



AML Policy

AMarkets LTD,
Suite 305, Griffith Corporate Centre 1510, Beachmont,
Kingstown, Saint Vincent and the Grenadines
info@amarkets.com

AML Policy

General Information about the Company:

AMarkets LTD maintains high standards in anti-money laundering, and is doing its best in preventing any activities that are aimed at or are facilitating decriminalization of any funds of illegal origin.

The jurisdiction of the Company's incorporation enjoys elaborated legislation in FOREX regulation domain. The Company undergoes annual audit in terms of any violations of the relevant legislation provisions, followed with a statement issued by the State Registrar (<http://svgfsa.com>) confirming that the Company is in good standing and is running in full compliance with national laws. In addition, the Company annually receives an independent legal opinion from among *The Legal 500* (<https://www.legal500.com>) companies, as an additional acknowledgment of the Company's lawful activity aligned with national regulations.

To detect, prevent and alarm about any transactions aimed at transforming the proceeds from illegal activity into another kind of money facilities which are deemed legal, the Company has established the following procedures:

Monitoring of Customers Activity.

Customers activity is monitored by many different ways at all levels of customers interest and involvement. Thus, on the first level, customers are given the status of **Lead**: those who have expressed their interest in the Company's services, who have been around at the Company's website for a while, and so on. The information collected about such customers will be represented in a report to be later used by the Company's financial advisors for further work with the customers and for scoring them. Next, the customers who have completed the registration and the KYC/AML procedure, are awarded a **New Client** status. Such customers, depending on how promising and how experienced in independent trading they are, and based on other reasons, will be grouped into **Silver**, **Gold** и **Platinum** categories; activity of such customers in each group will be monitored by the Company's staff in terms of various pivotal signs (particularly, a new customer deposition activity report: amounts, quantities, average bill, currency, a preferred way of payment – this is the information which allows making the primary customer risk assessment). Then, active customers will be divided by markets geography: quantitative indicators, deposition methods, preferred strategies of trading, frequency of transactions, use of Forex indicators, and other figures are recorded. At the end of customer cycle with no customer activity in trading accounts, such customers will be grouped into a separate report and shall undergo indirect review by financial advisors to specify a reason for their trading activity termination.

Funding and Withdrawal Transactions Monitoring.

All the customers transactions for money funding and withdrawal from their personal trading account must comply with the following requirements:

- Whenever money is transferred by a bank wire or from a plastic card, the name specified at the time of the customer's account registration must match the name of the bank account/plastic card owner.
- Whenever the account is funded by a payment method not acceptable for money withdrawal, the money shall be withdrawn to the Customer's bank account, or by another method agreed with a Company allowing to reliably identify the account owner.
- Whenever the account is funded by various payment methods, the money shall be withdrawn by the same methods in proportion to the deposited amounts.

Training our Staff in Modern AML Procedure Rules.

Financial department personnel responsible for customers' deposition and withdrawal transactions and for verification of major identification documents keep researching the market looking for any AML policy renewals, and are regularly trained in regulations updates according to FATF и Big4 Business Bulletins. On a quarterly basis, the personnel are certified for awareness in the information required for efficient performance, particularly, about the Company's CTF/AML/KYC procedures.

Timely Response to Red Flags and to Other Signs of Customer's Suspicious Behavior.

All non-commercial transactions undergo money laundering examination during all the stages of money movement in the process of money laundering:

- **Money Placement.**
At this stage, the funds are transformed into other financial instruments, such as cheques, bank accounts, wire transfers. Alternatively, the funds can be used to buy expensive commodity which can be easily resold later. The money can also be invested into banks and non-bank institutions (e.g., currency exchange offices). To avoid any suspicion from the Company, a money laundering person may opt to make several depositions instead of a lump sum investment. This method of money placement is known as smurfing.
- **Money Fragmentation.**
Money funds are transferred or moved onto other accounts and into other financial instruments. This is done to conceal the origin and prevent from identifying a person who has made several financial transactions. Transferring and reshaping the money facilities complicates the process of laundered money tracing.
- **Money Integration.**
The money is returned to circulation as legally earned to pay for goods and services.

The Company has introduced a unique practice called Moratorium: this is a standstill period of 10 days during which the money is forbidden to withdraw. The Moratorium is enabled whenever a customer has funded money but neglected to trade at financial markets. Transactions in money funding will also be checked for the "brute force" method (using several plastic cards via multiple payment agents offered by the Company, receiving specific error code while trying to make a payment, using cards issued by bank institutions located in different regions), using several payment methods within a short period of time (cards, e-wallets, wire transfers), refusal to verify any payment method, inconsistency between key elements geography (such as a country of citizenship, a country of mobile phone operator, IP-address location, a card's BIN, etc.), ultimate refusal to have a voice phone conversation, failure to provide a customer's photo holding an ID upon request, one account's computer CID coinciding with another account's CID in our system.

Thus, to prevent the Company's services being used by criminals for the purpose of money laundering, terrorism financing, or some other criminal activity, AMarkets LTD hereby undertakes:

- To request the relevant IDs for the purpose of Customer identification;
- To evaluate the risk of whether a Customer is engaged in money laundering or terrorism financing;
- To check if the Customer's country is among the countries which, according to FATF, fail to comply with requirements in prevention of money laundering and terrorism financing;
- To re-identify the Customer, should any doubts arise concerning validity of the information obtained during the primary identification;
- To avoid having any business relations with unidentified customers.

Three risk categories are considered during risk evaluation:

- a person's location or place of residence: country-based and geography-based risks are considered*;
- parameters characterizing a person who is a party of transaction: customer risk is considered;
- business activity of the person engaged in the transaction: product-related and services-related risks are considered;

*Countries which, according to FATF, fail to comply with requirements in prevention of money laundering and terrorism financing. The list of such countries is available at <http://www.fatf-gafi.org/countries/#high-risk>

Having evaluated the above-mentioned risks, we then evaluate each risk category on a scale of one to three:

- **Low Exposure Level**
No risk factors in each category, the customer's transactions are transparent, nothing adverse detected as compared to ordinary transactions; a reasonable person doing business in the relevant sphere. Thus, there's no reason to suspect that risk factors may, in general, cause any threat of money laundering or terrorism financing.
- **Middle Exposure Level**
There's one or more risk factors in the category, which differ from normal transactions of a person doing business in the relevant sphere, but the transactions are still transparent. Thus, there's no reason to suspect that risk factors may, in general, cause any threat of money laundering or terrorism financing.
- **High Exposure Level**
There's one distinctive feature or several symptoms in the category that generally undermine transparency of the person and his/her transactions, which results in the person's particulars being different from those of someone doing business in the relevant sphere. Thus, a risk of money laundering or terrorism financing occurrence is plausible.

The Company reserves the right to collect Customer's additional identification information for the purpose of AML / KYC policy.

Information and documents used for customer's identification by the Company shall be collected, stored, shared and protected in strict conformity with provisions of Law on Counteraction of the Legitimization (Laundering) of the Proceeds of Crime and Financing of Terrorism in accordance with the Company's internal privacy policy and the applicable guidelines.