# GUIDELINES FOR POSTAL REMITTANCE BUSINESS

# FOR COMBATING MONEY LAUNDERING

# AND TERRORIST FINANCING RISKS

# Preface

The techniques of Money Laundering and Terrorist Financing (ML/TF) are ever evolving process. The methods and techniques used for money laundering and terrorist financing are changing in response to developing counter measures. For that reason, Financial Action Task Force (FATF), the international standard setter for AML/CFT, has revised its 40 (forty) recommendations for anti money laundering (AML) and 9 special (nine) recommendations for combating financing of terrorism (CFT).

In line with the international standards and initiatives, Bangladesh has also amended its Money Laundering Prevention Act (MLPA), 2002 and enacted MLPA, 2009. Anti Terrorism Act (ATA), 2009 has also been enacted aiming to combat terrorism and terrorist financing. Both the Acts have empowered Bangladesh Bank (BB) to perform the anchor role in combating ML&TF through issuing instructions and directives for reporting agencies and building awareness among the financial communities.

In response to the changing circumstances, this guidance notes titled “Guidelines for postal remittance business for combating money laundering & terrorist financing risk" (hereinafter referred as Guideline), is prepared for Post Offices especially for postal remittances from aboard and postal transfer within Bangladesh for the first time.

The Guideline is deemed to be the best practice but should not necessarily be constitute as a legal interpretation of the said Acts. Because of vulnerabilities of postal sector being used by money launderers and terrorist financiers, Bangladesh Bank (BB), as part of its supervisory process, will assess the adequacy of procedures adapted to AML & CFT and the degree of compliance with such procedures. This guideline is designed to enable post offices to function in consistence with the Bangladesh's AML & CFT regulations.

An overriding aim of the money laundering prevention regulations and the Guideline is to ensure that appropriate identification information is obtained in relation to the clients (originator and beneficiary of any transaction) of post office and the payments made among them or remittances received on behalf of them. This is not only to assist the detection of suspect transactions but also to create an effective "audit trail" in the event of an investigation, if necessary.

## Table of Contents

# Chapter 1: Basics of Money Laundering and Terrorist Financing

## 1.1 Introduction

For most countries money laundering and terrorist financing raise significant issues with regard to prevention, detection and prosecution. Sophisticated techniques used to launder money and finance terrorism add to the complexity of these issues. Such sophisticated techniques for money laundering may involve: multiple financial transactions, the use of different financial instruments and other kinds of value-storing assets; different types of financial institutions, accountants, financial advisers, shell corporations and other service providers like remittance service; complex web of transfers to, through, and from different countries. On the other hand, terrorism financing involves intention to provide assets or assist in some way to do terrorist acts. A less simple concept, however, is defining terrorism itself, because the term may have significant political, religious, and national implications that may vary from country to country. Money laundering and terrorist financing often display similar transactional features, mostly having to do with concealment and disguise.

Money launderers send or try to send illicit funds through legal channels in order to conceal their criminal origins, while those who finance terrorism transfer funds that may be legal or illicit in origin in such a way as to conceal their source and ultimate use. But the result is the same—reward. When money is laundered, criminals profit from their actions; they are rewarded by concealing the criminal act that generates the illicit proceeds and by disguising the origins of what appear to be legitimate proceeds. Similarly, those who finance terrorism are rewarded by concealing the origins of their funding and disguising the financial support to carry out their terrorist stratagems and attacks.

## 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 offense, e.g. drug trafficking, or offenses or from an act of participation in such offense or offenses, 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 offense or offenses to evade the legal consequences of his actions;
- The concealing or disguising of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from an offense or offenses or from an act of participation in such an offense or offenses, and;
- The acquisition, possession or use of property, knowing at the time of receipt that such property was derived from an offense or offenses or from an act of participation in such offense or offenses.

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.”

Money Laundering is defined in Section 2 (k) of the Money Laundering Prevention Act, 2009 as follows:

**Money Laundering** means:

i) transfer, convert, bringing/remitting funds in and out of Bangladesh the money or properties acquired through commission of any predicate offence[1] with an intention to concealing or disguising the illicit origin of the property or smuggle fund or property earned through legal or illegal means to abroad;

ii) conduct, or attempt to conduct a financial transaction with an intent to avoid a reporting requirement under this Act (the MLPA, 2009).

iii) to do or attempt to do such activities so that the illegitimate source of the fund or property may be concealed or disguised or knowingly assist to perform or conspire to perform such activities.

### 1.3 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

[1] Predicate offence is the underlying criminal activity that generated proceeds, which when laundered, results in the offense of money laundering.

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 annex; 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. (Deleted by UN)

3. 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)[2].

Some countries face difficulties in defining terrorism as not all countries have adopted the conventions agreed on specifically what actions constitute terrorism. In addition, the meaning of terrorism is not universally accepted due to significant political, religious and national implications that differ from country to country. FATF, which is recognized as the international standard setter for combating financing of terrorism (CFT) efforts, does not specifically define the term financing of terrorism in its nine Special Recommendations on Terrorist Financing (Special Recommendations). Nonetheless, FATF urges countries to ratify and implement the 1999 United Nations International Convention for Suppression of the Financing of Terrorism. Thus, the above definition is the one most countries have adopted for purposes of defining terrorist financing.

According to the article 7 of the Anti Terrorism Act, 2009, **financing of terrorism** means:

---

[2] International Convention for the Suppression of the Financing of Terrorism (1999), Article, http://www.un.org/law/cod/finterr.htm. The treaties referred to annex in sub-paragraph 1(a) shall be available in this web link.

(1) Whoever provides or incites to provide money, service or property and intends that it should be used, or has reasonable ground to suspect that it will or may be used for the purpose of terrorist acts; commits an act of terrorist financing.

(2) Whoever receives money, service or property and intends that it should be used, or has reasonable ground to suspect that it will or may be used for the purpose of terrorist acts; commits an act of terrorist financing.

(3) Whoever arranges money, service or property and intends that it should be used, or has reasonable ground to suspect that it will or may be used for the purpose of terrorist acts; commits an act of terrorist financing.

(4) A person guilty of the offence as described in the subsections from 1 to 3 shall be punished with imprisonment for a term which may extend to twenty years and it shall not be less than three years, to which fine may also be added.

### 1.4 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. 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.

For these reasons, FATF has recommended that each country criminalizes the financing of terrorism, terrorist acts and terrorist organizations, and designates such offenses as predicate offenses of money laundering. Finally, FATF has stated that the nine Special Recommendations combined with The Forty Recommendations on money laundering constitute the basic framework for preventing, detecting and suppressing both money laundering and terrorist financing.

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

### 1.5 The reason of committing money laundering

Criminals engage in money laundering for three main reasons:

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

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.

### 1.6 The reason of committing terrorism financing

Terrorism financing is done mainly to facilitate an extremist group by providing financial support aiming to establish or circulate their ideology. Such financial assistance may be provided directly or indirectly or may be attempted and amount of money may be significantly low with several in numbers.

### 1.7 Laundering Techniques

Obviously there is no single way of laundering money or any other property. It can range from the simple method to highly complex schemes involving a web of international businesses and investments. In general, money laundering process comprises three stages:

***Placement* –** placing the criminal funds into the financial system directly or indirectly.

***Layering* –** the process of separating criminal proceeds from their source by using complex layers of financial transactions designed to hide the audit trail and provide anonymity.

***Integration* –** if the layering process succeeds, integration schemes place the laundered proceeds back into the legitimate economy in such a way that they appear to be legitimate.

This “three stages model” is more often occur simultaneously or overlap depending on the facilities of the launderer, the requirements of the criminals, and on the robustness, or otherwise, of the regulatory and legal requirements.

# Chapter 2: Vulnerabilities of ML/TF

## 2.1 Introduction

Criminals and terrorists succeed largely in concealing the origins or sources of their funds and sanitize the proceeds by moving them through national and international financial systems. Money laundering and the financing of terrorism have particularly significant economic and social consequences for a developing country like Bangladesh. The absence of, or a lax in AML/CFT regime in a particular country encourages criminals and terrorists to operate and expand their criminal pursuits fostering illegal activities such as corruption, drug trafficking, illicit trafficking and exploitation of human beings, arms trafficking, smuggling.

## 2.2 The Adverse Implications for Developing Countries

The magnitude of the adverse impact of money laundering and terrorist financing cannot be quantified with the precisions. There are so many adverse effects of money laundering and terrorist financing for a developing country like Bangladesh. Some of them are describes below:

### 2.2.1 Increased Crime and Corruption

If money laundering is prevalent in a country, it enhances crime and corruption in different ways. To the extent that a country is viewed as a safe haven for money laundering, it is likely to attract criminals and promote corruption. Safe haven includes-

- weak AML/CFT framework,
- little enforcement of AML/CFT provisions,
- limited number of predicate offences,
- limited inclusion of reporting institutions,
- ineffective penalties etc.

A comprehensive and effective AML/CFT framework, together with timely implementation and effective enforcement significantly reduce the profitable aspects of criminal activities and discourage criminals and terrorists. This is especially true when the proceeds from criminal activities are aggressively confiscated and forfeited as part of a country's overall AML/CFT legal framework.

### 2.2.2 Non-cooperation from Foreign Counterparts

Foreign financial institutions may decide to limit their transactions with institutions from money laundering havens, subject these transactions to extra scrutiny making them more expensive, or terminate correspondent or lending relationships altogether. Even legitimate businesses and enterprises from money laundering havens may suffer from reduced access to world markets or access at a higher cost due to extra scrutiny of their ownership, organization and control systems.

Any country known for lax enforcement of AML/CFT is less likely to receive foreign private investment. For developing nations, eligibility for foreign governmental assistance is also likely to be severely limited.

Foreign direct investment and foreign aid may be reduced or withdrawn because of lax enforcement of AML/CFT measures.

Finally, the Financial Action Task Force (FATF) on Money Laundering maintains a list of countries that do not comply with AML requirements or that do not cooperate sufficiently in the fight against money laundering i.e. "non-cooperating countries and territories" (NCCT) list, gives public notice that the listed country does not have in place even minimum standards. Beyond the negative impacts referred to here, individual FATF member countries could also impose specific counter-measures against a country that does not take action to remedy its AML/CFT deficiencies.

### 2.2.3 Compromised Economy and Private Sector

Money launderers may use *front companies*[3] to co-mingle the illicit funds with legitimate funds in order to hide the ill-gotten proceeds, not to earn profit. Access to illicit funds let front companies to subsidize the front company's products and services, even at below-market prices. As a consequence, legitimate companies find it difficult to compete with such front companies. Thus by using front companies and other investments in legitimate companies money laundering proceeds can be utilized to control whole industry or sectors of the economy of certain countries. This increases the potential for monetary and economic instability due to the misallocation of resources from artificial distortions in asset and commodity prices. It also provides a vehicle for evading taxation, thus depriving the country of revenue.

---

[3] Business enterprises that appear legitimate and engage in legitimate business but are, in fact, controlled by criminals

### 2.2.4. Damaged Privatization Efforts

Money launderers threaten the efforts of many countries to reform their economies through privatization. These criminal organizations are capable of outbidding legitimate purchasers of former state-owned enterprises. When illicit proceeds are invested in this manner, criminals increase their potential for more criminal activities and corruption, as well as deprive the country of what should be legitimate, market-based, taxpaying enterprise.

## 2.3 Vulnerabilities of Remittance Business

2.3.1. One of the main techniques commonly used at present is the conversion of large amounts of criminal proceeds in local currency into low bulk foreign currencies for physical smuggling out of the country. Some countries also evidenced the use of international money orders and mail services to send large sums of cash abroad.

2.3.2. Remittances is often used in the layering process. One of the most popular techniques is simply to transfer illicit funds through several different remittance operators to disguise the trail to the funds' original sources.

2.3.3. Another method is to make transfers from numerous accounts to a principal collection account which is often located in offshore financial centre.

2.3.4. Transfers are also made under false identities and sometimes it becomes difficult to identify the actual recipient of the funds.

2.3.5. Remittance operators, which traditionally encompass the non-banking segment of the population, notably immigrant workers or any other person having no bank account often transfer funds to the countries where banking services are less regulated.

Looking at the vulnerability of remittance service industry, the respective institutions should therefore be more vigilant to evolving money laundering and financing of terrorism threats to prevent their institutions from being abused to facilitate money laundering and financing of terrorism activities.

### 2.4 The Benefits of an Effective AML/CFT Framework

A strong AML/CFT institutional framework that includes a broad scope of predicate offenses for money laundering helps to fight against crime and corruption. An effective AML/CFT regime is deterrent to criminal activities. In this regard, confiscation and forfeiture of money laundering proceeds impedes to earn profits from criminal activities, thereby reducing the incentive to commit criminal acts.

In addition, an effective AML/CFT regime reduces the possibilities of losses to the institutions originating from fraudulent activities. Proper customer identification procedures and determination of beneficial ownership provide specific due diligence for higher risk policies and ensure monitoring for suspicious activities. Such prudential internal controls play a vital role for the safe and sound operation of a financial institution. This enhances public confidence and permits investments to be put into productive purposes that respond to consumer needs and help the productivity of the overall economy.

# Chapter 3: Measures to be taken by the Institutions engaged in Postal Remittances

## 3.1. Introduction

This section describes about various measures to be taken by the postal authority at the time of providing remittance services to prevent money laundering and combat financing of terrorism in line with the Money Laundering Prevention Act, 2009 and Anti Terrorism Act, 2009. This section highlights the role and responsibility of postal authority to mitigate money laundering & terrorist financing and enable them to alleviate such risks in an appropriate manner.

## 3.2. Definitions:

To understand all instructions of this guideline, the following definitions shall apply:

i) **“Postal remittance”** is a transaction carried out on behalf of an originator (both natural and legal) through a post office (local or overseas) with a view to making an amount of money available to a beneficiary (both natural and legal) at another post offices (local or overseas). These postal remittances include remittance received from foreign post offices and all types of local postal orders or any type of local remittance services provided by the postal authority.

ii) The **“applicant/originator”** is a natural or legal person who places order for postal remittances in a local or foreign postal counter.

iii) An **“Ordering post office”** is the one that originates a postal transfer as per the order placed by its customer (i.e. originator). Ordering post office may be local or foreign.

iv) A **“Foreign post”** means a post office situated in Bangladesh with the postal authority deals with foreign mails and remittances as an intermediary.

v) A **“Receiving post office”** is the one that makes payments to a beneficiary/recipient of a postal order.

vi) The term **“accurate”** is used to describe information that has been verified for accuracy.

vii) The term **“full”** is used to describe a situation in which all elements of required information are present. For example; the name and detail address of the originator, bank account number or a unique reference/photo identity card.

viii) The term **“meaningful”** is used to describe information which has meaning on its face, but not been verified for accuracy.

### 3.3. Measures to be taken by ordering post office:

(a) The ordering post office (local) is required to collect the full and accurate originator information and meaningful beneficiary/recipient information while providing postal remittance services more than BDT 50,000;

(b) The ordering post office (local) is required to collect and verify the following originator information:

- name of the originator;
- date of birth;
- purpose of the remittance;
- nationality;
- address (residential and/or official) and contact no. and
- obtain national ID card/registration/passport/any photo ID.
- name and detail address of beneficiary/recipient.

(c) The ordering post office (local) is required to transmit the following originator's information to the intermediary or receiving post office:

- name;
- nationality;
- address (residential and/or official) and contact no.
- purpose of the remittance;
- national registration or identification number/passport number;

(d) The ordering post office (local) must also preserve the information at least for a period of five years after the transaction is effected (as required under Money Laundering Prevention Act, 2009). Ordering post office should also ensure that preserved information will be supplied to the receiving post office as and when they are requested.

**3.4. Measures to be taken by Foreign Post**

(a) For international postal remittances, foreign post shall ensure that all required originators' and beneficiary/recipients' information are there.

(b) Records of information received from the ordering post office must be kept at least for five years (as required under Money Laundering Prevention Act, 2009) by foreign post.

**3.5. Measures to be taken by receiving post office:**

(a) A receiving post office should have effective risk-based procedures in place to identify postal remittance both local and foreign lacking complete originator information. The lack of complete originator information may be considered as a factor in assessing whether remittance(s) is suspicious and whether they should be reported to the Anti-Money Laundering Department (Financial Intelligence Unit), Bangladesh Bank. The receiving post office should also take up the matter with the ordering post office if a transaction is not accompanied by detailed information of the originator. If the ordering post office fails to furnish required information of the originator, the receiving post office should consider necessary precautions or even terminates its business relationship with the ordering post office.

(b) While making payment to the beneficiary/recipient, the receiving post office must preserve the identity documents and information. The receiving post office is required to keep the following beneficiary/recipient's information:

- name;
- address (residential and/or official) and contact no.
- a photo ID document.

(c) Receiving post office is required to preserve all records at least for 05 (five) years as required under Money Laundering Prevention Act, 2009.

**3.6. Reporting:**

(a) If a postal remittance has incomplete originator's information, it may be considered as a factor for suspicion and where appropriate, the receiving post office should lodge a suspicious transaction report to the General Manager, Bangladesh Financial Intelligence Unit (BFIU), Bangladesh Bank, Motijheel, Dhaka as per the annex format.

(b) If a postal remittance provider has reasonable ground to believe that the fund is coming from the person/entity (originator) listed under listed under UN sanction list[4] or local sanction list [5] or beneficiary/recipient is the same listed person/entity or the fund to be used in money laundering/terrorist activities, it should immediately be reported to the BFIU, Bangladesh Bank as per annexed reporting format.

(c) This Guideline provides some list (stated in para 3.8) of indicators (though this list is not exhaustive) for suspicion. A postal remittance provider should also consider this list while lodging a Suspicious Transaction Report (STR) to the BFIU, Bangladesh Bank.

**3.7. Cooperation with FIU and law enforcement agencies**

Postal remittance service provider should cooperate with the BFIU and law enforcement agencies on proactive and reactive basis. They should provide originator and beneficiary information to the BFIU, Bangladesh Bank or law enforcement agencies within 03 (three) working days of receiving request.

**3.8. Examples of transactions that may trigger suspicion**

- Transactions conducted are out of the usual norms or profile of customers carrying out such transactions.
- While conducting a transaction client uses different identity in each time.
- The same client conducting few small transactions in a day or at different branches/locations.
- If there are sudden or inconsistent changes in value/frequency/information.

[4] UN designated list refers UNSCR-1267 and UNSCR-1373 and its successors. These lists will be available by: www.un.org/sc/committees/1267/consolist.shtml

[5] Local list refers the sanction list of individual or entities by the Ministry of Home Affairs from time to time.

- Remittances from different originators/jurisdictions being sent to the same beneficiary without prior permission[6].
- Client frequently remitting money to the countries having lacks in AML/CFT (Anti Money Laundering/ Combating Financial Terrorism) regime.
- Originator ordering for numerous postal money orders in small amounts favoring numerous beneficiaries without prior permission[7].

### 3.9. Training and awareness of employees

Money laundering and terrorist financing can take place in various ways and using various techniques. So all the staff/employees of the postal remittance provider must be well equipped and acquainted with the existing rules & regulations to prevent money laundering and terrorist financing. They also need to be aware of the recent trends and typologies of ML/TF.

To prevent the remittance industry from such threats training and awareness building program for all staffs is required as a mandatory as per Money Laundering Prevention Act, 2009 and Anti Terrorism Act, 2009. And hereby Postal Academy, Rajshahi and all other training centers of Bangladesh Post Office are directed to include the topic as a sub-module in all training program they conduct.

---

[6] without prior permission means any institute/organization/company in Bangladesh approved with the postal authority to remit or receive fund frequently.

[7] Same as above in 6.

**Annexure**

# SUSPICIOUS TRANSACTION REPORT (STR)

POSTAL REMITTANCES)

**A. Reporting Post Office :**

1. Name of the Post Office:
2. Address:

**B. Details of Report:**

1. Date of sending report:
2. Is this the addition of an earlier report? Yes No
3. If yes, mention the date of previous report

**C. Suspect Account Details :**

1. Name:
2. Address:
3. Profession/Business:
4. Nationality/Ownership status:
5. Father's name/ Proprietor's name:
6. Mother's Name (where necessary):
7. Date of birth (where necessary):
8. Contact: Mobile No/Email.
9. Any other important Information:

**D. Reasons for considering the transaction(s) as unusual/suspicious?**

*(Mention summary of suspicion and consequence of events)*

*(Use separate sheet, if needed)*

| **E. List of Documents attached with the report** |
|---|
| |

Signature :
(Authorized officer)
Name :
Designation :
Phone :
Date :