Money laundering is converting money or other monetary instruments gained from illegal activity (fraud, corruption, terrorism, etc.) into money or investments that appear to be legitimate so that their illegal source cannot be traced.
In the event of circumstances in which Company's client, agent, or employee has attempted money laundering, Company will take all necessary measures to prevent the above circumstances and their possible consequences in compliance with domestic and international law.

Company anti-money laundering procedures

Company strictly follows the provisions of the anti-money laundering and counter-terrorism financing policy (AML/KYC). To help governments combat the threat of money laundering and financing terrorist activities around the world, all financial organizations commit to collecting, verifying, and storing an account holder's ID data. For that purpose, Company has set up a highly sophisticated electronic system for countering money laundering. This system documents and verifies client identification data and tracks detailed records of all transactions.
As part of its anti-money laundering program, Company follows the procedures described below:

Client Identification

For the purpose of complying with Anti-Money laundering laws, Company requires two different documents to verify the identity of the customer. The first document we require is a legal government-issued, identifying document with the picture of the customer on it. It may be a government-issued passport, driver's license (for countries where the driver's license is a primary identification document) or local ID card (no company access cards). The second document we require is a bill with the customer's own name and actual address on it issued 3 months ago at the earliest. It may be a utility bill, a bank statement, an affidavit, or any other document with the customer's name and address from an internationally recognized organization.

To make deposits using a bank card, clients are required to submit full-size color copies of the front and back sides of their bank cards within two days. Should a client refuse to provide such copies in time, his/her trading account will be blocked, and money will go back on the card. The front side of the bank card must feature the first six and last four digits of the card number, as well as the holder's name and the expiry date. The back of the card must be signed. The CVC/CVV code must be covered. According to VISA and Mastercard rules, the holder's signature must be located in the signature field on the back of the card. If a card doesn't have the holder's name or a virtual card is used, clients are required to provide a screenshot of their profile with a bank or a bank statement that shows the card number and the holder's name.

To change the phone number related to the Client Profile, Clients are

required to provide a document confirming ownership of a new phone number (agreement with a mobile phone service provider) and a photo of the ID held beside the Client's face. The Client's personal data shall be the same in both documents.
Clients must submit up-to-date identification information and immediately inform Company of any changes in their identification information.
All documents must be in English or translated into English by an official translator; the translation must be stamped and signed by the translator and sent together with the original document clearly showing the client's photo.

Tracking and Documentation

Company thoroughly monitors suspicious activities/transactions and reports such activities to the appropriate authorities on time. The international legal framework protects the Master Traders of such information.

No cash settlements

Company does not accept cash deposits, withdrawals, and any other cash payments under any circumstances to minimize the risk of money laundering and terrorist financing.

PEP monitoring

The client undertakes to declare their PEP (politically exposed person) status by ticking the appropriate field in the Verification section of their

Client Profile and providing copies of documents confirming such status and indicating the origin of funds used to make a deposit. A politically exposed person means a natural person who is or who has been entrusted with prominent public functions and includes the following:

a. heads of State, heads of government, ministers, and deputy or assistant ministers;
b. members of parliament or similar legislative bodies;
c. members of the governing bodies of political parties;
d. members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances;
e. members of courts of auditors or the boards of central banks;
f. ambassadors, chargés d'affaires and high-ranking officers in the armed forces
g. members of the administrative, management or supervisory bodies of State-owned enterprises;
h. directors, deputy directors and members of the board or equivalent functions.
i. mayors.

No public function referred to in points (a) to (i) shall be understood as covering middle-ranking or more junior officials.

Family members include the following:

a. a the spouse, or a person considered to be equivalent to a spouse, of a politically exposed person;

b. the children and their spouses, or persons considered to be equivalent to a spouse, of a politically exposed person;
c. a politically exposed person’s parents.

Persons known to be close associates means:

a. natural persons who are known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a politically exposed person;
b. natural persons who have sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a politically exposed person.

The Company is legally obliged to refuse service and return money if a politically exposed person (PEP) fails to provide documents explaining the origin of deposit funds. The Company undertakes to repeat identification of PEP statuses that have been confirmed every year to update the data.

Refusal to process suspicious transactions

Company reserves the right to refuse a transaction at any stage if, in Company’s opinion, the transaction may be related to money laundering or criminal activity. Company is not obligated under international law to inform the client that their activities have been reported as suspicious to the appropriate authorities.

System updates

Company regularly updates its electronic system to verify transactions and client identification data in compliance with current legislation.

Data storage

Upon closing access to the client's profile, the client's trading accounts on the website or in the mobile application, and the trading platforms, the following data will be stored for 5 years:

For individual Clients

Personal information:

- company name,
- full company corporate details,
- user ID,
- phone number,
- email address.

Financial information:

- payment details,
- trading history,
- correspondence with the company.

Photo and video:

- copies and/or photos of the company's supporting corporate documents,

- copies and/or photos of supporting documents of the individual representing the company.

Payment Policy: Deposits and Withdrawals

Please be aware that chargebacks to Skrill payment system and bank cards are prohibited. To make a withdrawal from a trading account to one of these systems, it is necessary to submit an application through the Client's Profile. Money will be loaded into the wallet within 3 business days. If money has been lost when trading, it cannot be reimbursed by means of a chargeback. Please read the risks disclosure before you start trading: https://www.wegolden.com/riskdisclosure/.

WeGolden (Pty) Ltd requires all deposits to come from the sender, whose name is matching the name of the customer in Company's records. Third party payments are not accepted.

As for withdrawals, money may be withdrawn from the same account and by the same way it was received. For withdrawals where the name of the recipient is present, the name must exactly match the name of the customer in our records. If the deposit was made by wire transfer, funds may be withdrawn only by wire transfer to the same bank and to the same account from which it originated. If the deposit was made by means of electronic currency transfer, funds may be withdrawn only by the means of electronic currency transfer through the same system and to the same account from which it originated.

To comply with the AML procedures, funds withdrawals have to be made solely in the same currency that was used to make a deposit.

When a bank card is used to withdraw funds, we require that the client's profile (ID, phone number, email, and address) be fully verified so that payment processing centers' requirements are observed.

When cryptocurrency is used to withdraw funds, we require that the client's profile (ID, phone number, email, and address) be fully verified for secure payments and the protection of the client's funds.

We act with due diligence and check users through a large database using Refinitiv World-Check. The database contains the main lists of sanctions and terrorist attacks. Thus, we can guarantee that dishonest persons do not have access to our platform.

The company has the right to revise this anti-money laundering program at any time and at its own discretion without notifying clients. Clients, employees, agents, and other related parties are responsible for complying with the AML program's provisions.

If you have any inquiries, please contact us via e-mail: support@wegolden.com.