First Finance Limited
Head Office

Guidelines on Prevention of Money Laundering & Terrorist Financing

Index

Chapter – I
INTRODUCTION

1.1 INTRODUCTION

- This Guidelines (Guidelines on Money Laundering & Terrorist Financing) of First Finance Limited has been developed keeping in consistency with the "Guidance Notes on Prevention of Money Laundering" & relevant circulars issued by Bangladesh Bank to facilitate implementation of the Money Laundering Prevention Act-2012 & Anti Terrorism (Amended) Act, 2012.
- Since FIs are vulnerable to being used by money launderers, Bangladesh Bank (Central FI of Bangladesh) assesses the adequacy of anti-money laundering procedures adopted by FIs and the degree of compliance with such procedures. Being a financial institute, First Finance Limited is in an obligation to comply with the rules, regulations and guidelines issued by Bangladesh Bank from time to time.
- This Guideline is designed /updated to assist First Finance Limited to comply with Bangladesh's anti-money laundering rules and regulations. First Finance Limited intends to use this policy as a criterion to assess the adequacy of its internal control, policies and procedures to counter money laundering and terrorist financing.

1.2 WHAT IS MONEY LAUNDERING

Money laundering can be defined in a number of ways. But the fundamental concept of Money laundering is the process by which proceeds from a criminal activity are disguised to conceal their illicit origins. Most countries subscribe to the definition adopted by the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988) (the Vienna Convention) and the United Nations Convention Against Transnational Organized Crime (2000) (the Palermo Convention):

> The conversion or transfer of property, knowing that such property is derived from any Offence, e.g. drug trafficking, or Offences or from an act of participation in such Offence or Offences, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an Offence or Offences to evade the legal consequences of his actions;
>
> 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 an Offence or Offences or from an act of participation in such an Offence or Offences, and;
>
> The acquisition, possession or use of property, knowing at the time of receipt that such property was derived from an Offence or Offences or from an act of participation in such Offence or Offences.

The Financial Action Task Force on Money Laundering (FATF), which is recognized as the international standard setter for anti-money laundering (AML) efforts, defines the term "money laundering" succinctly as "the processing of…criminal proceeds to disguise their illegal origin" in order to "legitimize" the ill-gotten gains of crime.

1.3 STAGES OF MONEY LAUNDERING

There is no single method of laundering money. In most of the criminal cases, the initial proceeds usually take the form of cash. For example, bribery, extortion, robbery and street level trade of drugs are almost always made with cash. This cash needs to enter into the financial system by some means so that it can be converted into a form which can be more easily transformed, concealed or transported.

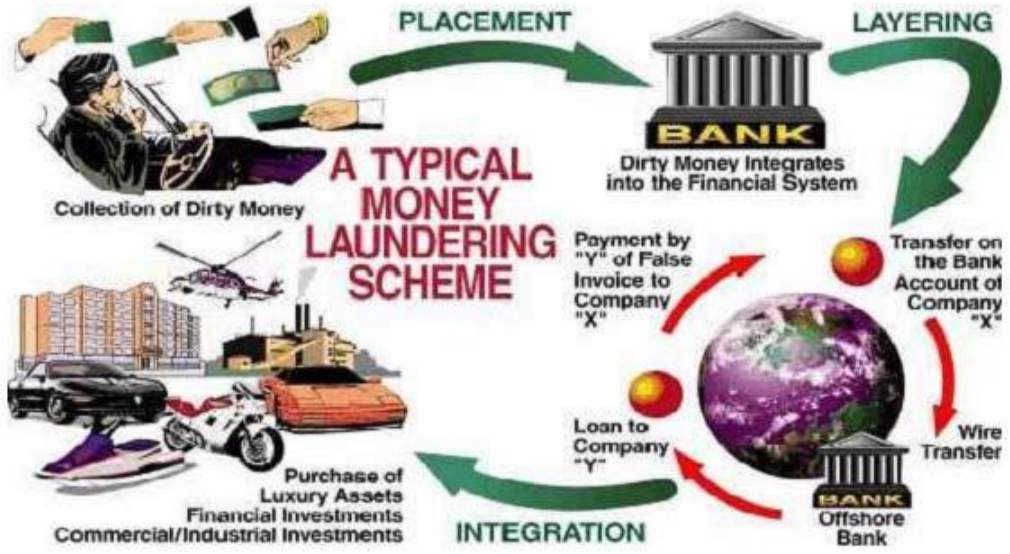
Despite the variety of methods employed, the laundering is not a single act but a process accomplished in 3(three) basic stages, placement, layering and integration.

Placement- the physical disposal of the initial proceeds derived from illegal activity. This is the movement of cash from its source. On occasion the source can be easily disguised or misrepresented. This is followed by placing it into circulation through financial institutions, casinos, shops, exchange houses, security brokers, and other businesses, both local and abroad.

Layering- separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity. The purpose of this stage is to make it more difficult to detect and uncover a laundering activity. It is meant to make the trailing of illegal proceeds difficult for the law enforcement agencies.

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 into the financial system appearing as normal business funds.

These three steps are illustrated in the following page:



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 organizations.

The table below provides some typical examples of the stages of money laundering.

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

1.4 WHY MONEY LAUNDERING IS DONE

First, money represents the lifeblood of the organization/person that engages in criminal conduct for financial gain because it covers operating expenses and pays for an extravagant lifestyle. To spend money in these ways, criminals must make the money they derived illegally appear legitimate.

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.

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.

1.5 WHY WE MUST COMBAT MONEY LAUNDERING

1. Money Laundering has devastating economic, security and social consequences. 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 for increased law enforcement and health care expenditures (for example, for treatment of drug addicts).
2. Money Laundering diminishes government tax revenue. It also makes government tax collection more difficult. This results in higher tax rates.
3. Money laundering distorts asset and commodity prices and leads to misallocation of resources. It can lead to an unstable liability base and to unsound asset structures thereby creating risks of monetary instability for FIs.
4. One of the most serious microeconomic effects of money laundering is felt in the private sector. Money launderers often use front companies, for co-mingling their illicit proceeds with legitimate funds, to hide the ill-gotten gains. Because of substantial illicit funds, these front companies can subsidize their products and services at levels well below market rates. This makes it difficult for legitimate businesses to compete against front companies. This situation can result in the crowding out of legitimate private sector businesses by criminal organizations.
5. Among its other negative socioeconomic effects, money laundering transfers economic power from the market, government and citizens to criminals.
6. 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, weakens collective ethical standards and corrupts our democratic institutions.
7. Nations cannot afford to have their reputation and financial institutions cannot have their image tarnished by an association with money laundering, especially in today's global economy.

8. Money laundering weakens confidence in and reputation of a financial institute. A financial institute tainted by money laundering accusations from regulators law enforcement agencies or the press risks the loss of its good market reputation as well as reputation of the country.

1.6 WHAT IS TERRORIST FINANCING

Terrorist financing can be simply defined as financial support, in any form, of terrorism or of those who encourage, plan, or engage in terrorism. The International Convention for the Suppression of the Financing of Terrorism (1999) under the United Nations defines TF in the following manner:

1) 'If any person commits an offense by any means, directly or indirectly, unlawfully and willingly, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out:
    a. An act which constitutes an offence within the scope of and as defined in one of the treaties listed in the link given below; or
    b. Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking any active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing an act.
2) For an act to constitute an offense set forth in the preceding paragraph 1, it shall not be necessary that the funds were actually used to carry out an offense referred to in said paragraph 1, subparagraph (a) or (b).

According to the article 7 of the Anti Terrorism (Amendment) Act, 2012 of Bangladesh, financing of terrorism means:
Offences relating to financing terrorist activities.– (1) If any person or entity knowingly provides or expresses the intention to provide money, services, material support or any other property to another person or entity and where there are reasonable grounds to believe that the same have been used or may be used in full or partially for any purpose by a terrorist person, entity or group or organization, he or the said entity shall be deemed to have committed the offence of financing terrorist activities.
(2) If any person or entity knowingly receives money, services, material support or any other property from another person or entity and where there are reasonable grounds to believe that the same have been used or may be used in full of partially for any purpose by a terrorist person or entity or group or organization, he or the said entity shall be deemed to have committed the offence of financing terrorist activities.
(3) If any person or entity knowingly makes arrangement for money, services, material support or any other property for another person or entity where there are reasonable grounds to believe that the same have been used or may be used in full or partially for any purpose by a terrorist person or entity or group or organization, he or the said entity shall be deemed to have committed the offence of financing terrorist activities.

(4) If any person or entity knowingly instigates another person or entity to provide or receive or make arrangement for money, services, material support or any other property in such a manner where there are reasonable grounds to believe that the same have been used or may be used in full or partially by a terrorist person or entity or group or organization for any purpose, he or the said entity shall be deemed to have committed the offence of financing terrorist activities.

1.7 WHY WE MUST COMBAT FINANCING OF TERRORISM

- Financing of Terrorism was criminalized under United Nations International Convention for the Suppression of the Financing of Terrorism in 1999. To reinforce the 1999 convention, United Nations adopted UNSC Resolutions 1373 and 1390 directing member states to criminalize Financing of Terrorism and adopt regulatory regimes to detect, deter and freeze terrorists' assets. The resolutions oblige all states to deny financing, support and safe harbour for terrorists.
- Bangladesh has actively involved in multinational and international institutions. Its international relationship and business, FIing business in particular are regulated by some domestic and international regulations. So it is mandatory to abide by those regulations. Financial Action Task Force (FATF), the international standard setter, adopted Special Eight Recommendations on Terrorist Financing. So we must be involved in international effort to combat Financing of Terrorism.
- It is increasingly evident that terrorists and their organizations need to raise significant amounts of cash for a wide variety of purposes for recruitment, training, travel and materials as well as often payment for safe heaven protection. So to root up terrorism, we must stop the flow of funds that keep them in business.
- The consequences of allowing the financial system to facilitate the movement of terrorist money are so horrendous that every effort must be made to prevent this from happening. So combating money laundering and financing of terrorism are not only the regulatory requirement but also an act of self interest.

1.8 THE LINK BETWEEN MONEY LAUNDERING AND TERRORIST FINANCING

The techniques used to launder money are essentially the same as those used to conceal the sources of, and uses for, terrorist financing. But funds used to support terrorism may originate from legitimate sources, criminal activities, or both. Nonetheless, disguising the source of terrorist financing, regardless of whether the source is of legitimate or illicit origin, is important. If the source can be concealed, it remains available for future terrorist financing activities. Similarly, it is important for terrorists to conceal the use of the funds so that the financing activity goes undetected.

As noted above, a significant difference between money laundering and terrorist financing is that the funds involved may originate from legitimate sources as well as criminal activities. Such legitimate sources may include donations or gifts of cash or other assets to organizations, such as foundations or charities that, in turn, are utilized to support terrorist activities or terrorist organizations.

1.9 HOW FIRST FINANCE LIMITED CAN HELP IN COMBATING MONEY LAUNDERING AND TERRORIST FINANCING

1. One of the best methods of preventing and combating money laundering and terrorist financing is a sound knowledge of a customer's business and pattern of financial transactions and commitments. In this principle, First Finance Limited has already adopted sound "Know Your Customer" procedure to record full and correct information of the customers so as to avoid inadvertent involvement in money laundering and terrorist financing.
2. Thus the FI's effort to combat money laundering and terrorist financing largely focuses on the process where the launderer's activities are more susceptible to recognition and therefore concentrates to a large extent on the deposit taking procedures i.e., the placement stage.
3. Branches must keep transaction records that are comprehensive enough to establish an audit trail. Such records can also provide useful information of the people and organizations involved in laundering schemes.
4. Anti-Money Laundering Department & Training Institute of the FI also deal with employees training programs which are designed to make awareness about money laundering techniques and tools etc so as to combat money laundering and terrorist financing.

Chapter- II
REQUIREMENTS OF THE LAW

2.1 DEFINITION OF MONEY LAUNDERING

Money Laundering is defined in Section 2 (v) of the Money Laundering Prevention Act 2012 as follows:

―money laundering means –
(i) knowingly moving, converting, or transferring proceeds of crime or property involved in an offence for the following purposes:-

1. concealing or disguising the illicit nature, source, location, ownership or control of the proceeds of crime; or
2. assisting any person involved in the commission of the predicate offence to evade the legal consequences of such offence;

(ii) smuggling money or property earned through legal or illegal means to a foreign country;
(iii) knowingly transferring or remitting the proceeds of crime to a foreign country or remitting or bringing them into Bangladesh from a foreign country with the intention of hiding or disguising its illegal source; or
(iv) concluding or attempting to conclude financial transactions in such a manner so as to reporting requirement under this Act may be avoided;
(v) converting or moving or transferring property with the intention to instigate or assist for committing a predicate offence;
(vi) acquiring, possessing or using any property, knowing that such property is the proceeds of a predicate offence;
(vii) performing such activities so as to the illegal source of the proceeds of crime may be concealed or disguised;
(viii) participating in, associating with, conspiring, attempting, abetting, instigate or counsel to commit any offences mentioned above;

2.2 PREDICATE OFFENCE

The offences from which the proceeds derived from committing or attempt to commit the following offences:

1. Corruption and bribery;
2. Counterfeiting currency;
3. Counterfeiting documents;
4. Extortion;
5. Fraud;
6. Forgery;
7. Illicit arms trafficking;
8. Illicit dealing in narcotic drugs and psychotropic substances;
9. Illicit dealing in stolen and other goods;
10. Kidnapping, illegal restraint, hostage-taking;

11. Murder, grievous bodily injury;
12. Woman and child trafficking;
13. Smuggling:
14. Unauthorized cross-border transfer of domestic and foreign currency;
15. Theft or robbery or Dacoity;
16. Trafficking in human beings;
17. Dowry;
18. Smuggling and vat related crime;
19. Tax related crime;
20. Plagiarism;
21. Terrorism and Terrorist Financing;
22. Counterfeiting and Piracy of Products;
23. Environmental Crime;
24. Sexual Exploitation;
25. Taking market advantage through transactions by using price sensitive information of the capital market before it becomes public and trying to control or manipulate the market to gain personal advantage (Insider trading and market manipulation);
26. Organized Crime;
27. Realizing money through intimidation and
28. Any other offence which Bangladesh Bank with the approval of the Government and by notification in the Official gazette declares as predicate offence for the purpose of this Act.

2.3 PROPERTY MEANS

1. Any kind of assets, whether tangible or intangible, movable or immovable, however acquired; or
2. Cash, legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets.

2.4 REPORTING ORGANIZATION

1. Banks;
2. Financial Institutions;
3. Insurance companies;
4. Money Changers;
5. Companies or organizations remitting or transferring money;
6. Other business organizations approved by Bangladesh Bank;
7. (i) Stock Dealer and Stock Broker,
   (ii) Portfolio Manager and Merchant FI,
   (iii) Security Custodian,
   (iv) Asset Manager;
8. (i) Non Profit Organization,
   (ii) Non Government Organization,
   (iii) Co-operative Society;
9. Real Estate Developer

10. Precious Metal & Stone business;
11. Trust & Company service provider;
12. Lawyer, Notary, Other law related profession & Accountant
13. Such other organizations as the Bangladesh FI with the approval of Government may notify from time to time

2.5 SUSPICIOUS OR UNUSUAL TRANSACTION

- A transaction that substantially deviates from the usual norm by which that transaction is usually conducted, or
- There is reasonable cause to believe that the transaction is related to any proceeds acquired through or earned from crime or predicate offence or related financing on terrorism.

2.6 THE OFFENCE OF MONEY LAUNDERING

The money laundering offences are, in summary:

1. **Offence of Money Laundering:** The act of money laundering will be treated as an offence [See Section 4(1) of the Act].
2. **Offence Committed by a Company:** If any offence under this Act has been committed by a company then every proprietor, director, manager, secretary, or other officer or employees or representative who had direct involvement with the offence shall be deemed to be guilty for such offence [See Section 27 of the Act]. However, it is a defense for any person as aforesaid can prove that such offence was committed without his knowledge or it has occurred despite his best efforts to prevent it [See Section 27 of the Act].
3. **Offence of Not Retaining Information:** It is an offence for reporting organizations not to retain correct and full information used to identify their customers during their account relationships. It is also an offence for reporting organizations not to retain transaction related records for at least 5 (Five) years after termination of relationships with the customers [See Section 25(1) Kha of the Act].
4. **Offence of Not Reporting Suspicious Transactions:** It is also an offence for reporting organizations not to make a report to Bangladesh Bank where they suspect that a money laundering offence has been or is being committed [See Section 25(1) Gha of the Act].
5. **Offence of Not Providing Information on Demand:** It is also an offence for reporting organizations not to provide customer identification and transaction records to Bangladesh Bank from time to time on demand.
6. **Offence of Violating Freezing or Attachment Order:** It is an offence for any person to violate any freezing order or attachment order passed under this Act [See Section 5 of the Act].
7. **Offence of Divulging Information:** It is an offence for a person to divulge any information relating to an investigation or any other related information to any person, organization or news media for the purpose of frustrating the investigation or making adverse influence over the investigation [Section 6(1) of the Act].
8. **Offence of Using or Publishing Information:** It is also an offence for any person, organization or agent authorized under the Act to use, publish or divulge

any information except for the purpose of the Act, which was collected, received, retrieved and known by him/her during the period of his/her employment or appointment period or after completion of his/her employment or appointment contract [Section 6(2) of the Act].

9. **Offence of Obstructing or Refusing to Assist an Investigation:** It is an offence under the Act for any person to obstruct or refuse to assist the investigating officer engaged in any investigation under the Act [Section 7(1)(Ka) of the Act].
10. **Offence of Refusing to Submit Reports:** It is an offence under the Act for any person or refuse to submit reports or supply information without any reasonable ground under the Act [Section 7(1)(Kha) of the Act].
11. **Offence of Providing False Information:** It is an offence for any person to provide false information knowingly about the sources of funds or the identity of an account holder or the beneficial owner or nominee of an account [Section 8(1) of the Act].

2.7 PENALTIES FOR MONEY LAUNDERING OFFENCES

All offences under the Act are cognizable, non-compoundable and non-bail able. All penalties for commencement of the offences have prison terms and/or fines as prescribed in the Act as follows:

i. **Penalty for Offence of Money Laundering:** Any person engaged in money laundering or abetting, aiding or conspiring in the commission of such offence shall be punishable with imprisonment for a term not less than 4 (four) years and a maximum not exceeding 12 (twelve) years, and in addition a fine of Taka 10 (ten) Lac or the double amount of assets value earned from the predicate crime(s), which is higher [See Section 4(2) of the Act]. Property involved with the offence may be forfeited in favor of the state [See Section 4(3) of the Act]. If any company has been engaged in money laundering activity, either directly or indirectly, then a fine of Tk 20 (twenty) Lac or the double amount of assets value earned from the predicate crime(s), which is higher. The registration of that company shall be liable for cancellation [See Section 4(4) of the Act].

ii. **Penalty for Offence of Violating Freezing or Attachment Order :** If any person violates a freezing order or an attachment order, then he/she will be punishable with an imprisonment not exceeding 3 (three) years or a fine amount of assets value related with freeze instruction, or both [See Section 5 of the Act].

iii. **Penalty for Offence of Divulging, Using or Publishing Information:** If any person divulges any information relating to an investigation or any other related information for frustrating the investigation or making adverse influence over the investigation or uses, publishes or divulges any information except for the purpose of the Act, then he/she will be punishable with an imprisonment not exceeding 2 (Two) years or a fine of not exceeding Taka 50 (fifty) thousand, or both [See Section 6(3) of the Act].

iv. **Penalty for Offence of Obstructing or Refusing to Assist an Investigation or Refusing to Submit Reports :** If any person obstructs or refuses to assist the investigating officer engaged in any investigation or refuses to submit reports or supply information without any reasonable ground under the Act, then he/she will be punishable with an imprisonment not exceeding 1 (One) year or a fine of not exceeding Taka 25 (twenty five) thousand, or both [See Section 7(2) of the Act].

v. **Penalty for Offence of Providing False Information:** If any person provides false information knowingly about the sources of funds or the identity of an account holder or the beneficial owner or nominee of an account, then he/she will be punishable with an imprisonment not exceeding 3 (three) years or a fine of not exceeding Taka 50 (Fifty) thousand, or both [See Section 8(2) of the Act].

2.8 RESPONSIBILITY OF REPORTING ORGANIZATIONS IN PREVENTION OF MONEY LAUNDERING:

For the purpose of preventing and identifying money laundering reporting organizations shall:

- keep the correct and full information of identification of its clients and during the operation of accounts;
- In case of closed account of any client, keep previous records of transactions of such account for at least five years from the date of closure;
- Provide, from time to time, the records kept under clause (a) and (b) to Bangladesh Bank time to time on demand from Bangladesh Bank;
- Inform proactively and immediately Bangladesh Bank, facts on suspicious / unusual / doubtful or transactions likely to be related to money laundering;

If any reporting organizations violate the directions mentioned in sub-section (1) Bangladesh Bank shall take the following actions:

- Bangladesh Bank may impose a fine of not less than Taka 50 (fifty) thousand and not more than Taka 25 (twenty five) Lac upon that reporting organization [See Section 25(2)(Ka) of the Act].
- In addition to the above fine as mentioned in sub section 25(2)(Kha) of the Act, Bangladesh Bank may cancel the permission or license of any Branch, Service Center, Booth or Agency of the company. And where appropriate, Bangladesh Bank shall inform the permitting or licensing authority of the reporting organizations so that the concerned authority may take necessary actions against the concerned reporting organization in accordance with their own laws or rules and regulations [See Section 25(2)(Kha) of the Act].
- Bangladesh Bank will collect the penalty money imposed under subsection (2) in its self determined manner and shall deposit the collected money into the government treasury.

2.9 PROTECTION AGAINST PROCEEDINGS UNDERTAKEN IN GOOD FAITH

No suit, prosecution either civil or criminal or other legal proceedings shall lie against government or any government officials or any reporting organizations if any person is affected or likely to be affected due to the proceedings done in good faith under this Act.

2.10 COMPLIANCE REQUIREMENTS UNDER ANTI TERRORISM (AMENDED) ACT, 2012

According to section 16 of Anti Terrorism (Amendment) Act, 2012, reporting agencies' responsibilities to combat financing of terrorism are -

1) Every reporting agency shall take necessary measures, with appropriate caution and responsibility, to prevent and identify financial transactions which are connected to any offence under this Act and if any suspicious transaction is identified, the agency shall spontaneously report it to the Bangladesh Bank without any delay.
2) The Board of Directors, or in the absence of the Board of Directors, the Chief Executive Officer, by whatever name called, of each reporting organization shall approve and issue directions regarding the duties of its officers, and shall ascertain whether the directions issued by Bangladesh Bank under section 15, which are applicable to the reporting agency, have been complied with or not.

2.11 PENALTIES UNDER ANTI TERRORISM (AMENDED) ACT, 2012

The provision laid down in section 16 (3) of Anti Terrorism (Amendment) Act, 2012, if any reporting agency fails to comply with the directions issued by Bangladesh Bank under section 15 or knowingly provides any wrong or false information or statement, the said reporting agency shall be liable to pay a fine determined and directed by Bangladesh Bank not exceeding Taka 10 (ten) lacs and Bangladesh Bank may suspend the registration or license with intent to stop operation of the said agency or any of its branches, service centers, booths or agents within Bangladesh or, as the case may be, shall inform the registering or licensing authority about the subject matter to take appropriate action against the agency. According to section 16 (4) if any reporting agency fails to pay or does not pay any fine imposed by Bangladesh Bank according to sub-section 16 (3) of ATA, Bangladesh Bank may recover the amount from the reporting agency by debiting its accounts maintained in any FI or financial institution or Bangladesh Bank and in case of any unrealized or unpaid amount, Bangladesh Bank may, if necessary, apply before the concerned court for recovery.

2.12 SUPERVISORY POWER OF BANGLADESH BANK

According to the provision laid down in the section 23 of MLPA, 2012 and section 15 of Anti terrorism (Amendment) Act, 2012, Bangladesh Bank is the core implementing agency. The major supervisory powers are:
Under MLPA, 2012, Bangladesh FI shall have the following powers and responsibilities to prevent money laundering and to resist any such activities:

a) to analyze or review information related to cash transactions and suspicious transactions received from any reporting organization and to collect additional information relating thereto for the purpose of analyzing or reviewing from the reporting organizations and maintain data on the same and, as the case may be, provide with the said information to the relevant law enforcement agencies for taking necessary actions;
b) ask for any information or obtain a report from reporting organizations with regard to any transaction in which there are reasonable grounds to believe that the transaction is involved in money laundering or a predicate offence;
c) issue an order to any reporting organization to suspend or freeze transactions of any account for a period not exceeding 30 (thirty) days if there are reasonable grounds to suspect that any money or property has been deposited into the account by committing any offence. Provided that such order may be extended for additional period of a maximum of 6 (six) months by 30 (thirty) days, if it appears necessary to find out correct information relating to transactions of the account;
d) issue, from time to time, any direction necessary for the prevention of money laundering to the reporting organizations;
e) monitor whether the reporting organizations have properly submitted information and reports requested by Bangladesh Bank and whether they have duly complied with the directions issued by it, and where necessary, carry out on-site inspections of the reporting organizations to ascertain the same;
f) arrange meetings and seminars including training for the officers and staff of any organization or institution, including the reporting organizations, considered necessary for the purpose of ensuring proper implementation of this Act by Bangladesh Bank;
g) carry out any other functions necessary for the purposes of this Act.

The power and responsibilities of Bangladesh FI under section 15(1) of Anti Terrorism (Amendment) Act, 2012 are as follows:
The Bangladesh Bank shall have the power and authority to take necessary measures to prevent and detect transaction intended to commit offence under ATA through any FIs channel, and for that matter BB is empowered and authorized to –

- Call for STRs from reporting organizations and keep such report confidential if law does not allow disclosure;
- Compile and preserve all statistics and records;
- Create and maintain a database of all STRs;
- Analyze the STRs;

- Issue order in writing to reporting organizations to suspend a transaction for a period of 30 days where it has reasonable grounds to suspect that the transaction involves connection with terrorist acts, and extend the order to maximum 180 days.
- Monitor and observe the activities of reporting organizations;
- Issue instructions to reporting organizations directing them to take preventive measures against terrorist financing activities.
- Inspect reporting organizations for the purpose of detection of suspicious transactions connected with terrorist financing; and
- Provide training to staff and officers of reporting organizations for the purpose of detection and prevention of suspicious transactions as may be connected with terrorist financing.

It is to be noted that no law enforcement authority shall have any access to the documents or files of a financial institution without approval from the chief executive of the concerned financial institution or from Bangladesh Bank.

Chapter- III

POLICY FOR PREVENTION OF MONEY LAUNDERING & TERRORIST FINANCING

In order to arrest money laundering and bring about discipline and transparency in financial system and for safeguarding the economy, society and security First Finance Limited has made an attempt to frame Guidelines on Prevention of Money Laundering & terrorist Financing which would cover the following:

1. Broad Policy for Prevention of Money Laundering & Terrorist Financing
2. Organization chart for implementing AML/CFT Policy
3. Establishment of Customer's Identity
4. Anti- Money Laundering Process
5. Recognition and Reporting of Suspicious Transactions
6. Cash Transaction Report (CTR)
7. Self Assessment Independent Testing Procedure
8. Record keeping

3.1 BROAD POLICY FOR PREVENTION OF MONEY LAUNDERING & TERRORIST FINANCING

It includes senior management commitment to the anti-money laundering program. More clearly, senior management must evolve such a culture for the First Finance Ltd. so that all the employees strictly adhere to each and every provision of Money Laundering Prevention Act-2012 and Anti Terrorist (Amended) Act-2012. An ethos should be created amongst the organization that money laundering and terrorist financing, the criminal acts, must be combated and each and every officer has a bounden responsibility to make our organization free from the clutches of money launderers.

There should be a policy of compliance with all laws and regulations which are designated to deter money laundering and it should go to all employees of the First Finance Ltd. as a message from the top management. There should also be a policy that every new entrant, either fresh or lateral, must give a declaration that he/she will strictly adhere to anti-money laundering policy pursued by the organization. Besides, all employees of the organization irrespective of the positions they hold are accountable to the top management and regulatory body for their activities which might directly or indirectly relate to money laundering.

The Chief Executive Officer of the First Finance Ltd. shall, on annual basis, send a statement of compliance policy in this regard to all employees of the organization which, at minimum, must contain the following:

i. That each and every employee of the First Finance Ltd. is required to comply with applicable laws and regulations and maintain ethical standards ;

ii. That all activities being carried out by our organization are in conformity with laws, regulations in force and instructions of Bangladesh Bank issued from time to time.

iii. That complying with relevant laws, rules and regulations is the individual responsibility of each employee working in the organization. It should be made clear that ignorance of any of the provisions of law, rules, regulations is no excuse for non- compliance.

iv. That there is a well defined reporting procedure for compliance with Money Laundering Prevention Program of the organization.

v. That customer's identity is appropriately established by the officers rendering services to him either in liability or in asset viewpoint and also for other ancillary services. KYC procedures should be followed in this regard.

3.2.1 ORGANIZATION CHART FOR IMPLEMENTING AML/CFT POLICY

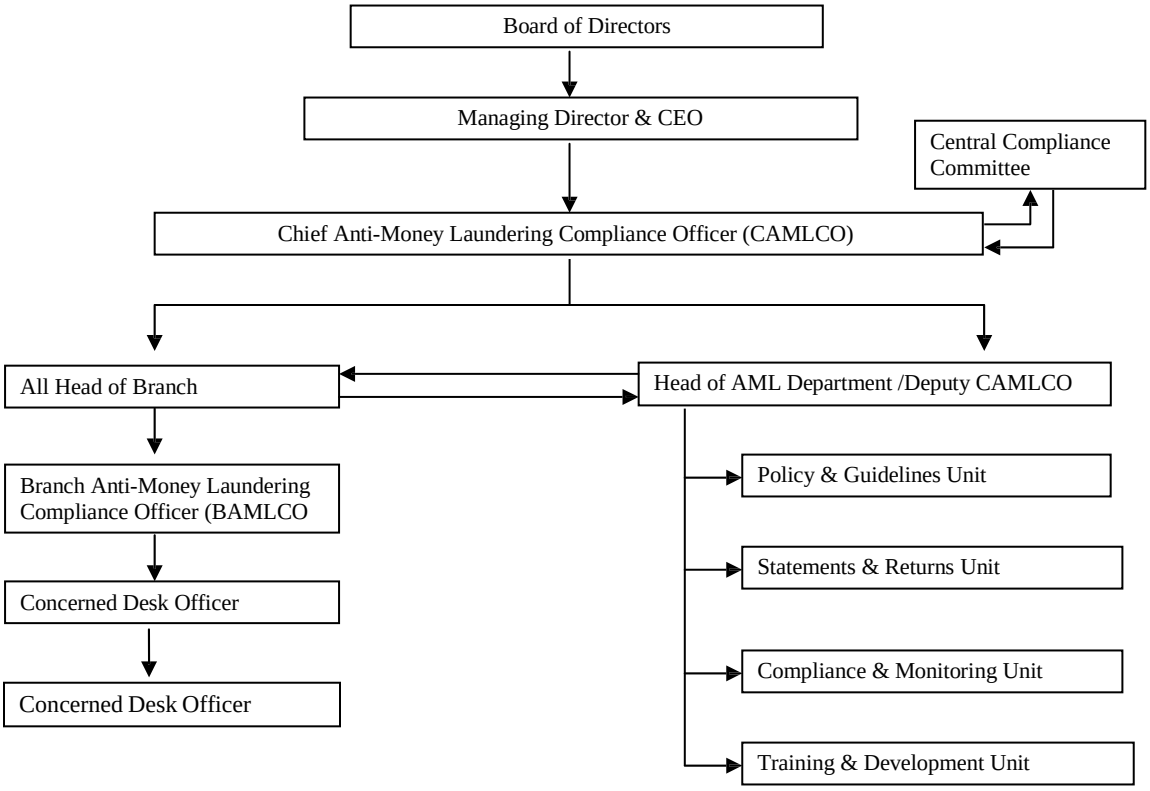
With a view to implementing any policy it is imperative that an organization should have an organogram depicting the position of people working there with job description and responsibilities having dot lines for making them accountable to the organization for their activities. Anti –money laundering program has been taken up as a serious and important policy to be implemented in our organization for which it is proposed that there should be a Central Compliance Committee in the organization which may consist of the following members:

Sl.	Position in the FI	Position in the Committee
1.	Chief Financial Officer (CFO)/CAMLCO	Chairman
2.	Head of Treasury/DCAMLCO	Member
3.	Chief Operating Officer (COO)	Member
4.	Head of ICCD	Member
5.	Head of ICT	Member

The Central Compliance Committee shall directly report to the Chief Executive Officer. The Central Compliance Officer shall report to the Regulatory Body i.e. Bangladesh Bank for any matter relating to money laundering or any transaction susceptible to money laundering under intimation to the Central Committee and the Chief Executive Officer.

Organizational Chart for implementing AML/CFT Policy:

Organization Chart



3.2.2 JOB DESCRIPTION AND RESPONSIBILITIES

Chief Anti Money Laundering Compliance Officer (CAMLCO):

i. To monitor, review and coordinate application and enforcement of the FI's compliance policies including Anti-Money Laundering Compliance Policy. This will include anti-money laundering risk assessment, practices, procedures and controls for account opening, KYC procedures and ongoing account/ transaction monitoring for detecting suspicious transactions and account operational records.

ii. To monitor changes in laws, rules and regulations and also the instructions of Bangladesh Bank which may require the AML program to be revised from time to time.

iii. To respond to questions relating to compliance and concerns of employees and advise operational units in Head Office, Branches, SME Service Centers and Booth(s).

iv. To assist Operational Units in Head Office, Branches, SME Service Centers and Booth(s) in providing solutions to problems cropped up from activities or transactions related to money laundering.

v. To ensure that the FI's AML program is comprehensive and updated.

vi. To maintain ongoing awareness of new and changing business activities susceptible to money laundering risks and identify potential compliance issues deemed to be reasonably vulnerable to money laundering risks.

vii. To develop knowledge of all employees, particularly the compliance officers in respect of AML program.

viii. To develop and maintain ongoing relationships with regulatory authorities, external and internal audit teams, Head of Branches, SME Service Centers and Booth(s) for assisting them in early identification of issues which may be susceptible to money laundering risks.

ix. To assist in review of control procedures in the FI so as to ensure legal and regulatory compliance and in the development of adequate testing procedures to detect and prevent lapses in compliance issues.

x. To monitor business self-testing for AML compliance and take corrective action.

xi. To manage Suspicious Activity Reporting Process which refers to :

- reviewing transactions referred by operational units in Head Office, Branches, SME Service Centers and Booth(s) as suspicious.
- reviewing the Transaction Monitoring Reports
- ensuring that internal suspicious activity reports:

Y are prepared as and when they appear to be appropriate.

Y reflect the uniform standard for " suspicious activity involving possible money laundering established in the policy".

Y are accompanied by documentation of the Branches' decisions to retain or terminate the account, as required under the policy.

Y are advised to other branches who may have relationship with customer.

Y are reported to the Chief Executive Officer and the Board of Directors when the suspicious activity is adjudged to represent sufficient risk to the FI including reputation risk.

- ensuring that a documented plan of corrective action appropriate for the seriousness of the suspicious activity.
- 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.
- managing the process for reporting suspicious activity to Bangladesh Bank authorities after appropriate internal consultations.

Besides the above, a brief description of role and responsibilities of individual officer/ executive involved in anti-money laundering program of the FI in branch level/head office level is given below:

Account Officer / Relationship Manager / Officers involved in Account opening	:	• To exercise due diligence in establishing the identity of customer prior to opening the Account. • To obtain as much information as possible on the customer that might help proper consideration of the nature and type of account. • To ensure that all required documents in respect of account opening are obtained and proper documentation is complete in case of loan account. • To ensure that transaction profile is obtained and reviewed when transactions are being carried out. • To obtain documentary evidence of large cash transactions are being carried out. • To report to Branch Manager and concerned higher authority for any suspicious transaction, he deems necessary.
Customer Service Officer	:	• To support the account officer in respect of the above • To perform the jobs of Account Officer in his absence.

Operations Manager	:	• To ensure that all control points are taken into account prior to taking place of any transaction. • To exercise ongoing due diligence in respect of trends of transactions on customers' accounts. • To update customer transaction profile in the ledger.
Branch Anti-Money Laundering Compliance Officer (BAMLCO)	:	• To manage transaction monitoring process • To report on suspicious transaction to Head of Branch • To make Officials of Branch aware of AML program. • To update FI's AML Policy in line with any change or revision in the country's AML policy. • To submit Branch Returns to Chief Compliance Committee
Head of Branch or Booth/ Operational Head in Head Office	:	• To ensure that AML program is effectively accomplished in the Branch or Booth. • To act as first point of contact in respect of any AML issue.
Head of Ant-Money Laundering Department	:	• To Assist Central Compliance Committee/Central Compliance Officer in implementing and enforcing the FI's AML Policies. • To implement and to enforce the FI's AML policies. • To report on suspicious clients to Bangladesh Bank through Central Compliance Committee/Central Compliance Officer. • To inform Head of Branch or all Divisional Head in the Head Office of required action related to AML program. • To turn up the employees on AML program as an ongoing policy.
Central Compliance Committee		• To ensure that the FI's all business activities are carried out in conformity with AML program and that an effective AML program is in place in the FI.

3.3.1 GENERAL PROCEDURE FOR CUSTOMER DUE DILIGENCE (CDD) OR KNOW YOUR CUSTOMER (KYC)

i. Having sufficient information about your customer - "know 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 FI itself, or to ensure that s/he cannot be traced or linked to the crime the proceeds of which the FI 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.

ii. Section 25(Ka) of the Prevention of Money Laundering Act 2012 requires all concerned to seek satisfactory evidence of the identity of those with whom they deal. Unless satisfactory evidence of the identity of potential customers is obtained in good time, the business relationship must not proceed.

iii. When a business relationship is being established, the nature of the business that the customer expects to conduct with the FI 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, the concerned officer needs to have a clear understanding of the business carried on by their customers.

iv. The concerned officer must establish to his satisfaction that he is dealing with a real person (natural, corporate or legal), and must verify the identity of persons who are authorized to operate any FI or investment account, or transact business for the customer. Whenever possible, the prospective customer should be interviewed personally.

v. 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 identifying 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 an ongoing process. The overriding principle is that every concerned officer must know who are his customers, and he must have the necessary documentary evidence to verify this.

Section 25(Kha) 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 is terminated.

vi. The concerned officers should include some key elements in the design of KYC program. Such essential elements should start from the FI's 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. They should not only establish the identity of their customers, but should also monitor account activity to determine those transactions that do not conform to the normal or expected transactions for that customer or type of account. KYC should be a core feature of the FI's risk management and control procedures, and be complemented by regular compliance reviews and internal audit.

vii. The ICT Division will be responsible for developing automated systems and processes for classifying customers on the basis of the risk matrix provided by Bangladesh Bank, monitoring transactions with the transaction profile provided by the customers. These new systems will improve our ability to detect unusual transactions, help the authorities to identify and respond to new money laundering and terrorist financing techniques. We will continue to enhance the use of automated systems to monitor account activities and, in conjunction with the relevant authorities, to respond to new and more sophisticated trends and techniques adopted by criminals.

viii. Branch Managers/ BAMLCOs will monitor customers transaction regularly in order to identify suspicious transaction/activities relates to both money laundering and terrorist financing. He will also oversee the day to day activities at the branch and confirm compliance of the instructions of concerned authority.

3.3.2 CUSTOMER ACCEPTANCE POLICY

Customers are vitally important for FIs business. Increasing competition is forcing FIs to pay much more attention to satisfy customers. Our motto is to extend best services to our customers. We are also aware that sometimes customers pose the risk of money laundering and financing of terrorism to the financial institutions particularly the FIs. So the inadequacy or absence of KYC standards can result in serious customer and counterparty risks, especially reputational, operational, legal and compliance risks. Collecting sufficient information about our customers is the most effective defense against being used as the medium to launder the proceeds of crimes and to finance the terrorism through FI accounts. As per Sec. 25 of Money Laundering Prevention Act-2012 each FI requires to keep satisfactory evidence of the identity of those it deals with and also requires making necessary arrangement to prevent any transaction related to crimes as described in Anti Terrorism Act (Amend)-2012. It is also the responsibility of each FI to identify suspicious transactions of their customers with due care and diligence. Pursuant to above legal bindings, Sec. 5.3 of Guidance Notes on Prevention of Money Laundering issued by Bangladesh Bank and apropos to international standard the Management of the FI has developed the Customer Acceptance Policy as under:

1) No account shall be opened in anonymous or fictitious name.
2) No numbered account (A/C without a title) shall be opened.
3) Uniform A/C Opening Forms, KYC Profile Form and Transaction Profile Form developed in line with the guidelines of Bangladesh Bank should be properly filled in.

4) Customers' risk must be assessed as per parameters of risk perception as clearly defined in KYC Profile Form.
5) Documentation requirements and other information must be collected keeping in mind the instructions contained in AML Circular No. 2 dated 17.06.2002, the requirements of the AML Act-2012, the Anti-Terrorism Act(Amend)-2012 and other Circulars and guidelines issued by Bangladesh Bank from time to time.
6) The branch shall not open an account, where the FI is unable to apply appropriate customer due diligence measures i.e. the branch is unable to verify the identity and/or obtain documents required due to non-cooperation of the customer or non reliability of the data/information furnished to the branch. But the branch must be careful to avoid unnecessary harassment of the customer.
7) If it becomes necessary to close an existing account due to non-cooperation of the customer in providing necessary documents/information required by law/regulatory authority or non-reliability of the information/documents furnished by the customer, the branch must be vigilant in doing so. For example, decision to close an account should be taken at a reasonably high level after giving due notice to the customer explaining the reasons for such a decision.
8) In case of opening a Politically Exposed Person's (PEP) account, the branch shall comply the instructions contained in AML Circular No. 14 dated 25.09.2007 issued by Bangladesh Bank. Such types of account will be classified as high risk and will be required very high level monitoring.
9) At the time of opening new account the branch must take care to seek only such information from the customer which is relevant and is not intrusive. It is mentioned that the customer profile is a confidential document and the details contained therein shall not be divulged for any other purposes.
10) Source of funds, income or wealth and complete information on the actual or beneficial owners of the accounts holding 20% or more share of the account must be obtained at the time of opening of any account.
11) The branch will strive not to cause inconvenience to the general public, especially those who are financially or socially disadvantaged.
12) The branch will conduct necessary checks before opening a new account so as to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations etc.
13) In case of establishing correspondent FIs relationship, the branch/concerned division/department shall follow the guidelines as contained in AML Circular No. 7 dated 14.08.2005 meticulously.
14) The branch shall verify the identity of the customer using reliable sources, documents etc. but it must retain copies of all references, documents used to verify the identity of the customer.
15) The branches, where locker service facilities exist, will follow the identification procedure for their customers.

It is important to bear in mind by all employees of the FI that the customer identification process does not end at the point of application. Once account relationship has been established, reasonable steps should be taken by the branch from time to time to ensure that descriptive information is kept updated.

In developing customer acceptance policy the following important factors are required to be taken into consideration:

i) Customer's background
ii) Country of origin
iii) Public or high profile position
iv) Linked accounts
v) Volume of business activities
vi) Risks associated in the business of customers
vii) Other risk indicators
viii) Basic requirements for Account Opening
ix) All information available for judging the creditworthiness of borrowers.
x) All information on walk-in customers as required in AML circular

3.3.3 CUSTOMER IDENTIFICATION

1. Customer identification is an essential element of KYC standards. For proper identification a customer includes the following:
   - the person or entity that maintains an account with the FI 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 FI.
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 the concerned officers 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 an officer becomes aware at any time that it lacks sufficient information about an existing customer, he should take steps to ensure that all relevant information are obtained as quickly as possible.
3. Whenever the opening of an account or business relationship is being considered, or a one-off transaction or series of linked transactions to be undertaken, identification procedures must be followed. Identity must also be verified in all cases where money laundering is known, or suspected.
4. Once verification of identity has been satisfactorily completed, no further evidence is needed when other transactions are subsequently undertaken.

What Constitutes a Person's Identity:

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 purpose of this guideline, the two elements are:

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

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.

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 description required will depend on the concerned officer's own understanding of the applicant's business.

4. When commencing a business relationship, concerned officers 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 FI or the applicant's employer, or be the proceeds of a matured insurance policy, etc.

5. Once account relationship has been established, reasonable steps should be taken by the concerned officer 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.

Individual Customers :

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 concerned officer himself/herself:
    - 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

2. One or more of the following steps is recommended to verify addresses:
    - provision of a recent utility bill, tax assessment or FI 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.

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 the FI does not breach UN or other international financial sanctions.

4. Identification of 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 FI.

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 the concerned officer is unfamiliar, either because of origin, format or language, he must take reasonable steps to verify that the document is indeed genuine, which may include contacting the relevant authorities or obtaining a notarized translation. *The concerned officers* should also be aware of the authenticity of passports.

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.

7. There is obviously a wide range of documents which might be provided as evidence of identity. It is for each concerned officer 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.

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.

9. Any subsequent change to the customer's name, address, or employment details of which the concerned officer 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.

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. In case of one-off transactions the details should be recorded in a manner which allows cross reference to transaction records. Such institutions may find it convenient to record identification details on a separate form, to be retained with copies of any supporting material obtained.

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.

Persons without Standard Identification Documentation:

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 the concerned officer 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.

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.

3. In these cases it may be possible for the concerned officer 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 Head of Branch 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.

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. Under normal circumstances, a family member or guardian who has an existing relationship with the FI 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.

Corporate Bodies and other Entities:

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.

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, stuck off, wound-up or terminated. In addition, if the concerned officer 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.

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, concerned officer 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.

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. 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.

6. Where the business relationship is being opened in a different name from that of the applicant, the concerned officer should also satisfy himself that the reason for using the second name makes sense.

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

    - 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 acceptable in lieu of passport or other photo identification documents of their shareholders, directors and authorized signatories. Where the concerned officer already knows their identities and identification records already accord with the requirements of these guidelines, there is no need to verify identity again.

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.

Partnerships and Unincorporated Businesses:

1. In the case of partnerships and other unincorporated businesses whose partners/directors are not known to the FI, 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.

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).

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.

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.

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

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 this general guideline 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 FI. Consequently, all relevant financial businesses must review existing business relationships commenced prior to 30th April 2002 to establish whether any documentary evidence required by their current KYC procedures is lacking. **Bangladesh Bank has fixed the deadline on 31st March 2010 to complete the KYC for Accounts opened before 30th April 2002.**

2. In order to review a pre 2002 account the **Uniform KYC Form** should be used. **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.**

3. In carrying out their review of pre-2002 accounts, they must decide whether they will have 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.

4. When the nature of a business relationship is revised they 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 FI 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. Where it is decided to seek missing documentation, the concerned executives 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, they should consider termination of the business relationship.
6. As per Bangladesh Bank's instruction vide AML Circular No. 23 dated 23/02/2010 the Account opened before 30th April 2002 which KYC procedures are not completed must be marked as "Dormant". Customer should not be allowed for any withdrawal from the Account but he can make deposit in the Account. The Account may be regularized on customer written application after completion of KYC Procedures.

Internet or Online FIing

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

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 this general guideline.
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 this general guideline

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 the FI will follow the identification procedures set out in these general guidelines. In addition, such facilities should only be made available to account holders.

Timing and Duration of Verification:

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.

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.

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

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.

3.4.1 KNOW YOUR CUSTOMER PROCEDURES

1. Each concerned officer 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, FI 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 its most basic level.

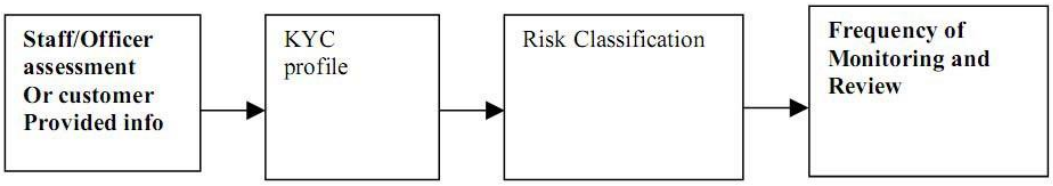
2. Once the identification procedures have been completed and the client relationship is established, the concerned officers should monitor the conduct of the relationship/account to ensure that it is consistent with the nature of business stated when the relationship/account was opened. The concerned officers do this firstly by way of 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.

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.

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.

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

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



3.4.2 RISK MANAGEMENT

1. **Risk Categorization, Based on Activity/KYC Profile** : At the time of opening accounts, the concerned 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 Uniform KYC Profile Form 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

2. **Risk Assessment**: 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. However, management may judgmentally override this automatic risk assessment to "Low Risk" if it believes that there are appropriate mitigates to the risk. This overriding decision must be documented (reasons why) and approved by the Branch Manager, and Branch AML Compliance Officer.

3. **Annual Update of KYC and Transaction Profile**: 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.

4. **Account of NGO/NPO:** Accounts of Charities, Non-Profit Organizations, Non Government Organizations to be treated as high risk accounts by default and Enhanced

Due Diligence (EDD) must be performed for opening and operating such accounts in relation to combat financing of terrorism.

5. **Politically Exposed Persons (PEPs)**: While opening and/or operating account of Politically Exposed Persons (PEPs) enhanced due diligence shall have to be exercised. PEPs means *"Individuals who are or have been entrusted with prominent public functions in a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials"*. All instructions as detailed for PEPs shall equally apply if business relationship is established with the family members and close associates of these persons who may pose reputational risk to the FI. If the customer is a Politically Exposed Person the account will automatically become a High Risk Account.

Following instructions shall have to be followed to ensure Enhanced Due Diligence, while opening and operating the account of Politically Exposed Persons (PEPs):

i. a risk management system shall have to be introduced to identify risks associated with the opening and operating accounts of PEPs;
ii. obtain senior management approval for establishing business relationships with such customers;
iii. take reasonable measures to establish the source of wealth and source of funds;
iv. ongoing monitoring of the transactions have to be conducted; and
v. the FIs/financial institutions should observe all formalities as detailed in Guidelines for Foreign Exchange Transactions while opening accounts of non-residents;

The above instructions shall also be applicable to customers or beneficial owners who become PEPs after business relationship have been established.

3.4.3 TRANSACTION MONITORING PROCESS

1. **Transaction Profile (TP)**: Transaction Profile (TP) is an important document for monitoring transactions and recognizing suspicious transactions. The following steps and points should be noted while preparing transaction profiles:

- Take interview with the customer and request him/her to fill in the Transaction Profile Form as recommended by Bangladesh Bank. The main features of the Form for both deposit and withdrawal would be:
-
    - Various types of transactions (i.e. nature of transactions)
    - No. of transactions (monthly)
    - Maximum size (per transaction)
    - Total value (monthly)

- Before filling in, it has to be ensured by the Designated Officer that the customer's understanding is sufficient to fill the required cells of Transaction Profile Form.

- Assist customer in filling the Transaction Profile Form if any complexity arises.
- Officer must match the information mentioned in TP with all points covered in KYC guidelines. He has to establish normal resemblances between the two declared statements. Questions might be politely asked to customer for any noted discrepancy.

2. **Transaction Monitoring Process**: There should be 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 the FI 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

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. The floor levels may be fixed up by the Branch Management and Central Compliance Committee, as the case may be.

3.5 DETECTION AND REPORTING OF SUSPICIOUS TRANSACTIONS

1. **Statutory Obligation for Reporting of Suspicious Transactions**: Section 25(1)(Gha) of the Money Laundering Prevention Act-2012 obligates us to make a report to Bangladesh Bank where a suspicion arises that a money laundering offence has been or is being committed.

In this regard, all branches must ensure that,

- each relevant employee knows the person whom they should report as suspicious;
- there is a clear reporting chain under which those suspicions will be passed without delay to the Chief Anti Money Laundering Compliance Officer (CAMLCO).

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

2. **How to Detect Suspicious Transactions:** As there are unlimited types of transactions that a money launderer or a terrorist financier may use, it is difficult to define a suspicious transaction. However, in most of the cases, a suspicious transaction will be one that is inconsistent with a customer's known, declared, legitimate business or other personal activities. Therefore, the first key to detect that a transaction, or series of transactions, may be unusual is to know enough about the customer's transactions with the FI.

At the time of determining whether a customer's transaction may be suspicious, a branch must consider the following questions:

- 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?

3. **Procedure for Reporting of Suspicious Transactions:** Every Business and individual has normally certain kind of transactions in line with their business/ individual needs, which is declared in the Transaction Profile (TP) of the customer. Transactions inconsistent with the declared TP will be considered unusual. All officials of the FI must be alert to transactions that are inconsistent with the customer's KYC information. If any unusual transaction is found, then the employees who have noticed it should follow the following procedures to determine whether a STR should be filed or not:

- Review the account opening form, KYC documentation, transaction profile etc.
- Check to see if the subject has been reported previously for suspicious activity.
- Seek information about the subject of the investigation from other people, if necessary.
- Review account statement and transaction records of the customer who is the subject of the investigation. At least 6 months' review of account activity should be done.
- Seek information from the respective officer who is responsible for opening the account or directly from the customer, if necessary. Before contacting with the customer, BAMLCO must be consulted with to assess whether it is appropriate to contact the customer.

If the issue appears reportable, then the concerned employee will immediately prepare a report as per the prescribed form (As per AML Circular No. 19 dated 14/08/2008) and then send it to the BAMLCO. BAMLCO should acknowledge receipt of the report.

Sufficient information should be disclosed on the report, including the followings:

- Full details of the customer and 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 minimum delay.
- Where additional relevant evidence is held which could be made available to the investigating officer, this should be noted on the form.

BAMLCO will analyze the reported incident properly in the light of all other relevant information and record in writing with reasons in details whether the transaction is connected with money laundering or terrorist financing or not. If the reported issue does not appear to be connected with money laundering, then BAMLCO will close the issue at his end after putting his comments on the STR form annexed in the Instruction Circular No.19/08 dated 21/09/2008. If the reported issue appears to be connected with money laundering or terrorist financing, then BAMLCO will send immediately the details of the incident along with a copy of the above form to the CAMLCO.

4. **Maintaining Secrecy**: The above review will be done as a part of the daily functions of the branch. It should be kept in mind that all exceptions may not be suspicious. Also, branch officials should be very much cautious in dealing with customers. They should perform the job in a manner that do not create any panic and do not disclose any information to any person.

5. **Documents to be enclosed with the STR**: At the time of forwarding an STR to the CAMLCO, BAMLCO should enclose the following documents with the STR Form:
- Photocopy of Account Opening Form, KYC, Transaction Profile etc.
- Photocopy of all documents related to Account Opening (including Passport, National
- ID Card, Trade License etc.),
- Statement of the Account for at least 1 (One) year.
- Relevant vouchers.

6. **STR Register**: All investigation issues must be documented in a register. The register should include the investigation issue and the rationale for the disposition of the case. In addition, any unusual activity for which decision was taken not to file a STR should also be documented in the register.

7. **Disclosure to Bangladesh Bank**: CAMLCO will examine and analyze the reports received and record its observations on the above form and if they consider the incident to be reportable, then they will submit the same directly to the General Manager & Operational Head, Bangladesh Bank Financial Intelligence Unit, Bangladesh Bank within 7(Seven) days (for suspicion of Money Laundering) or 3(Three) days (for suspicion of Terrorist Financing) and maintain confidentiality.

At the time of deciding whether or not a report should be submitted to Bangladesh Bank, all other relevant information available within the FI concerning the person or business should be considered. This may include a review of the followings:
- 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.

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

However, if employee continues to encounter suspicious activities on an account which they have reported previously, they should continue to make reports whenever a further suspicious transaction occurs.

8. **Requirements for Documentation**: All suspicious Activity Reports should be kept in custody for the following tenures:

- Records of suspicions, which were raised internally with the CAMLCO but not disclosed to Bangladesh Bank, should be retained for 5 (Five) years from the date of the transaction.
- Records of suspicions which Bangladesh Bank has advised to be of no interest should be retained for a similar period.
- Records of suspicions that assist with investigations should be retained until First Finance Limited is informed by Bangladesh Bank that they are no longer required.

9. **Internal Reporting**: All reports, statements, queries and communications related to anti-money laundering functions must be addressed to the following:

Deputy CAMLCO
Anti-Money Laundering Department First
Finance Limited
Head Office
Jahangir Tower (3rd Floor), 10 Kawran
Bazar, Dhaka-1215
Telephone: +880-2-9145487-29
Fax : +880-2-9142374
E-Mail : ashfaq@first-finance.com.bd

9. **External Point of Contact for Reporting**: The national reception point for reporting of suspicions by the CAMLCO is:

The General Manager & Operational Head
Bangladesh Bank Financial Intelligence
Unit, Bangladesh Bank
Head Office, Dhaka-1000.

Bangladesh Bank Financial Intelligence Unit of Bangladesh Bank can be contacted during office hours at the following numbers:
Telephone: +880-2-9530118
Fax : +880-2-9530089

3.6 REPORTING OF CASH TRANSACTION REPORT (CTR)

The Branch Anti-Money Laundering Compliance Officer (BAMLCO) will monitor and analyze the daily cash transaction and prepare daily Cash Transaction Report (CTR) as per BFIU circular – 11 in case of cash deposit, cash withdrawal and cash remittance/online deposit of Tk.10.00 lac and above in a single transaction or multiple transactions in any account in a single day. He or she will send CTR to Anti-Money Laundering Cell of Head Office by the 1st week of subsequent month for onward submission of the same to BFIU of Bangladesh Bank.

The BAMLCO will analyze the CTR(s) meticulously before reporting the same to AML Department. If something is found suspicious/unusual, the BAMLCO will report the Account as STR in prescribed format. If s/he don't find anything suspicious/unusual s/he will make a comments "we checked and didn't find any suspicious in the CTR" and will send the forwarding to AML Cell of Head Office.

3.7 SELF ASSESSMENT & INDEPENDENT TESTING PROCEDURES SYSTEM

1. **Self Assessment Process**: All branches should establish self-assessment process that will assess how effectively the branch's anti-money laundering procedures enable management to identify areas of risk or to assess the need for additional control mechanisms. Branches should follow the following steps to assess itself in a quarterly basis:

- Branches shall assess themselves and prepare a Report on the basis of Self Assessment Checklist attached with AML Circular No. 15 dated 24/03/2008 issued by Bangladesh Bank on a quarterly basis.
- On the basis of such assessment, the branch shall arrange a meeting on monthly basis of all important officials of the branch and to be presided over by the Branch Manager of the branch.

  The meeting shall –
  - discuss the branch's self assessment report;
  - identify areas of risk/problem; if any
  - find out ways or recommendations to mitigate the risk/problem areas; and
  - maintain minutes;

  Next meetings shall also discuss -
  - the issues discussed in the previous meeting;
  - assigned responsibilities; and
  - their implementation status;
- Every branch shall send their
  - Self Assessment Report;
  - steps taken by the branch; and
  - recommendations in this regard;

  to the Anti-Money Laundering Cell and Internal Audit Department of Head Office within the 15th of the next month after completion of each quarter.

2. **Independent Testing Procedures**: Internal Audit Department shall perform the following duties:

- Internal Audit Department shall examine the Self Assessment Reports received from branches and shall inspect instantly any branch where any risky area has been identified. Audit Department shall report the same to the senior management of the FI.
- As a part of its own natural branch audit/inspection program/schedule, Audit Department shall check the anti-money laundering performance of the branch at the time of performing branch audit/ inspection program. Internal Audit Department shall include a separate Chapter on Anti- Money Laundering in its Branch Audit Report on the basis of Independent Testing Procedures Checklist attached in the AML Circular No.15/08 dated 24/03/2008. A copy of the anti-money laundering chapter of the inspection report shall be submitted to the Anti-Money Laundering Cell on a Quarterly basis.

Anti-Money Laundering Cell shall perform the following duties:

- Anti-Money Laundering Cell shall examine the Self Assessment Reports received from branches, prepare an overall Assessment Report and submit it to the CEO & Managing Director with comments and recommendations on a half-yearly basis.
- AML Cell shall prepare a checklist based Assessment Report of the branches inspected in a quarter on the basis of inspection reports submitted by Internal Audit Department after inspecting branches. Such report should be submitted to the CEO & Managing Director with comments and recommendations. Comments also should be added taking into consideration the Self Assessment Reports submitted by the branches inspected.
- Anti- Money Laundering Cell shall submit a report on the above to the Bangladesh Bank Financial Intelligence Unit of Bangladesh Bank, Head Office, Dhaka on a half-yearly
  basis within 60 days after completion of the concerned half year.
- After reviewing the Independent Testing Reports received from Audit Department, AML Cell of HO shall conduct special inspection in those branches which is rated Unsatisfactory & Marginal. AML Cell of HO shall also take necessary measures to improve the compliance standard of those branches and report the same to the senior management of the FI.

3.8 KEEPING OF RECORDS

1. **Statutory Requirements**: Section 25(1)(Ka) of the Money Laundering Prevention Act-2012 requires us to retain correct and full information used to identify customers during their account relationships. Section 25(1)(Kha) of the Act requires us to retain transaction related records for at least 5 (Five) years after termination of relationships with the customers. The records prepared and maintained by Branches and Head Office 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 FI's observance of money laundering policies and procedures;
- any customer can be properly identified and located;

- all suspicious activity reports received internally and those made to Bangladesh Bank can be identified; and
- the FI can satisfy within a reasonable time any enquiries or court orders from the appropriate authorities as to disclosure of information.

2. **Documents Verifying Evidence of Identity and Transaction Records**: Records relating to verification of identity will generally comprise:

- a description of the nature of all the evidences 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.

Records relating to transactions will generally comprise:

- details of personal identity, including the names and addresses, etc. as prescribed by Bangladesh Bank under M.L.P. Circular No. 02 dated 17-07-2002 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:
    1) the nature of such transactions;
    2)customer's instruction(s) and authority;
    3)source(s) and volume of funds;
    4)destination(s) of funds;
    5)book entries;
    6)custody of documentation;
    7) the date of the transaction;
    8) the form (e.g. cash, cheque) in which funds are offered and paid out.

These records of identity must be kept for at least 5 (Five) years from the date when the relationship with the customer has been terminated. This is the date of:

i. the carrying out of the one-off transaction, or the last transaction 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.

3. **Formats and Retrieval of Records**: Records may be retained in any of the following formats:

- documents can be retained in their original hard copy form, or
- the FI may establish reliable procedures for holding records in electronic form.

Whatever the format may be, all records should be capable of retrieval without undue delay.

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
- identifying where the transaction took place and in what form.

4. **Wire Transfer Transactions**: Investigations of major money laundering cases have shown that criminals make extensive use of telegraphic transfers (TT) and electronic payment and message systems because of the complexity of cross-border investigations. Investigations become more difficult if the identity of the original ordering customer (i.e. purchaser) or the ultimate beneficiary is not clearly shown in a TT and electronic payment message instruction.

In such a situation, all branches must include accurate and meaningful information of the followings on all outgoing funds transfers:

- the originator (name, account number, and where possible address),
- the beneficiary (account name and/or account number) and
- the related messages that are sent.

All these information should remain with the transfer or related message throughout the payment chain.

Records of electronic payments and messages must be kept for at least 5 (Five) years.

5. **Investigations**: The only valid role that a FI plays in assisting law enforcement agencies, investigating a money laundering case, is a provider of relevant information, particularly where the money launderer has used a complex web of transactions specifically for the purpose of confusing/obscuring the audit trail.

Where First Finance Limited has submitted a report of suspicious activity to Bangladesh Bank or where the branch knows that a client or transaction is under investigation, the Branches shall not destroy any relevant records without the agreement of the Bangladesh Bank even though the 5 (Five) years limit is over.

The Branches and Anti-Money Laundering Section at Head Office shall maintain a register or tabular records of all investigations related to anti-money laundering made to it by the Bangladesh Bank and all disclosures to the Bangladesh Bank. The register should contain at a minimum the following details:

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

6. **Training Records**: Anti-Money Laundering Section & FFL Training Institute will conduct training courses on anti-money laundering and maintain records of the followings:

details of the content of the training programs provided,

i. the names of employees who have received the training,
ii. the date on which the training was imparted,
iii. the results of any testing carried out to measure employees understanding of the money laundering requirements, and
iv. an on-going training plan.

Chapter – IV
TRADE BASED MONEY LAUNDERING

4.1 DEFINITION & PROCESS

The process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origins. Trade-based money laundering involves using of the following techniques to disguise the illicit origin of money:

- over- and under-invoicing of goods and services;
- multiple invoicing of goods and services; or
- false description of goods and services.

4.2 RESPONSE OF FIRST FINANCE LIMITED TO COMBAT TRADE BASED MONEY LAUNDERING

First Finance Limited is well-aware of trade based money laundering. Authorized Dealer (AD) branches of First Finance Limited are instructed to closely monitor over- and under- invoicing of goods and services. Continuous training courses are arranged on "Trade Based Money Laundering" for the concerned officers working in the Foreign Exchange Desks.

4.3 CORRESPONDENT BANKING

Correspondent Banking shall mean providing services which are approved by Bangladesh Bank like credit, deposit, collection, clearing, payment or other similar services by one bank (correspondent) to another bank (respondent).

While establishing and continuing correspondent Banking relationship following drill should be observed so that Banking system cannot be abused for the purpose of money laundering :

- Before providing correspondent Banking service senior management approval must be obtained on being satisfied about the nature of the business of the respondent Bank through collection of information as per AML circular No. 24 dated 03/03/2010 issued by Bangladesh Bank.
- FIs should establish or continue a correspondent relationship with a foreign Bank only if it is satisfied that the FI is effectively supervised by the relevant authority.
- FIs should not establish or continue a correspondent Banking relationship with any shell Bank. [Here shell Bank refers to such Bank as are incorporated in a jurisdiction where it has no branches or activities and which is unaffiliated with a regulated financial group.]

- Correspondent Banking relationship shall not be established or continued with those respondent Banks that established correspondent Banking relationship or maintain account with a shell Bank.
- FI should pay particular attention when maintaining a correspondent Banking relationship with Banks incorporated in a jurisdiction that do not meet international standards for the prevention of money laundering (such as the countries and territories enlisted in Financial Action Task Force's Non-cooperating Countries and Territories list). Enhanced due diligence shall be required in such cases. Detailed information on the beneficial ownership of such Banks and extensive information about their policies and procedures to prevent money laundering shall have to be obtained.
- Enhanced Due Diligence shall have to be exercised in case of the respondent Banks that allow direct use of the correspondent account by their customers to transact business on their behalf(i.e. payable through account)
- The instructions described in this circular shall be applicable to the entire existing correspondent banking relationship.

4.4 BRANCHES AND SUBSIDIARIES SITUATED/LOCATED IN FOREIGN JURISDICTION

1. Reporting organizations (in applicable cases) under Money Laundering Prevention Act-2012 and Anti Terrorism Act (Amend)-2012 having branches and subsidiaries abroad shall also comply with the provisions of Money Laundering Prevention Act-2012 and Anti Terrorism Act (Amend)-2012.

2. If branch or a subsidiary located abroad, for any reason fails to comply with the instructions of Money Laundering Prevention Act-2012 and Anti Terrorism Act (Amend)-2012 it shall without any delay report to such cases to Anti Money Laundering Department mentioning the reason of the failure.

Chapter- V
TRAINING AND AWARENESS

5.1 STATUTORY REQUIREMENTS

Section 23(1)(Cha) of the Act requires Bangladesh Bank to provide training and arrange meetings, seminars etc. for the officers and staffs of the reporting organizations or any other organizations or institutions as Bangladesh Bank may consider necessary for the purpose of proper implementation of the Act.

Since FIs themselves have responsibilities under the Act in relation to identification, reporting and retention of records, First Finance Limited must ensure that its employees are adequately trained to discharge their responsibilities.

First Finance Limited shall take appropriate measures to make its employees aware of:

- Policies and procedures to prevent money laundering and for identification, record keeping and internal reporting;
- Legal requirements; and
- Provide employees with training in recognition and handling of suspicious transactions;

5.2 THE NEED FOR EMPLOYEES AWARENESS

The effectiveness of this Policy depends on the extent to which FI's employees appreciate the serious nature of the background against which the legislation has been enacted.

It this context, First Finance Limited shall introduce comprehensive measures to ensure that-

- All employees are fully aware of their own responsibilities and statutory obligations;
- All employees are aware that they can be personally liable for failure to report information in accordance with internal procedures.
- All employees are trained in a manner that they co-operate fully and provide prompt reports of any suspicious transaction.

5.3 EDUCATION AND TRAINING PROGRAMS

All relevant employees of the FI should be educated in "Know Your Customer (KYC)" requirements. The training in this respect should cover:

- the need to know the true identity of the customer; and
- the need to know about the type of business activities expected in relation to that customer at the outset to understand what might constitute a suspicious activity;

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

5.4 NEW EMPLOYEES

All new employees, irrespective of the level of seniority shall be trained on:

- background to money laundering,
- anti-money laundering laws, regulations, circulars and instructions,
- reporting of suspicious transactions,
- reporting of cash transactions, and
- self assessment and independent testing procedures.

5.5 EMPLOYEES OF FRONT DESK

Members of employees who are in a position to deal with account opening, or to accept new customers, or to receive Pay Order/DD/TT/FDR application forms and cheques for deposit into customer's account or other investments must receive appropriate training on the processing and verification procedures.

In addition, these employees must understand and be trained on:

- the need to verify the identity of the customer,
- the FI's account opening and customer/client verification procedures.

Such employees should be aware that:

- the offer of suspicious funds or the request to undertake a suspicious transaction need to be reported to the Branch Anti-Money Laundering Compliance Officer, whether or not the funds are accepted or the transactions proceeded, and
- must know what procedures to follow in these circumstances.

5.6 BRANCH MANAGERS

Persons responsible for supervising or managing employees should be provided with a higher level of instruction covering all aspects of money laundering procedures.

Such instruction should also highlight the followings:
- 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.

5.7 BRANCH ANTI-MONEY LAUNDERING COMPLIANCE OFFICER (BAMLCO)

BAMLCOs should receive in-depth training on:
- all aspects of the money laundering legislation,
- Bangladesh Bank directives,
- internal policies,
- validation and reporting of suspicious transactions, and
- new trends, techniques and patterns of criminal activity.

5.8 REFRESHERS' TRAINING

In addition to the above relatively standard requirements, training should be tailored to the needs of specialized areas of the FI's business. Contents of training programs should be kept under review and updated when necessary.

To ensure that employees do not forget their responsibilities, Anti-Money Laundering Section and FFL Training Institute should arrange refreshers' training at regular intervals.