'KNOW YOUR CUSTOMER' (KYC) POLICY AS PER ANTI MONEY LAUNDERING STANDARDS

KEY CONTENTS

1. SCOPE OF THE DOCUMENT

This document applies to the **ModulTrade Group** ("**MT**") in relation to the adopted KYC guidelines.

The **ModulTrade Group** is defined as ModulTrade, Ltd., U.K., its subsidiaries or holding companies from time to time and any subsidiary of any holding Company from time to time.

2. GOALS

The KYC guidelines in this document are aimed at preventing MT from being used, intentionally or unintentionally, by criminal elements for money laundering activities or terrorist financing activities. KYC procedures shall also enable MT to know and understand its Customers and its financial dealings better which in turn will help it to manage its risks prudently. Thus, the KYC policy has been framed by MT for the following purposes:

1. To prevent criminal elements from using MT for money laundering activities;
2. To enable MT to know and understand its Customers and their financial dealings better which, in turn, would help the MT to manage risks prudently;
3. To put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws/laid down procedures;
4. To comply with applicable laws and regulatory guidelines;
5. To ensure that the concerned staff are adequately trained in KYC/AML/CFT procedures

3. DEFINITIONS

3.1. DEFINITION OF USERS AND OF ACCOUNT

- **User**: A customer is generally defined as an individual, corporation, partner and any other entity recognised as a legal person that opens a new account or to whom MT provides certain services in accordance with MT Terms of Use. A person that opens a new account for another person is not considered a customer unless the person for whom the account is opened lacks legal capacity, as a minor.
- **Account**: An account is defined as a business relationship to provide MT services and transaction in accordance with MT Terms of Use

●.1. OTHER DEFINITIONS

- **ModulTrade Group**: ModulTrade, its subsidiaries or holding companies from time to time and any subsidiary of any holding Company from time to time.
- **Money Laundering**: Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets. Generally, money laundering occurs in three stages. Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.
- **Terrorist Financing**: Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of the funds or their intended use, which could be for criminal purposes. Legitimate sources of funds are a key difference between terrorist financiers and traditional criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership and personal employment. Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist

operations can be the same as or similar to methods used by other criminals to launder funds. Funding for terrorist attacks does not always require large sums of money and the associated transactions may not be complex.

- **KEY ELEMENTS**

MT is prohibited from transacting business with individuals, companies and countries that are on prescribed sanctions lists.

MT will therefore screen against United Nations, European Union, UK Treasury and US Office of Foreign Assets Control (OFAC) sanctions lists in all jurisdictions in which MT operates. Respective MT's AML policies, procedures and internal controls are designed to ensure compliance with all applicable regulations and rules, including, but not limited to FATF, OFAC, EU PSD2 and MLD5 Directives, other internationally accepted regulations, local and national regulations (Regulations), and will be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place to account for both changes in regulations and changes in our business.

MT operates so that it is compliant with 'anti-money laundering' ("AML") and 'know your customer' ("KYC") rules and regulations in the jurisdictions it operates in or provides products or services to and has developed this KYC and AML Policy to protect itself from involvement in money laundering or suspicious activity as follows:

- ● MT is performing an enterprise-wide risk assessment to determine the risk profile of the Company.
- ● MT has established KYC and AML policies and procedures that have been reviewed and approved by the MT's Board of Directors (the "Board").
- ● MT is implementing internal controls throughout its operations that are designed to reduce risks of money laundering, including designating a person responsible for AML compliance.
- MT has systems to verify the identification of clients.

- MT has processes where any knowledge or suspicions of money laundering will be reported.
- MT performing know your customer (“KYC”) procedures on all users.

MT, in compliance with applicable Regulations is adopting the following KYC policies:

- User Acceptance Policy (“UAP”)
- User Identification Procedures (“UIP”)
- Monitoring of Transactions
- Risk Management
- Training Program
- Recordkeeping
- Appointment of principal officer
- Reporting to Financial Intelligence Unit

Enhanced User review may be carried out periodically at MT discretion as part of MT ongoing risk assessment. In addition to this, any attempt to abuse MT or its platform will result in immediate account suspension and reporting violations to respective authorities.

MT insists on a comprehensive and thorough KYC and AML compliance framework. This includes monitoring of suspicious transactions and obligatory reporting to local regulators and other compliance bodies, including, without limitations, MAS, Republic of Singapore, FCA, United Kingdom, and submitting documents and information to regulators as required and without prior notification to registered users.

MT reserves the right to refuse registration to persons from jurisdictions that do not meet international AML standards. MT may at any time without liability and without disclosing any reason, suspend the operation of respective user.

●.1. USER ACCEPTANCE POLICY

MT's CAP lays down the criteria for acceptance of Customers. The guidelines in respect of user/customer relationship in the MT broadly includes verification in accordance with Annex I hereto.

●.2. USER IDENTIFICATION PROCEDURES

MT's User Identification Program (UIP) sets forth the requirements for determining and verifying the identity of any person seeking to establish a relationship with MT.

These requirements, which are consistent with international standards and satisfy MT's obligations under regulatory requirements, enable MT to form a reasonable belief that it knows the true identity of each of its customers.

Specific identification information must be obtained and some or all of this information must be verified by documentary and non-documentary methods in accordance with Annex I hereto.

Scope

MT CIP requirements must be followed by all MT businesses and legal entities. These requirements apply globally to achieve consistency and uniformity in the verification of identification of all MT customers.

Target

The target of the CIP is all MT employees and non-employees responsible for establishing customer relationships and opening and maintaining accounts and processing transactions.

Owner

The CIP is owned by the CEO [NOTE: UNDER CERTAIN RULES THERE SHOULD BE A SEPARATE POSITION] or the Head of AML Compliance who is responsible for its day-to-day oversight and administration. The Program and any material amendments must be approved by the Board or by a designed AML Committee.

Effective date

The CIP becomes effective to all MT customers.

Related Policies

The Customer Identification Program policy must to be read in conjunction with Anti-Money Laundering (AML) Policy and Know Your Customer (KYC) Policy.

Testing and quality assurance (QA) control assessment

Periodic testing of the requirement of the CIP and the other relevant implementing procedure are conducted by the Compliance Team.

Management must include the requirements of the CIP in the Manager's Control Assessment (MCA) in accordance with the Manager's Control Assessment Standards and Operational Risk Management Policy.

The business is also responsible to developing a QA process to analyse and identify any control weaknesses with regards to the requirements of the CIP and opportunities for process and performance improvement.

Customer Identification Program (CIP)

The CIP must include reasonable and practical risk-based procedures for verifying the identity of customer. Where required by local law, a country or region may implement procedure that apply to a business or businesses within that specific region or country in accordance with Annex I hereto.

CIP procedure can be incorporated into other business-specific AML policies, programs and procedures in accordance for the effective implementation and requirements.

If legally permitted, CIP must include procedures for providing new customers notice prior to account opening that information will be requested in order to verify identity prior to account opening. Such notice may be provided through new account forms, mailings, posters, web notices, telephone and other means as applicable. Countries that lack these practical means of providing notice prior to account opening may provide the notice after opening.

The CIP is a critical first step as part of the KYC Program. Verification of identity does not replace the requirement to conduct appropriate due diligence prior to establishing a customer relationship and opening an account.

Gathering and verifying required customer identification information

The first step in the CIP process is to gather the required customer identification information in accordance with Annex I hereto. This information must be obtained prior to opening an account or otherwise establishing a relationship and before any transactions are permitted.

In accordance with the KYC principles, no transactions are permitted until the identification number has been received.

Customer identification information that has been obtained from the prospective customer has to be verified. A periodic review and client refresh has to be conducted. Depending on a customer's risk profile, activity in an account may be permitted before verification of identification has been completed. In this case approval is required by the AML Committee. If the identity of a customer cannot be verified within 30 days of account opening, the account must be closed and the relationship terminated.

An integration of activities for screening against any government issued list of known or suspected terrorist should be considered.

Furthermore, a business may rely on a third party to perform some or all of the MT CIP requirements. In this case, verification has to be conducted whether a third party may be relied upon to perform some or all CIP on MT's behalf. In case of uncertainty matter must be referred to the AML Committee.

Record Retention Requirements

All identification information collected must be retained in accordance with the MT Records Management Policy for a period of five years after the customer's last account is closed unless otherwise required by local law. Procedures for retaining such records must be documented.

Roles and responsibilities

Responsibilities of the business include:

- Collecting and verifying information as set forth in the CIP and maintaining relevant CIP records.
- Screening customer against government list of known or suspected terrorists.
- Closing accounts or existing relationship when a reasonable belief that the relevant MT business knows the true identity of the customer cannot be formed.
- Developing and implementing reasonable business/country specific risk-based CIP procedures.
- Escalating to the appropriate AML Committee for appropriate investigation in case of any potential suspicious situations or risk issues discovered during the identification information collection and verification process.
- Establishing and implementing a Quality and Assurance process and Manager Control procedures.
- Conducting assessment and Periodic Review and Client Refresh cycle controls.
- Providing training to business and operations personnel involved in the CIP process.
- Documenting any local law deviations and peculiarities and monitoring changes to local laws.

Senior management is responsible for providing oversight of the CIP, in particular with regard to:

- The review and approval of the relevant CIP results and any relevant exception requests.
- Consulting with the business to develop reasonable and practical risk-based procedures for implementing the CIP.
- Advising on policy and procedures requirement and QA reviews or MCAs prepared by the business.
- Advising on the need to freeze or block accounts and/or exit relationship when identification information cannot be obtained and verified.
- Oversight on the need of training related to the requirements of the CIP and AML compliance roles and responsibilities.
- Evaluating needs of specific investigation activities when necessary.

1. Customer Identification means identifying the Customer and verifying his/her identity by using reliable, independent source documents, data or information. MT shall obtain sufficient information necessary to verify the identity of each new Customer along with brief details of its promoters and management, wherever applicable, whether regular or occasional and the purpose of the intended nature of business relationship. The requirement as mentioned herein may be moderated according to the risk perception.
2. Besides risk perception, the nature of information/documents required would also depend on the type of Customer (individual, corporate etc). For Customers that are natural persons, MT shall obtain sufficient identification data to verify the identity of the Customer, his address/location, and also his recent photograph. For customers that are legal persons or entities, the MT shall i) verify the legal status of the legal person/ entity through proper and relevant documents, ii) verify that any person purporting to act on behalf of the legal person/entity is so authorized and identify and verify the identity of that person,
3. Understand the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person. Customer identification requirements keeping in view the provisions applicable of Prevention of Money Laundering & its Rules and as per guidance note issued in this respect are indicated in Annex I. An indicative list of the nature and type of documents/information that may be relied upon for customer

identification is given in Annex I. MT will frame internal guidelines based on its experience of dealing with such persons/entities, normal prudence and the legal requirements.

●.3. MONITORING OF TRANSACTIONS

MT will monitor transactions of Users in accordance with applicable laws and regulations.

●.4. RISK MANAGEMENT

The Management of MT under the supervision of the Board of Directors shall ensure that an effective KYC program is put in place by establishing appropriate procedures and ensuring their effective implementation. It will cover proper management oversight, systems and controls, segregation of duties, training and other related matters. Responsibility will be explicitly allocated within the MT for ensuring that the policies and procedures as applicable to Company are implemented effectively. MT shall devise procedures for creating Risk Profiles of their existing and new Customers and apply various Anti Money Laundering measures keeping in view the risks involved in a transaction, account or business relationship.

●.5. TRAINING PROGRAM

MT will apply Employee Training Programs on a regular basis and as required by applicable international and national law and regulations, respectively.

●.6. RECORDKEEPING

MT will keep all records above for at least 5 (five) years.

●.7. REPORTING TO FINANCIAL INTELLIGENCE UNIT

MT will report any suspicious users and /or transactions as per applicable international and national law and regulations, respectively.

ANNEXES

ANNEX 1 – USER IDENTIFICATION REQUIREMENTS (INDICATIVE GUIDELINES)

Natural persons

Identification of individuals who are customers or beneficial owners or authorised signatories

MT should collect the following information for identification purposes from the customer or any other available source, subject to GDPR consent, if the customer is the resident of EU country:

Natural persons

Identification information

At a minimum	**Potential additional information (on the basis of risks)**
Legal name (i.e. first and last name);	Any other names used (such as marital name, former legal name or alias);

Complete residential address;	Business address, post office box number, e-mail address and landline or mobile telephone numbers;
Nationality, an official personal identification number or other unique identifier;	Residency status;
Date and place of birth.	Gender.

Information related to the customer's risk profile

Natural persons

Risk profile's information

Key attributes	**Potential additional information (on the basis of risks)**
Occupation, public position held;	Name of employer, where applicable;

Income;	Sources of customer's wealth;
Expected use of the account: amount, number, type, purpose and frequency of the transactions expected;	Sources of fiat or crypto funds passing through the account;
Financial products or services requested by the customer.	Destination of funds passing through the account.

Verification of identity of natural persons

The measures to verify the information produced should be proportionate to the risk posed by the customer relationship and should enable MT to satisfy itself that it knows who the customer is.

(a) Documentary verification procedures

- confirming the identity of the customer or the beneficial owner from an unexpired official document (eg passport, identification card, residence permit, social security records, driver's licence) that bears a photograph of the customer, matching this document with live selfie (face rec);

- confirming the date and place of birth from an official document (eg birth certificate, passport, identity card, social security records);
- in specific cases, confirming the validity of official documentation provided through certification by an authorised person (eg embassy official, public notary);
- confirming the residential address (eg utility bill, tax assessment, bank statement, letter from a public authority);
- confirming power of attorney of representative, if any.

(b) Non-documentary verification procedures

- contacting the customer by telephone, sms or via email to confirm the information supplied, after an account has been opened (eg a disconnected phone, returned mail etc should warrant further investigation);
- checking references provided by other institutions;
- utilising an independent information verification process, such as by accessing public registers, private databases or other reliable independent sources (eg credit reference agencies).

Further verification of information on the basis of risks

Customers with high-risk profiles, such as PEPs, will be rejected by MT as a rule.

However, if decided by authorized management particular attention needs to be focused on those customers assessed as having higher-risk profiles.

Additional sources of information and enhanced verification procedures may include:

- confirming an individual's residential address on the basis of official papers, a credit reference agency search;
- contact with the bank regarding the customer;
- verification of income sources, funds and wealth identified through appropriate measures; and
- verification of employment and of public positions held;
- personal reference.

Legal persons and arrangements and beneficial ownership

The procedures above should also be applied to legal persons and arrangements. MT should identify and verify the identity of the customer, and understand the nature of its business, and its ownership and control structure, with a view to establishing a customer risk profile.

Legal persons

Includes any entity (eg business or non-profit organisation, distinct from its officers and shareholders) that is not a natural person or a legal arrangement.

In considering the customer identification guidance for the different types of legal persons, particular attention should be given to the different levels and nature of risk associated with these entities.

Identification of legal persons

For legal persons, the following information should be obtained for identification purposes:

Legal persons

Identification information

At a minimum	**Potential additional information (on the basis of risks)**
Name, legal form, status and proof of incorporation of the legal person;	
Permanent address of the principal place of the legal person's activities;	

Official identification number (company registration number, tax identification number, VAT VIES number, if applicable);	Legal entity identifier (LEI) if eligible;
Mailing and registered address of legal person;	Contact telephone and fax numbers.
Identity of natural persons who are authorised to operate the account. In the absence of an authorised person, the identity of the relevant person who is the senior managing official.	Identity of relevant persons holding senior management positions.
Identity of the beneficial owners;	
Powers that regulate and bind the legal person (such as the articles of incorporation for a corporation).	

"Beneficial owner" is the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.

Information for defining the risk profile of a customer which is a legal person

When the account opening is the start of a customer relationship, further information should be collected with a view to developing an initial customer risk profile:

Legal persons

Risk profile information

At a minimum	**Potential additional information (on the basis of risks)**
Nature and purpose of the activities of the legal entity and its legitimacy;	Financial situation of the entity;
Expected use of the account: amount, number, type, purpose and frequency of the transactions expected.	Sources of funds paid into the account and destination of funds passing through the account.

Verification of identity of legal persons

MT should obtain:

- a copy of the certificate of incorporation and memorandum and articles of association, or partnership agreement (or any other legal document certifying the existence of the entity, eg abstract of the registry of companies/commerce);

(a) Documentary verification

- for established corporate entities – reviewing a copy of the latest financial statements (audited, if available).

(b) Non-documentary verification

- undertaking a company search and/or other commercial enquiries to ascertain that the legal person has not been, or is not in the process of being, dissolved, struck off, wound up or terminated;

- utilising an independent information verification process, such as by accessing public corporate registers, private databases or other reliable independent sources (eg lawyers, accountants);

- validating the data in the public access service;

- obtaining prior bank references;

- contacting the corporate entity by telephone, sms, mail or e-mail.

Verification of identity of authorised signatories and of beneficial owners of the customer shall be conducted in accordance with the procedure for natural persons above.

Further verification of information on the basis of risks

As part of its broader customer due diligence measures, MT should consider, on a risk-sensitive basis, whether the information regarding financial situation and source of funds and/or destination of funds should be corroborated.