TS Software Ltd.

Anti-Money Laundering/ Combating financing terrorism and Compliance Procedures

Revised: March 2022

Table of contents

1. Goals....3
2. Compliance function....5
3. "Know your customer" procedures....6
4. Training of personnel....8

1. Goals

Money Laundering/Combating financing terrorism (AML/CFT) is the process of concealing financial transactions to make illegitimate money, derived from illegal activities such as embezzlement/corruption/illegal gambling/terrorism/organized crime, appear legitimate.

Under a broad definition, the laundering process is accomplished in three stages:

(a) Placement – the physical disposal of cash proceeds derived from criminal activity.
(b) Layering – separating the illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity.
(c) Integration – the provision of apparent legitimacy to wealth derived from crime. If the layering process is successful, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing as normal business funds.

Its main objective is to hide the true source of illegal proceeds and make them legally usable, by converting them into legitimate money through a series of financial transactions. Technological advancements have helped money launderers adopt innovative means to transfer funds faster across continents making detection and preventive action more difficult. The attempted misuse of the financial system for perpetration of frauds has been recognized globally as a major problem that needs to be continuously tackled at every level in a dynamic manner.

As a Responsible Company, we consider it our moral, social and economic responsibility to prevent the misuse of the financial system for laundering proceeds of criminal activities and to coordinate the global war against money laundering. Our role in curbing this global reality begins with stringent "Know Your Customer" procedures.

Imbibing the true spirit behind the international financial community's resolve to fight money laundering, the Company has resolved to conduct day - to - day business with due skill, care and diligence and seek to always comply with both the letter and the spirit of relevant laws, rules, regulation, codes and standards of good practices.

The purpose of the Anti-Money Laundering/Combating financing terrorism measures is to prevent the system of the Company from being used for money laundering and financing terrorism. Therefore, AML and CFT measures formulated include:

1. Customer Identification Procedure – "Know Your Customer" procedures;
2. Monitoring of suspicious transactions;
3. Appointment of Compliance function;
4. Personnel Training;
5. Maintenance of Records;
6. Periodic testing of implementation of AML/CFT and Compliance measures.

"Customer due diligence" (CDD) procedures include:

(a) Identifying a customer;
(b) Determining whether the customer is acting for a third party and, if so, identifying the third party;
(c) Verifying the identity of the customer and any third party for whom the customer is acting;

Scope of these procedures and policies applies to all branches, offices, contractors and affiliated companies of the Company and is to be read in conjunction with related operational guidelines issued from time to time.

These procedures address the responsibility of management and employees for:

- ☐ Creating and implementing policies, procedures and controls related to customer's acceptance, maintenance and monitoring;
- ☐ Customer due diligence;
- ☐ Declining or terminating business relationships or transactions;
- ☐ Personnel training with regards to customer's acceptance, maintenance and monitoring;
- ☐ Monitoring accounts, activities, policies, procedures and plans;
- ☐ Awareness and communication; and
- ☐ Management reporting
- ☐ Reporting (SAR/STR) to Financial Intelligence Unit (FIU).

Key Principles and Objectives

This procedure manual has the following key principles and objectives:

- ☐ The Company will introduce necessary policies and procedures to ensure that the risk of possible money laundering, proliferation financing or financing of terrorism and related activities associated with customers' relationships and transactions is managed and mitigated.
- ☐ Customer due diligence procedures with regard to business relationships and transactions will be developed and implemented as required by applicable legislation.
- ☐ To establish a business relationship with a potential customer, appropriate information has to be obtained from the person seeking to establish the relationship. The information obtained is to be verified by comparing it with information obtained from source(s) as required by legislation.
- ☐ The Company may decline or terminate business relationships or transactions where there appears to be a risk that its services and infrastructure will be abused for the purposes of money laundering and/or terrorist financing.
- ☐ The Company will provide the appropriate training to all affected employees on customer's acceptance, maintenance and monitoring.
- ☐ The Company will proactively monitor adherence to this procedures manual, ensuring compliance with its obligations as required by legislation.

- ☐ Affected company employees must be made aware of the contents of this manual, inclusive of their responsibilities and actions expected of them.
- ☐ Management reports must be produced to allow the company actively and effectively to monitor customer's acceptance, maintenance and monitoring initiatives.

2. Compliance function

Compliance function of the Company consists of two levels and addresses responsibilities of Money Laundering Reporting Officer as well as Money Laundering Compliance Officer.

1. CEO (who also serves as Money Laundering Reporting Officer) and the Board of Directors of the Company.

   Responsibilities of the CEO and the Board of Directors include:

   I. Create a culture within the Company that supports achievement of compliance objectives by ensuring rigor in the recruitment, selection, individual development and monitoring of compliance personnel.
   II. Develop and promote, among Company's personnel at all levels, high degree of awareness to crucial importance of compliance with AML/CFT and KYC procedures.
   III. Oversee development, on-going update and implementation of compliance related policies and procedures.
   IV. Work in close collaboration with the Compliance department to ensure there is an effective relationship between the Compliance department and the members of the Board.

2. Company's Compliance department, headed by Chief Operational Officer (who serves as Money Laundering Compliance Officer).

   The Money Laundering Compliance Officer is responsible for:
   I. Appointment of compliance officers (personnel of the Compliance department);
   II. Monitoring, coordination and control over the day-to-day activity of compliance officers;
   III. Training of compliance officers;
   IV. Reporting to the CEO and the Board of directors of the Company if the Compliance department has a reason to believe that a suspicious transaction has / may have resulted in money laundering;
   V. Periodic control of implementation of AML/CFT measures and compliance procedures;
   VI. Periodic review and updating the present Manual.

   Responsibilities of Compliance department include:

I. Putting in place necessary controls for detection of suspicious transactions;
II. Canceling or forbidding the transaction;
III. Receiving disclosures related to suspicious transactions from the staff or otherwise;
IV. Training of staff and preparing detailed guidelines / handbook for detection of suspicious transactions.

3. "Know your customer" procedures

All transactions should be undertaken only after proper identification of the customer.

Customer identification is an essential element of KYC standards.

The Company maintains a systematic procedure for identifying new customers and cannot enter into a service relationship until the identity of a new customer is satisfactorily verified.

Procedures document and enforce policies for identification of customers. The best documents for verifying the identity of customers are those which are most difficult to obtain illicitly and to counterfeit.

The customer identification process is applied naturally at the outset of the relationship. To ensure that records remain up-to-date and relevant, the company undertakes regular reviews of existing records. However, if the Compliance department becomes aware at any time, through compliance and/or AMLO reviews, that it lacks sufficient information about an existing customer, it takes immediate steps to ensure that all relevant information is obtained as quickly as possible.

The company can be exposed to reputational risk, and should therefore apply enhanced due diligence to such operations.

Particular safeguards have been put in place internally to protect confidentiality of customers and their business, the Company ensures that equivalent scrutiny and monitoring of these customers and their business is conducted, e.g. it is available to be reviewed by the Compliance department and auditors.

The Company maintains clear standards and policies, on what records must be kept on customer identification and individual transactions. Such practice is essential to permit the company to monitor its relationship with the customer, to understand the customer's on-going business and, if necessary, to provide evidence in the event of disputes, legal actions, or a financial investigation that could lead to criminal prosecution.

The Company obtains all information necessary to establish to its full satisfaction the identity of each new customer and the purpose and intended nature of the business relationship. The extent and nature of the information depend on the type of an applicant (personal, corporate, etc.) and the expected size of the transactions.

When an account has been opened, but problems of verification arise in the service relationship, which cannot be resolved, the company can close the account and return the money to the source from which they were received.

The company will never agree to open an account or conduct ongoing business with a customer who insists on anonymity or who gives a fictitious name.

Customers Acceptance Policy

The Customer Acceptance Policy will ensure the following aspects of customer relationship:

- ☐ If the customer is a new customer, an account will be opened only after ensuring that Know Your Customer (KYC) documentation has been received and applicable procedures have been applied;
- ☐ If the customer is an existing customer, KYC procedures might be omitted only after it has been ensured that the identification of the customer has been completed by the Company at an earlier stage.
- ☐ No account is opened in an anonymous or fictitious name(s);
- ☐ No account is opened where the Company is unable to apply appropriate customer due diligence measures, i.e. the Company is unable to verify the identity and /or obtain documents required as per the risk categorization (see below for details) due to non-co-operation of the customer or non-reliability of the data/information furnished to the Company.
- ☐ Risk in terms of the location (citizenship, country of residence) of a customer and the mode of payments are duly checked;

For each new Customer the Company collects and permanently updates by all agreed and proper means the following details (Customer's file):

1. Full legal name, any former name and any other names used by the individual, based on the official identity card or passport.
2. Gender.
3. Full permanent address, including zip code, supported by a recent (up to 6 months) telephone bill, electricity, municipal taxes, or bank account statement, or similar documents.
4. Phone number, landline and/or mobile.
5. E-mail address.
6. Date and place of birth
7. Nationality/Citizenship.

A Customer's file should be confirmed and supported by a full set of the documents, as listed below:

Proof of Identity

One certified copy of any one of the following:

(i) Passport
(ii) National ID Card
(iii) Driving license
(iv) Proof of identity and address can also be established by any official document containing photograph, address and signature of the customer, duly attested by a notary public.

Proof of Address

One original document of any one of the following:

(i) Utility bill
(ii) Account statement from a financial institution
(iii) Letter from any recognized public authority
(iv) Proof of identity and address can also be established by any official document containing photo, address and signature, duly attested by a notary public.

Since most of Company's customers do not have face-to-face interaction with the Company personnel, apart from applying customer identification procedures mentioned above, the Company records all of its telephonic communication with the customers.

Proof of Credit Card transactions

(i) Copies of both sides of credit card: front side with the name and last 4 digits, back side with CVV or imprinting.

Monitoring of withdrawal requests

Company's withdrawal policy is set as follows:

- Customer has a right to withdraw funds at any time. Company's bonus, if applicable, can be withdrawn only upon meeting certain conditions, as defined by the promotion campaign that has resulted in granting the bonus to the Customer.
- Customer has to provide the Company with the signed withdrawal application form.
- The requested amount must be withdrawn to the same account that was a source of funds subject to the withdrawal request. Examples: if the Customer used a bank wire transfer – the withdrawal will be done via a wire transfer to the same account, if it was charged from a credit card – the withdrawal will be credited to the same credit card and so on.

The appropriate compliance procedure for withdrawals is set below.

Compliance procedures applicable in cases of withdrawals by the Customers

Step	Transaction/function	Responsible staff	Result
Compliance procedures applicable in cases of withdrawals by the Customers			

1.	- Customer provides the Company with a signed withdrawal form.	Staff responsible for Retention for the Customers.	Review the withdrawal from and proceed to Step 2.
2.	- Identification of the Customer (ID, telephone number, and other details). Confirming that the Customer's account has sufficient funds for withdrawal and, to the extent bonus funds are involved, that the Customer met all conditions, as defined by the promotion campaign that has resulted in granting the bonus to the Customer.	Staff responsible for Retention for the Customers.	If identification and confirmation are successful, submit the withdrawal form to the Compliance department. If not – inform the customer.
3.	- Identification of the Customer, review of Customer's recent transactions and determining the appropriate method of withdrawal.	Compliance department. CEO (if applicable) The Board of directors (if applicable).	If the review is successful - submit the withdrawal form to the Financial Department for withdrawal execution. In case any problem occurs, the Compliance department may return the application to the staff responsible for retention for the Customers for additional information. In high-risks situations the Compliance department may report to the CEO of the Company. In such cases the CEO may take a final decision upon the withdrawal or, if the situation is extraordinary, report to the Board of directors.

To the extent possible, all suspicious transactions should be reported to the Compliance department before they are executed. Full details of all suspicious transactions, whether executed or not, should be reported to the Compliance department.

A suspicious transaction, noted prior to its execution, should be executed only with a pre-approval of the Compliance department.

The Compliance department shall have reasonable access to all necessary information/documents that might be needed to execute its responsibilities in an effective and due diligent manner.

The Compliance department is responsible for informing the CEO about any significant suspicious activity noted. The CEO should escalate any extraordinary suspicious activity to the Board of Directors of the Company.

The Board of Directors takes a decision to:

- escalate any extraordinary suspicious activity to Financial Intelligence Unit (FIU) by Suspicious Activity Report (SAR) or Suspicious Transaction Report (STR). SARs and STRs include detailed information about transactions that are or appear to be suspicious. The goal of SARs and STRs filings is to help the government identify individuals, groups and organizations involved in fraud, terrorist financing, money laundering, and other crimes. The purpose of a suspicious activity report is to report known or suspected violations of law or suspicious activity observed;
- take reasonable measures to ascertain the purpose of the transaction, the origin and ultimate destination of the funds involved and the identity and address, of any ultimate beneficiary.

4. Training of personnel

The Company maintains an onboarding and ongoing employee-training program to ensure that relevant staff is adequately trained in KYC procedures. The timing and content of training varies based on the target audience. Training requirements should have a different focus for new staff, staff dealing with new customers or customer retention.

New staff is educated about the basics of AML/CFT and KYC procedures and the importance of implementation of all relevant compliance policies. These basic compliance requirements are presented to them during two-week onboarding training that every new staff member has to attend. Staff members who deal directly with the customers are trained to verify the identity of new customers, to exercise due diligence in handling accounts of existing customers on an ongoing basis and to detect patterns of suspicious activity.

Regular refresher training is provided to ensure that employees are reminded of their responsibilities and are kept informed of new developments.

It is crucial that all relevant staff fully understand the need for and implement KYC policies consistently. A culture within services that promotes such understanding is the key to a successful implementation.

Penalties Due to Non Compliance

The employees are expected to comply with compliance policies and procedures outlined in this manual. Failure to comply might have serious implications including disciplinary action and in some cases even individual criminal penalties.

Communication with Employees

Open channels of communication are set between the Compliance department of the Company and all other employees of the Companies. Periodic updates about AML/CFT and KYC issues are provided to the staff of the Company. The Company has established an onboarding and ongoing employee-training program to ensure that the staff is adequately trained in compliance procedures. Training objectives have different focuses for frontline staff, compliance staff and retention staff to ensure that all those concerned fully understand the rationale behind the procedures and policies and implement them consistently.