

**Operational Guidelines on  
Prevention of Money Laundering and Terrorist Financing**



**United Finance Limited**

**OPERATIONAL GUIDELINES ON PREVENTION OF MONEY LAUNDERING AND  
TERRORIST FINANCING**

---

**CONTENTS**

PROLOGUE.....	3
Money Laundering (ML) .....	3
Stages of Money laundering.....	3
Predicated offences .....	4
Terrorist Financing (TF) .....	5
Terrorist financing methods and techniques .....	5
CHAPTER 1: COMPLIANCE REQUIREMENTS .....	6
CHAPTER 2: COMPLIANCE INFRASTRUCTURE .....	7
2.1 Central Compliance Unit (CCU) .....	7
Roles of CCU .....	7
2.2 AML/CFT Committee.....	8
Roles of AML/CFT Committee.....	8
CHAPTER 3: HUMAN RESOURCE DEPLOYMENT FOR AML/CFT INITIATIVES .....	9
3.1 CAMLCO .....	9
3.2 DCAMLCO .....	9
3.3 BAMLCO .....	9
3.4 AML/CFT Compliance Officer .....	9
CHAPTER 4: RESPONSIBILITIES UNDER COMPLIANCE FRAMEWORK .....	10
4.1 CAMLCO .....	10
4.2 DCAMLCO .....	11
4.3 BAMLCO .....	11
4.4 AML/CFT Compliance Officer .....	11
4.5 Specific key personnel .....	12
4.5.1 Branch Manager .....	12
4.5.2 Chief Service Officer (CSO) .....	12
4.5.3 Chief Operations Officer (COO) .....	12
4.5.4 Chief Risk Officer (CRO).....	13
4.5.5 Chief Financial Officer (CFO).....	13
4.5.6 Chief Business Officer (CBO).....	13
4.5.7 Deputy Managing Director (DMD) & Managing Director (MD) .....	13
4.5.8 Other Employees .....	14
CHAPTER 5: INDEPENDENT AUDIT FUNCTION.....	15
5.1 Role of Internal Audit and Compliance Department .....	15
5.2 Role of External Auditor .....	15

**OPERATIONAL GUIDELINES ON PREVENTION OF MONEY LAUNDERING AND  
TERRORIST FINANCING**

---

CHAPTER 6: TRAINING AND RESOURCE DEVELOPMENT .....	16
6.1    General Training .....	16
6.2    Job Specific Training.....	16
CHAPTER 7: AML/CFT RISK MANAGEMENT PROCESS .....	17
7.1    Risk Assessment Methodology .....	17
7.1.1    Risk identification.....	17
7.1.2    Risk assessment .....	17
7.1.3    Risk treatment .....	18
7.1.4    Risk monitoring & review .....	18
7.2    Risk Register .....	19
CHAPTER 8: CUSTOMER DUE DILIGENCE .....	24
8.1    Know Your Customer (KYC) .....	24
8.1.1    Components of KYC Program .....	24
8.2    Know Your Employee (KYE) .....	24
CHAPTER 9: RECORD KEEPING.....	25
9.1    Statutory Requirement .....	25
9.2    Retrieval of Records .....	25
9.3    STR and Investigation .....	25
9.4    Training Records.....	26
9.5    Branch Level Records .....	26
9.6    Sharing of Record/Information of/to a Customer .....	26
CHAPTER 10: STR/SAR .....	26
10.1    Reasons for Reporting of STR/SAR.....	27
10.2    Identification and Evaluation of STR/SAR.....	27
10.3    Reporting of STR/SAR.....	27
10.4    Tipping Off.....	27
10.5    “Safe Harbor” Provisions for Reporting .....	27
CHAPTER 11: ANNEXURE.....	28

## **PROLOGUE**

### **Money Laundering (ML)**

Money laundering (ML) refers to a financial transaction or scheme that aims to conceal the identity, source and destination of illicitly obtained money.

#### **Stages of Money laundering**

Money laundering is not a single act but a process accomplished in 3 basic stages stated below:

##### **i. Placement**

Placement means movement of illegally obtained fund from its source. The source can be disguised or misrepresented. The fund is placed into circulation through financial institutions and/or any other businesses, both local and foreign.

The process of placement can be carried out through many processes including but not limited to the following:

- Currency smuggling and currency exchange
- Bank complicity (when financial institution is owned or controlled by individuals suspected to be involved with criminals or other organized crime groups)
- Structuring large deposits of cash through security brokers to disguise the original source of the funds
- Smurfing or breaking down a transaction into smaller transactions to avoid detection
- Blending of illegal funds with legal transaction
- Purchase of less conspicuous assets with the illegal money
- Undervaluing or overvaluing of invoices
- Electronic transfer and remittance of funds through informal (unofficial) channels

##### **ii. Layering**

Layering is conversion of the illegal money in a less suspicious form. This makes the tracking of the illegal money difficult for regulators and law enforcement agencies. Following are some popular methods of layering activity:

- Cash converted into Monetary Instruments
- Material assets bought with cash and then sold

## **OPERATIONAL GUIDELINES ON PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING**

---

### **iii. Integration**

Integration is the step of acquiring wealth generated from the transactions of the illicit funds. Some known methods of integration include the following:

- The sale of assets previously bought with illegal fund
- Creating false loans
- Taking assistance of overseas financial institutions in countries and jurisdictions where local laws and regulations are lax
- Creating false and overvalued export/import invoices to justify the funds later deposited in domestic banks and/or the value of funds received from exports

### **Predicated offences**

Predicate offence is the underlying criminal activity that generated proceeds, which when laundered, results in the offense of money laundering. This includes:

- Counterfeiting currency;
- Unauthorized cross-border transfer of domestic and foreign currency;
- Counterfeiting deeds & documents;
- Corruption and bribery;
- Fraud;
- Forgery;
- Extortion;
- Robbery or theft;
- Breaking copy right/ intellectual right rules;
- Adulteration or breaking the copy right;
- Smuggling and duty related crime;
- Trafficking in human beings and migrant smuggling;
- Organized crime;
- Tax related crime;
- Insider trading & market manipulation;
- Illicit arms trafficking;
- Illicit dealing in narcotic drugs;
- Illicit dealing in stolen and other goods;
- Kidnapping, illegal restraint, hostage-taking;
- Murder, grievous bodily injury;
- Financing for terrorist activity;

## **OPERATIONAL GUIDELINES ON PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING**

---

### **Terrorist Financing (TF)**

Terrorist financing (TF) refers to activities that provides financing or financial support to individual terrorists or terrorist groups. Terrorist organizations use funds for various purposes such as operational activities, propaganda and recruitment, training of members, salaries and compensation to members, social services for killed militant's families, to build support within local populations and aid recruitment efforts, etc.

### **Terrorist financing methods and techniques**

Terrorist financing methods and techniques include but are not limited to the following:

- Private donations
- Abuse and misuse of non-profit organizations
- Proceeds of criminal activities
- Manipulating local populations and businesses
- Kidnapping for ransom
- Abuse and misuse of legitimate commercial enterprises
- State sponsorship of terrorism
- Self-funding

# **OPERATIONAL GUIDELINES ON PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING**

---

## **CHAPTER 1: COMPLIANCE REQUIREMENTS**

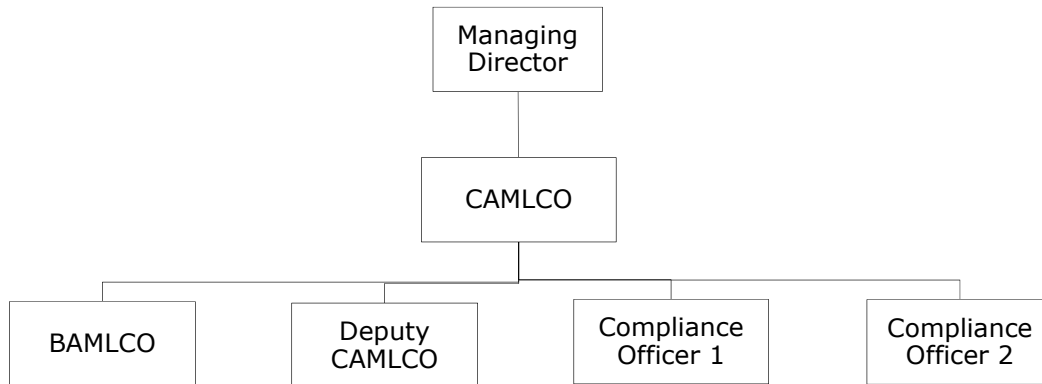
United Finance Limited, like all Banks and Non-Banking Financial Institutions, is vulnerable to money laundering and terrorist financing activities. In order to comply with regulatory requirements and as a responsible corporate citizen of Bangladesh, the Company has taken initiatives for preventing money laundering and combating terrorist financing, in line with the following legal, regulatory and internal directives:

- Money Laundering Prevention Act 2012 and Amendment Act 2015 [especially, but not limited to the responsibilities stated in section 25, which are:
  - i. to maintain complete and correct information with regard to the identity of its customers during the operation of their accounts;
  - ii. if any account of a customer is closed, to preserve previous records of transactions of any customer's account for at least 05 (five) years from the date of closure;
  - iii. to provide the information maintained under clauses (a) and (b) to Bangladesh Bank's designated unit from time to time, on its demand;
  - iv. if any doubtful transaction as defined in the "Money Laundering Prevention Act 2012 (with all amendments)" is observed or attempted, to promptly report the matter as "Suspicious Transaction" in the prescribed format to BFIU (Bangladesh Financial Intelligence Unit) immediately]
- Anti Terrorism Act 2009 and Amendment Act 2013
- Guidance Notes on Prevention of Money Laundering and Terrorist Financing" issued vide BFIU circular No: 4 dated 16 September 2012
- BFIU Circular No:12- dated 29 June 2016 Master Circular regarding Instructions to be followed by the Financial Institutions for the prevention of Money Laundering & Terrorist Financing
- Recommendations by the Financial Action Task Force (FATF)
- Policy Statement and Guidelines of United Finance Limited on "Prevention of Money Laundering, Terrorist Financing, Bribery and Unethical Financing"
- "Risk Assessment Report on Money Laundering & Terrorist Financing" of United Finance Limited

**CHAPTER 2: COMPLIANCE INFRASTRUCTURE**

**2.1 Central Compliance Unit (CCU)**

Central Compliance Unit (CCU) has been formed as a dedicated unit to ensure that the organization complies with applicable laws, policies, guidelines, regulations and directives issued by applicable internal and external authorities regarding prevention of money laundering and combating terrorist financing activities. Following is the structure of this unit:



**Figure:** Structure of CCU

**Roles of CCU**

- i. Issue and update the policies and instructions to be followed throughout the organization in order to prevent activities of money laundering and terrorist financing, in compliance with legal and regulatory requirements
- ii. Ensure mechanisms to identify and assess potential AML/CFT compliance and risk issues, to formulate mitigation plan, implement controls, and then to monitor and report these issues
- iii. Prepare overall assessment report after evaluating the self-assessment reports received from the branches. CCU will submit it with comments and recommendations to the Managing Director (MD).
- iv. Prepare overall assessment report based on assessment and inspection done by Internal Audit/Compliance.
- v. Submit report to Bangladesh Financial Intelligence Unit (BFIU) within stated time period.
- vi. Arrange training programs to educate all levels of employees regarding AML/CFT compliance issues



## **OPERATIONAL GUIDELINES ON PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING**

---

### **2.2 AML/CFT Committee**

Anti-money Laundering & Combating the Financing of Terrorism (AML/CFT) Committee has been formed to facilitate programs for prevention of money laundering and terrorist financing. Following is the structure of the Committee:

Chairman	CAMLCO (Chief Anti-Money Laundering Compliance Officer)
Member Secretary	DCAMLCO (Deputy Anti-Money Laundering Compliance Officer)
Members	Chief Risk Officer (CRO) Chief Service Officer (CSO) Product Manager (Liability Products) Supervisor-Data Control Unit AML/CFT Compliance Officer

### **Roles of AML/CFT Committee**

- i. Conduct discussion on AML/CFT compliance requirements already in place and to be introduced throughout the organization and ensure implementation of them at all levels.
- ii. Review AML/CFT non-compliance, STR/SAR and potential risk issues identified by any party and formulate action plan as per review and assessment.
- iii. Assess whether branches and departments are complying with AML/CFT compliance requirements or not and formulate action plan based on assessment.
- iv. Conduct training need assessment on AML/CFT compliance initiatives and formulate action plan.
- v. Respond to compliance questions and concerns of the staff. Advise regional offices/branches/units and assist in providing solutions to potential issues involving compliance and risk

**OPERATIONAL GUIDELINES ON PREVENTION OF MONEY LAUNDERING AND  
TERRORIST FINANCING**

---

**CHAPTER 3: HUMAN RESOURCE DEPLOYMENT FOR AML/CFT INITIATIVES**

**3.1 CAMLCO**

The Company has designated appropriate personnel (as per regulatory guidelines and directives) to act as Chief Anti-Money Laundering Compliance Officer (CAMLCO) of the organization. CAMLCO is primarily responsible to implement and enforce company-wide AML/CFT policies, procedures and measures. The CAMLCO is accountable to the Managing Director (MD) of the Company.

**3.2 DCAMLCO**

A Deputy Chief Anti-Money Laundering Compliance Officer (DCAMLCO) has been appointed to assist the CAMLCO in performing his responsibilities.

**3.3 BAMLCO**

Branch Anti-Money Laundering Compliance Officer (BAMLCO) has been appointed in each branch to ensure implementation of AML/CFT initiatives at branch level. BAMLCO will work under supervision of the CAMLCO and with assistance from the respective Branch Manager.

**3.4 AML/CFT Compliance Officer**

AML/CFT Compliance Officer has been appointed with the primary responsibility to ensure regular monitoring of whether AML/CFT initiatives are being complied at all levels of the Company or not.

**OPERATIONAL GUIDELINES ON PREVENTION OF MONEY LAUNDERING AND  
TERRORIST FINANCING**

---

**CHAPTER 4: RESPONSIBILITIES UNDER COMPLIANCE FRAMEWORK**

**4.1 CAMLCO**

- i. Monitor, review and coordinate development, updating and enforcement of the Company's policies, guidelines and procedures for prevention of money laundering and terrorist financing.
- ii. Monitor changes of laws/regulations and directives of BFIU and revise its internal policies accordingly
- iii. Respond to compliance questions and concerns of the employees, advise regional offices/branches/units and assist in providing solutions to potential issues involving compliance and risk;
- iv. Assess risks of new and changing business activities and products and to identify potential compliance issues that should be considered;
- v. Arrange training to develop the compliance knowledge of all staff;
- vi. Develop and maintain relationships with regulatory authorities, external and internal auditors, and regional/branch/unit heads and compliance resources to assist in early identification of compliance issues;
- vii. Assist in review of control procedures in the Company to ensure legal and regulatory compliance and in the development of adequate and sufficient testing procedures to prevent and detect compliance lapses
- viii. Monitor the business through self-testing for AML/CFT compliance and take any required corrective action;
- ix. Managing the STR/SAR process by ensuring the followings:
  - Reviewing transactions referred to as suspicious
  - Reviewing the transaction monitoring reports
  - Ensuring that Suspicious Activity Reports (SARs):
    - are prepared when appropriate
    - reflect the uniform standard for reporting of "suspicious activity involving possible money laundering or terrorist financing" established in our policy
    - are accompanied by documentation of the branch's decision to retain or terminate the account as required under its policy
    - are advised to other branches who are known to have a relationship with the customer
    - are reported to the Managing Director (MD) and the Board of Directors when the suspicious activity is judged to represent significant risk, including reputation risk
  - Ensuring that a documented plan of corrective action, appropriate for the seriousness of the suspicious activity, be prepared and approved by the branch manager
  - Maintaining a review and follow up process to ensure that planned corrective action, including possible termination of an account, be taken in a timely manner
  - Managing the process for reporting suspicious activity to regulatory authorities after appropriate internal consultation

## **OPERATIONAL GUIDELINES ON PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING**

---

### **4.2 DCAMLCO**

- i. Assist CAMLCO in development, updating and enforcement of the Company's AML/CFT compliance policy statements, guidelines, procedures in line with laws/regulations and directives of regulatory bodies
- ii. Assist CAMLCO in responding to compliance questions and concerns of the staff and advice regional offices/branches/units and assist in providing solutions to potential issues involving compliance and risk
- iii. Assist CAMLCO in monitoring, controlling, record keeping and reporting of compliance issues regarding prevention of money laundering and terrorist financing
- iv. Arrange statutory and ad-hoc meetings of CCU, prepare meeting agenda, record meeting minutes and ensure implementation and compliance of the decisions taken
- v. Assist CAMLCO in awareness raising, training and information dissemination among employees regarding AML/CFT compliance issues

### **4.3 BAMLCO**

- i. Monitor compliance of laws, regulation and directives regarding prevention of money laundering and terrorist financing by internal and external authorities at branch level.
- ii. Conduct periodic meeting with relevant parties regarding prevention of money laundering and terrorist financing and take necessary action regarding the following issues in line with applicable laws, regulation and directives by internal and external authorities:
  - Customer identification (Know Your Customer)
  - Transaction Monitoring
  - Identification and reporting of STR/SAR
  - Record keeping
  - Training to branch staff
- iii. Comply with policy, guidelines, regulations and directives by internal or external authorities
- iv. Report any suspicious activity to Branch Manager, and if necessary to the CAMLCO
- v. Provide training to Branch staff
- vi. Submit branch returns to CAMLCO in a timely manner

### **4.4 AML/CFT Compliance Officer**

- i. Accumulate data regarding AML/CFT non-compliance, STR/SAR and potential risk issues, analyze the data and present findings in the monthly AML/CFT meeting.
- ii. Provide support to CAMLCO and DCAMLCO to manage AML/CFT initiatives taken throughout the organization.

#### **4.5 Specific key personnel**

##### **4.5.1 Branch Manager**

- i. KYC Profile Approval
- ii. Quarterly meeting for finalizing self-assessment report
- iii. Monitoring utilization of lease/loans
- iv. Monitoring pre-mature encashment of deposits and early settlement of lease/loans
- v. Monitoring high risk customers
- vi. Reporting suspicious account activity or transaction

##### **4.5.2 Chief Service Officer (CSO)**

- i. Communicate internal and external policies, guidelines and procedures to all concerned service personnel to prevent money laundering and terrorist financing activities
- ii. Ensure that all concerned service personnel comply AML/CFT requirement at the time of confirmation/opening of customer account
- iii. Review account opening procedure and guidelines as and when required
- iv. Monitor client account, transaction, statements etc. as and when required
- v. Address potential risk issues and present them in the monthly AML/CFT meeting
- vi. Implement risk mitigation plans provided by internal and external authorities in department(s) under own jurisdiction
- vii. Ensure all mandatory and required data is captured through account opening form, required documents & KYC procedure before account opening
- viii. Review and update KYC information of the client as per customer's risk profile
- ix. Report any suspected AML/CFT issues with existing or new client to CCU

##### **4.5.3 Chief Operations Officer (COO)**

- i. Communicate internal and external policies, guidelines and procedures to all concerned operations personnel to prevent money laundering and terrorist financing activities
- ii. Ensure that all concerned operations personnel comply AML/CFT requirement at the time of confirmation/opening of customer account
- iii. Implement risk mitigation plans provided by internal and external authorities in department(s) under own jurisdiction
- iv. Report any suspected AML/CFT issues with existing or new client to CCU

## **OPERATIONAL GUIDELINES ON PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING**

---

### **4.5.4 Chief Risk Officer (CRO)**

- i. Develop company-wide action plan to combat money laundering and terrorist financing risk in line with applicable laws, regulations and directives by internal and external regulatory authorities.
- ii. Conduct periodic review of whether existing internal policies and procedures are adequate to identify and prevent AML/CFT risks and arrange to update the plan accordingly
- iii. Ensure upgrading and implementation of physical procedure to combat money laundering and terrorist financing risk
- iv. Report any suspected AML/CFT issues with existing or new client to CCU

### **4.5.5 Chief Financial Officer (CFO)**

- i. Develop mechanism to ensure good governance, disclosure and transparency
- ii. Establish and maintain internal controls and evaluate the effectiveness of internal control systems of the Company
- iii. Implement risk mitigation plans provided by internal and external authorities in department(s) under own jurisdiction
- iv. Report any suspected AML/CFT issues with existing or new client to CCU

### **4.5.6 Chief Business Officer (CBO)**

- i. Communicate internal and external policies, guidelines and procedures to all concerned sales and customer relationship personnel in order to prevent money laundering and terrorist financing activities
- ii. Ensure that all concerned sales and customer relationship personnel comply with AML/CFT requirement at the time of opening and operations of customer account
- iii. Implement risk mitigation plans provided by internal and external authorities in department(s) under own jurisdiction
- iv. Report any suspected AML/CFT issues with existing or new client to CCU

### **4.5.7 Deputy Managing Director (DMD) & Managing Director (MD)**

- i. Overall responsibility to ensure that the Company has an AML/CFT program in place and it is working effectively

**OPERATIONAL GUIDELINES ON PREVENTION OF MONEY LAUNDERING AND  
TERRORIST FINANCING**

**4.5.8 Other Employees**

<b>Function</b>	<b>Roles/Responsibilities</b>
<p>Staff Responsible for account opening (Liability Products):</p> <ul style="list-style-type: none"> <li>• Sales Personnel (DA/GC/TC)</li> <li>• Deposit Account Approver</li> </ul>	<ul style="list-style-type: none"> <li>▪ Perform due diligence on prospective clients before opening an account</li> <li>▪ Be diligent regarding the identification of account holder and the transactions relating to the account</li> <li>▪ Ensure all required documentation is completed</li> <li>▪ Complete the KYC Profile for the new customer</li> <li>▪ Ongoing monitoring of customer’s KYC profile and transaction activity</li> <li>▪ Escalate any suspected AML/CFT issues with existing or new client to Supervisor and/or CCU</li> </ul>
<p>Staff Responsible for account opening (Asset Products):</p> <ul style="list-style-type: none"> <li>• Sales Personnel (BE/BDM)</li> <li>• Financial Proposal Approver</li> </ul>	<ul style="list-style-type: none"> <li>▪ Perform due diligence on prospective clients before opening an account</li> <li>▪ Be diligent regarding the identification of account holder and the transactions relating to the account</li> <li>▪ Ensure all required documentation is completed</li> <li>▪ Complete the KYC Profile for the new customer</li> <li>▪ Ongoing monitoring of customer’s KYC profile and transaction activity</li> <li>▪ Escalate any suspected AML/CFT issues with existing or new client to Supervisor and/or CCU</li> </ul>
<ul style="list-style-type: none"> <li>• Head of Credit</li> <li>• Credit Officer</li> </ul>	<ul style="list-style-type: none"> <li>▪ Perform Risk Assessment for the Company</li> <li>▪ Perform periodic Quality Assurance on the program in the unit</li> <li>▪ Communicate updates in laws and internal policies</li> <li>▪ Escalate any suspected AML/CFT issues with existing or new client to Supervisor/CCU/CAMLCO.</li> </ul>
<ul style="list-style-type: none"> <li>• Head of Operations-Documentation</li> <li>• Head of Operations-Disbursement</li> <li>• Head of Collection</li> </ul>	<ul style="list-style-type: none"> <li>▪ Ensure that all requirements are completed prior to account opening and transaction in the account</li> <li>▪ Be vigilant of transaction trends of the client and raise concern immediately, as and when applicable</li> <li>▪ Update customer transaction profiles in the ledger/system</li> </ul>
<ul style="list-style-type: none"> <li>• Head of Management Information System (MIS)</li> </ul>	<ul style="list-style-type: none"> <li>▪ Ensures that the required reports are in place to maintain an effective program</li> </ul>
<ul style="list-style-type: none"> <li>• Head of System Administration</li> </ul>	<ul style="list-style-type: none"> <li>▪ Ensures that adequate technologies and required systems are in place to maintain an effective program</li> </ul>

**CHAPTER 5: INDEPENDENT AUDIT FUNCTION**

**5.1 Role of Internal Audit and Compliance Department**

- i. Address the adequacy of AML/CFT risk assessment
- ii. Examine/attest the overall integrity and effectiveness of the management systems and the control environment
- iii. Examine the adequacy of Customer Due Diligence (CDD) policies, procedures and processes, and whether they comply with internal requirements
- iv. Determine personnel adherence to AML/CFT policies, procedures and processes
- v. Perform appropriate transaction testing with particular emphasis on high risk operations (products, service, customers and geographic locations)
- vi. Assess the adequacy of processes for identifying and reporting suspicious activity
- vii. Communicate the findings to the Board and/or senior management in a timely manner
- viii. Recommend corrective action for deficiencies
- ix. Track previously identified deficiencies and ensure that they are corrected
- x. Assess training adequacy, including its comprehensiveness, accuracy of materials, training schedule and attendance tracking
- xi. Assess that the training programs and materials include topics prescribed by the regulator from time to time

**5.2 Role of External Auditor**

External auditors should focus their audit programs on risk factors and conduct intensive reviews of higher risk areas where controls may be deficient. External auditors shall communicate their findings and recommendations to management of the Company



# **OPERATIONAL GUIDELINES ON PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING**

---

## **CHAPTER 6: TRAINING AND RESOURCE DEVELOPMENT**

The Company will arrange suitable and adequate training programs on a regular basis in order to ensure that all employees, both permanent and contractual, are aware of their responsibilities.

The person responsible for designing the training must identify which, if any, of these topics relate to the target audience. Effective training should present real life money laundering scenarios, preferably cases that have occurred and attempted in the Company or in similar institutions, including how the pattern of activity was first detected and its ultimate impact on the institution (where applicable).

### **6.1 General Training**

Issues covered in a general training Program may include, but are not limited to following:

- General information on the risks of money laundering and terrorist financing schemes, methodologies, and typologies;
- Legal framework, how AML/CFT related laws apply to FIs and their employees;
- Institution's policies and systems with regard to customer identification and verification, due diligence, monitoring;
- How to react when faced with a suspicious client or transaction;
- How to respond to customers who want to circumvent reporting requirements;
- Stressing the importance of not tipping off clients;
- Suspicious transaction reporting requirements and processes;
- Duties and accountabilities of employees;

### **6.2 Job Specific Training**

A Job specific Training is required because the nature of responsibilities/activities performed by the different employees of the Company is different from one another. To Provide Job specific AML/CFT trainings, employees of the Company may be categorized as follows:

- New Employees
- Customer Service/Relationship Managers
- Credit Officers
- Operations staff
- Internal Audit and compliance staff
- AML/CFT Compliance Officer
- Operations Supervisors and Managers
- Senior Management and Board of Directors

# **OPERATIONAL GUIDELINES ON PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING**

## **CHAPTER 7: AML/CFT RISK MANAGEMENT PROCESS**

### **7.1 Risk Assessment Methodology**

The Company will prepare periodic risk assessment report by identifying inherent AML/CFT risks that the Company may encounter while conducting its regular business activities. CCU will conduct this assessment through a systematic analysis of the Company's Customers base, products & services, service delivery channel & geographical presence within the country.

#### **7.1.1 Risk identification**

The first stage of the risk assessment is to identify customers, products, services, transactions, and geographical locations specific to the United Financing Limited. Depending on specific characteristics of and delivery channels for certain customers, products, services and transactions, the threat of and vulnerability to money laundering and terrorism financing varies.

#### **7.1.2 Risk assessment**

In the second stage, the money laundering and terrorist financing risks that may be encountered by the Company will be analyzed as a combination of likelihood that the risks will occur and the impact of cost or damages if the risks occur. This impact can consist of financial loss to the business from the crime, from fines from the authorities or from enhanced mitigation measures. It can also consist of reputational damages to the business. Risk analysis will be carried out step by step as stated below:

##### **i. Likelihood Scale**

A Likelihood scale refers to the potential of an ML/TF risk occurring in business for the particular risk being assessed. Three level of risk are shown in below Table:

<b>Frequency</b>	<b>Likelihood of an ML&amp;TF risk</b>
Very likely	Almost certain: it will probably occur several times in a year
Likely	High probability: it will happen once a year
Unlikely	Unlikely, but not impossible

**OPERATIONAL GUIDELINES ON PREVENTION OF MONEY LAUNDERING AND  
TERRORIST FINANCING**

**ii. Impact Scale**

An impact scale refers to the seriousness of the damage (or otherwise) which could occur should the event (risk) happen. In assessing the possible impact or consequences, the assessment can be made from several viewpoints. Three level of risk are shown in below Table:

<b>Consequence</b>	<b>Impact – of an ML &amp; TF risk</b>
Major	Huge consequences – major damage or effect. Serious terrorist act or large-scale money laundering
Moderate	Moderate level of money laundering or terrorist financing impact
Minor	Minor or negligible consequences or effects

**iii. Risk Matrix (Threat Level)**

By blending likelihood & impact of a certain risk we can have the risk score (threat level). That is 'Likelihood X Impact'= Level of Risk (Risk Score).

<b>Likelihood</b>	Very Likely	Medium	High	Extreme
	Likely	Low	Medium	High
	Unlikely	Low	Low	Medium
		Minor	Moderate	Major
		<b>Impact</b>		

**7.1.3 Risk treatment**

In the third stage, The Company will, based on the analysis, apply risk management strategies and implement policies and procedures accordingly. To effectively mitigate the risk, adequate systems and controls will be implemented.

**7.1.4 Risk monitoring & review**

In the final stage, the risks and the management of the risks have to be monitored and reviewed. The Company will do this by developing a monitoring regime through its compliance and audit programs. The assessment of ML/TF risks will be revised periodically, based on the extent risks have changed or the operations or strategies have changed.

**OPERATIONAL GUIDELINES ON PREVENTION OF MONEY LAUNDERING AND  
TERRORIST FINANCING**

**7.2 Risk Register**

As per above stated risk assessment methodology, companywide money laundering and terrorist financing risks that may arise through customers, products or services, delivery channels, geographical presence and through failure to comply with regulatory requirements are tabulated in the following Risk Register with risk score & action plan:

<b>Risk group: Customers</b>				
<b>Categories of Risks</b>	<b>Likelihood</b>	<b>Impact</b>	<b>Risk Score</b>	<b>Treatment/ Action Plan</b>
1. New Customer	Very likely	Minor	Medium	Simplified Customer Due Diligence (CDD) [Note:01]
2. New customer who wants to carry out a large transaction	Unlikely	Major	Medium	
3. Customer or a group of customers maintaining several accounts in the same name or group	Unlikely	Major	Medium	
4. Customer who has a business which involves large amounts of cash	Unlikely	Major	Medium	
5. Customer whose identification is difficult to check	Unlikely	Major	Medium	
6. Customers who conduct their business or transactions from a significantly distant geographic location from the location of United Finance's office	Unlikely	Major	Medium	
7. Customers who frequently move to different institutions without having any reasonable explanation	Unlikely	Major	Medium	
8. Non-resident customers (Foreigner)	Unlikely	Moderate	Medium	
9. Trustees & Associations	Likely	Moderate	Medium	
10. Local or Foreign NGOs	Unlikely	Major	Medium	
11. Charities and other 'not-for-profit' organizations	Unlikely	Major	Medium	
12. Customer or group of customers who conduct regular transactions with the same individual or group of individuals	Unlikely	Major	Medium	
13. Professional service providers (e.g., attorneys, accountants, doctors, real estate brokers, etc.)	Likely	Moderate	Medium	

**OPERATIONAL GUIDELINES ON PREVENTION OF MONEY LAUNDERING AND  
TERRORIST FINANCING**

<b>Categories of Risks</b>	<b>Likelihood</b>	<b>Impact</b>	<b>Risk Score</b>	<b>Treatment/ Action Plan</b>
14. Corporate customer whose ownership structure is unclear or unusual or excessively complex	Unlikely	Major	Medium	Simplified Customer Due Diligence (CDD) [Note:01]
15. Customer who does not have any apparent source of Income but relies on others' income source	Likely	Moderate	Medium	
16. Customers who are politically exposed persons (PEPs) or head of international organizations and their family members and close associates	Unlikely	Major	Medium	
17. Customers who are influential persons (IPs)	Likely	Moderate	Medium	
18. Customer who comes for premature encashment of fixed deposit	Unlikely	Major	Medium	
19. Customer who generally tries to convince for cash deposit but insists for financial instrument while withdrawing the deposit	Unlikely	Major	Medium	
20. Government employee having several large fixed deposit accounts	Unlikely	Major	Medium	
21. Domestic Corporations	Likely	Minor	Low	Standard identification documents [Note:03]
22. Government Corporations	Likely	Minor	Low	
23. Customer who requests for early settlement of loan	Unlikely	Moderate	Low	
24. Customer who opens account in the name of family members to deposit large amount of money which is inconsistent with the known legitimate sources of family income	Likely	Major	High	Enhanced due diligence (EDD) [Note:02]

**OPERATIONAL GUIDELINES ON PREVENTION OF MONEY LAUNDERING AND  
TERRORIST FINANCING**

<b>Risk group: Products or Services</b>				
<b>A. Asset Products</b>				
<b>Categories of Risks</b>	<b>Likelihood</b>	<b>Impact</b>	<b>Risk Score</b>	<b>Treatment/ Action Plan</b>
1. Long Term Lending Products	Unlikely	Major	Medium	Simplified Customer Due Diligence (CDD) [Note:01]
2. Mid Term Lending Products	Likely	Major	High	Enhanced due diligence (EDD) [Note:02]
3. Short Term Lending Products	Unlikely	Major	Medium	Simplified Customer Due Diligence (CDD) [Note:01]
4. Revolving Lending Products	Unlikely	Major	Medium	
5. Quick Loan against deposit products	Likely	Moderate	Medium	
<b>B. Liability Products</b>				
1. Term Deposits	Likely	Major	High	Enhanced due diligence (EDD) [Note:02]
2. Build up Schemes	Unlikely	Minor	Low	Standard identification documents [Note:03]
3. Build up schemes (Insured)	Unlikely	Minor	Low	
4. Millionaire Schemes	Likely	Moderate	Medium	Simplified Customer Due Diligence (CDD) [Note:01]
<b>Risk group: Delivery methods or channels used</b>				
<b>Categories of Risks</b>	<b>Likelihood</b>	<b>Impact</b>	<b>Risk Score</b>	<b>Treatment/ Action Plan</b>
1. BEFTN and RTGS	Unlikely	Moderate	Low	Standard identification documents [Note:03]
2. Account Payee Cheque	Unlikely	Moderate	Low	
3. Fund Transfer	Unlikely	Moderate	Low	
4. Pay order	Unlikely	Moderate	Low	
5. Bkash	Unlikely	Moderate	Low	

**OPERATIONAL GUIDELINES ON PREVENTION OF MONEY LAUNDERING AND  
TERRORIST FINANCING**

<b>Risk group: Regulatory Risk</b>			
<b>Categories of Risks</b>	<b>Likelihood</b>	<b>Impact</b>	<b>Risk Score</b>
1. Failure in proper identification and verification of customer/beneficial owner	Unlikely	Moderate	Low
2. Failure to keep record properly	Unlikely	Moderate	Low
3. Failure to scrutinize staffs properly	Unlikely	Moderate	Low
4. Failure to train staff adequately	Likely	Moderate	Medium
5. Not having an AML & CFT program	Unlikely	Major	Medium
6. Not having an AML & CFT compliance officer	Unlikely	Major	Medium
7. Failure of doing Enhanced due diligence (EDD) for high risk customers (i.e. PEPs, IPs)	Unlikely	Major	Medium
8. Not submitting required report to BFIU regularly	Unlikely	Major	Medium
9. Not complying with any order for freezing or suspension of transaction issued by BFIU or Bangladesh Bank	Unlikely	Major	Medium
10. Not submitting accurate information or statement requested by BFIU or Bangladesh Bank	Unlikely	Major	Medium
11. Failure to report STR/SAR/CTR	Unlikely	Major	Medium
<b>Risk group: Geographical presence</b>			
<b>Categories of Risks</b>	<b>Likelihood</b>	<b>Impact</b>	<b>Risk Score</b>
1. Branch located in border, sea-port & land-port areas	Unlikely	Moderate	Low

## **OPERATIONAL GUIDELINES ON PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING**

---

### **Note:01**

#### **Simplified Customer Due Diligence (CDD):**

Performing simplified Customer Due Diligence (CDD) measures which includes:

- Obtaining the identity of the customer and the beneficial owner
- Verifying the identity of the customer and the beneficial owner if account transactions rise above a defined monetary threshold.
- Updates customer identification once in every two years
- Monitoring and scrutinizing transactions that is above a reasonable monetary threshold

### **Note:02**

#### **Enhanced Due Diligence (EDD):**

Performing Enhanced due diligence (EDD) measures which will includes-

- Examining the background and purpose of transactions;
- Obtaining and verifying additional information (e.g. occupation, volume of assets, information available through public databases, internet, etc.),
- Updating the identification data of customer and beneficial owner every year or at the time of every transactions whichever is earlier
- Obtaining and verifying additional information on the intended nature of the business relationship
- Obtaining and verifying information on the source of funds or source of wealth
- Obtaining and verifying information on the reasons for intended or performed transactions
- Obtaining approval of senior management to commence or continue the business relationship
- Applying enhanced monitoring of the customers
- Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

### **Note:03**

#### **Standard identification document:**

- Valid passport;
- Valid driving license;
- National ID card;
- Employer provided ID card, bearing the photograph and signature of the applicant;



## **CHAPTER 8: CUSTOMER DUE DILIGENCE**

### **8.1 Know Your Customer (KYC)**

Money Laundering Prevention Act, 2012 (with all amendments) requires all reporting agencies to maintain correct and concrete information with regard to identity of its customer during the operation of their accounts. The Company should not open the account, commence business relations or perform the transaction; or should terminate the business relationship; and should consider making a suspicious transactions report in relation to the customer in cases where the Company faces limitations such as:

- Unable to identify the customer and verify that customer's identity using reliable, independent source documents, data or information,
- Identify the beneficial owner, and to take reasonable measures to verify the identity of the beneficial owner
- Unable to obtaining information on the purpose and intended nature of the business relationship

#### **8.1.1 Components of KYC Program**

The KYC program includes:

- i. Customer acceptance policy (Annexure-7)
- ii. Customer identification procedure
- iii. Procedure for monitoring of high risk accounts
- iv. Procedure for identification of suspicious transactions.

### **8.2 Know Your Employee (KYE)**

Our employment processes as well as employee evaluation process require to be updated in the light of issues related to Money Laundering, Terrorist Financing, Bribery and Unethical Financing.

The Company will review and all our procedures related to pre-employment background screening of prospective, of current employees, conflicts of interest and susceptibility to money laundering complicity, especially investigate for any criminal history. These should include verification of references, experience, education and professional qualification.

Moreover our policies, procedures, internal controls, job description, code of conduct/ethics, levels of authority, compliance with personnel laws and regulations, accountability, data access control need to be revisited to incorporate issues raised in section 7.4 of Guidance Notes on Prevention of Money Laundering and Terrorist Financing.

## **CHAPTER 9: RECORD KEEPING**

### **9.1 Statutory Requirement**

- i. The requirement contained in Section 25 (1) of Money Laundering Prevention Act 2012 (with all amendments)
  - to retain complete and correct information with regard to the customer's identity while operating an account of a customer
  - if any account of a customer is closed, to preserve previous records of transactions of such account for at least 5(five) years from the date of such closure.
- ii. FATF recommendation 11 states that Reporting Agency should maintain, for at least five years, all necessary records on transactions, to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity.
- iii. The Company must keep records of information regarding:
  - Customer relationship
  - Verification of identity
  - Account transactions

These records must be kept for at least five years from the date when the relationship with the customer has ended as prescribed in the Guidance Notes on Prevention of Money Laundering and Terrorist Financing and should be made available to the competent authorities upon request without delay. The Company must not destroy any record of customer or transaction under investigation without the consent of the regulatory authority or conclusion of the case even though the five-year limit may have been elapsed

### **9.2 Retrieval of Records**

Records should be retrievable without undue delay and the documents held, in any form, must be capable of distinguishing between the transactions relating to different customers and identifying where the transaction took place and in what form.

### **9.3 STR and Investigation**

The Company must report suspicious transactions or account activity to applicable regulatory authorities. The Company must not destroy any record of customer or transaction under investigation without the consent of the regulatory authority or conclusion of the case even though the five-year limit may have been elapsed. To ensure the preservation of such records Reporting Agency should maintain a register or tabular records of all investigations and inspection made by the investigating authority or Bangladesh Bank's designated unit and all disclosures to the regulatory authority. The register should be kept separate from other records and contain as a minimum the following details:

- i. the date of submission and reference of the STR/SAR;
- ii. the date and nature of the enquiry;
- iii. the authority who made the enquiry, investigation and reference; and
- iv. details of the account(s) involved

## **OPERATIONAL GUIDELINES ON PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING**

---

### **9.4 Training Records**

The following training records are to be preserved:

- i. details of the content of the training programs provided;
- ii. the names of staff who have received the training;
- iii. the date/duration of training;
- iv. the results of any testing carried out to measure staffs understanding of the requirements; and
- v. an on-going training plan

### **9.5 Branch Level Records**

The following records are to be made available at the branch level:

- i. Information regarding Identification of the customer
- ii. KYC information of a customer
- iii. Transaction report
- iv. Suspicious Transaction/Activity Report
- v. Exception report
- vi. Training record
- vii. Return submitted or information provided to the Head Office or competent authority

### **9.6 Sharing of Record/Information of/to a Customer**

Under Money Laundering Prevention Act, 2012 (with all amendments) and Anti Terrorism Act, 2009 (with all amendments), Reporting Agency shall not share account related information to investigating authority i.e., ACC or person authorized by ACC to investigate the said cases without having court order or prior approval from Bangladesh Bank's designated unit

## **CHAPTER 10: STR/SAR**

Suspicious Transaction Report (STR) or Suspicious Activity Report (SAR) has to be submitted to regulatory authority as per provided format for such transactions which deviates from usual transactions; of which there is ground to suspect that:

- i. the property is the proceeds of an offence
- ii. it is financing to any terrorist activity, a terrorist group or an individual terrorist
- iii. any other transaction or attempt of transaction delineated in the instructions issued by Bangladesh Bank's designated unit from time to time.

In Anti Terrorism Act, 2009 (with all amendments) STR/SAR refers to the transaction that relates to financing for terrorism or terrorist individual or entities. The Company need not to establish any proof of occurrence of a predicate offence; it is a must to submit STR/SAR only on the basis of suspicion. As per the Money Laundering Prevention Act, 2012 (with all amendments), the Company is obligated to submit STR/SAR to applicable regulatory authority. Such obligation also prevails for the Anti Terrorism Act, 2009 (with all amendments). Other than the legislation, BFIU has also instructed to submit STR/SAR through Circulars issued by BFIU time to time.

## **OPERATIONAL GUIDELINES ON PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING**

---

### **10.1 Reasons for Reporting of STR/SAR**

STR/SAR is very crucial for the safety and soundness of the Company. We should submit STR/SAR considering the followings:

- It is a legal requirement in Bangladesh;
- It helps protect our reputation;
- It helps to protect the Company from unfounded allegations of assisting criminals, including terrorists;
- It helps the authorities to investigate money laundering, terrorist financing, and other financial crimes.

### **10.2 Identification and Evaluation of STR/SAR**

In order to establish detection and evaluation mechanism in line with "Guidance Notes on Prevention of Money Laundering and Terrorist Financing", a separate process for identification and evaluation is drawn up. All members involved in CPU, CCU and Internal Audit must read the process and abide by them.

### **10.3 Reporting of STR/SAR**

Institutions enlisted as per Money Laundering Prevention 2012 (with all amendments) and Anti Terrorism Act, 2009 (with all amendments) which includes United Finance Limited, are obligated to submit STR/SAR to BFIU. As per Master Circular 12, such report must come to the BFIU from CCU by using goAML web and specified format/instruction given by the BFIU.

### **10.4 Tipping Off**

Money Laundering Prevention Act, 2012 (with all amendments) and FATF Recommendation prohibits the Company, their directors, officers and employees from disclosing the fact that an STR or related information is being reported to regulatory authority. A risk exists that customers could be unintentionally tipped off when we are seeking to perform its CDD obligation in those circumstances. The customer's awareness of a possible STR or investigation could compromise future effort to investigate the suspected money laundering or terrorist financing operation.

### **10.5 "Safe Harbor" Provisions for Reporting**

Safe harbor laws encourage the Company to report all suspicious transactions by protecting the Company and employees from criminal and civil liability when reporting suspicious transactions in good faith to competent authorities. Section 28 of Money Laundering Prevention Act, 2012 (with all amendments) provides the safe harbor clause for reporting.

**CHAPTER 11: ANNEXURE**

- Annexure-1: BAMLCO Monthly AML/CFT Meeting Template
- Annexure-2: Branch Quarterly Self-Assessment Template
- Annexure-3: Branch AML/CFT Committee Formation Template
- Annexure-4: Transaction Screening Format
- Annexure-5: Internal Control Questionnaire
- Annexure-6: Independent Testing Procedure (AML/CFT)
- Annexure-7: Customer Acceptance Policy

United Finance Limited	
BAMLCO Monthly AML/CFT Meeting Template	
Branch Name:	Reporting Month:
<p><b>A. Committee Update</b></p> <p>1. Is there any update in Branch AML Committee?  <input type="checkbox"/> Yes    <input type="checkbox"/> No            If yes, please attach updated committee list.</p>	
<p><b>B. Document Collection and Verification</b></p> <p>1. Were all required documents (NID, Professional/Business documents, TIN, CHQ, PO, BANK DETAILS &amp; sources of fund documents) of deposit collected before instrument issue in the month?  <input type="checkbox"/> Yes    <input type="checkbox"/> No            If No, please specify the reason and deadline for collection.</p>	
<p>2. Were all deposit forms &amp; KYC verified and signed properly in the reporting month?  <input type="checkbox"/> Yes    <input type="checkbox"/> No            If No, please prepare the list and complete verification &amp; signature before meeting.</p>	
<p>3. Did any marketing person face any obstacle to collect documents and information from depositor in the reporting month?  <input type="checkbox"/> Yes    <input type="checkbox"/> No            If Yes , please prepare a list of documents required but not collected and attach.</p>	
<p>4. Was there any High Risk account (PEPs, IPs) opened in the branch?  <input type="checkbox"/> Yes    <input type="checkbox"/> No            If Yes, please update the List of High Risk Customers &amp; send it to CAMLCO for review and approval.</p>	
<p><b>C. Transaction monitoring and Source of Fund of Liability Products</b></p> <p>1. Was any inconsistency found between depositors' source of fund with their deposited amount?  <input type="checkbox"/> Yes    <input type="checkbox"/> No            If Yes, what action has been taken for this deposit?</p>	
<p>2. Was any deposit made from third party source?  <input type="checkbox"/> Yes    <input type="checkbox"/> No            If Yes, what action has been taken for this deposit?</p>	
<p>3. How many accounts more than Tk. 10 Lac were opened in the branch?</p>	
<p><b>D. Transaction monitoring and Unitization of Fund of Asset Products</b></p> <p>1. How many disbursements were made against Lease Loan &amp; Term Loan Facility in last month?</p>	
<p>2. Were all customers for new disbursement against lease loan &amp; Term loan physically visited to check proper utilization of the disbursed loan?  <input type="checkbox"/> Yes    <input type="checkbox"/> No</p>	
<p>3. Was any Lease Loan or Term Loan early terminated &amp; settled through payment with Pay-Order &amp; Cash in the reporting month?  <input type="checkbox"/> Yes    <input type="checkbox"/> No            if yes, pl attach the account information.</p>	

<p><b>E. KYC</b></p> <p>1. How many new account opened in last month?</p>
<p>2. Is the client's profession justified with the deposit amount?</p> <p><input type="checkbox"/> Yes    <input type="checkbox"/> No</p>
<p>3. Were all KYCs done thoroughly with correct and complete information?</p> <p><input type="checkbox"/> Yes    <input type="checkbox"/> No</p> <p>If No, please specify the reason.</p>
<p>4. How many accounts has been selected for updating KYC in the reporting month?</p>
<p>5. Have all KYC been updated for selected Accounts in the reporting month?</p> <p><input type="checkbox"/> Yes    <input type="checkbox"/> No</p> <p>If No, please specify the reason and new deadline for updating KYC.</p>
<p>6. Is the beneficial owner's KYC done?</p> <p><input type="checkbox"/> Yes    <input type="checkbox"/> No</p> <p>If No, please specify new deadline for performing KYC procedure.</p>
<p><b>F. Suspicious Transaction Report/ Suspicious Activity Report</b></p> <p>1. Was there any suspicious account opened in the branch?</p> <p><input type="checkbox"/> Yes    <input type="checkbox"/> No</p> <p>If Yes, please send it to CAMLCO immediately for review</p>
<p>2. Was there any suspicious activities (SA) found at the time of opening or discussion with any customer?</p> <p><input type="checkbox"/> Yes    <input type="checkbox"/> No</p> <p>If Yes, please send it to CAMLCO immediately with required documents if any.</p>
<p><b>G. Record Keeping</b></p> <p>1. Does the branch keeping all records relating to deposit accounts, transactions &amp; AML/CFT programs?</p> <p><input type="checkbox"/> Yes    <input type="checkbox"/> No</p> <p>If No, please specify the reason and action taken regarding this.</p>
<p>2. Are all the circular, circular letter, guideline, policy kept, UN Sanction list &amp; Local Jangee Group list in a separate file?</p> <p><input type="checkbox"/> Yes    <input type="checkbox"/> No</p>

<p><b>H. Training</b></p> <p>1. Have all the employees/staffs of the branch got AML/CFT training?  <input type="checkbox"/> Yes      <input type="checkbox"/> No                  If No, please mention the initiatives taken for AML/CFT training for untrained employees/staffs.</p>			
<p><b>I. Others</b></p> <p>1. Did the branch submit any return to CCU in the last month?  <input type="checkbox"/> Yes      <input type="checkbox"/> No                  If Yes, please specify the Return name and submission date.</p>			
<p>2. Please specify if any there was any discussion about latest circulars, letter, guideline &amp; policy.</p>			
<p>3. Please specify if there were any BB inspection report &amp; Internal Audit report in the last month and actions taken to resolve the observations noted in the report.</p>			
<p><b><u>Signature of BAMLCO</u></b></p>  <p>_____</p> <p>Name:</p>		<p><b><u>Signature of Branch Manager</u></b></p>  <p>_____</p> <p>Name:</p>	
<p><b>Participants in the Meeting:</b></p>			
<b>Sl. #</b>	<b>Name</b>	<b>Designation</b>	<b>Signature</b>
01			
02			
03			
04			
05			



**United Finance Limited**  
**Branch Quarterly Self assessment Template**

**Branch Name:** \_\_\_\_\_ **Quarter Name:** \_\_\_\_\_

1.1 Total no of officer/staff (with designation).

1.2 Has any staff/official been trained up on prevention of money laundering & terrorist financing?

Yes  No

If yes, please mention the number of officials trained up

If no, please mentioned the reason and set-up training deadline

2.1 Is the compliance officer (BAMLCO) experienced and senior official?

Yes  No

If no, please put your comments:

2.2 Is the designated compliance officer get any training on prevention of money laundering and terrorist financing within last two years?

Yes  No

If no, please put your recommendation:

2.3 Is the BAMLCO continuously monitor and review the effectiveness of prevention of money laundering & Terrorist Financing activities?

Yes  No

If no, please put your recommendation:

3 Are all officers/staffs well conversant with the AML/CFT acts, BFIU circulars and guidance notes and United Finance internal policy & guideline regarding prevention of money laundering & terrorist financing?

Yes  No

If no, please mention the action plan to develop their knowledge & awareness:

4 Does the Monthly meeting at brnach regularly held on prevention of money laundering & terrorist financing activities?

Yes  No

If no, please put your comments:

5 Is the KYC profile properly filled up while opening individual, corporate and other accounts as per requirement of of AML & CFT Acts and master circular by BFIU?

Yes  No

If no, please put your comments:

6 Does branch classify the Cusotmers on the basis of risk?

Yes  No

If no, please mention your plan to classify all customers on the basis of risk.

**Annexure - 2**

7 Does the branch take necessary initiatives for mitigating ML & TF related risk as per BFIU's direction and United Finance internal policy?

Yes  No

If no, please put your comments:

8 Does the branch review and up-date the information of KYC profile on periodical basis as per BFIU's direction?

Yes  No

If no, please put your comments:

9 Does the Branch take adequate measures to prevent terrorist financing as per Anti-Terrorism Act, 2009?

Yes  No

If Yes, Please mention those measures.

If no, please put your comments:

10 Has any suspicious transaction (STR) been identified & reported in this Quarter?

Yes  No

If yes, please mention the Reference numbers:

11 Does the Branch preserve separate files for AML Act, CFT act, circulars, training records, schedule and other AML related notes?

Yes  No

If no, please put your comments:

12 Are the copies of acts, circulars etc. provided to all officers/staffs of the branch?

Yes  No

If no, please put your comments:

13 Does any political exposed persons (PEPs), powerful person, chief of internaional organization or high official maintains any account with the branch?

Yes  No

If yes, please mention the number:

14 Are all AML/CFT related weakness/irregularities observed by Internal Audit & BFIU inspection Team regularized?

Yes  No

If no, please put your comments:

**Branch Manager**

\_\_\_\_\_  
Name:

\_\_\_\_\_  
Signature:

\_\_\_\_\_  
Date:

\_\_\_\_\_  
Seal:

**UNITED FINANCE LIMITED****Branch Anti Money Laundering Committee**

---


Updated on \_\_\_\_\_

SI No.	Name	Designation
1		President (Branch Manager/Unit Manager)
2		Member Secretary (BAMLCO)
3		Member
4		Member
5		Member
6		Member
7		Member
8		Member
9		Member
10		Member

Sign &amp; Seal

-----  
Branch Manager/Unit Manager


UNITED FINANCE LIMITED						
ACCOUNT/TRANSACTION SCREENING						
MONTH:						
Report should be based on Deposit Amount/Value & Date						
1	2	3	4	5	6	7
Serial No.						
Branch Name						
Depositor's Type						
Name of Deposit Associate						
Depositor's Name						
Instrument/ FDR No.						
Name of Product						
Date of Opening						
Maturity Date						
Profession/ Position & Name of Organization						
Source of Fund						
Income Level	Service & Business					
	Other Source					
Depositor's Age						
Depositor's Service/ Business Tenure						
Deposit Amount in the Month						
Cumulative Deposit Amount						
Total Number of Accounts						
Mode of Collection						
Banking Information	Own	Bank Name & Branch: A/c No.				
		Bank & Branch Name & A/c No.				
	Third Party	Name				
		Relation with Depositor				
		Pay Order details				
Nominee & Relation						
Reason for Suspicion						
Resolution/ Decision						

 <b>United Finance Limited</b> <b>INTERNAL CONTROL QUESTIONNAIRE</b> <b>Branch Name :</b>		COMPLIANCE			Ref.	REMARKS
		Yes	No	N/A		
<b>TEST NO.</b>	<b>TEST DESCRIPTION</b>					
a.	Have you carried out a review of processes in your business to identify where Money laundering is most likely to occur?					
b.	Is this review regularly updated?					
c.	Have you established procedures and controls to prevent or detect money Laundering?					
d.	Is the effectiveness of such controls tested?					
e.	Do you have a comprehensive written policy on money laundering?					
f.	Is all staff aware of this policy?					
g.	Does your money laundering policy include clear guidelines on accepting corporate hospitality and gifts?					
h.	Is all staff aware of their responsibilities with regard to money laundering?					
i.	Do they receive regular money laundering training?					
j.	Are all members of staff sufficiently capable of identifying suspicious transactions?					
k.	Are your systems capable of highlighting suspicious transactions (i.e. those not conforming to usual parameters)?					
l.	Do all members of staff know the identity of their Anti Money Laundering Compliance Officer (AMLCO)?					
m.	Are your systems capable of providing the AMLCO will all the information required for the Annual Management Report?					
n.	Do you thoroughly check and verify the identity of all your clients?					
o.	Do you have client accounts in the name of fictitious persons/entities?					
p.	Do you know the identity of the beneficial owner of all your corporate clients?					
q.	Is this identity verified?					
r.	Are all suspicious transactions reported to Bangladesh Bank?					

Date: \_\_\_\_\_

Date: \_\_\_\_\_

Tick where applicable (✓)

 <b>United Finance Limited</b> <b>INDEPENDENT TESTING PROCEDURES (AML/CFT)</b> <b>Branch Name :</b>		Completed by		Reviewed by			
		Date:		Date:			
SL	TEST DESCRIPTION	COMPLIANCE			SCORE	OBTAINED SCORE	REMARKS
		Yes	No	N/A			
1.	Branch Compliance Unit	1			1		
		2			1		
		3			1		
		4			3		
		5			2		
		6			2		
					3		
					6		

2.	Staff/Officers awareness	1	How many staff/officers received formal training on AML & CFT program?				3	
		2	Are the all staffs/officers of branch well conversant with the AML & CFT acts, circular, guidance notes and United Finance internal policy & guideline regarding prevention of money laundering & terrorist financing?				4	
		3	Is there any quarterly meeting to evaluate the activities of money laundering & terrorist financing prevention activities organized by branch manager?				5	
		4	Does Branch take adequate measures to prevent money laundering and terrorist financing risk as per BFIU's directions & United Finance Internal Policy?				3	
			<b>KYC for account holders:</b>					
3.	KYC Procedure	1	Does the KYC procedure properly followed while opening all types of account as per the act of AML & CFT and master circular by BFIU?				6	
		2	Are the customers classified on the basis of risk involved as per master circular by BFIU?				6	
		3	Is any additional information obtained in case of high-risk customers?				5	
		4	Does the branch review and up-date the KYC on periodical basis?				5	
4.	Compliance of Anti-Terrorism Act, 2009		Does Branch take adequate measures to prevent terrorist financing as per Anti-Terrorism Act, 2009? If take what are these?				5	
5.	Suspicious Transaction Reporting (STR) and Cash Transaction Reporting (CTR)	1	Do all staffs/officers of the branch know the system of reporting suspicious transaction?				5	
		2	Is there any effective system to identify suspicious transactions in the branch? How many suspicious transactions have been reported so far to CCU by BAMLCO?				4	
		3	Does the branch send cash transaction report properly & accurately?				2	N/A

6.	Submission of Returns to CCU	1	How many returns are scheduled for submission to the CCU? Does the branch submit the returns on timely basis?					3		
		2	Does Branch regularly perform Self-Assessment? Is the prepared Self-Assessment report complete and appropriate?					3		
7.	Record Keeping	1	Are there procedures in place to ensure maintenance of record in respect of customer identification (KYC) and transactions in accordance with the regulatory and company's own requirements?					4		
		2	Does these records are provided to CCU or regulatory authority as per their requirement?					3		
8.	Overall branch management on AML/CFT function	1	Does branch manager (if he is not the BAMLCO) play important role in implementation of AML/CFT Program?					5		
		2	Are there any violations or weakness as noted by previous internal & external audit/inspection report of the branch? Has the branch taken any corrective actions?					4		
		3	Is the overall function of the branch satisfactory?					6		
			Total					100		

**Branch Overall Evaluation:**

Score	Rating
90+ to 100	Strong
70+ to 90	Satisfactory
55+ to 70	Fair
40+ to 55	Marginal
40 & below	Unsatisfactory

**Consent by:**

Signature of BAMLCO -----  
 Name -----  
 Date -----



**Customer Acceptance Policy | United Finance Limited**

**Policy Statement**

The Company will ensure proper due diligence in compliance with relevant rules and regulations to identify associated risks with the customers and prevent the Company to be used for money laundering or terrorist financing activities.

**Policy Guidelines**

The Company will:

1. Accept business relationship with either individual having Bangladeshi nationality or entity registered in Bangladesh, in line with all other regulatory and internal directives and guidelines.
2. Identify and verify the customer's and beneficial owner's identity, and the "source of fund" of the customer.
3. Identify and verify the customer/beneficial owner's information in the event of any change in customer/beneficiary's personal data.
4. Report to the appropriate regulatory authority in the event of any doubt about the identity of the customer or the beneficial owner and/or the legitimate source of fund.

The Company will ensure that it does not:

1. Open accounts or deal with customers/beneficiaries who have unknown identity, fictitious/unreal names or unverifiable source of funds.
2. Enter or maintain any business relationship with any individual or business entity dealing with any prohibited business as per the prevailing government regulation.
3. Enter or maintain business relationship where the customer and/or the beneficiary belong to any terrorist organization as per sanction list of any national or international authority.

**Note:** Due diligence measures must not lead to harassment of any customer/beneficiary or should not be too restrictive which may result into denial of financial service to general people, especially to people who are financially or socially disadvantaged.