ANTI-MONEY LAUNDERING POLICY

MEETING

The term "money laundering" includes all methods used to conceal the source of illicit proceeds so that they appear to be derived from a legal source. Newmar Group Ltd, Dreikönigstrasse 31A, 8002 Zürich, Switzerland. (The "Company") strives to identify, control and minimize the risks associated with money laundering and terrorist financing. The company has implemented a strict policy aimed at identifying, preventing, or reducing the risks associated with any suspicious customer activities.

A company must constantly monitor the degree of its vulnerability to the risks of money laundering and terrorist financing.

The company believes that with a good knowledge of its client and a deep understanding of their instructions, it will be better prepared to assess risks and detect suspicious activities.

PROPER CUSTOMER IDENTIFICATION

Effective Customer Due Diligence ("NIC") measures play a key role in managing the risks associated with money laundering and terrorist financing. CDD involves establishing the identity of the customer and confirming its authenticity on the basis of documents, data or information both when establishing a business relationship with the client and in the course of its further maintenance. Customer identification and verification procedures include, firstly, data collection, and secondly, attempts to verify them.

When registering on the newmargroup.com website, an individual provides the Company with the following identification information:

Full name of the client; Client's date of birth; Country of residence or location of the client; Mobile phone number and email address. In the course of registration for newmargroup.com, corporate clients provide the Company with the following identification information:

Full name of the company; Registration number and date of registration; Country of incorporation or incorporation; Address of the legal entity; Mobile phone and email.

After receiving the identification data, the Company's employees are obliged to verify this data by requesting the necessary documents.

The documents required to verify the client's identity include, but are not limited to, the following:

For an individual client: A scanned copy or photo of the pages of the passport or other state identity card in high quality indicating the surname, first name, date and place of birth, passport number, date of issue and expiration date, country of issue and signature of the Client; For a corporate client: a copy of high-resolution documents proving the existence of

the legal entity, such as a certificate of incorporation, as well as, if necessary, a certificate of change of name, certificate of good standing, memorandum of association, business license, government business license (if applicable), etc. issued in the appropriate name of the client:

A copy of a high-resolution utility bill (landline, water, electricity) issued in the last 3 months; A copy of the tax or tariff invoice from the local authorities; A copy of a bank statement (for a current account, deposit account or credit card account); A copy of a letter of recommendation from the bank. When depositing or withdrawing funds using a credit/debit card, the customer is required to provide a scanned copy or photo of the credit/debit card (front and back). The front of the card must contain the holder's full name, the expiration date of the card, and the first six and last four digits of the card number (the remaining digits may be hidden). On the back of the card, the signature of the owner must be visible in the scanned copy or photo, and the CVC2/CVV2 code must be masked.

If a current client refuses to provide the above information or intentionally provides incorrect data, the Company, after assessing the risks involved, may decide to close any of the client's accounts.

The requirements of the Regulation provide for the need for further analysis and identification of customers who may carry a potentially high risk in relation to money laundering or terrorist financing. If the Company concludes that the business relationship with the client involves high risk, it will take the following additional measures:

It will be necessary to obtain information about the source of funds or the state of the client's wealth (this can be done via email or phone); Request additional information from the client, or use the Company's internal research and data from third-party sources to clarify or update information about the client, as well as to obtain any additional information and clarification of the nature and purpose of the client's transactions with the Company.

When collecting information to verify a client's claims regarding the source of funds or wealth, the Company's employees will generally request and carefully review the client's employment status or occupation/occupation. Employees of the Company may also ask for any additional details or evidence of the job/profession that may be considered necessary in a particular situation, including relevant supporting documents (employment contracts, bank statements, letter from employer or company, etc.).

The Company will carry out ongoing comprehensive customer due diligence and account monitoring for all its business interactions with them. In particular, this involves regularly reviewing and updating the Company's perceptions of clients' activities, the level of risk they carry, as well as checking for possible discrepancies with previously obtained information or beliefs about the client. This may also include any significant changes in the nature or purpose of the client's business relationship with the Company.

Payment policy

The Company's payment policy is governed by the Terms and Conditions and is available on the Company's website.

STAFF

AML Compliance Officer
The Company is required to appoint an AML Compliance Officer who will be fully responsible for the implementation of the Company's AML and CFT program and report to the Company's Board of Directors or its committee on any significant non-compliance with the Company's internal AML policies and procedures, as well as rules, codes and standards of good practice.

The responsibilities of an AML compliance officer include:

Ensuring that the Company complies with the requirements of the Regulations; Developing and maintaining an internal anti-money laundering (AML) program; Establishment of an audit function to control procedures and systems for the prevention of money laundering and terrorist financing; Training employees in the skills of identifying suspicious transactions; Receiving and reviewing internal reports from staff on suspicious activities and transactions and, if necessary, forwarding reports to the FIU; Ensuring proper retention of AML records; Obtaining and updating international recommendations for countries with inadequate anti-money laundering systems, laws or measures.

Employees
All employees, managers and directors of the Company must be aware of this policy. Employees, managers and directors who perform AML-related duties must be subject to appropriate background checks. This includes criminal background checks upon hiring, as well as monitoring during employment. Any violation of this policy or AML program must be confidentially reported to the employee, AML compliance officer, except in cases where the violation concerns the AML compliance officer himself; In this case, the employee must notify the general director of the violation.

Employees working in areas exposed to money laundering or terrorist financing risks must be trained to comply with this anti-money laundering (AML) policy or program. This includes being aware of how to be vigilant about money laundering and terrorist financing risks, as well as what actions to take once they are identified.

Staff training program
The Company organizes AML training for employees who will interact with customers or participate in any AML verification, verification or monitoring processes. Training can be conducted both internally and with the involvement of external consultants.

Each employee of the Company is assigned a supervisor who educates him or her in all policies, procedures, forms and requirements of client documentation, forex markets, trading platforms, etc. For each new employee, a training plan and tests are developed, which take place within 2-3 months (depending on the level in the company).

The Company's AML/CFT training programmes are aimed at providing employees with an appropriate level of training in the context of any potential AML/CFT-related risks.

Content of the training program
The Company's AML and risk awareness training program includes the following sections:

The Company's obligations to prevent, detect and report ML and TF crimes. Examples of ML and TF identified in similar organizations to raise employees' awareness of the possible ML and TF risks they may face. Well known or recognized typologies, especially if provided by supervisory bodies such as the FATF or AML. The impact of ML and TF on the Company, including possible legal consequences. Liability of the Company in accordance with the AML Law and Regulations. The specific responsibilities of employees provided for in this AML Policy and how they must comply with the Company's AML procedures. How to identify and report unusual activity if it may constitute suspicious transactions or attempted transactions. Rules on the prevention of unlawful disclosure of information on suspicious transactions ("tipping off").

Newmar Group Ltd.,

Dreikönigstrasse 31A,

8002

Zurich

Switzerland