Credit Guarantee Fund Trust for Micro and Small Enterprises

(AML & Sanction Policy)

Table of Contents

ABBREVIATIONS

1	AML	Anti-Money Laundering
2	AML	Anti-Money Laundering
3	BO	Beneficial Owner
4	CAP	Customer Acceptance Policy
5	CDD	Customer Due Diligence
6	CGTMSE	Credit Guarantee Fund Trust for Micro and Small Enterprises
7	CIP	Customer Identification Procedures
8	CRS	Common Reporting Standards
9	CTF	Counter Terrorism Financing
10	EU	European Union
11	FATF	Financial Action Task Force
12	FATCA	Foreign Account Tax Compliance Act
13	FIU-IND	Financial Intelligence Unit-India
14	KYC	Know Your Customer
15	MLI	Member Lending Institutions
16	MSME	Micro, Small and Medium Enterprises
17	MSE	Micro and Small Enterprises
18	PEP	Politically Exposed Person
19	PMLA	Prevention of Money Laundering Act
20	RBA	Risk Based Approach
21	RTI	Right To Information
22	SIDBI	Small Industries Development Bank of India
23	STR	Suspicious Transaction Reports
24	TF	Terrorist Financing
25	UAPA	Unlawful Activities Prevention Act
26	UN	United Nations
27	UNSC	United Nations Security Council

1. INTRODUCTION

1.1 Introduction

CGTMSE is committed to the highest standards of Anti-Money Laundering (AML) and Counter Terrorism Financing (CTF). All employees and stake holders are required to adhere to these standards to protect CGTMSE and its reputation from being misused for money laundering and/or terrorist financing or other illegal purposes.

CGTMSE has its headquarters in Mumbai, India and it is setup by ministry of MSME and the Government of India and the Small Industries Development Bank of India (SIDBI). The primary objective of CGTMSE is to facilitate credit availability to Micro and Small Enterprises (MSE) by providing a credit guarantee cover to Member Lending Institutions (MLI). CGTMSE aims to reduce the risk perception of the lenders and encourages them to extend financial support to micro and small businesses.

CGTMSE, being the pioneer institution for providing credit guarantee to the Micro and Small Enterprises (MSEs) with a specific objective to strengthen credit flow to MSEs in India, has partnered with World Bank and KfW to implement Solar Rooftop Credit Guarantee Scheme for MSMEs, to support lending to MSMEs / RESCOs for scaling solar rooftop installations in MSME sector. CGTMSE will be the Facility Manager for the proposed Scheme.

India is a member country of the Financial Action Task Force (FATF) and has enacted laws and rules designed to implement the anti-money laundering policies of FATF. The goal of these laws is to detect and prevent money laundering and potential terrorist financing. CGTMSE will adhere to all applicable laws of India, Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, as amended from time to time by the Government of India as notified by the Government of India.

1.2 Objective

The major goal of the CGTMSE KYC, AML, and CTF Policy is to prevent the organization from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorism financing. The CGTMSE and MLI employees must be alert in the battle against money laundering and must not enable the credit facility to be utilised for money laundering activities. The MLI should not become a party to a legal infraction. As a result, stopping money laundering operations is the MLI obligation and responsibility.

The MLI should pay close attention to potential money laundering and financing of terrorism concerns that may come from new or evolving technologies, such as internet banking, which may encourage anonymity, and take appropriate precautions to avoid their use in money laundering schemes if necessary. All the MLI are required to ensure full compliance with all KYC/AML/CTF guidelines issued from time to time.

1.3 Key Elements of The Policy

The KYC Policy of the CGTMSE contains the following key elements:

(a) Customer Acceptance Policy (CAP)

(b) Risk Management

(c) Customer Identification Procedures (CIP) and

(d) Monitoring of Transactions

1.3.1 Customer Acceptance Policy (CAP)

CGTMSE facilitates credit availability to MSE by providing a credit guarantee cover to MLI, hence onboarding and managing the MSE customers is driven by the MLI.

Before starting an MLI relationship, CGTMSE should be satisfied that the available information is sufficient to understand the ownership structure, the identity and source of wealth of the ultimate beneficial owner, and how ownership is held.

The Customer Acceptance Policy refers to the broad criteria that MLI follow when they allow customers to create a credit account with them. In general, the standards provide that no accounts shall be formed in anonymous or false names, or where the customer's identification matches any person with a known criminal history or banned entities. Similarly, accounts should not be opened if the MLI is unable to verify the identification or get the appropriate documentation under the policy.

If the MLI cannot form a reasonable belief that it knows the true identity of the client and/or Beneficial Owner (BOs) and/or the nature of business or formal requirements concerning the identification of the client and/or BOs are not met, it must refuse to open an account/enter into a relationship or must close an existing account/terminate a relationship.

- No credit facility is offered in anonymous or fictitious/benami name.
- No credit facility can be offered when MLI are unable to apply appropriate CDD measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer.
- A suitable system is in place to ensure that the customer's identification does not match any person or entity whose name appears on the sanctions lists.
- Will not enter into or maintain business relationships with individuals or entities known or suspected to be a terrorist or a criminal organization or which are associated with money laundering activities.
- Cannot accept assets that are known or suspected to be the proceeds of criminal activity.

1.3.2 Risk Management

CGTMSE expects its MLI to classify customers as low, medium, or high risk depending on risk perception and assessment, as per RBI, FIU-IND, PMLA guidelines.

Risk classification will be performed based on parameters such as the customer's identity, social/financial status, nature of business activity, PEP status and information about the customer's business and location, geographical risk covering customers as well as transactions, type of products/services offered, delivery channel used for product/service delivery, types of transactions undertaken - cash, cheque/monetary instruments, wire transfers, forex transactions, and so on.

To avoid tipping off the customer, the risk classification of a client and the exact reasons for such categorisation as well as a potential suspicion related to money laundering or terrorism finance must be kept confidential and not divulged to the consumer.

1.3.3 Customer Identification Procedures (CIP)

The MLI are expected to perform Customer identification and verification using credible and independent documents, data, and information.

The customer identification procedure is to be carried out at different stages.

- while establishing a credit facility
- when the bank has doubts regarding the legitimacy, veracity, or sufficiency of previously collected client / identifying data
- When there is cause to believe that a consumer is purposefully avoiding reporting threshold
- The MLI must gather adequate information to satisfy themselves about the identification of each customer, whether regular or occasional, and the purpose of the planned nature of the credit facility. Must be able to demonstrate to the appropriate authorities that due diligence was carried out based on the customer's risk profile and in accordance with the existing requirements.

Accounts of Politically Exposed Persons (PEPs): Politically exposed persons are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States / Governments, senior politicians, senior government / judicial / military officers, senior executives of state-owned corporations, important political party officials, etc.

The decision to provide credit facility to a PEP account / PEP being beneficial owner should be made at a senior level. Branches should additionally subject such accounts to continuing heightened scrutiny. On the PEPs, sufficient information, including information about the sources of funds, accounts of family members and close relatives, has to be acquired. The foregoing standards may also be applied to the accounts of PEPs' family members or close relatives when the PEP is the beneficial owner.

If an existing customer or the beneficial owner of an existing account becomes a PEP, the MLI must obtain senior management approval to continue the business relationship and subject the account to the enhanced CDD measures that apply to PEP customers, including enhanced monitoring on an ongoing basis.

1.3.4 Monitoring of Transactions

The instructions for opening accounts and monitoring transactions must be strictly followed in order to minimize the operations of "Money Mules / Benami" who are used to launder the proceeds of fraud schemes (e.g., phishing, corruption and identity theft) by criminals who gain illegal access to deposit accounts by recruiting third parties who act as "money mules / Benami."

The MLI shall take necessary precautions, such as post-event or real-time monitoring to mitigate the risk of Fraud and Money laundering using the credit facility offered. Regular monitoring and management of accounts is required to eliminate the possibility of fraud and to prevent money laundering.

1.4 Periodic Updation

The MLI must perform KYC updation at least once every two years for high-risk clients, once every eight years for medium risk customers, and once every ten years for low-risk customers from the date of account establishment / last KYC updation.

1.5 Record Retention

The MLI needs to maintain all client records for a period of a minimum of 5 years from the date of the transaction, even after the closure of accounts. All the records are critical and important in nature, especially in regard to complaints, court cases, RTI requests, and so on.

1.5.1 Digitization of Records

The most cost-effective, efficient, and long-lasting approach to keep records is to digitize them. It aids in the effective preservation of records for a longer period of time and easy reproduction in the event of a reference.

1.6 Anti Money Laundering Standards

As per the Prevention of Money Laundering Act (PMLA) 2002, the offence of Money Laundering is defined as: Whoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of a crime and projecting the same as a untainted property – shall be guilty of offence of Money Laundering. Money Laundering is the process by which the criminals attempt to hide and disguise the origin and ownership of the proceeds of their criminal activities like drug trafficking, trafficking women and children, murder, extortion, child pornography etc. 'Proceeds of crime' means any property derived or obtained, either directly or indirectly by any person as a result of criminal activities relating to a scheduled offence or the value of such property. Money Laundering, therefore, besides being a Statutory or Regulatory requirement, is also a moral responsibility for all the CGTMSE and MLI Employees.

Terrorists use similar methods for moving their funds. Some of the terrorist groups also indulge in criminal activities for funding their acts. Any Kind of support towards terrorism will be termed as Terrorist Financing.

1.6.1 Nomination of Designated Director

All MLI are required to appoint a "Designated Director" to their boards under the terms of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (Rules), to ensure overall compliance with the Act and Rules.

The term "Designated Director" refers to a person designated by the Banks Board to ensure overall compliance with the obligations imposed under Chapter IV of the PML Act and the Rules and includes the Managing Director or a whole-time Director duly authorised by the Board of Directors if the reporting entity is a company. The Principal Officer shall never be nominated as the Designated Director. The Designated Director's name, designation, and address must be communicated to the Director, FIU-IND.

The Designated Director and ultimately, the Board of Directors are responsible for AML/CFT matters.

The Designated Director shall have professional experience and knowledge of the applicable legal and regulatory framework relating to AML/CFT, fraud, bribery and corruption of the hierarchy and powers within the entity.

The Designated Director needs to dedicate sufficient time and availability necessary to the effective and autonomous exercise of his/her functions. The Designated Director monitors the realization of the training and awareness-raising programme for the personnel.

The Designated Director has the power to suggest, on his/her initiative, any necessary or useful measures, including the release of the required means to the Board of Directors. The AML and CFT Officer is the privileged contact person for the AML/CFT competent authorities as regards AML/CFT issues. He/she is also in charge of the transmission of any suspicious transactions to these authorities, i.e., with the Financial Intelligence Unit of the State prosecutor.

1.6.2 Principal Officer

"Principal Officer" refers to an individual appointed by the MLI who is responsible for providing information in accordance with Rule 8 of the PML rules. The Principal Officer is in charge of maintaining compliance, monitoring transactions, and sharing and reporting information as needed by law or regulation. The Principal Officer's name, designation, and address must be communicated to the Director, FIU-IND.

1.6.3 Money Laundering and Terrorist Financing (ML/ TF) Risk Assessment

The MLI is expected to conduct a 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise on a regular basis to identify, assess, and implement effective steps to reduce its money laundering and terrorist financing risk.

The MLI risk assessment must be properly documented and proportionate to size, geographical presence, complexity of activities/structure, and so on. Furthermore, the Board shall establish the frequency of the risk assessment exercise in accordance with the outcome of the risk assessment exercise. It should, however, be evaluated at least once a year.

The MLI must use a Risk Based Approach (RBA) to mitigate and manage the identified risk, and it must have Board-approved policies, controls, and procedures in place. Furthermore, the MLI will monitor the execution of the restrictions and, if necessary, improve them.

1.6.4 Suspicious Transactions

Suspicious transaction means a transaction, including an attempted transaction, whether or not made in cash, that to a person acting in good faith:

- gives rise to reasonable suspicion that it may involve the proceeds of a crime regardless of the value involved:
- appears to be made in circumstances of unusual or unjustified complexity.
- appears to have no economic rationale or bona fide purpose.
- gives rise to reasonable suspicion that it may involve the proceeds of a crime
- if the MLI is unable to verify the customer's identity and/or obtain required documents, or if the data/information furnished to the MLI is untrustworthy, and thus believes that it will no longer be satisfied that it knows the true identity of the customer, it should file a STR with FIU-IND in addition to deciding whether to continue the business relationship.

1.6.5 Reporting to FIU-IND

The MLI shall furnish suspicious transactions and activities to the Director, Financial Intelligence Unit-India (FIU-IND), along with an intimation to CGTMSE upon offering credit facility to the client. Suspicious Transaction Reports (STR) plays a vital role in combating money laundering and terrorist financing.

If a consumer abandons / aborts a transaction after being asked to produce details / or supply information, the bank should record all attempted transactions, regardless of the value of transaction, in STR.

Accounts reported in STR should be classified as high risk and subject to increased scrutiny. If there is significant activity in these accounts, a repeated STR may be filed.

There are no restrictions as such on the MLI to discontinue an account that was reported in STR to FIU-IND. If any limitation has been placed on any account, the branches must guarantee that there is no tipping off the customer at any level. Tipping off would imply informing/communicating to the consumer that his/her/their account has been or will be reported to the Regulators/FIU-IND for suspicious conduct.

1.7 Sanctions Screening

Sanctions are international community responses to violations or threats to international peace and security. CGTMSE and the MLI are dedicated to combating financial crime and adhering to all applicable sanction laws and regulations. Relationships or transactions involving sanctioned individuals and entities, as well as comprehensively sanctioned countries, territories, and their governments, are typically prohibited under the Policy.

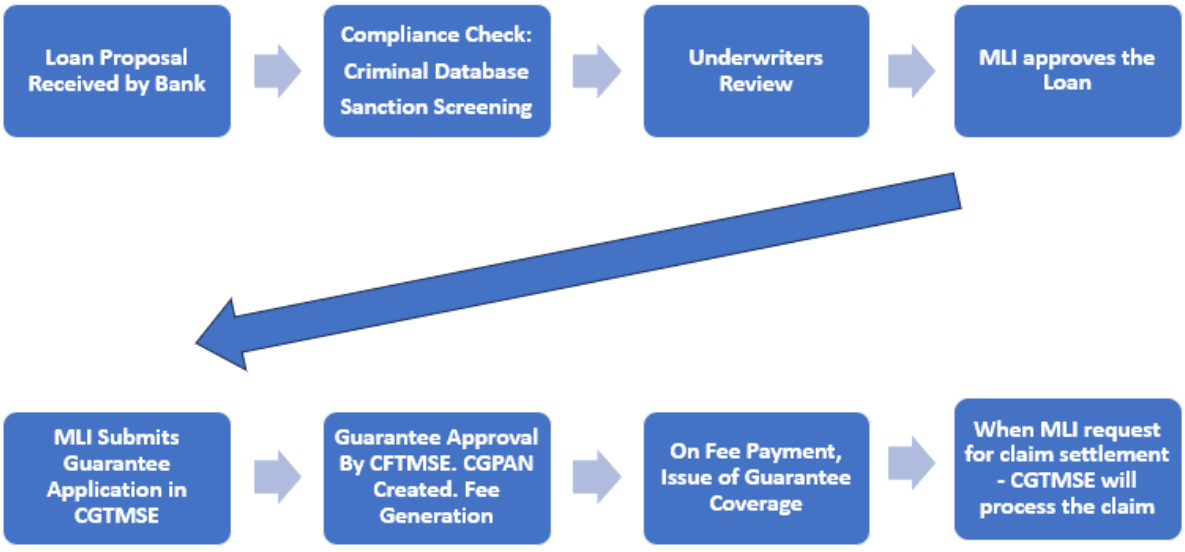
CGTMSE and the MLI adheres to identify entities in Indian Sanction list and Criminal database along with international sanctioning regimes, including United Nations (UN) and the European Union (EU).

The MLI must ensure that, in accordance with Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967 and amendments thereto, they do not have any accounts in the names of individuals/entities appearing on lists of individuals and entities suspected of having terrorist links, which are approved and circulated on a regular basis by the United Nations Security Council (UNSC).

1.8 Flow Chart

1.8.1 Flow Chart of Current Credit Guarantee Process

1.8.2 Flow Chart of Proposed Credit Guarantee Process



1.9 Reporting Requirement Under FATCA and CRS

on July 9, 2015, India has agreed and signed the Inter-Governmental Agreement with United States of America for implementing the Foreign Account Tax Compliance Act (FATCA) of the United States of America and improving International Tax Compliance.

on June 3, 2015, India has also signed a multilateral agreement to automatically exchange information based on Article 6 of the Convention on Mutual Administrative Assistance in Tax Matters under the Common Reporting Standards (CRS).

The MLI must receive FATCA / CRS declaration / self-certification forms from all customers. In the case that the self-certification form is not received, the account(s) will be stopped, and transactions by the account holder in such blocked accounts will be permitted once the duly completed self-certification is obtained and due diligence is performed. In accordance with the Foreign Account Tax Compliance Act (FATCA) and the Common Reporting Standards (CRS),

1.10 Reporting to KfW

CGTMSE shall share the suspicious reports received from MLI and suspicious activities found by CGTMSE to the KfW Portfolio Manager

1.11 Controls

To ensure that the CGTMSE efforts are successful, compliance with the AML/CTF programme must be assessed on a regular basis. As a result, CGTMSE and MLI are required to execute adequate controls and all applicable AML and CTF requirements are met, and security measures are functioning correctly by adopting suitable customer and business-related controls.