Act, 1947 (VII of 1947);
(ঘ) Anti-Corruption Act. 1957 (XXVI of 1957);
(ঙ) Special Powers Act. 1974 (XIV of 1974);
(চ) মাদক দ্রব্য নিয়ন্ত্রণ আইন, ১৯৯০ (১৯৯০ সনের ২০ নং আইন)
~~(ছ) জন নিরাপত্তা (বিশেষ বিধান) আইন, ২০০০ (২০০০ সনের ৭ নং আইন);~~
(জ) নারী ও শিশু নির্যাতন দমন আইন, ২০০০ (২০০০ সনের ৮নং আইন) ৷;
(ঝ) আইন-শৃংখলা বিঘ্নকারী অপরাধ (দ্রুত বিচার) আইন, ২০০২ (২০০২ সনের ১১ নং আইন)।"

কাজী রকিবউদ্দীন আহমদ
সচিব

১১