ANTI-MONEY LAUNDERING POLICY

Money laundering activity is highly regulated by global and international legislation; therefore, AS FINANCIAL SERVICES LLC ("ASF Markets", "the Company") is strongly advised to implement AML Code of Practice, to avoid illegal procedures and transactions in the future.
The Company follows the UK legislations for money laundering and terrorist funding. The requirements of the UK anti-money laundering legislations are set out in:

- The Terrorism Act 2000 (as amended by the Anti-Terrorism, Crime and Security Act 2001, the Terrorism Act 2006 and the Terrorism Act 2000 and Proceeds of Crime Act 2002 (Amendment) Regulations 2007)
- The Proceeds of Crime Act 2002 (as amended by the Crime and Courts Act 2013 and the Serious Crime Act 2015)
- The Money Laundering Regulations 2007

SCOPE OF POLICY

This policy applies to all ASF Markets officers, employees, appointed producers and products and services offered by ASF Markets to create an organized effort in the fight against money laundering. The Compliance is responsible for starting Suspicious Activity Reports ("SARs") or other required reporting to the appropriate law enforcement or regulatory agencies. Any contacts by law enforcement or regulatory agencies related to the policy shall be directed to the Compliance.
The Compliance shall:

- Receive internal suspicions activity reports of money laundering and investigate
- Make reports of relevant suspicious events to the relevant authorities
- Ensure the appropriateness of arrangements made for the awareness and training of staff and advisers
- Monitor the day-to-day operation of anti-money laundering policies in relation to: the development of new products; the taking on of new customers; and changes in the company's business profile.

THE POLICY

It is the policy of ASF Markets to actively pursue the prevention of money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities. ASF Markets is committed to AML compliance in accordance with applicable law and requires its officers, employees and appointed producers to adhere to these standards in preventing the use of its products and services for money laundering purposes.
For the purposes of the Policy, money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the unlawful proceeds appear to have been derived from legitimate origins or constitute legitimate assets.

WHAT IS MONEY LAUNDERING?

Money laundering is the process by which criminally obtained money or other assets (criminal property) are exchanged for "clean" money or other assets with no obvious link to their criminal origins.
Criminal property may take any form, including money or money's worth, securities, tangible

property and intangible property. It also covers money, however come by, which is used to fund terrorism.
Money laundering activity includes:

- Buying, using or possessing criminal property
- Handling the proceeds of crimes such as theft, fraud and tax evasion
- Being knowingly involved in any way with criminal or terrorist property
- Entering into activities to facilitate laundering criminal or terrorist property
- Transferring criminal property

There is no single stage of money laundering; methods can range from the purchase and resale of luxury items such as a car to passing money through a complex web of legitimate operations. Usually the starting point will be cash but it is important to appreciate that money laundering is defined in terms of criminal property. This can be property in any conceivable legal form, whether money, rights, real estate or any other benefit, if you know or suspect that it was obtained, either directly or indirectly, as a result of criminal activity and you do not speak up then you too are taking a part in the process.
The money laundering process follows three stages:

1. **Placement:** Disposal of the initial proceeds derived from illegal activity e.g. into a bank account.
2. **Layering:** The money is moved through the system in a series of financial transactions in order to cover the origin of the cash with the purpose of giving it the appearance of legitimacy.
3. **Integration:** Criminals are free to use the money as they choose once it has been removed from the system as apparently “clean” funds.

COUNTER TERRORIST FINANCING

Terrorist financing is the process of legitimate businesses and individuals that may choose to provide funding to resource terrorist activities or organizations for ideological, political or other reasons.
We therefore ensure that:

- customers are not terrorist organizations themselves
- they are not providing the means through which terrorist organizations are being funded

Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal the origin or intended use of the funds, which will later be used for criminal purposes.

RISK BASED APPROACH

The level of due diligence required when considering anti-money laundering procedures within the Company, it should take a risk-based approach.
This means the amount of resources spent in conducting due diligence in any one relationship that is subject risk should be in proportion to the extent of the risk that is posed by that relationship.
These can be broken down into the following areas:

1) Customer Risk

Different customer profiles have different levels of risks attached to them. A basic Know your Customer (KYC) check can establish the risk posed by a customer.
For example, near-retired individuals making small, regular contributions to a savings account in line

with their financial details poses less of a risk than middle-aged individuals making ad-hoc payments of ever-changing sizes into a savings account that does not fit into the profile of the customers' standing financial data.
The intensity of the due diligence conducted on the latter would be higher than that carried out on the former as the potential threat of money laundering in the second case would be perceived as being greater.

2) Product Risk

This is the risk posed by the product or service itself. The product risk is driven by its functionality as a money laundering tool.
Companies typically deal into three risk bands; reduced, intermediate and increased. Typically, pure protection contracts are categorized as reduced risk and investments in unit trusts as increased risk. Additionally, a factor that will contribute to the classification of the risk category is sales process associated with the product. If the transaction in the product takes place on an advisory basis as a result of a KYC, this will carry less risk than an execution only transaction, whereby you know significantly less about the customer.

3) Country Risk

The physical location of the client or origin of the business activity has a risk associated with it. This stops from the fact that countries around the globe have different levels of risk attached to them.
We would determine the extent of the due diligence measure required initially and on an ongoing basis using the above described risk areas.

CUSTOMER IDENTIFICATION

ASF Markets follows a Customer Identification plan. ASF Markets will provide notice to customers that it is requesting information from them to verify their identities, as required by applicable law.

KNOW YOUR CUSTOMER

When a business relationship is made, in order to establish what might institute normal activity later in the relationship, it is necessary for the company to discover the nature of the business a client expects to conduct.
Once an on-going business relationship has been established, any regular business undertaken for that customer can be evaluated against the expected form of activity of the customer. Any mysterious activity can then be scrutinized to determine whether there is a suspicion of money laundering or terrorist financing.

SOURCE OF FUNDS

When a transaction takes place, the source of funds, i.e. how the payment is to be made, from where and by who, must always be ascertained and recorded in the client profile.

IDENTIFICATION

The standard identification requirement for customers who are private individuals are generally governed by the circumstances relating to the customer and the product type that is being dealt in, i.e. the level of risk attributed to the product whether it is a reduced risk, intermediate risk or an increased risk product. Taking that into account, the following pieces of information are required as

a standard for identification purposes:

- Full Name
- Residential Address

VERIFICATION

If documentary evidence of an individual's identity is to provide a high level of confidence, it will typically have been issued by a government department because there is a greater likelihood that the authorities will have checked the existence and characteristics of the persons concerned. In cases where such documentary evidence of identity may not be available to an individual, other evidence of identity may give the Company reasonable confidence in the customer's identity, although the Company should weigh these against the risks involved.

1) Proof of Identification

If the identity is to be verified from documents, this should be based on:

- Either a government issued document which incorporates:
    a. The customer's full name, and
    b. Their residential address
- Photographic Government Issued Identity Documents

    a. Valid passport
    b. National Identity card

2) Proof of Address

- Current bank statements, or credit/debit card statements, issued by a regulated financial sector (but not ones printed off the internet and not less than 3 months old)
- Utility bills (not including mobile phone bills, not ones printed off the internet and not less than 3 months old)

For increased risk level products, in addition to obtaining the standard information detailed above, the following know your customer information should be obtained and recorded:

- Employment and income details
- Source of wealth (i.e. source of the funds being used in the transaction)

MONITORING AND REPORTING

Transaction based monitoring will occur within ASF Markets. Monitoring of specific transactions will include but is not limited to transactions accumulating $5,000 or more and those with respect to which ASF Markets has a reason to suspect suspicious activity.

SUSPICIOUS ACTIVITY

There are signs of suspicious activity that suggest money laundering. These are commonly referred to as "red flags." If a red flag is detected, additional due diligence will be performed before proceeding with the transaction. If a reasonable explanation is not determined, the suspicious activity shall be reported to the Compliance.
Examples of red flags are:

- The customer exhibits unusual concern regarding the firm's compliance with government reporting requirements and the Company's AML policies, particularly with respect to his or her identity, type of business and assets, or is hesitant or refuses to disclose any information concerning business activities, or provides unusual or suspect identification or business documents.
- The customer wishes to engage in transactions that lack business sense or outward investment strategy, or are inconsistent with the customer's stated business strategy.
- The information provided by the customer that identifies a legitimate source for funds is false, misleading, or significantly incorrect.
- Upon request, the customer refuses to identify or fails to indicate any legitimate source for his or her funds and other assets.
- The customer (or a person publicly associated with the customer) has a questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations.
- The customer displays a lack of concern regarding risks, commissions, or other transaction costs.
- The customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person or entity.
- The customer attempts to make frequent or large deposits of currency, insists on dealing only in cash equivalents, or asks for exemptions from the Company's policies relating to the deposit of cash and cash equivalents.
- For no obvious reason, the customer has multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers.
- The customer's account has unexplained or sudden extensive activity, especially in accounts that had little or no previous activity.
- The customer's account has a large number of wire transfers to unrelated third parties inconsistent with the customer's legitimate business purpose.
- The customer's account has wire transfers that have no apparent business purpose to or from a country identified as money laundering risk or a bank secrecy haven.
- The customer's account indicates large or regular wire transfers, immediately withdrawn by check or debit card without any apparent business purpose.
- The customer makes a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another Company, without any apparent business purpose.
- The customer requests that a transaction be processed in such a manner to avoid the Company's normal documentation requirements.

INVESTIGATION

Upon notification to the Compliance, an investigation will be commenced to determine if a report should be made to the appropriate law enforcement agencies. The investigation will include, but not necessarily be limited to, review of all available information, such as payment history, birth dates, and address.

If the results of the investigation warrant, a recommendation will be made to the Compliance to report to appropriate law enforcement agency. The Compliance is responsible for any notice or filing with law enforcement or regulatory agency.

Investigation results will not be disclosed or discussed with anyone other than those who have a legitimate need to know. Under no circumstances shall any officer, employee or appointed agent disclose or discuss any AML concern, investigation, notice report filing with the person or persons

subject of such, or any other person, including members of the officer's, employee's or appointed agent's family.

FREEZING OF ACCOUNTS

Where we know that the funds in an account derive from criminal activity, or that they arise from fraudulent instructions, the account must be frozen. Where it is believed that the account holder may be involved in the fraudulent activity that is being reported, then the account may need to be frozen.

ABOUT US

AS FINANCIAL SERVICES LLC is formed in the St. Vincent and the Grenadines (company no 172 LLC 2019) with its registered office address of business at First Floor, First St. Vincent Bank Ltd. Building, James Street, Kingstown, VC0100, St. Vincent and Grenadines and is licensed and regulated under Financial Services Authority (FSA), St. Vincent and the Grenadines.